Citrix Gateway 13.0

Copyright © 1997–2026. Citrix Systems, Inc. All Rights Reserved.

Contents

NetScaler Gatewayリリースノート 48

NetScaler Gatewayについて 49

- NetScaler Gateway アーキテクチャ 50
- ユーザー接続の仕組み 52
- NetScaler Gateway プラグインで接続する 52
- Citrix Workspace アプリとの接続 54
- iOS および Android デバイスと接続する 54

一般的なNetScaler Gatewayの展開 55

- DMZにNetScaler Gateway を展開する 55
- DMZでのNetScaler Gateway接続 56
- NetScaler Gateway を安全なネットワークに展開する 56

クライアントソフトウェア要件 58

- NetScaler Gateway プラグインのシステム要件 58
- エンドポイント分析の要件 59

NetScaler Gateway とCitrix 製品の互換性 62

- Citrix 製品とサポート対象バージョン 62
- Citrix Workspace アプリ、Citrix業務用モバイル アプリ、プラグイン 62

NetScaler Gatewayライセンス 64

- NetScaler Gateway ライセンスの種類 64
  - プラットフォームライセンス 65
  - ユニバーサル・ライセンス 65
    - ユニバーサルライセンスの取得 66
    - ユニバーサルライセンスのインストール 67
    - ユニバーサルライセンスのインストールの確認 67
- 関連情報 68
- NetScaler Gateway にライセンスをインストールする 68

© 1997–2026 Citrix Systems, Inc. All rights reserved.

最大ユーザー数を設定する 68
ユニバーサルライセンスのインストールを確認する 69
GUI を使用してユニバーサルライセンスのインストールを確認するには 69
CLI を使用してユニバーサルライセンスのインストールを確認するには 69
NetScaler Gateway ライセンスに関するよくある質問 69
トライアルライセンスまたはデモライセンスのサポートを受けるにはどうすればよいですか 69
ライセンスをインストールするには 70
Gateway ライセンスにはどのような種類がありますか 70
サポートされる同時ユーザーセッションはいくつありますか 70
現在の同時ユーザーセッションのライセンスを確認するにはどうすればよいですか? 70
ライセンスされたスループット制限に達しているかどうかを確認する方法 71
ライセンススループットに達するとパケットがドロップされるかどうかを確認する方法 71
NetScaler ADCアプライアンスのライセンスされたスループットはどのようにして調べることができますか? 71
既存の Gateway ライセンスにユーザーを追加するにはどうすればよいですか? 71
開始する前に 72
NetScaler Gateway をインストールするための前提条件 73
セキュリティの計画 74
セキュアな証明書管理を構成する 74
認証サポート 74
NetScaler Gateway 展開環境のセキュリティ保護 75
Gatewayインストール前のチェックリスト 76
ユーザーデバイス 76
NetScaler Gateway の基本的なネットワーク接続 76
NetScaler Gateway を介してアクセス可能な内部ネットワーク 77
高可用性 77
認証と承認 78
LDAP認証 78

© 1997–2026 Citrix Systems, Inc. All rights reserved.

RADIUS 認証および認可 79
SAML認証 79
ファイアウォールを介してポートを開く（シングルホップ DMZ） 80
セキュリティで保護されていないネットワークと DMZ の間のファイアウォール上 80
セキュリティで保護されたネットワーク間のファイアウォール上 80
Citrix Virtual Desktops、Citrix Virtual Apps、Web Interface、またはStoreFront 80
Citrix Endpoint Management 81
Citrix Virtual Apps を使用したダブルホップ DMZ 展開 81
最初のDMZのNetScaler Gateway 81
2番目のDMZのNetScaler Gateway 82
NetScaler Gatewayアプライアンスのインストールと構成 83
ウィザードを使用してNetScaler Gateway アプライアンスを構成する 83
初回セットアップウィザード 84
初回セットアップウィザードでNetScaler Gateway を構成する 84
クイック構成ウィザード 85
クイック構成ウィザードで設定を構成する 86
NetScaler Gateway ウィザード 90
NetScaler Gateway ウィザードを使用して設定を構成する 90
セットアップウィザード 91
公開アプリケーションウィザード 91
統合されたCitrix Endpoint Management 構成 92
NetScaler Gatewayを構成します 92
構成ユーティリティの使用 93
構成ユーティリティにログオンします 93
仮想サーバーを作成する 94
仮想サーバーを作成するには 95
ネットプロファイルを VPN 仮想サーバーにバインドする際の注意点 95
仮想サーバ上の現在のユーザーと接続しているユーザーの総数 96

© 1997–2026 Citrix Systems, Inc. All rights reserved.

仮想サーバーで接続タイプを構成する 97
ワイルドカード仮想サーバー用のリッスンポリシーを構成する 97
NetScaler Gateway でIPアドレスを構成する 99
NetScaler GatewayがIPアドレスを使用する方法 99
サブネット IP アドレス 100
ユーザー接続用の IPv6 を構成する 101
セキュリティで保護されたネットワークにある DNS サーバーを解決する 102
DNS サービスと DNS モニターを構成するには 102
DNS サービスを DNS 仮想サーバーにバインドするには 103
DNS 仮想サーバーを構成する 103
DNS 仮想サーバーを構成するには 103
ネームサービスプロバイダーの設定 103
NetScaler Gateway にDNSサーバーを追加するには 104
WINSサーバーをNetScaler Gateway に追加するには 104
名前ルックアップの優先度を指定するには 104
サーバー起動接続を構成する 105
NetScaler Gateway でルーティングを構成する 106
スタティックルートの設定 106
オートネゴシエーションの設定 107
オートネゴシエーションを有効または無効にするには 108
NetScaler Gateway でホスト名とFQDNを構成する 108
証明書の FQDN を表示するには 108
NetScaler Gateway のポリシーとプロファイル 109
ポリシーの仕組み 109
条件付きポリシー 110
ポリシーの優先順位 110
NetScaler Gateway でポリシーを作成する 111
システム式の設定 111

© 1997–2026 Citrix Systems, Inc. All rights reserved.

クライアントセキュリティ式の設定 112
NetScaler Gateway での証明書管理 112
証明書署名要求を作成する 113
NetScaler Gateway ウィザードを使用してCSRを作成する 113
NetScaler ADC GUIを使用してCSRを作成する 114
NetScaler Gateway に署名付き証明書をインストールする 114
中間証明書を構成する 115
中間証明書をインストールする 116
中間証明書をサーバー証明書にリンクする 117
認証にデバイス証明書を使用する 117
デバイス証明書を構成する手順 118
クラシック EPA ポリシーの仮想サーバーでデバイス証明書チェックを有効にする 119
Windows マシンでのデバイス証明書の検証 119
既存の証明書をインポートしてインストールする 120
NetScaler Gateway に証明書と秘密キーをインストールするには 120
証明書失効リスト 121
CRL リフレッシュパラメータ 123
OCSPで証明書のステータスを監視する 125
OCSP 証明書ステータスの設定 126
NetScaler Gateway の構成設定の管理 128
NetScaler Gateway 構成を保存する 128
NetScaler Gateway で構成を保存するには 128
NetScaler Gateway で構成ファイルを表示して保存するには 128
現在の実行構成を表示するには 129
保存済み構成と実行構成を比較するには 129
NetScaler Gateway の構成をクリアする 129
NetScaler Gateway の構成設定をクリアするには 130
NetScaler Gateway での証明書管理 130

© 1997–2026 Citrix Systems, Inc. All rights reserved.

証明書署名要求を作成する 131
NetScaler Gateway ウィザードを使用してCSRを作成する 131
NetScaler ADC GUIを使用してCSRを作成する 131
NetScaler Gateway に署名付き証明書をインストールする 132
中間証明書を構成する 133
中間証明書をインストールする 134
中間証明書をサーバー証明書にリンクする 134
認証にデバイス証明書を使用する 135
デバイス証明書を構成する手順 136
クラシック EPA ポリシーの仮想サーバーでデバイス証明書チェックを有効にする 136
Windows マシンでのデバイス証明書の検証 137
既存の証明書をインポートしてインストールする 137
NetScaler Gateway に証明書と秘密キーをインストールするには 138
証明書失効リスト 139
CRL リフレッシュパラメータ 141
OCSPで証明書のステータスを監視する 143
OCSP 証明書ステータスの設定 144
NetScaler Gateway の構成をテストする 146
GUI を使用してユーザアカウントを作成する 146
NetScaler Gatewayソフトウェアのアップグレード 148
ソフトウェアアップデートの確認 148
アップグレードウィザードを使用してNetScaler Gateway をアップグレードする 149
コマンドプロンプトを使用してNetScaler Gateway をアップグレードする 149
NetScaler Gateway をダブルホップDMZに展開する 150
ダブルホップ展開の仕組み 150
ダブルホップ DMZ 展開の準備 152
展開を開始するために必要なコンポーネント 152
ダブルホップ DMZ 展開での通信フロー 152

© 1997–2026 Citrix Systems, Inc. All rights reserved.

接続プロセス 153
ダブルホップDMZでのNetScaler Gateway のインストールと構成 156
最初のDMZにNetScaler Gatewayをインストールする 156
最初のDMZでNetScaler Gatewayを構成する 156
第2のDMZにNetScaler Gatewayをインストールする 157
NetScaler Gateway プロキシの仮想サーバーの設定を構成する 157
GUIを使用してNetScaler Gateway プロキシ上の仮想サーバーでダブルホップを有効にするには 157
GUIを使用してNetScaler Gateway プロキシ上の仮想サーバーで認証を無効にするには 158
アプライアンスのプロキシと通信するようにアプライアンスを設定する 158
NetScaler Gateway プロキシと通信するようにNetScaler Gateway を構成するには 158
NetScaler Gateway ネクストホップサーバーをグローバルにバインドするには 159
NetScaler Gateway ネクストホップサーバーを仮想サーバーにバインドするには 159
STAおよびICAトラフィックを処理するようにNetScaler Gatewayを構成する 159
ファイアウォールの適切なポートを開きます 160
システムのメンテナンスとモニタリング 163
委任管理者の構成 163
委任管理者のコマンドポリシーの設定 164
NetScaler Gateway で管理ユーザーを作成するには 165
管理グループの作成 165
委任管理者用のカスタムコマンドポリシーの設定 165
簡単なカスタムコマンドポリシーを作成するには 166
高度なカスタムコマンドポリシーを作成するには 166
カスタムコマンドポリシーをユーザーまたはグループにバインドするには 167
NetScaler Gateway での監査の構成 167
NetScaler Gateway でのログの構成 168
監査ポリシーを作成するには 168
監査ポリシーをグローバルにバインドするには 169

© 1997–2026 Citrix Systems, Inc. All rights reserved.

監査ポリシーを変更するには 169
監査ポリシーを削除するには 170
ACL ロギングの設定 170
構成ユーティリティを使用して ACL ロギングを構成するには 171
NetScaler Gateway でACLまたはTCPのログを有効にするには 171
NetScaler Gateway プラグインログの有効化 171
ICA 接続を監視するには 173
認証と承認 174
デフォルトのグローバル認証タイプの設定 175
認証をグローバルに設定するには 175
認可なしの認証の設定 176
認可の設定 176
承認ポリシーの構成 176
承認ポリシー表現の例 178
GUI を使用して認可ポリシーを設定するには 178
GUI を使用して認可ポリシーをユーザにバインドするには 179
GUI を使用して認可ポリシーをグループにバインドするには 179
デフォルトのグローバル認証の設定 179
認証の無効化 180
認証を無効にするには 180
特定の時刻の認証の設定 180
時刻、日付、または曜日の認証を設定するには 180
認証ポリシーの仕組み 181
認証プロファイルの設定 182
構成ユーティリティを使用して認証ポリシーを作成するには 182
構成ユーティリティを使用して認証ポリシーを変更するには 182
認証ポリシーを削除するには 183
認証ポリシーのバインド 183

© 1997–2026 Citrix Systems, Inc. All rights reserved.

GUI を使用して認証ポリシーをグローバルにバインドするには 183
GUI を使用してグローバル認証ポリシーをバインド解除するには 183
認証ポリシーの優先度の設定 184
グローバル認証ポリシーのプライオリティを設定または変更するには 184
仮想サーバーにバインドされた認証ポリシーの優先順位を変更するには 184
ローカルユーザの設定 184
ローカルユーザーを作成するには 185
ユーザーパスワードを変更するには 185
ユーザーの認証方法を変更するには 185
ユーザーを削除するには 185
グループの設定 186
グループを作成するには 186
グループを削除するには 186
グループへのユーザーの追加 187
グループを使用したポリシーの設定 187
LDAP認証の構成 188
構成ユーティリティを使用して LDAP 認証を構成するには 190
LDAP ディレクトリ内の属性を決定する 192
LDAP グループ抽出の設定 193
LDAP グループ抽出がユーザオブジェクトから直接動作する仕組み 193
LDAP グループ抽出がグループオブジェクトから間接的に動作する仕組み 194
LDAP 認可グループ属性フィールド 194
LDAP 認証を設定するには 194
LDAP ネストされたグループ抽出の設定 195
複数ドメインの LDAP グループ抽出の設定 196
グループ抽出のためのセッションポリシーの作成 196
複数ドメインの LDAP 認証ポリシーの作成 197

© 1997–2026 Citrix Systems, Inc. All rights reserved.

複数ドメインの LDAP グループ抽出のためのグループおよびバインディングポリシーの作成 198
LDAP認証の14日間パスワード有効期限通知 199
クライアント証明書認証の構成 199
GUI を使用してクライアント証明書をデフォルトの認証タイプとして設定するには 200
クライアント証明書からのユーザー名の抽出 200
クライアント証明書認証ポリシーの構成およびバインド 200
2 要素クライアント証明書認証の設定 202
スマートカード認証の構成 202
セキュアな ICA 接続を使用したスマートカード認証の構成 203
RADIUS認証の構成 204
ジェムアルトプロティバの設定 205
セーフワードを構成する 205
RADIUS認証を構成するには 205
RADIUS 認証プロトコルの選択 206
IP アドレス抽出の設定 207
RADIUS グループ抽出の設定 208
Windows Server 2003 での RADIUS の設定 208
Windows Server 2008 での認証用の RADIUS の設定 209
RADIUS 認可を設定するには 210
RADIUS ユーザアカウンティングの設定 211
RADIUS ポリシーを作成するには 212
セッションポリシーを作成するには 213
セッションポリシーをグローバルにバインドするには 213
セッションポリシーをNetScaler Gateway 仮想サーバーにバインドするには 214
SAML認証の構成 214
Active Directory フェデレーションサービス 2.0 の構成 215
SAML 二要素認証の設定 217

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SAML 認証を設定するには 218
参照ドキュメント 219
SAML認証を使用してNetScaler Gateway にログインする 220
サポートされているプラットフォームとアプリ 220
高度な SAML ポリシーを使用した SAML 認証の設定 220
SAML 認証の改善 220
解決策 221
プラットフォーム 221
構成 221
TACACS+ 認証の設定 222
設定のクリアベーシック TACACS の設定をクリアしてはならない 223
新しいコマンド 224
CLI 構成 224
多要素認証の設定 225
カスケード認証の設定 225
グローバル認証ポリシーのプライオリティを設定するには 226
仮想サーバーにバインドされた認証ポリシーの優先順位を変更するには 226
2 要素認証の設定 226
2 要素認証を構成するには 227
シングルサインオンの認証タイプの選択 227
クライアント証明書と LDAP の 2 要素認証の設定 228
認証のためのネイティブOTPサポート 230
ネイティブOTPサポートの利点 231
ネイティブ OTP ワークフロー 231
前提条件 232
GUI を使用したネイティブ OTP の設定 232
第 1 ファクタのログインスキーマの作成 232
認証、承認、および監査仮想サーバーの構成 233

© 1997–2026 Citrix Systems, Inc. All rights reserved.

第 2 要素 OTP のログインスキーマの作成 234
OTP を管理するためのコンテンツスイッチングポリシーを構成する 235
CLI を使用したネイティブ OTP の設定 235
OTP デバイスの登録および管理ページを設定するには 235
LDAP ログオンアクションを作成するには 236
LDAP ログオンの認証ポリシーを追加するには 236
Loginschemaを使用して UI を表示するには 236
デバイスの登録と管理ページを表示する 237
CLI を使用してユーザログインページを設定するには 237
NetScalerでデバイスを登録する 239
OTPを使用してNetScalerにログインします 240
OTP のプッシュ通知 240
プッシュ通知の利点 241
プッシュ通知の動作 241
プッシュ通知を使用するための前提条件 241
プッシュ通知の設定 242
プッシュ・サービスの作成 243
OTP管理とエンドユーザーログインのためのCitrix Gateway の構成 243
デバイスをCitrix Gateway に登録する 244
Citrix Gateway にログインします 246
障害状態 247
iOSでのCitrix SSO アプリケーションの動作 — 注意すべきポイント 248
通知のショートカット 248
Citrix SSO からのパスワードトークンの削除 249
シングルサインオンの設定 249
Windows でのシングルサインオンの構成 250
Windows でシングルサインオンをグローバルに構成するには 250
セッションポリシーを使用して Windows でシングルサインオンを構成するには 250

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Web アプリケーションへのシングルサインオンの構成 251
Web アプリケーションへのシングルサインオンをグローバルに構成するには 251
セッションポリシーを使用して Web アプリケーションへのシングルサインオンを構成するには 251
Web アプリケーションへのシングルサインオン用の HTTP ポートを定義するには 252
LDAP を使用した Web アプリケーションへのシングルサインオンの構成 252
ドメインへのシングルサインオンの設定 253
ドメインへのシングルサインオンを構成するには 253
Microsoft Exchange 2010 のシングルサインオンの構成 253
CLI を使用して、次の操作を実行します 254
CLI を使用した設定の書き換え 254
ワンタイムパスワードの使用の設定 255
RSA SecurID 認証の設定 256
RADIUS を使用したパスワードリターンの設定 257
Configuring SafeWord Authentication 259
Gemalto プロティバ認証の設定 259
ゲートウェイ認証用の nFactor 260
認証、認可、監査機能のライセンス要件 260
使用例 262
認証レスポンスの処理 263
クライアントサポート 263
コマンドライン設定 263
相互運用性の課題 264
エンドポイント分析 (EPA) 264
設定ミスに関する考慮事項 264
Citrix クライアントの定義 264
ゲートウェイの nFactor の制限 265
ログインスキーマ 265

© 1997–2026 Citrix Systems, Inc. All rights reserved.

パラメータの説明 266
ログインスキーマと nFactor の知識が必要 266
loginSchema を使用せずに二要素認証を構成する 267
ユーザ名とパスワードの表現 267
nFactor 構成のハイレベルな手順 268
GUI 構成 268
仮想サーバーの作成 268
認証仮想サーバーを作成する 272
認証 CERT プロファイルの作成 273
認証ポリシーを作成する 274
LDAP 認証サーバーを追加する 274
LDAP 認証ポリシーを追加する 275
RADIUS 認証サーバーを追加する 275
RADIUS 認証ポリシーを追加する 276
認証ログインスキーマの作成 277
ポリシーラベルを作成する 277
nFactor 認証の設定を再キャプチャする 278
キャプチャの設定 278
NetScaler ADC標準ライセンスでnFactor認証用のゲートウェイ仮想サーバーを作成する 282
参照ドキュメント 283
Unified Gateway ビジュアライザー 284
Unified Gateway の設定 284
GUI 構成 286
VPN 仮想サーバーの詳細 286
`The Pre Auth Block` 287
`The Auth Block` 287
StoreFront の追加 288

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SaaS を追加する 288
ウェブアプリの追加 289
モバイル/タブレットデバイスでRADIUSおよびLDAP認証を使用するようにNetScaler Gatewayを構成する 290
1つのActive Directory yグループのメンバーに対するNetScaler Gatewayへのアクセスを制限する 292
概要 293
前提条件 293
1 つの Active Directory グループのメンバーに対して LDAP 検索フィルタを構成する手順 293
高可用性の使用 295
高可用性の仕組み 296
高可用性の設定に関するガイドライン 296
高可用性の設定の構成 297
高可用性ノードを追加するには 298
セカンダリノードを有効または無効にするには 298
高可用性の設定を構成するには 299
RPC ノードのパスワードを変更する 299
RPC ノードのパスワードを変更してセキュアな接続を有効にするには 299
CLIを使用してRPCノードのパスワードを変更するには 300
プライマリアプライアンスとセカンダリアプライアンスの高可用性の設定 301
通信間隔の設定 301
セカンダリNetScaler Gateway の通信間隔を構成するには 301
NetScaler Gateway アプライアンスの同期 302
高可用性同期を有効または無効にするには 302
アプライアンス間で同期を強制するには 302
高可用性セットアップの設定ファイルの同期 303
高可用性セットアップでファイルを同期するためのパラメータ 303
構成ユーティリティを使用して高可用性セットアップのファイルを同期するには 304

© 1997–2026 Citrix Systems, Inc. All rights reserved.

コマンド伝播の設定 304
プライマリノードで伝播を有効または無効にするには 304
コマンド伝播のトラブルシューティング 305
フェイルセーフモードを構成する 305
フェールセーフモードを構成するには 307
仮想 MAC アドレスの設定 307
IPv4 仮想 MAC アドレスの設定 308
IPv4 仮想 MAC アドレスの作成または変更 308
IPv6 仮想 MAC アドレスの設定 310
IPv6 用の仮想 MAC アドレスの作成または変更 310
異なるサブネットでの高可用性ペアの設定 311
独立したネットワーク構成の仕組み 311
リモートノードの追加 312
独立ネットワークコンピューティングモード用のリモートノードを追加するには 313
リモートノードを削除するには 313
ルートモニタの設定 313
ルートモニタの追加または削除 315
ルートモニタを追加するには 315
ルートモニタを削除するには 315
リンク冗長性の設定 316
リンク冗長性を設定するには 316
フェールオーバーインターフェイスセットからインターフェイスを削除するには 316
フェールオーバーインターフェイスセットを削除するには 316
フェイルオーバーの原因を理解する 317
ノードからのフェイルオーバーの強制 318
プライマリノードまたはセカンダリノードでフェールオーバーを強制する 318
プライマリノードまたはセカンダリノードでフェールオーバーを強制するには 319
プライマリノードを強制的にプライマリのままにする 319

© 1997–2026 Citrix Systems, Inc. All rights reserved.

プライマリノードを強制的にプライマリに保つには 319
セカンダリノードを強制的にセカンダリに維持する 319
セカンダリノードを強制的にセカンダリに保つには 320
NetScaler Gateway をアクティブな高可用性アプライアンスとしてサービスに戻すには 320
クラスタリングの使用 321
クラスタリングの構成 321
構成ユーティリティを使用してNetScaler Gateway クラスターインスタンスを作成するには 322
NetScaler Gateway クラスターへのノードの追加 323
クラスタノードグループの作成 324
ローカルクラスタノードをクラスタノードグループにバインドします 324
NetScaler Gateway 仮想サーバーをクラスターノードグループにバインドする 325
Unified Gateway 326
Unified Gateway を備えたNetScaler ADC：1つのURL 326
Unified Gateway 構成ウィザード 327
追加の構成管理 328
コンテンツスイッチング仮想サーバー 329
VPN 仮想サーバー 329
Unified Gateway に関するよくある質問 329
Unified Gateway とは何ですか 329
Unified Gateway を使用する理由 330
複数の Unified Gateway 仮想サーバを使用できますか 330
Unified Gateway でコンテンツスイッチングが必要なのはなぜですか 330
11.0 より前のリリースでは、コンテンツスイッチングを使用して複数の仮想サーバのトラフィックを受信できます。その使用方法は Unified Gateway とも呼ばれますか 331
Unified Gateway のコンテンツスイッチングポリシーで何が変わったのですか 331
Unified Gatewayで現在サポートされていないNetScaler Gatewayの機能は何ですか? 331
Unified Gateway では、EPA スキャンの動作はどのようなものですか 331
Unified Gateway のライセンス要件は何ですか 332

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Unified Gatewayで使用されるNetScaler Gateway 仮想サーバーには、IP/ポート/SSL構成が必要ですか? 332

NetScaler Gateway 仮想サーバー上にあるSSL/TLS証明書を、Unified Gateway 仮想サーバーで使用するために再プロビジョニングする必要がありますか 332

単一の URL とマルチホスト展開の違いは何ですか? どちらが必要ですか 332

Unified Gateway ではどのような認証メカニズムを使用できますか 333

「selfAuth」認証とは何ですか 333

「StepUp」認証」って何ですか 333

ステップアップ認証はNetScaler ADC AAA TM仮想サーバーでサポートされていますか 333

`login once/logout once`って何ですか 334

負荷分散仮想サーバーレベルでNetScaler ADC AAA TM負荷分散仮想サーバー固有の認証バインドを使用して、共通の認証ポリシーをUnified Gatewayレベルで指定できますか? このユースケースをサポートするための構成手順を教えてください 334

バインドされたNetScaler ADC AAA TM仮想サーバーが独自の認証ポリシーを持つように、Unified Gatewayをどのように構成しますか 334

NetScaler ADC AAA TM認証仮想サーバーは、Unified Gateway 仮想サーバーを介して来るユーザーを認証するために必要ですか? 334

NetScaler Gateway 認証ポリシーは、Unified Gateway 仮想サーバーまたはNetScaler Gateway 仮想サーバーでどこで指定しますか 334

Unified Gateway コンテンツスイッチング仮想サーバーの背後にあるNetScaler ADC AAA TM仮想サーバーで認証を有効にするにはどうすればよいですか 335

コンテンツスイッチの後ろに TM 仮想サーバーを追加する方法 (単一の URL とマルチホスト) 335

仮想サーバーがUnified Gateway 仮想サーバーの背後に移動された場合、NetScaler ADC AAA TM負荷分散仮想サーバーにバインドされた認証ポリシーはどうなりますか? 335

NetScaler ADC AAA TMセッションのセッションポリシーをどのように構成しますか? 335

NetScaler ADC 11.0のNetScaler Gatewayポータルの変更点は何ですか? 336

NetScaler ADC 11.0はNetScaler Gatewayポータルのカスタマイズをサポートしていますか 336

ポータル・テーマは、NetScaler ADCの高可用性またはクラスター展開でサポートされていますか? 336

© 1997–2026 Citrix Systems, Inc. All rights reserved.

カスタマイズは、NetScaler ADC 11.0アップグレードプロセスの一環として移行されますか? 337

NetScaler ADC 11.0のポータルテーマの準備をするために従うべきアップグレード前の手順はありますか 337

rc.confまたはrc.netscalerによって呼び出されるNetScaler ADCインスタンスに保存されているカスタマイズがあります。ポータル・テーマに移動するにはどうすればよいですか 337

NetScaler ADC 11.0にアップグレードする前に、現在のカスタマイズをエクスポートして保存するにはどうすればよいですか? エクスポートしたファイルを別のNetScaler ADCアプライアンスに移動できますか? 337

ポータル・テーマは、NetScaler ADC AAA TM 仮想サーバーでサポートされていますか 338

NetScaler Gateway 11.0のRDPプロキシ機能の変更点は何ですか? 338

ライセンスの変更 338

コマンドを有効にする 338

RDP プロキシのその他の変更 338

NetScaler ADC 10.5.eに基づくリモートデスクトッププロトコル（RDP）プロキシ構成をNetScaler ADC 11.0にどのように移行しますか 339

NetScaler ADC 11.0リリースを使用して、RDPプロキシ構成用にNetScaler Gateway をどのようにセットアップしますか 339

HDX Insight はUnified Gateway と互換性がありますか 339

既存のHDX Insight構成を移行するにはどうすればよいですか 340

NetScaler Gateway アプライアンスでのVPN構成 341

ユーザーがNetScaler Gateway プラグインを使用して接続する方法 342

セキュアトンネルの確立 343

セキュアな接続を介してプライベートネットワークトラフィックをトンネルする 343

ファイアウォールとプロキシ経由で接続する 344

NetScaler Gateway プラグインのアップグレードを制御する 344

要件 344

プラグインビヘイビア 345

VPN プラグインのアップグレードを制御するための CLI パラメータ 345

© 1997–2026 Citrix Systems, Inc. All rights reserved.

EPA プラグインのアップグレードを制御するための CLI パラメータ 346
VPN 構成 346
EPA 構成 346
NetScaler Gatewayでの完全VPNのセットアップ 347
前提条件 347
NetScaler Gateway アプライアンスで完全VPNセットアップを構成する 348
その他のパラメーター 350
分割トンネリングの設定 351
分割トンネリングオプション 353
分割トンネルオフ 353
分割トンネル ON 354
リバース分割トンネル 354
ネームサービス解決を構成する 355
参照ドキュメント 356
ユーザーのアクセス方法を選択します 356
ユーザーアクセス用にNetScaler Gateway プラグインを展開する 358
MSIインストーラーパッケージを使用してNetScaler Gateway プラグインを展開する 358
一元化された展開ツールを使用する利点 359
展開するソフトウェアプラグインを決定する 359
ユーザー用のNetScaler Gateway プラグインを選択する 359
プラグインをグローバルに構成する 360
セッションプロファイルで Windows または macOS のプラグインタイプを構成する 360
Windows向けNetScaler Gatewayプラグイン 360
Windows版NetScaler Gateway プラグインをインストールする 362
Windows版NetScaler Gateway プラグインのログオンダイアログボックスを構成する 362
Windows版NetScaler Gateway プラグインのインターセプトモードを設定する 362
ADC 構成に基づいてエンドユーザーにローカル LAN アクセスを強制する 363
Java向けNetScaler Gateway プラグイン 363

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Java 用NetScaler Gatewayプラグインの設定 364
インターセプトモードを設定するには 364
Windows ベースのコンピューターで HOSTS ファイルを更新します 365
NetScaler Gateway プラグインをActive Directory から展開する 365
構成ユーティリティからNetScaler Gateway プラグインのMSIパッケージをダウンロードするには 366
配布ポイントを作成するには 367
Active Directory を使用してNetScaler Gateway プラグインを管理する 367
ユーザーデバイスからNetScaler Gateway プラグインを削除する 368
Active Directory yを使用してNetScaler Gateway プラグインのインストールをトラブルシューティングする 368
NetScaler Gateway プラグインとCitrix Workspace アプリを統合する 368
ユーザーがCitrix Workspace アプリに接続する方法 369
Citrix Workspace アプリのアイコンを切り離す 370
CLI を使用したアイコン統合の設定 370
GUI を使用したアイコン統合の設定 370
ICA 接続用の IPv6 を構成する 371
CLI を使用して ICA プロキシの IPv6 を構成するには 371
NetScaler Gateway でCitrix Workspaceアプリのホームページを構成する 372
Citrix Workspace アプリのホームページをグローバルに構成するには 373
セッションプロファイルでCitrix Workspace アプリのホームページを構成するには 373
Citrix Workspace アプリのテーマをNetScaler Gateway のログオンページに適用する 373
NetScaler Gateway ログオンページのカスタムテーマを作成する 374
CLI を使用したカスタムテーマの作成と展開 374
NetScaler Gateway Windows VPN クライアントレジストリキー 375
認証Cookieに HttpOnly フラグを強制する 379
対応シナリオ 379
CLI を使用して HTTPOnly 機能を設定します 380

© 1997–2026 Citrix Systems, Inc. All rights reserved.

制限事項 380
VPN ユーザー用のユーザーポータルをカスタマイズする 380
ポータル・テーマの適用 381
キャクストンのテーマ 381
グリーンバブルのテーマ 381
X1のテーマ 381
ポータル・テーマを VPN 仮想サーバーにバインドする 381
CLI を使用してポータル・テーマを VPN 仮想サーバーにバインドする 381
GUI を使用してポータル・テーマを VPN 仮想サーバーにバインドする 381
ポータル・テーマを VPN グローバルにバインドする 382
CLI を使用してポータルテーマを VPN グローバルにバインドする 382
GUI を使用してポータルテーマを VPN グローバルにバインドする 382
ポータル・テーマの作成 383
ストックポータル・テーマをカスタム・ポータル・テーマのテンプレートとして使用する 383
CLI を使用したポータル・テーマの作成 383
GUI を使用したポータル・テーマの作成 383
ポータル・テーマのカスタマイズ 384
ポータル・テーマ・インターフェースについて 384
カスタマイズ可能なページ属性のタイプ 384
古いポータルのカスタマイズ 386
カスタムポータル構成を手動で作成する 386
カスタマイズしたテーマを VPN グローバルパラメータとして選択します 387
EULA を作成する 388
CLI を使用して EULA エンティティを作成する 388
GUI を使用して EULA エンティティを作成する 389
CLI を使用して EULA を VPN グローバルにバインドする 389
GUI を使用して EULA を VPN グローバルにバインドする 389
CLI を使用して EULA を VPN 仮想サーバーにバインドする 389

© 1997–2026 Citrix Systems, Inc. All rights reserved.

GUI を使用して EULA を VPN 仮想サーバーにバインドする 389

カスタムページを作成して、古いブラウザまたはサポートされていないブラウザをアップグレードするようにユーザに促す 390

SSLに基づいてサポートされていない古いブラウザをアップグレードするようにユーザーに促すカスタムページを作成する方法 390

NetScaler Gateway でクライアントレスVPNアクセスを構成する 391

クライアントレス VPN アクセスポリシーの仕組み 391

クライアントレス VPN アクセスを有効にする 393

クライアントレスアクセスをグローバルに有効にするには 394

セッションポリシーを使用してクライアントレスアクセスを有効にするには 394

Web アドレスをエンコードする 394

Web アドレスエンコーディングをグローバルに構成する 395

セッションポリシーを作成して Web アドレスエンコーディングを構成する 395

クライアントレスアクセスポリシーの作成 396

デフォルト設定を使用してクライアントレスアクセスポリシーを作成する 396

クライアントレスアクセスポリシーを仮想サーバにバインドする 396

クライアントレスアクセスポリシー式の作成と評価 396

NetScaler Gateway を使用した高度なクライアントレス VPN アクセス 397

前提条件 397

高度なクライアントレス VPN アクセスの設定 398

注意事項 399

ユーザーのドメインアクセスを構成する 399

NetScaler Gateway ウィザードを使用してドメインアクセスを構成するには 400

構成ユーティリティを使用してドメイン設定を構成するには 400

SharePoint 2003、SharePoint 2007、およびSharePoint 2013のクライアントレス VPN アクセス 401

NetScaler ADC GUIを使用してSharePointのクライアントレスアクセスを構成する 401

SharePoint サイトをホームページとして設定する 401

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SharePoint 2007 サーバーの名前解決を有効にする 402
DNS サフィックスを構成する 402
クライアントレス VPN アクセスパーシステント Cookie を有効にする 403
SharePoint のクライアントレス VPN アクセス用の永続クッキーを構成する 403
Web Interface を介したクライアントレスアクセスのユーザ設定の保存 404
構成ユーティリティを使用して Web インターフェイス永続性の Cookie をバインドするには 404
コマンドラインを使用して Web インターフェイスの永続性のために Cookie をバインドするには 405
モバイルデバイス用のCitrix SSO VPNクライアント 405
参照ドキュメント 405
ページの設定 406
ログオン時に ページを表示する 407
クライアントの選択肢オプションをグローバルに有効にする 407
セッションポリシーの一部としてクライアントの選択肢を有効にする 408
クライアント選択オプションの設定 408
承認グループを作成する 408
クライアント選択用のセッションプロファイルを作成する 409
STA サーバをグローバルに設定する 410
STA を仮想サーバにバインドする 410
アクセスシナリオのフォールバックの設定 410
アクセスシナリオフォールバックのポリシーの作成 411
検疫グループを作成する 412
ユーザー接続を検疫するための設定を構成する 413
アクセスシナリオフォールバックのセッションポリシーを作成する 413
セッションポリシーを検疫グループにバインドします 414
グローバルクライアントセキュリティポリシーを作成する 414
NetScaler Gateway プラグインの接続を構成する 414

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ユーザセッション数の設定 415
グローバルユーザー制限を設定するには 415
仮想サーバーあたりのユーザー制限を設定するには 416
タイムアウト設定を構成する 416
強制タイムアウトを構成する 417
セッションタイムアウトまたはアイドルタイムアウトの設定 418
GUI を使用してセッションまたはクライアントのアイドルタイムアウトをグローバルに設定するには 418
GUI を使用してセッションポリシーを使用してセッションまたはクライアントのアイドルタイムアウト設定を構成するには 419
内部ネットワークリソースに接続する 419
内部ネットワークリソースへのネットワークアクセスを構成する 420
分割トンネリングの設定 420
分割トンネリングを設定するには 421
分割トンネリングおよび認可の設定 421
クライアント傍受を構成する 422
NetScaler Gateway プラグイン用のイントラネットアプリケーションを構成する 422
1 つの IP アドレス用のイントラネットアプリケーションを作成するには 423
IP アドレス範囲を設定するには 424
ホスト名のイントラネットアプリケーションを作成するには 424
Java向けNetScaler Gateway プラグインのイントラネットアプリケーションを構成する 425
Java向けNetScaler Gateway プラグインのイントラネットアプリケーションを構成するには 425
ネームサービス解決を構成する 426
セッションプロファイル内に DNS サーバーまたは WINS サーバーを追加する 426
ユーザー接続のプロキシサポートを有効にする 427
プロキシ設定 427
ユーザー接続のプロキシサポートを構成するには 428

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler Gateway のすべてのプロトコルを使用するように1つのプロキシサーバーを構成するには 428
NetScaler Gateway をプロキシサーバーとして構成するには 429
アドレスプールの設定 429
イントラネット IP DNS 登録 431
ユーザー、グループ、または仮想サーバーのアドレスプールを構成する 432
アドレスプールをグローバルに設定 433
アドレスプールオプションの定義 433
アドレスプールを定義するには 434
転送ログオンページの設定 434
DNS サフィックスを構成する 435
VoIP 電話のサポート 435
Access Interfaceの設定 436
Access Interfaceの変更 437
Access Interfaceをカスタムホームページに置き換える 438
Web リンクの作成と適用 438
エンタープライズブックマークの作成 439
個人用ブックマークの作成 442
ブックマークでユーザー名トークンを構成する 442
トラフィックポリシー 442
トラフィックポリシーを作成する 443
トラフィックポリシー表現の例 443
GUI を使用したトラフィックポリシーの設定 444
フォームベースのシングルサインオンの設定 444
フォームベースのシングルサインオンの設定 445
SAML シングルサインオンの設定 445
SAML シングルサインオンの設定 446
トラフィックポリシーをバインドする 446

© 1997–2026 Citrix Systems, Inc. All rights reserved.

GUI を使用してトラフィックポリシーをグローバルにバインドする 446
トラフィックポリシーの削除 446
GUI を使用してトラフィックポリシーをバインド解除する 447
GUI を使用してトラフィックポリシーを削除する 447
セッションポリシー 447
セッションポリシーを作成する 448
セッションポリシー表現の例 448
セッションポリシーのバインド 449
GUI を使用してセッションポリシーを仮想サーバーにバインドする 449
GUI を使用して、セッションポリシーを認証、承認、および監査グループにバインドする 449
GUI を使用して、セッションポリシーを認証、承認、および監査中のユーザーにバインドする 449
セッションプロファイルを作成する 450
セッションプロファイルでユーザー接続のネットワーク設定を構成する 450
セッションプロファイルで接続設定を構成する 450
セッションプロファイルでセキュリティ設定を構成する 451
セッションプロファイルでのCitrix Virtual Apps and Desktops の設定の構成 452
StoreFront のNetScaler Gateway セッションポリシーを構成する 453
最小要件 453
StoreFront でNetScaler Gateway を構成する 453
StoreFront の認証を構成する 457
参照ドキュメント 458
エンタープライズブックマークの高度なポリシーサポート 458
VPN URL を高度なポリシーとして設定する 458
GUI について 458
CLI で 460
エンドポイントポリシー 463

© 1997–2026 Citrix Systems, Inc. All rights reserved.

エンドポイントポリシーの仕組み 463
EPA 表現のサンプル 465
ユーザーログオンオプションの評価 466
EPA スキャンをスキップする 467
Ubuntu でサポートされるエンドポイント分析スキャン 467
事前認証ポリシーとプロファイル 468
事前認証プロファイルの設定 469
カスタムエクスプレッションの設定 470
複合式の設定 471
事前認証ポリシーのバインド 472
事前認証ポリシーのバインド解除と削除 472
事前認証ポリシーのプライオリティの設定 473
認証ポリシーの投稿 474
認証後ポリシーを構成する 475
認証後スキャンの頻度を構成する 475
検疫グループと承認グループ 476
ユーザーデバイスの事前認証デバイスチェック表現 479
ウイルス対策、ファイアウォール、インターネットセキュリティ、またはスパム対策の表現を構成する 479
サービスポリシーの設定 481
プロセスポリシーの設定 482
オペレーティングシステムポリシーを構成する 483
レジストリポリシーを構成する 484
複合クライアントデバイスチェック表現の設定 487
NOT (!) 演算子を使用してポリシーを設定 488
EPA コンポーネントとしての nFactor でのデバイス証明書 488
デバイス証明書を NFactor で EPA コンポーネントとして構成する 489
nFactor 認証の要素としての EPA スキャン 490

© 1997–2026 Citrix Systems, Inc. All rights reserved.

EPA ファクター相互排他性 492
EPA の実行 492
定期的な EPA スキャンを nFactor 認証の要素として構成する 493
参照ドキュメント 498
Advanced Endpoint Analysisスキャン 498
GUI について 498
CLI で 500
EPA ライブラリをアップグレードする 500
高度なエンドポイント分析スキャンのトラブルシューティング 501
高度なエンドポイント分析ポリシー式リファレンス 502
エクスプレッションフォーマット 502
エクスプレッション文字列 502
アプリケーションのスキャン方法 504
MAC アドレスの EPA スキャン 510
GUI を使用して MAC アドレスの EPA スキャンを設定します 510
CLI を使用して MAC アドレスの EPA スキャンを設定します 511
注意事項 513
参照ドキュメント 513
ユーザーセッションの管理 513
GUI を使用したユーザーセッションの管理 514
ユーザーセッションを表示するには 514
セッションリストを更新するには 514
エンドユーザーまたはグループセッション、または特定のイントラネット IP アドレスを持つセッションを終了するには 514
CLI を使用してユーザセッションを管理する 515
常時オン 515
Always On をいつ使用するのか 515
Always On フレームワークを理解する 516

© 1997–2026 Citrix Systems, Inc. All rights reserved.

トンネルの自動再確立 516

シームレストンネル確立でサポートされるユーザ認証方式 516

Always On の設定要件 517

常時オン機能を有効にする際の考慮事項 517

常時オンの設定 518

IIP に関する注意事項 519

管理者ユーザーと管理者以外のユーザーの異なる設定の動作の概要 520

「常時オン」がダウンしているときに選択した URL を許可する 521

AlwaysOnAllowList レジストリを設定するには 521

Windows ログオン前に常時接続の VPN (正式には常時接続サービス) 522

Windows ログオン前に常にオン VPN 機能 522

Windows ログオン前に常時接続の VPN について理解する 523

Windows ログオン構成の前に常時接続の VPN の後の Windows 認証情報マネージャ画面524

Windows ログオン前に常時接続の VPN を構成する 524

前提条件 524

大まかな設定手順 524

マシンレベルトンネル 525

ユーザーレベルトンネル 529

クライアント側の設定 532

アドバンスポリシーを使用した VPN ポリシーの作成 535

クラシックポリシーからアドバンスポリシーに移行する理由 535

高度な EPA を使用した事前認証 EPA 536

高度な EPA を使用したポスト認証 EPA 536

高度なポリシーを使用した事前認証および認証後 EPA 536

nFactor 認証の要素としての定期的な EPA スキャン 537

SSL VPN 仮想サーバを使用した DTLS VPN 仮想サーバの構成 539

注意事項 539

GUI を使用して DTLS VPN 仮想サーバーを構成する 540

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CLI を使用して DTLS VPN 仮想サーバーを設定します 541
サポートされている DTLS VPN 仮想サーバーパラメーター 542
サポートされていない DTLS VPN 仮想サーバーパラメーター 542
XenAppおよびXenDesktopウィザードを使用してDTLS仮想サーバーを構成します 543
制限事項 544
Citrix製品との統合 545
ユーザーがアプリケーション、デスクトップ、ShareFileに接続する方法 545
NetScaler Gateway とStoreFront の統合 547
StoreFront で使用するようにNetScaler Gatewayを構成する方法 548
前提条件 548
NetScaler Gateway をCitrix Virtual Apps and Desktops 統合する 550
Citrix Endpoint Management、Citrix Virtual Apps and Desktopsを使用した展開 551
Citrix Endpoint Management 環境の設定を構成する 552
NetScaler機能のライセンス要件 553
NetScaler for Citrix Endpoint Management ウィザード 554
Citrix Endpoint ManagementまたはCitrixXenMobile Serverの負荷分散サーバーを構成する 556
NetScaler ADC VIPでSSLブリッジモードを使用するには 556
NetScaler ADC VIPでSSLオフロードモードを使用するには 557
電子メールセキュリティフィルタを使用した Microsoft Exchange の負荷分散サーバーを構成する 558
Citrix Endpoint Management を構成する NetScaler ADCコネクタ（XNC）ActiveSyncフィルタリング 558
Citrix 業務用モバイルアプリでモバイルデバイスからのアクセスを許可する 559
NetScaler Gateway でSecure Browse を構成する 559
アプリケーションと MDX トークンのタイムアウトを構成する 562
モバイルデバイスのエンドポイント分析を無効にする 563
Android デバイスの DNS サフィックスを使用して DNS クエリをサポートする 563
Citrix Endpoint Managementのドメインおよびセキュリティトークン認証を構成する 565

© 1997–2026 Citrix Systems, Inc. All rights reserved.

前提条件 566
ドメインとセキュリティトークンの認証を構成するには 566
クライアント証明書またはクライアント証明書とドメイン認証を構成する 567
GUIを使用してクライアント証明書認証用にNetScaler Gateway を構成する 567
GUIを使用してクライアント証明書とドメイン認証用にNetScaler Gateway を構成する 568
Citrix ADC証明書失効一覧（CRL） 569
Microsoft Intune グレーション 570
Citrix マイクロVPNとMicrosoft Endpoint Managerとの統合 570
統合 Intune MDM ソリューションを使用する場合 571
NetScaler Gateway MDM と Intune の統合を理解する 572
単一要素ログイン用のNetScaler Gateway 仮想サーバーのネットワークアクセス制御デバイスチェックを構成する 572
ライセンス 573
システム要件 573
前提条件 574
参照ドキュメント 574
ゲートウェイ展開用に nFactor を搭載した NetScaler Gateway 仮想サーバーを追加するには 574
認証ログインスキーマを認証仮想サーバーにバインドして、VPN プラグインが /cgi/login 要求の一部としてデバイス ID を送信するように指示するには 578
トラブルシューティング 578
一般的な問題 578
NetScaler Gatewayの問題 579
NetScaler Gateway OAuthのステータスとエラー状態 579
Intune 構成チェック 580
Azure Portalでの NetScaler Gateway アプリケーションの構成 580
前提条件 580
Azure で NetScaler Gateway アプリを作成するには 581
Azure ADAL トークン認証について 584

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Microsoft ADALトークン認証用のNetScaler Gateway 仮想サーバーの構成 584
Microsoft Endpoint ManagerでマイクロVPNを使用するようにNetScaler Gateway をセットアップする 587
システム要件 587
前提条件 587
Azure Active Directory (AAD) アプリケーションのアクセス許可を付与する 588
NetScaler Gateway をマイクロVPN用に構成する 588
Microsoft Edge Browserの設定 589
トラブルシューティング 590
一般的な問題 590
NetScaler Gatewayの問題 591
NetScaler Gateway OAuthのステータスとエラー状態 591
Azure AD グラフの拡張サポート 592
HDX Enlightened Data Transport サポート 593
Enlightened Data Transport サポートを使用する場合 593
EDTおよびHDX InsightをサポートするようにNetScaler Gatewayを構成 594
Enlightened Data Transport をサポートするようにNetScaler Gateway を構成する 595
GUIを使用してEDTをサポートするようにNetScaler Gateway を構成するには 595
CLIを使用してEDTサポート用にNetScaler Gateway を構成するには 596
HDX InsightをサポートするようにNetScaler Gatewayを構成する 596
GUIを使用してHDX InsightをサポートするようにNetScaler Gateway を構成するには 596
CLIを使用してHDX Insightサポート用にNetScaler Gateway を構成するには、次のコマンドを入力します 598
非 NSAP HDX セッションの HDX Insightを無効にする 598
L7 遅延しきい値処理 598
L7 レイテンシは L4 レイテンシとどう違うのですか 599
ICA RTT と L7 のレイテンシー計算の違い 599
CLI を使用した L7 遅延しきい値の設定 599

© 1997–2026 Citrix Systems, Inc. All rights reserved.

引数 600

GUI を使用した L7 遅延しきい値の設定 601

NetScaler ADMでL7レイテンシーパラメーターを表示する 602

L7 クライアントのレイテンシー値を計算する時間間隔を指定するパラメーター 602

CLI を使用してレイテンシー頻度を設定するには 602

CLI を使用してレイテンシー頻度を設定するには 603

L7 レイテンシ測定モデルと L7 レイテンシしきい値レポートモデル 603

L7 レイテンシー測定モデル 603

L7 遅延しきい値レポートモデル 603

RDPプロキシ 604

クライアントレス VPN を介した導入 605

ICA プロキシを介した展開 605

強制の詳細 605

強制用にサポートされている RDP パラメータ 605

接続フロー 606

ステートレス (デュアル) ゲートウェイの互換性 606

シングルゲートウェイの互換性 607

シングルリスナーのサポート 608

RDP プロキシのライセンス要件 608

ブックマーク 608

ブックマークを作成する 608

RDP プロキシで有効にする機能とモード 609

RDP プロキシの概要設定手順 609

クライアントプロファイルを構成する 609

サーバープロファイルを構成する 610

CLI を使用した RDP プロキシの設定 611

GUI を使用した RDP プロキシの設定 612

SSO を無効にするオプション 615

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ステートレス RDP プロキシ 615
接続フロー 616
前提条件 617
CLI を使用したステートレス RDP プロキシの設定 617
GUI を使用してステートレス RDP プロキシを構成する 619
接続カウンタ 620
アップグレードノート 620
RDP 接続リダイレクト 620
前提条件 621
接続ブローカの存在下で RDP プロキシを展開する 621
CLI を使用して、接続ブローカの存在下で RDP プロキシを構成する 621
NetScaler ADC GUIを使用してRDP接続リダイレクトを構成する 622
LDAP 属性に基づいて RDP URL を設定 622
CLI を使用して LDAP 属性に基づいて RDP URL を入力するには 622
LDAP サーバ設定 623
GUI を使用して LDAP 属性に基づいて RDP URL を入力するには 623
RDP プロキシで RDP ファイル名をランダム化する 623
RDP プロキシを使用した RDP ファイル名のランダム化のサポートを構成する 624
RDP ファイルの名前を設定する 624
RDP ファイルの名前を設定する 624
送信ICAプロキシのサポート 626
アウトバウンドICAプロキシのサポートについて 626
NetScaler ADC LANプロキシでのSSLサポート 626
アウトバウンドICAプロキシの構成 627
ICAアウトバウンドプロキシ用のNetScaler ADC LANプロキシを構成する 627
NetScaler Gateway の ICA プロキシを構成する 628
NetScaler Gateway 対応の PCoIP プロキシサポート（VMware Horizon View） 629
VMware Horizon View 用の NetScaler Gateway 有効な PCoIP プロキシの構成 629

© 1997–2026 Citrix Systems, Inc. All rights reserved.

前提条件 629
USB リダイレクトを有効にする手順 633
Unified Gateway のコンテンツスイッチング式の更新 633
PCoIP ゲートウェイを使う 634
VMware Horizon View 接続サーバの構成 634
NetScaler Gateway の送信プロキシサポートのプロキシ自動構成 635
CLIを使用して送信プロキシのPACをサポートするようにNetScaler Gateway グローバルパラメーターを構成する 635
CLIを使用してセッションプロファイルでPACをサポートするようにNetScaler Gateway を構成する 635
GUIを使用して送信プロキシのPACをサポートするようにNetScaler Gateway グローバルパラメーターを構成する 636
GUIを使用してセッションプロファイルでPACをサポートするようにNetScaler Gateway を構成する 636
SameSite Cookie属性の構成サポート 637
`SameSite` Cookie属性を設定する 637
CLIを使用した`SameSite`属性の設定 638
CLI を使用したへの `patset` Cookie のバインド 638
GUI を使用して sameSite 属性を設定する 638
CloudBridge によるネットワークトラフィックの最適化 640
トラフィックポリシーを作成するには 641
ゲートウェイ UX 構成での RfWebUI ペルソナ 642
RfWebUI ペルソナを使用する時は 642
RfWebUI ペルソナによって提供される機能 642
GO 643
アプリケーションの集約 643
ユーザ設定の RDP プロキシリンク 643
お気に入りのアプリケーション 643
RfWebUI ペルソナを有効にする際の考慮事項 644

© 1997–2026 Citrix Systems, Inc. All rights reserved.

RfWebUI ペルソナの設定 644
RfWebUI 設定パラメーター 644
NetScaler Gateway ポータルのカスタマイズ 649
カスタムプラグインを使用したゲートウェイポータルのカスタマイズ 649
設定例 650
ログインスキーマの作成とカスタマイズ 652
ログインスキーマプロファイルの作成 652
ログインスキーマプロファイルを認証、承認、および監査仮想サーバーにバインドする 653
管理 UI からのポータルのカスタマイズ 653
共通属性 654
文字列のカスタマイズ 654
NetScaler Gateway VPN 分割トンネルのOffice365用に最適化 656
GUI を使用した設定 656
GUI を使用して分割トンネリングを設定するには 656
GUI を使用して VPN イントラネットアプリケーションを作成するには 657
CLI を使用した設定 657
Office 365 サービス (EXO、SPO、およびMicrosoft Teams) の IP アドレスのリスト 658
IPv4 アドレス範囲 658
IPv6 アドレス範囲 659
UDP トラフィックのサービスタイプサポート 660
サーバー名表示拡張機能の設定 661
SSL ハンドシェイク中のサーバ証明書の検証 662
テンプレートを使用した簡略化された SaaS アプリ設定 664
テンプレートを使用したアプリの構成と公開-NetScaler Gateway 固有の構成 664
テンプレートを使用したアプリの構成と公開-アプリサーバー固有の構成 666
Web Interfaceを使用したNetScaler Gateway の展開 673
Web Interface をセキュアなネットワークに展開する 674
DMZ内のNetScaler Gateway と並行してWeb Interfaceを展開する 675

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DMZのNetScaler Gateway の背後にWeb Interfaceを展開する 675
Web Interfaceの機能 676
Web Interfaceのサイトのセットアップ 676
Web インターフェイス 5.4 サイトの作成 677
設定ファイルの使用 678
Citrix Web Interface管理コンソールを使用したサイトの構成 678
Web InterfaceでのNetScaler Gateway 設定の構成 5.4 679
Web InterfaceでNetScaler Gateway 設定を構成するには 679
Web インターフェイス 5.3 サイトの作成 681
Web Interface 5.3のサイトを作成するには 681
Web Interface 5.3でのNetScaler Gateway 設定の構成 683
NetScaler Gateway のWeb Interface5.3設定を構成するには 683
単一サイトへのCitrix Virtual Apps and Desktops の追加 684
Web Interface 5.3または5.4を使用してCitrix Virtual Apps and Desktops を単一のサイトに追加するには 684
NetScaler Gateway を介したユーザー接続のルーティング 684
Citrix XenApp 6.5サーバーのプロパティを構成して、NetScaler Gateway 経由でルーティングされた接続のみを受け入れるようにするには 685
NetScaler Gateway を介してルーティングされた接続のみを受け入れるようにCitrix 仮想デスクトップサーバーのプロパティを構成するには 685
Web インターフェイスとの通信の設定 686
公開アプリケーションとデスクトップのポリシーの構成 686
NetScaler Gateway でWeb Interfaceをグローバルに構成するには 686
Web Interface のセッションポリシーを構成するには 687
セッションポリシーを仮想サーバーにバインドするには 687
公開アプリケーションウィザードで設定を構成する 687
公開アプリケーションウィザードを使用して Web Interface の設定を構成するには 688
NetScaler Gateway でのSecure Ticket Authority 構成 688

© 1997–2026 Citrix Systems, Inc. All rights reserved.

STA をグローバルにバインドするには 688
STA を仮想サーバーにバインドするには 689
参照ドキュメント 689
NetScaler Gateway での追加のWeb Interface設定の構成 689
Web インターフェイスフェールオーバーの設定 690
Web インターフェイスフェールオーバーを設定するには 690
Web インターフェイスを使用したスマートカードアクセスの構成 691
Web Interface でのアプリケーションおよび仮想デスクトップへのアクセスの構成 691
アプリケーションおよびデスクトップにアクセスするためのNetScaler Gateway プラグインのグローバル設定を構成するには 692
イントラネットアプリケーションを構成するには 693
イントラネットアプリケーションをグローバルにバインドするには 693
イントラネットアプリケーションを仮想サーバーにバインドするには 693
SmartAccess 設定 694
SmartAccess がCitrix Virtual Apps and Desktops どのように機能するのか 695
Citrix Virtual Apps ポリシーとフィルターの構成 696
SmartAccess のセッションポリシーを構成するには 696
Citrix Virtual Apps でのユーザーデバイスマッピングの構成 696
Citrix XenApp 6.5 で制限の厳しいポリシーを構成するには 697
Citrix XenApp 6.5で非制限ポリシーを構成するには 698
検疫アクセス方法としてのCitrix Virtual Apps 有効化 699
検疫グループのセッションポリシーおよびエンドポイント分析スキャンの作成 699
SmartAccess 向けの Citrix Virtual Desktops の構成 700
Citrix Virtual Desktops で SmartAccess のセッションポリシーを構成するには 700
Citrix Virtual Desktops でポリシーとフィルターを構成するには 5 701
Desktop Delivery Controller を STA として追加するには 702
SmartControl の設定 702
ポリシー 704

© 1997–2026 Citrix Systems, Inc. All rights reserved.

追加 704
編集 704
削除 705
バインディングを表示 705
ポリシーマネージャ 705
バインディングを追加 706
ポリシーバインディング 706
ポリシーのバインド解除 706
バインドNOPOLICY 707
編集 707
バインディングを編集 707
ポリシーの編集 707
アクションを編集 708
アクション 708
アクション 709
追加 709
編集 709
アクションの設定 710
削除 710
アクション 710
アクセスプロファイル 710
GUI を使用したアクセスプロファイルの作成 711
GUI を使用してアクセスプロファイルをポリシーに追加する 711
追加 711
編集 712
アクセスプロファイルの設定 712
削除 712
共通プロセス 712

© 1997–2026 Citrix Systems, Inc. All rights reserved.

アクションを作成する 712
アクションを選択 713
アクセスプロファイルの作成 713
既存のアクセスプロファイルを選択する 713
式 713
グループ識別 715
事前認証 715
セッション 715
ログアクションの作成 715
監査メッセージの作成アクション 715
ログアクションの改訂 716
監査メッセージアクションの設定 716
既存のポリシーを選択する 717
ポリシーを作成する 717
事前認証および認証後のエンドポイント分析の設定 717
認証後の設定 718
NetScaler Gateway セッションプロファイルの作成 718
事前認証の設定 720
事前認証プロファイルの作成 721
Web インターフェイスへのシングルサインオンの設定 722
Web アプリケーションへのシングルサインオンをグローバルに構成するには 723
セッションポリシーを使用して Web アプリケーションへのシングルサインオンを構成するには 723
Web アプリケーションへのシングルサインオン用の HTTP ポートを定義するには 723
その他の設定ガイドライン 724
Web Interface へのシングルサインオン接続をテストするには 724
スマートカードを使用した Web インターフェイスへのシングルサインオンの構成 725

© 1997–2026 Citrix Systems, Inc. All rights reserved.

スマートカードを使用してシングルサインオン用のセッションプロファイルを作成するには 726
スマートカードを使用してシングルサインオン用にクライアント証明書を構成するには 726
Citrix Virtual Apps およびファイル共有のシングルサインオンを構成するには 727
ファイルタイプの関連付けを許可する 727
Web インターフェイスサイトの作成 728
NetScaler Gateway でファイルタイプの関連付けを構成する 730
ファイルタイプの関連付けのセッションポリシーとプロファイルを作成するには 730
ファイルタイプの関連付けのトラフィックプロファイルを作成するには 731
トラフィックポリシーでファイルタイプの関連付けを設定するには 731
__index__ 732
一般的な展開 732
Citrix Endpoint Management 環境の設定の構成 732
Citrix ADC機能のライセンス要件 734
Citrix Endpoint Management ウィザード用Citrix ADCウィザード 734
Citrix モバイル生産性アプリを使用したモバイルデバイスからのアクセスの許可 737
Citrix Gateway でのSecure Browse 構成 738
アプリケーションおよびMDXトークンのタイムアウトの構成 741
モバイルデバイスのエンドポイント分析の無効化 741
AndroidデバイスでDNSサフィックスを使用したDNSクエリのサポート 742
Citrix Endpoint Management、Citrix Virtual Apps、およびデスクトップを使用した展開 744
ダブルホップDMZでの展開 745
ダブルホップDMZでのCitrix Gateway の展開 746
ファイアウォールで適切なポートを開く 746
システムのインストール 748
証明書のインストールと管理 749
証明書署名要求の作成 749
既存の証明書のインポートとインストール 751

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix Gateway への署名付き証明書のインストール 752
認証にデバイス証明書を使用する 754
DNS 仮想サーバの構成 755
DNS 仮想サーバーを構成するには 755
ユーザ接続用の IPv6 の設定 756
初回セットアップウィザードを使用したCitrix Gateway の構成 757
Citrix Gateway ウィザードを使用した設定の構成 757
Citrix Gateway ウィザードを起動するには 758
Configuring Settings with the Quick Configuration Wizard 758
クイック構成ウィザードで設定を構成するには 760
仮想サーバーの作成 763
仮想サーバでの接続タイプの設定 763
Web Interfaceを使用したCitrix Virtual Apps and Desktops のリソースへのアクセス 764
NetScaler Gateway とCitrix Virtual Apps and Desktops の統合 765
サーバーファームへのセキュアな接続を確立する 765
プロセスの概要:サーバーファーム内の公開リソースへのユーザーアクセス 766
Citrix Gateway とCitrix Virtual Apps and Desktops の統合 767
ライセンス 768
Citrix Gateway にライセンスをインストールするには 768
最大ユーザー数を設定するには 769
Citrix Gateway のライセンスの種類 769
プラットフォームライセンス 770
ユニバーサルライセンス 770
認証のネイティブ OTP サポート 771
ネイティブ OTP サポートの利点 772
ネイティブ OTP ワークフロー 772
前提条件 773
GUI を使用したネイティブ OTP の設定 773

© 1997–2026 Citrix Systems, Inc. All rights reserved.

最初の要素のログインスキーマの作成 773
認証、承認、監査仮想サーバーの構成 774
第 2 要素 OTP のログインスキーマの作成 776
OTP を管理するためのコンテンツスイッチングポリシーを構成する 776
CLI を使用したネイティブ OTP の設定 777
OTP デバイスの登録および管理ページを構成するには 777
LDAP ログオンアクションを作成するには 777
LDAP ログオンの認証ポリシーを追加するには 778
ログインスキーマを使用して UI を表示するには 778
デバイスの登録と管理ページを表示する 778
CLI を使用してユーザログインページを設定するには 779
Citrix ADCでデバイスを登録する 781
OTPを使用してCitrix ADCにログインします 782
インストール前のチェックリスト 782
ユーザーデバイス 782
Citrix Gateway の基本的なネットワーク接続 782
Citrix Gateway を介してアクセス可能な内部ネットワーク 783
高可用性 783
認証と承認 784
LDAP 認証 784
RADIUS 認証および認可 785
SAML 認証 785
ファイアウォールを介したポートのオープン（シングルホップ DMZ） 785
セキュリティで保護されていないネットワークと DMZ 間のファイアウォール 786
セキュリティで保護されたネットワーク間のファイアウォール 786
Citrix Virtual Desktops、Citrix Virtual Apps、Web Interface、またはStoreFront 786
Citrix Endpoint Management 786
Citrix Virtual Apps を使用したダブルホップDMZ展開 787

© 1997–2026 Citrix Systems, Inc. All rights reserved.

最初のDMZでのCitrix Gateway 787
2番目のDMZのCitrix Gateway 788
Citrix Endpoint Management またはStoreFront との統合 788
NetScaler Gateway とEndpoint Management 統合 788
NetScaler Gateway とStoreFront の統合 789
Endpoint Management とStoreFront のポリシーの構成 790
Citrix Gateway プラグインのシステム要件 791
クライアントインターセプションの設定 793
Citrix Gateway プラグイン用のイントラネットアプリケーションの構成 793
1 つの IP アドレスに対してイントラネットアプリケーションを作成するには 794
IP アドレス範囲を構成するには 795
ホスト名のイントラネットアプリケーションを作成するには 795
注意点 795
ユーザ接続のプロキシサポートの有効化 796
ユーザー接続のプロキシサポートを構成するには 796
Citrix Gateway のすべてのプロトコルを使用するように1つのプロキシサーバーを構成するには 796
Citrix Gateway をプロキシサーバーとして構成するには 797
アドレスプールの設定 797
ユーザー、グループ、または仮想サーバーのアドレスプールを構成するには 798
アドレスプールをグローバルに設定するには 798
SmartAccess 設定 798
複合クライアントセキュリティ式の設定 799
AND (&&) 演算子を使用したポリシーの構成 800
OR (\|\|) 演算子を使用したポリシーの構成 800
NOT (!) 演算子を使用したポリシーの構成 800
認証後ポリシーの設定 801
トラフィックポリシーの作成 801

© 1997–2026 Citrix Systems, Inc. All rights reserved.

トラフィックポリシーを設定するには 802
フォームベースのシングル・サインオンの設定 803
フォームベースのシングルサインオンを構成するには 803
Active Directory からのCitrix Gateway プラグインの展開 804
構成ユーティリティからCitrix Gateway プラグインのMSIパッケージをダウンロードするには 805
配布ポイントを作成するには 805
Java用Citrix Gateway プラグインを使用した接続 806
Java用にCitrix Gateway プラグインを構成するには 807
インターセプションモードを設定するには 807
Windows ベースのコンピュータでの HOSTS ファイルの更新 808
Citrix 製品との統合 808

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler Gatewayリリースノート

リリースノートには、特定のビルドでソフトウェアがどのように変更されたか、およびそのビルドに存在する既知の問題が記載されています。

リリースノートドキュメントには、次のセクションのすべてまたは一部が含まれています。

- **新機能**:ビルドでリリースされた機能強化とその他の変更。
- **修正された問題**:ビルドで修正される問題。
- **既知の問題**:ビルドに存在する問題。
- **注意点**:ビルドを使用する際に留意すべき重要な点です。
- **制限事項**:ビルドに存在する制限事項。

重要： NetScaler Gateway リリースノートは、NetScaler ADCリリースノートの一部としてカバーされています。 NetScaler Gateway 13.0の拡張機能、既知の問題、およびバグ修正の詳細については、 リリースノートのページを参照してください 。

注：

- 問題の説明の下にある［# XXXXXX］ラベルは、Citrix ADCチームが内部的に使用する追跡IDです。
- これらのリリースノートには、セキュリティ関連の修正は記載されていません。セキュリティに関する修正とアドバイスの一覧については、Citrixセキュリティ情報を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler Gatewayについて

NetScaler Gateway は導入が簡単で、管理も簡単です。最も一般的な展開構成は、DMZに NetScaler Gateway アプライアンスを配置することです。ネットワーク内に複数のNetScaler Gatewayアプライアンスをインストールして、より複雑な展開環境を実現することができます。

NetScaler Gateway を初めて起動するときに、シリアルコンソール、構成ユーティリティのセットアップウィザード、または動的ホスト構成プロトコル（DHCP）を使用して初期構成を実行できます。MPX アプライアンスでは、アプライアンスの前面パネルにある LCD キーパッドを使用して初期設定を実行できます。IP アドレス、サブネットマスク、デフォルトゲートウェイ IP アドレス、ドメインネームシステム (DNS) アドレスなど、内部ネットワークに固有の基本設定を構成できます。基本的なネットワーク設定を構成したら、認証、承認、ネットワークリソース、仮想サーバー、セッションポリシー、エンドポイントポリシーのオプションなど、NetScaler Gateway 操作に固有の設定を構成します。

NetScaler Gateway をインストールして構成する前に、このセクションのトピックで展開の計画に関する情報を確認してください。展開計画には、アプライアンスを設置する場所の決定、DMZ への複数のアプライアンスのインストール方法の理解、およびライセンス要件が含まれます。NetScaler Gateway は、セキュリティで保護されたネットワークで実行されている既存のハードウェアまたはソフトウェアを変更することなく、任意のネットワークインフラストラクチャにインストールできます。NetScaler Gateway は、サーバーロードバランサー、キャッシュエンジン、ファイアウォール、ルーター、IEEE 802.11ワイヤレスデバイスなどの他のネットワーク製品をサポートしています。

NetScaler Gateway を構成する前に、インストール前チェックリストに設定を書いて、手元に置くことができます。

NetScaler Gatewayアプライアンス	NetScaler Gateway アプライアンスおよびアプライアンスのインストール手順について説明します。
インストール前のチェックリスト	確認する計画情報と、NetScaler Gateway をネットワークにインストールする前に完了する必要があるタスクの一覧を示します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

一般的な展開	ネットワークDMZ、DMZのない安全なネットワーク、および負荷分散とフェイルオーバーをサポートするための他のアプライアンスとのNetScaler Gateway の展開に関する情報を提供します。また、Citrix Virtual Apps and Desktopsを使用したNetScaler Gateway の展開に関する情報も記載されています。
Licensing	アプライアンスにライセンスをインストールする方法について説明します。また、複数のNetScaler Gateway アプライアンスにライセンスをインストールする方法についても説明しています。

NetScaler Gateway アーキテクチャ

NetScaler Gateway のコアコンポーネントは次のとおりです：

- **仮想サーバー**。NetScaler Gateway 仮想サーバーは、ユーザーが利用できるすべての構成済みサービスを代表する内部エンティティです。仮想サーバは、ユーザがこれらのサービスにアクセスするためのアクセスポイントでもあります。単一のアプライアンスに複数の仮想サーバーを構成して、1つのNetScaler Gatewayアプライアンスで、認証およびリソースアクセスの要件が異なる複数のユーザーコミュニティにサービスを提供することができます。
- **認証、承認、監査**。認証、承認、およびアカウンティングを構成して、セキュリティ保護されたネットワーク内のNetScaler GatewayまたはLDAPやRADIUSなどの認証サーバーのいずれかで認識される資格情報を使用して、ユーザーがNetScaler Gatewayにログオンできるようにします。承認ポリシーは、ユーザーのアクセス許可を定義し、特定のユーザーがアクセスを許可されるリソースを決定します。認証と承認について詳しくは、「認証と承認の構成」を参照してください。監査サーバーは、ユーザーログオンイベント、リソースアクセスインスタンス、操作エラーなど、NetScaler Gateway アクティビティに関するデータを保持します。この情報は、NetScaler Gatewayまたは外部サーバーに保存されます。監査について詳しくは、「NetScaler Gateway での監査の設定」を参照してください。
- **ユーザー接続**。ユーザーは、次のアクセス方法を使用してNetScaler Gateway にログオンできます。
    - Windows用NetScaler Gateway プラグインは、Windowsベースのコンピューターにインストールされているソフトウェアです。ユーザーは、Windows ベースのコンピューターの通知領域のアイコンを右クリックしてログオンします。ユーザーがNetScaler Gateway プラ

© 1997–2026 Citrix Systems, Inc. All rights reserved.

グインがインストールされていないコンピューターを使用している場合は、Webブラウザーを使用してログオンし、プラグインをダウンロードしてインストールできます。ユーザーがCitrix Workspace アプリをインストールしている場合、ユーザーはCitrix WorkspCitrix Workspace アプリからNetScaler Gateway プラグインを使用してログオンします。Citrix Workspace アプリとNetScaler Gateway プラグインがユーザーデバイスにインストールされている場合、Citrix Workspace アプリはNetScaler Gateway プラグインを自動的に追加します。

- macOS Xを実行しているユーザーがログオンできるようにするmacOS X用NetScaler Gateway プラグイン。Windows向けNetScaler Gateway プラグインと同じ機能を備えています。このプラグインバージョンのエンドポイント分析サポートを提供するには、NetScaler ADC Gateway 10.1、ビルド120.1316.eをインストールします。
- Web InterfaceまたはCitrix StoreFront を使用して、サーバーファーム内の公開アプリケーションおよび仮想デスクトップへのユーザー接続を可能にするCitrix Workspaceアプリ。
- Citrix Workspace アプリ、Secure Hub、WorxMail、およびWorxWeb。ユーザーは、Citrix Endpoint ManagementでホストされているWebおよびSaaSアプリケーション、iOSおよびAndroidモバイルアプリ、およびShareFileデータにアクセスできます。
- ユーザーは、NetScaler Gateway Webアドレスを使用するAndroidデバイスから接続できます。ユーザーがアプリを起動すると、接続はMicro VPNを使用してネットワークトラフィックを内部ネットワークにルーティングします。ユーザーがAndroidデバイスから接続する場合は、NetScaler Gateway でDNS設定を構成する必要があります。詳細については、「Android デバイスの DNS サフィックスを使用した DNS クエリのサポート」を参照してください。
- ユーザーは、NetScaler Gateway Webアドレスを使用するiOSデバイスから接続できます。Secure Browse は、グローバルに、またはセッションプロファイルで構成します。ユーザーがiOSデバイスでアプリを起動すると、VPN接続が開始され、接続がNetScaler Gateway 経由でルーティングされます。
- クライアントレスアクセス。ユーザーデバイスにソフトウェアをインストールしなくても、必要なアクセスをユーザーに提供します。

  NetScaler Gateway を構成するときに、ユーザーのログオン方法を構成するポリシーを作成できます。また、セッションおよびエンドポイントの分析ポリシーを作成して、ユーザーのログオンを制限することもできます。

- **ネットワークリソース**。これには、ファイルサーバー、アプリケーション、Webサイトなど、ユーザーがNetScaler Gateway を介してアクセスするすべてのネットワークサービスが含まれます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **仮想アダプター**。NetScaler Gateway 仮想アダプターは、IPスプーフィングを必要とするアプリケーションをサポートします。仮想アダプタは、NetScaler Gateway プラグインのインストール時にユーザーデバイスにインストールされます。ユーザーが内部ネットワークに接続すると、NetScaler Gateway と内部サーバー間の送信接続では、イントラネットIPアドレスが送信元IPアドレスとして使用されます。NetScaler Gateway プラグインは、構成の一部としてサーバーからこのIPアドレスを受信します。

  NetScaler Gateway で分割トンネリングを有効にすると、すべてのイントラネットトラフィックが仮想アダプタを介してルーティングされます。イントラネットにバインドされたトラフィックをインターセプトする場合、仮想アダプタは A および AAAA レコードタイプの DNS クエリをインターセプトし、他のすべての DNS クエリはそのまま残します。内部ネットワークにバインドされていないネットワークトラフィックは、ユーザーデバイスにインストールされているネットワークアダプタを介してルーティングされます。インターネットとプライベート LAN (LAN) 接続はオープンで接続されたままです。分割トンネリングを無効にすると、すべての接続が仮想アダプタを介してルーティングされます。既存の接続はすべて切断され、ユーザーはセッションを再確立する必要があります。

  イントラネット IP アドレスを構成すると、内部ネットワークへのトラフィックは、仮想アダプタを介してイントラネット IP アドレスでスプーフィングされます。

ユーザー接続の仕組み

ユーザーは、電子メール、ファイル共有、およびその他のネットワークリソースにリモートの場所から接続できます。ユーザーは、次のソフトウェアを使用して内部ネットワークリソースに接続できます。

- NetScaler Gateway プラグイン
- Citrix Workspaceアプリ
- WorxMailとWorxWeb
- Android と iOS のモバイルデバイス

NetScaler Gateway プラグインで接続する

NetScaler Gateway プラグインを使用すると、次の手順で内部ネットワークのリソースにユーザーがアクセスできます：

1. ユーザーは、WebブラウザーにWebアドレスを入力して、NetScaler Gateway に初めて接続します。ログオンページが表示され、ユーザーはユーザー名とパスワードの入力を求められます。外部認証サーバーが構成されている場合、NetScaler Gateway はサーバーに接続し、認証

© 1997–2026 Citrix Systems, Inc. All rights reserved.

サーバーはユーザーの資格情報を確認します。ローカル認証が構成されている場合、NetScaler Gateway はユーザー認証を実行します。

2. 事前認証ポリシーを構成する場合、ユーザーがWindowsベースのコンピューターまたはmacOS XコンピューターのWebブラウザーにNetScaler Gateway Webアドレスを入力すると、NetScaler Gateway は、ログオンページが表示される前にクライアントベースのセキュリティポリシーが適用されているかどうかを確認します。セキュリティチェックは、ユーザーデバイスがオペレーティングシステムの更新、ウイルス対策保護、適切に構成されたファイアウォールなどのセキュリティ関連の条件を満たしていることを確認します。ユーザーデバイスがセキュリティチェックに失敗すると、NetScaler Gateway はユーザーのログオンをブロックします。ログオンできないユーザーは、必要な更新プログラムまたはパッケージをダウンロードし、ユーザーデバイスにインストールする必要があります。ユーザーデバイスが事前認証ポリシーを通過すると、ログオンページが表示され、ユーザーはログオン資格情報を入力できます。NetScaler Gateway 10.1、ビルド120.1316.eをインストールすると、macOS Xコンピューターで高度なエンドポイント分析を使用できます。
3. NetScaler Gateway がユーザーを正常に認証すると、NetScaler Gateway はVPNトンネルを開始します。NetScaler Gateway は、Windows用のNetScaler GatewayプラグインまたはmacOS X用のNetScaler Gatewayプラグインをダウンロードしてインストールするようにユーザーに求めます。
4. 認証後スキャンを構成すると、ユーザーが正常にログオンした後、NetScaler Gateway はユーザーデバイス上で必要なクライアントセキュリティポリシーをスキャンします。事前認証ポリシーと同じセキュリティ関連条件を要求できます。ユーザーデバイスがスキャンに失敗すると、ポリシーが適用されないか、ユーザーが検疫グループに配置され、ネットワークリソースへのユーザーのアクセスが制限されます。
5. セッションが確立されると、ユーザーはNetScaler Gateway ホームページにリダイレクトされ、ユーザーはアクセスするリソースを選択できます。NetScaler Gateway に含まれているホームページは、Access Interfaceと呼ばれます。ユーザーがWindows向けNetScaler Gatewayプラグインを使用してログオンすると、Windowsデスクトップの通知領域にアイコンが表示され、ユーザーデバイスが接続され、接続が確立されたことを示すメッセージが表示されます。ユーザーは、Microsoft Outlook を開いて電子メールを取得するなど、Access Interfaceを使用せずにネットワーク内のリソースにアクセスすることもできます。
6. ユーザー要求が事前認証と認証後の両方のセキュリティチェックに合格すると、NetScaler Gateway は要求されたリソースに接続し、ユーザーデバイスとそのリソース間の安全な接続を開始します。
7. ユーザーは、Windowsベースのコンピューターの通知領域にあるNetScaler Gateway アイコンを右クリックし、［ログオフ］をクリックすることで、アクティブなセッションを閉じることができます。また、非アクティブが原因でセッションがタイムアウトすることもあります。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

セッションが閉じられると、トンネルはシャットダウンされ、ユーザは内部リソースにアクセスできなくなります。ユーザーは、ブラウザーにNetScaler Gateway Webアドレスを入力することもできます。ユーザーが Enter キーを押すと、Access Interfaceが表示され、そこからログオフできます。

注： Citrix Endpoint Managementを内部ネットワークに展開する場合、内部ネットワークの外部から接続するユーザーは、最初にNetScaler Gateway に接続する必要があります。ユーザーが接続を確立すると、ユーザーはCitrix Endpoint ManagementでホストされているWebアプリケーション、SaaSアプリケーション、AndroidおよびiOSモバイルアプリ、およびShareFileデータにアクセスできます。ユーザーは、クライアントレスアクセス、またはCitrix Workspaceアプリまたは Secure Hubを使用して、NetScaler Gateway プラグインに接続できます。

Citrix Workspace アプリとの接続

ユーザーはCitrix Workspace アプリに接続して、Windowsベースのアプリケーションと仮想デスクトップにアクセスできます。ユーザーは、Endpoint Managementからアプリケーションにアクセスすることもできます。リモートの場所から接続するには、ユーザーはデバイスにNetScaler Gateway プラグインをインストールします。Citrix Workspace アプリは、NetScaler Gateway プラグインをプラグインのリストに自動的に追加します。ユーザーがCitrix Workspace アプリにログオンすると、NetScaler Gateway プラグインにもログオンできます。また、ユーザーがCitrix Workspaceアプリにログオンしたときに NetScaler Gateway プラグインへのシングルサインオンを実行するようにNetScaler Gateway を構成することもできます。

iOS および Android デバイスと接続する

ユーザーは、Secure Hubを使用して、iOSまたはAndroidデバイスから接続できます。ユーザーは Secure Mailを使用して電子メールにアクセスし、WorxWebでWebサイトに接続できます。

ユーザーがモバイルデバイスから接続すると、接続はNetScaler Gateway を介して内部リソースにアクセスします。ユーザーが iOS に接続する場合は、セッションプロファイルの一部として Secure Browse を有効にします。ユーザーが Android で接続する場合、接続はマイクロ VPN を自動的に使用します。さらに、 Secure MailとWorxWebは、マイクロVPNを使用して、NetScaler Gateway を介した接続を確立します。NetScaler Gateway でマイクロVPNを構成する必要はありません。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

一般的なNetScaler Gatewayの展開

組織の内部ネットワーク（またはイントラネット）の境界にNetScaler Gateway を展開して、内部ネットワークに存在するサーバー、アプリケーション、およびその他のネットワークリソースへの安全な単一アクセスポイントを提供できます。すべてのリモートユーザーは、内部ネットワークのリソースにアクセスする前に、NetScaler Gateway に接続する必要があります。

NetScaler Gateway は、通常、ネットワーク内の次の場所にインストールされます。

- ネットワークDMZで
- DMZのないセキュアなネットワークで<

また、Citrix Virtual Desktops、Citrix Virtual Desktops、StoreFront、およびCitrix Endpoint ManagementとともにNetScaler Gatewayを展開して、ユーザーがWindows、Web、モバイル、およびSaaSアプリケーションにアクセスできるようにすることもできます。展開環境にCitrix Virtual Apps、StoreFront、およびデスクトップ7が含まれている場合は、NetScaler Gateway をシングルホップまたはダブルホップDMZ構成で展開できます。ダブルホップ展開は、以前のバージョンのCitrix Virtual DesktopsまたはCitrix Endpoint Managementではサポートされていません。

これらのソリューションおよびその他のサポートされているCitrixソリューションを使用したNetScaler Gateway インストールの拡張について詳しくは、「 Citrix itrix製品との統合 」を参照してください。

DMZにNetScaler Gateway を展開する

多くの組織は DMZ で内部ネットワークを保護しています。DMZ は、組織のセキュアな内部ネットワークとインターネット (または任意の外部ネットワーク) の間にあるサブネットです。DMZにNetScaler Gateway を展開すると、ユーザーはNetScaler GatewayプラグインまたはCitrix Workspaceアプリで接続します。

図1：DMZに展開されたNetScaler Gateway



前の図に示す構成では、DMZにNetScaler Gateway をインストールし、インターネットと内部ネットワークの両方に接続するように構成します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DMZでのNetScaler Gateway接続

DMZにNetScaler Gateway を展開する場合、ユーザー接続は最初のファイアウォールを通過してNetScaler Gateway に接続する必要があります。デフォルトでは、ユーザー接続はポート 443 でSSL を使用してこの接続を確立します。ユーザ接続が内部ネットワークに到達できるようにするには、最初のファイアウォールを介してポート 443 で SSL を許可する必要があります。

NetScaler Gateway は、ユーザーデバイスからのSSL接続を復号化し、ユーザーに代わって2番目のファイアウォールの背後にあるネットワークリソースへの接続を確立します。2 番目のファイアウォールを介して開く必要があるポートは、外部ユーザーにアクセスを許可するネットワークリソースによって異なります。

たとえば、外部ユーザに内部ネットワーク内の Web サーバへのアクセスを許可し、このサーバがポート 80 で HTTP 接続をリッスンする場合、ポート 80 で HTTP を 2 番目のファイアウォール経由で許可する必要があります。NetScaler Gateway は、外部ユーザーデバイスに代わって、第2のファイアウォールを介して、内部ネットワーク上のHTTPサーバーへの接続を確立します。

NetScaler Gateway を安全なネットワークに展開する

NetScaler Gateway はセキュリティで保護されたネットワークにインストールできます。このシナリオでは、1 つのファイアウォールがインターネットとセキュリティで保護されたネットワークの間に立っています。NetScaler Gateway は、ネットワークリソースへのアクセスを制御するために、ファイアウォールの内部に常駐します。

図1：セキュリティで保護されたネットワークに展開されたNetScaler Gateway

NetScaler Gateway をセキュリティで保護されたネットワークに展開するときは、NetScaler Gateway の1つのインターフェイスをインターネットに接続し、もう1つのインターフェイスをセキュリティで保護されたネットワークで実行されているサーバーに接続します。NetScaler Gateway をセキュリティで保護されたネットワークに配置すると、ローカルユーザーおよびリモートユーザーにアクセスできます。この構成にはファイアウォールが 1 つしかないため、リモートロケーションから接続するユーザーの展開の安全性が低下します。NetScaler Gateway はインターネットからのトラフィックを傍受しますが、トラフィックはユーザーが認証される前に安全なネットワークに入ります。NetScaler Gateway をDMZに展開すると、ネットワークトラフィックがセキュリティで保護されたネットワークに到達する前にユーザーが認証されます。

NetScaler Gateway がセキュリティで保護されたネットワークに展開されている場合、NetScaler Gateway プラグイン接続はファイアウォールを通過してNetScaler Gateway に接続する必要があります。デフォルトでは、ユーザー接続はポート 443 で SSL プロトコルを使用してこの接続を確

© 1997–2026 Citrix Systems, Inc. All rights reserved.

立します。この接続をサポートするには、ファイアウォールでポート 443 を開く必要があります。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

クライアントソフトウェア要件

NetScaler Gateway は、NetScaler Gateway プラグインを使用したユーザー接続をサポートしています。ユーザがプラグインを使用してログオンすると、完全な VPN トンネルが確立されます。NetScaler Gateway プラグインを使用すると、ユーザーはアクセスを許可するネットワークリソースに接続できます。

NetScaler Gateway でエンドポイントポリシーが構成されている場合、NetScaler Gateway は、ユーザーがログオンしたときにCitrix EPAクライアントをユーザーデバイスに自動的にダウンロードしてインストールします。

NetScaler Gateway プラグインのシステム要件

NetScaler Gateway プラグインは、クライアントマシンからNetScaler Gateway アプライアンスへの安全な接続を確立します。

このプラグインは、Microsoft Windows、macOS X、Linuxオペレーティングシステム用のデスクトップアプリとして配布されている。WebブラウザーでNetScaler Gateway アプライアンスのセキュアURLを認証すると、プラグインがマシンに自動的にダウンロードされ、インストールされます。

プラグインは、Android および iOS デバイス用のモバイルアプリとしてプロビジョニングされます。

注：

- プラグインをインストールするには、オペレーティングシステムの admin/root 権限が必要です。
- NetScaler Gateway プラグインをサポートするブラウザーは、クライアントレスVPNもサポートしています。

デスクトップアプリとしてのNetScaler Gateway プラグインは、次のオペレーティングシステムおよびWebブラウザーでサポートされています。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

オペレーティングシステム	サポートされているブラウザー
macOS X (10.9 以降)	Safari 7.1 以降、Google Chrome リリース 30 以降、Mozilla Firefox リリース 30 以降
Windows 10 (x86とx64)	Internet Explorer 11、Google Chrome リリース 30 以降、Mozilla Firefox リリース 24 以降、Edge Chromium
Linux、Ubuntu 18.04 LTS 32 ビットおよび 64 ビット OS がサポートされています。	Mozilla Firefox リリース 44 以降。Google Chrome 50 以降

必要な依存関係パッケージが見つからない場合、コマンドはそれらを一覧表示し、プラグインのインストールは失敗します。これらの依存関係パッケージは手動でインストールする必要があります。管理者は、コマンドラインインターフェイスを使用して次のコマンドを入力して、不足しているパッケージをインストールできます。

```
apt-get install <dependency package>
```

モバイルアプリとしてのNetScaler Gateway プラグインは、次のオペレーティングシステムでサポートされています。

VPN アプリ	サポートされるオペレーティングシステム
Android	Android 7.0 以降
iOS	iOS 12.0 以降

注：

macOS 14/iOS 17以降などの最新のApple OSバージョンを使用している場合は、Citrix Secure Accessクライアント/Citrix SSOバージョン23.09.1以降にアップグレードすることをお勧めします。

エンドポイント分析の要件

NetScaler Gateway は、Citrix EPA クライアントをユーザーデバイスにインストールします。Citrix EPAクライアントは、NetScaler Gatewayで構成したエンドポイントセキュリティ要件について

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ユーザーデバイスをスキャンします。要件には、オペレーティングシステム、ウイルス対策、Web ブラウザのバージョンなどの情報が含まれます。

ユーザーがブラウザーを使用してNetScaler Gateway に初めて接続すると、ポータルはCitrix EPA クライアントのインストールを要求します。その後ログオンを試みると、Citrix EPAクライアントはアップグレード制御構成を検証して、Citrix EPAクライアントのアップグレードが必要かどうかを確認します。必要に応じて、最新のCitrix EPAクライアントをダウンロードしてインストールするように求めるプロンプトがユーザーに表示されます。Windows 用 Citrix EPA クライアントは Windows 32 ビットアプリケーションとしてインストールされます。macOS向けCitrix EPAクライアントは、64ビットアプリケーションとしてインストールされます。Citrix EPA クライアントのインストールまたは使用には、EPA を使用してデバイス証明書にアクセスする場合を除き、特別な権限は必要ありません。デバイス証明書認証に EPA を使用する方法の詳細については、「デバイス証明書を認証に使用する」を参照してください。

管理 UI コンソールのツールチップには、スキャンの詳細が説明されています。EPA ライブラリの詳細については、`<https://www.citrix.com/en-in/downloads/citrix-gateway/epa-libraries/>`を参照してください。

重要：

- EPA をサポートするブラウザは、クライアントレス VPN もサポートしています。
- 事前認証エンドポイント分析では、ユーザーがエンドポイント分析プラグインをインストールしない場合、またはスキャンをスキップした場合、ユーザーはNetScaler Gateway プラグインを使用してログオンできません。
- 認証後のエンドポイント分析では、ユーザーはクライアントレスアクセスまたはCitrix Workspace アプリを使用して、スキャンが不要なリソースにアクセスできます。
- OPSWAT 関連のスキャンでは、クライアントマシンにバイナリパッケージ`epaPackage.exe`をインストールする必要があります。

Endpoint Analysis プラグインを使用するには、ユーザーデバイスで次のソフトウェアが必要です。

オペレーティングシステム	サポートされているブラウザー
macOS (10.9 以降)	Safari 7.1 以降、Google Chrome リリース 30 以降、Mozilla Firefox リリース 30 以降

© 1997–2026 Citrix Systems, Inc. All rights reserved.

オペレーティングシステム	サポートされているブラウザー
Windows 10	Internet Explorer 11、Google Chrome リリース 30 以降、Mozilla Firefox リリース 24 以降、Edge Chromium
Linux; Ubuntu 18.04 LTS。32 ビットと 64 ビットの両方の OS がサポートされています。32 ビットと 64 ビットの両方の OS がサポートされています。	Mozilla Firefox リリース 44 以降。Google Chrome 50 以降

注：

- 前述のオペレーティングシステムバリアントのすべてのエディションがサポートされています。
- Windows 10 と Windows 11 の S モードはサポートされていません。
- Windows エディションの場合は、すべてのサービスパックと重要な更新プログラムをインストールする必要があります。
- Internet Explorer のバージョンでは、クッキーを有効にする必要があります。最低限必要なバージョンは 7.0 です。
- Mozilla Firefox のバージョンでは、エンドポイント分析はプラグインを有効にする必要があります。最低限必要なバージョンは 3.0 です。
- 現在、Citrix Secure Access クライアントと Ubuntu 用 Citrix EPA クライアントは、デフォルトの GNOME ディスプレイマネージャーのみをサポートしています。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler Gateway とCitrix 製品の互換性

次の表に、NetScaler Gateway 13.0と互換性があるCitrix製品とバージョンを示します。

注：

NetScaler Gateway の機能は、NetScaler ADC VPXで利用できます。

Citrix 製品とサポート対象バージョン

CITRIX製品	リリースバージョン
Citrix SD-WAN	10.2, 11.0
NetScaler ADC プラットフォーム	FIPS 準拠のアプライアンスを含む、現行のすべての MPX および VPX モデル。
StoreFront	現在サポートされているすべてのStoreFront バージョン。
Citrix Virtual Apps and Desktops	7.15、1808、1811、1903、1906、1909、2003、2009、2112、1912 LTSR、2203 LTSR
XenMobile	10.5, 10.6, 10.7, 10.8, 10.9, 10.10, 10.11, 10.12

Citrix Workspace アプリ、Citrix業務用モバイル アプリ、プラグイン

*各ソフトウェアリリースで最初にサポートされているビルドを次の表に示します。特に指定がない限り、以降のビルドはすべてサポートされます。リリースライフサイクルの詳細については、「製品マトリックス」を参照し てください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CITRIX WORKSPACE アプリまたはプラグイン	最低サポートバージョン*
macOS X向けNetScaler Gatewayプラグイン	3.1.8
Windows向けNetScaler Gatewayプラグイン	12.0
iOS向けNetScaler Gatewayプラグイン	3.1.4
Android向けNetScaler Gatewayプラグイン	2.0.14
Android向けCitrix Workspaceアプリ	3.11
iOS向けCitrix Workspaceアプリ	7.1.3
Mac向けCitrix Workspaceアプリ	12.4
Windows向けCitrix Workspaceアプリ	4.4
Linux向けCitrix Workspaceアプリ	13.4
HTML5向けCitrix Workspaceアプリ	2.3
Chrome向けCitrix Workspaceアプリ	2.3
Secure Hub for iOS	10.5
Secure Hub for Android	10.5
Secure Mail for iOS	10.5
SecureWeb for iOS	10.5
Secure Mail for Android	10.5
SecureWeb for Android	10.5

注：

- 各VPNクライアントでサポートされている一般的に使用される機能について詳しくは、「NetScaler Gateway VPNクライアントとサポートされる機能」を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler Gatewayライセンス

NetScaler Gateway をインストールすると、プラットフォームまたはユニバーサルライセンスファイルをCitrixから取得できます。Citrix Webサイトにログオンして、使用可能なライセンスにアクセスし、ライセンスファイルを生成します。ライセンスファイルが生成されたら、コンピュータにダウンロードします。ライセンスファイルがコンピューター上にある場合は、NetScaler Gatewayにアップロードします。Citrixライセンスについて詳しくは、「Citrixライセンスシステム」を参照してください。

ライセンスファイルを取得する前に、セットアップウィザードを使用してアプライアンスのホスト名を設定してから、アプライアンスを再起動してください。

ライセンスを取得するには、 Citrix ライセンスのアクティブ化、アップグレード、管理 ］Web ページに移動します。このページでは、新しいライセンスを取得し、Citrix ライセンスをアクティブ化、アップグレード、および管理できます。

重要：

- NetScaler Gateway にライセンスをインストールする必要があります。アプライアンスは、Citrix ライセンスサーバーからライセンスを取得しません。
- 受け取ったすべてのライセンスファイルのローカルコピーを保持することをお勧めします。構成ファイルのバックアップコピーを保存すると、アップロードしたすべてのライセンスファイルもバックアップに含まれます。NetScaler Gateway アプライアンスソフトウェアを再インストールする必要があり、構成のバックアップがない場合は、元のライセンスファイルが必要です。

NetScaler Gateway にライセンスをインストールする前に、アプライアンスのホスト名を設定してから、NetScaler Gateway を再起動します。セットアップウィザードを使用して、ホスト名を設定します。NetScaler Gateway のユニバーサルライセンスを生成すると、ホスト名がライセンスで使用されます。

NetScaler Gateway ライセンスの種類

NetScaler Gateway にはプラットフォームライセンスが必要です。プラットフォームライセンスでは、ICAプロキシを使用したCitrix Virtual Apps、Citrix Virtual Desktops、またはStoreFront への接続を無制限に許可します。NetScaler Gateway プラグイン、SmartAccessログオンポイント、またはSecure Hub、WorxWeb、またはSecure Mailからネットワークへの VPN接続を許可するには、

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ユニバーサルライセンスも追加する必要があります。NetScaler Gateway VPXには、プラットフォームライセンスが付属しています。

プラットフォームライセンスは、次のNetScaler Gateway バージョンでサポートされています。

- Citrix Gateway 12.1
- NetScaler Gateway 12.0
- NetScaler Gateway 11.1
- NetScaler Gateway 11.0
- NetScaler Gateway 10.5
- NetScaler Gateway 10.1
- Access Gateway 10
- NetScaler ADC VPX

重要：

受信するすべてのライセンスファイルのローカルコピーを保持することをお勧めします。構成ファイルのバックアップコピーを保存すると、アップロードされたすべてのライセンスファイルがバックアップに含まれます。NetScaler Gateway アプライアンスソフトウェアを再インストールする必要があり、構成のバックアップがない場合は、元のライセンスファイルが必要です。

プラットフォームライセンス

プラットフォームライセンスでは、Citrix Virtual Apps上の公開アプリケーションまたはCitrix Virtual DesktopsからのCitrix Virtual Desktops への無制限のユーザー接続を許可します。Citrix Receiverを使用した接続では、NetScaler Gateway ユニバーサルライセンスは使用されません。これらの接続には、Platform ライセンスのみが必要です。プラットフォームライセンスは、物理または仮想を問わず、すべての新しいNetScaler Gateway 注文とともに電子的に提供されます。保証または保守契約の対象となるアプライアンスをすでに所有している場合は、 Citrix Webサイトからプラットフォームライセンスを取得できます。

ユニバーサル・ライセンス

NetScaler Gateway ユニバーサルライセンスは、同時ユーザーセッションの数を購入したライセンスの数に制限します。100個のライセンスを購入した場合、いつでも100の同時セッションを使用できます。Standard エディションのライセンスを購入すると、いつでも 500 の同時セッションを持つことができます。ユーザーがセッションを終了すると、そのライセンスは次のユーザーに対して解放されます。複数のコンピューターからNetScaler Gateway にログオンするユーザーは、セッションごとにライセンスを占有します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

すべてのライセンスが使用されている場合、ユーザーがセッションを終了するか、管理者が構成ユーティリティを使用してセッションを終了するまで、追加の接続を開くすることはできません。接続が閉じられるとライセンスが解放され、新しいユーザーが使用できます。

NetScaler Gateway アプライアンスを受け取ると、ライセンスは次の順序で行われます。

- ライセンスアクセスコード (ライセンスキー) が電子メールで届きます。
- セットアップウィザードを使用して、ホスト名でNetScaler Gateway を構成します。
- NetScaler Gateway のライセンスは、Citrix のWebサイトから割り当てます。割り当てプロセス中にホスト名を使用して、ライセンスをアプライアンスにバインドします。
- ライセンスファイルはNetScaler Gateway にインストールします。

ユニバーサルライセンスは、次の機能をサポートしています。

- 完全な VPN トンネル
- マイクロVPN
- エンドポイント分析
- ポリシーベースのSmartAccess
- Web サイトおよびファイル共有へのクライアントレスアクセス

ユニバーサルライセンスの取得

ユニバーサルライセンスのCitrix Webサイトにアクセスする前に、次の情報が必要です。

Citrixアカウントのユーザー IDとパスワード。

> Citrix Webサイト（`<https://www.citrix.com/welcome/create-account/>`）で登録して、ユーザーIDとパスワードを受け取ります。
>
> 注：ライセンスコードまたはユーザーIDとパスワードが見つからない場合は、Citrixカスタマーサービスに連絡してください。

> NetScaler Gateway のホスト名
>
> Citrix Webサイトのこの名前の入力フィールドでは大文字と小文字が区別されるため、NetScaler ADCアプライアンスで構成されているとおりにホスト名をコピーしてください。

-

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ライセンスファイルに含めるライセンスの数

> 使用できるライセンスのすべてを一度にダウンロードする必要はありません。たとえば、100ライセンスを購入した場合は、50ライセンスをダウンロードできます。残りは後で別のライセンスファイルに割り当てることができます。
>
> NetScaler Gateway には複数のライセンスファイルをインストールできます。
>
> **注：** ライセンスを取得する前に、セットアップウィザードを使用してNetScaler ADCアプライアンスのホスト名を構成し、アプライアンスを再起動してください。

ユニバーサルライセンスを取得するには

1. Citrix の資格情報を使用してCitrix Webサイト（`<https://www.citrix.com/en-in/account/>`）にログインします。
2. 「**Citrix Manage Licenses はここにあります**」で、指示に従ってライセンスファイルを取得します。

ユニバーサルライセンスのインストール

ライセンスをインストールするには、「ライセンスのインストール」を参照してください。インストール後、ライセンスが正しくインストールされていることを確認します。

ユニバーサルライセンスのインストールの確認

続行する前に、ユニバーサルライセンスが正しくインストールされていることを確認します。

CLI を使用してユニバーサルライセンスのインストールを確認するには

1. PuTTYなどのSSHクライアントを使用して、NetScaler ADCアプライアンスへのSSH接続を開きます。
2. 管理者の資格情報を使用してNetScaler ADCアプライアンスにログオンします。
3. show license コマンドを使用して、「SSL VPN = YES」と最大ユーザ数が 5 から予想される同時ユーザ数に増加していることを確認します。

GUI を使用してユニバーサルライセンスのインストールを確認するには

1. Webブラウザーで、NetScaler ADCアプライアンスのIPアドレス（`http://192.168.100.1` など）を入力します。
2. ［User Name］ ボックスと ［Password］ ボックスに管理者資格情報を入力します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. ナビゲーションペインで、［System］ を展開し、［ Licenses］ をクリックします。
4. ［ライセンス］ペインで、 **Citrix Gateway**の横に緑色のチェックマークが表示されます。［許可されるNetScaler Gateway ユーザーの最大数］フィールドには、NetScaler ADCアプライアンスでライセンスされている同時ユーザーセッションの数が表示されます。

関連情報

- Citrix ライセンスシステム
- NetScaler ADC データシート
- NetScaler ADCおよびNetScaler Gatewayライセンスの種類

NetScaler Gateway にライセンスをインストールする

ライセンスファイルをコンピューターに正常にダウンロードしたら、NetScaler Gateway にライセンスをインストールできます。ライセンスは /nsconfig/license ディレクトリにインストールされます。

セットアップウィザードを使用してNetScaler Gateway の初期設定を構成した場合は、ウィザードの実行時にライセンスファイルがインストールされます。ライセンスの一部を割り当てた後、追加の番号を割り当てる場合は、セットアップウィザードを使用せずにライセンスをインストールできます。

1. 構成ユーティリティの タブのナビゲーションペインで、 を展開し、 をクリックします。
2. 詳細ペインで、 **［Manage Licenses］** をクリックします。
3. ［ **新しいライセンスの追加**］をクリックし、［ **参照**］をクリックしてライセンスファイルに移動し、［ **OK］**をクリックします。

   構成ユーティリティに、NetScaler Gateway を再起動する必要があることを示すメッセージが表示されます。再起動をクリックします。

最大ユーザー数を設定する

アプライアンスにライセンスをインストールしたら、アプライアンスへの接続を許可するユーザーの最大数を設定する必要があります。グローバル認証ポリシーで最大ユーザー数を設定します。

1. 構成ユーティリティの［構成］タブのナビゲーションペインで、［ **Citrix Gateway** ］を展開し、［ **グローバル設定**］をクリックします。
2. 詳細ペインの で、 をクリックします。
3. 「最大ユーザー数」に、ユーザーの合計数を入力し、 **「OK」**をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

このフィールドの数は、ライセンスファイルに含まれているライセンスの数に対応しています。この数は、アプライアンスにインストールされているライセンスの総数以下である必要があります。たとえば、100ユーザーライセンスを含むライセンスと400ユーザーライセンスを含むもう一つのライセンスをインストールするとします。ライセンスの総数は500になります。その場合、ログオンできるユーザーの最大数は500人以下です。500 人のユーザーがログオンしている場合、その数を超えてログオンしようとすると、ユーザーがログオフするかセッションを終了するまで、アクセスが拒否されます。

ユニバーサルライセンスのインストールを確認する

先に進む前に、ユニバーサルライセンスが正しくインストールされていることを確認してください。

GUI を使用してユニバーサルライセンスのインストールを確認するには

1. 構成ユーティリティの タブのナビゲーションペインで、 を展開し、 をクリックします。

   ライセンスペインで 、NetScaler Gateway の横に緑色のチェックマークが表示されます。［許可されるNetScaler Gateway ユーザーの最大数］フィールドには、アプライアンスでライセンスされている同時ユーザーセッションの数が表示されます。

CLI を使用してユニバーサルライセンスのインストールを確認するには

1. PuTTY などの SSH クライアントを使用して、アプライアンスへのセキュアシェル（SSH）接続を開きます。
2. 管理者の資格情報を使用してアプライアンスにログオンします。
3. コマンドプロンプトで、; と入力します。

```
show license
```

SSL VPN パラメータが Yes に等しく、最大ユーザパラメータがライセンス数に等しい場合、ライセンスは正しくインストールされます。

NetScaler Gateway ライセンスに関するよくある質問

トライアルライセンスまたはデモライセンスのサポートを受けるにはどうすればよいですか

Citrix 製品の多くは、包括的でプライベートな 1:1 のエキスパート主導のデモ体験として提供されています。Citrix エキスパートが、お客様のニーズ、ユースケース、アクティブなプロジェクトに

© 1997–2026 Citrix Systems, Inc. All rights reserved.

合わせてデモをカスタマイズします。ダウンロード、ライセンス、インストールは不要です。インスタントデモを見るには最小限の設定が必要です。デモの後、サービスに適用されるCitrix ソリューションの概念実証または試用を進めるには、Citrix 専門家にお問い合わせください。デモの場合は、`<https://demo.citrix.com/>`をクリックします。

ライセンスをインストールするには

ライセンスのインストールについて詳しくは、「NetScaler Gateway にライセンスをインストールするには」を参照してください。

Gateway ライセンスにはどのような種類がありますか

プラットフォームライセンスでは、ICAプロキシを使用したCitrix Virtual Apps、Citrix Virtual Desktops、またはStoreFront への接続を無制限に許可します。 ユニバーサルライセンスは、NetScaler ADCプラットフォームライセンスの上にあるアドオンライセンスです。これにより、NetScaler Gateway プラグイン、SmartAccessログオンポイント、またはSecure Hub、Secure Web、またはSecure Mailからネットワークへの VPN接続が可能になります。詳しくは、「NetScaler Gateway ライセンスの種類」を参照してください。

サポートされる同時ユーザーセッションはいくつありますか

サポートされるセッションは、ゲートウェイライセンスタイプによって異なります。詳しくは、「NetScaler Gateway ライセンスの種類」を参照してください。

考慮すべきもう1つの要素は、基盤となるハードウェア自体の容量です。パフォーマンスに関する考慮事項については、 NetScaler ADC MPX/SDXデータシートまたはCitrixADC VPXデータシートを参照してください 。

現在の同時ユーザーセッションのライセンスを確認するにはどうすればよいですか?

構成ユーティリティの タブで、 を展開し、 をクリックします。 **ライセンス**ペインで 、NetScaler Gateway の横に緑色のチェックマークが表示されます。［**許可されるCitrix Gateway の最大ユーザー数**］フィールドには、アプライアンスでライセンスされている同時ユーザーセッションの数が表示されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ライセンスされたスループット制限に達しているかどうかを確認する方法

リアルタイムスループットは、`newnslog`を使用して抽出できます。たとえば、ライセンススループットが 500 Mbps の場合、次のコマンドを使用して 500 を超えるリアルタイムスループットを抽出できます。

```
nsconmsg -K newnslog -g mbits -d past -s disptime=1 -s ratecount=500 |
more
```

ライセンススループットに達するとパケットがドロップされるかどうかを確認する方法

次のコマンドを使用して、パケットがドロップされているかどうかを確認できます。

```
nsconmsg -K newnslog -d current -g nic_err_rl_pkt_drops -s disptime=1 |
more
```

NetScaler ADCアプライアンスのライセンスされたスループットはどのようにして調べることができますか?

CLI から`show license`コマンドを実行し、モデル番号を使用して、ADC またはゲートウェイ MPX、SDX、および VPX のデータシートからスループットを取得します。

既存の Gateway ライセンスにユーザーを追加するにはどうすればよいですか?

追加のユニバーサルライセンスをインストールできます。たとえば、100 のユーザライセンスを含む 1 つのユニバーサルライセンスをインストールしたとします。400 のユーザライセンスを含む 2 つ目のユニバーサルライセンスをインストールすると、ユーザライセンスの総数は 500 になります。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

開始する前に

NetScaler Gateway をインストールする前に、インフラストラクチャを評価し、情報を収集して、組織の特定のニーズを満たすアクセス戦略を計画する必要があります。アクセス戦略を定義するときは、セキュリティの影響を考慮し、リスク分析を完了する必要があります。また、ユーザーが接続できるネットワークを決定し、ユーザー接続を有効にするポリシーを決定する必要があります。

ユーザーが使用できるリソースの計画に加えて、展開シナリオも計画する必要があります。NetScaler Gateway は以下のCitrix 製品に対応しています。

- Citrix Endpoint Management
- Citrix Virtual Apps
- Citrix Virtual Desktops
- StoreFront
- Web Interface
- Citrix SD-WAN

NetScaler Gateway の展開について詳しくは、「 一般的な展開」および「 Citrix 製品との統合」を参照してください

アクセス戦略を準備するには、次の予備的な手順を実行します。

- リソースを特定する。リスク分析で定義したWeb、SaaS、モバイルまたは公開アプリケーション、仮想デスクトップ、サービス、データなど、アクセスを提供するネットワークリソースを一覧表示します。
- アクセスシナリオを開発する。ユーザーがネットワークリソースにアクセスする方法を説明するアクセスシナリオを作成します。アクセスシナリオは、ネットワークへのアクセスに使用される仮想サーバー、エンドポイント分析スキャン結果、認証タイプ、またはその組み合わせによって定義されます。また、ユーザがネットワークにログオンする方法を定義することもできます。
- クライアントソフトウェアを識別します。NetScaler Gateway プラグインを使用して完全なVPNアクセスを提供し、ユーザーにCitrix Workspaceアプリ、Secure Hub、またはクライアントレスアクセスによるログオンを要求できます。また、Outlook Web App または WorxMail への電子メールアクセスを制限することもできます。これらのアクセスシナリオは、ユーザーが

© 1997–2026 Citrix Systems, Inc. All rights reserved.

アクセス権を取得したときに実行できるアクションも決定します。たとえば、ユーザーが公開アプリケーションを使用してドキュメントを変更できるか、ファイル共有に接続してドキュメントを変更できるかを指定できます。

- ポリシーをユーザー、グループ、または仮想サーバーに関連付けます。NetScaler Gateway で作成するポリシーは、個人またはユーザーのセットが指定された条件を満たすときに適用されます。条件は、作成したアクセスシナリオに基づいて決定します。次に、ユーザーがアクセスできるリソースと、それらのリソースに対してユーザーが実行できるアクションを制御することにより、ネットワークのセキュリティを拡張するポリシーを作成します。ポリシーは、適切なユーザー、グループ、仮想サーバー、またはグローバルに関連付けます。

このセクションでは、アクセス戦略の計画に役立つ次のトピックについて説明します。

- セキュリティの計画には、認証と証明書に関する情報が含まれています。
- 必要になる可能性があるネットワークハードウェアとソフトウェアを定義する前提条件。
- NetScaler Gateway を構成する前に設定を書き留めるために使用できるインストール前チェックリスト。

NetScaler Gateway をインストールするための前提条件

NetScaler Gateway の設定を構成する前に、次の前提条件を確認してください：

- NetScaler Gateway はネットワークに物理的にインストールされ、ネットワークにアクセスできます。NetScaler Gateway は、DMZまたはファイアウォールの背後にある内部ネットワークに展開されています。また、ダブルホップDMZでNetScaler Gateway を構成し、サーバーファームへの接続を構成することもできます。DMZにアプライアンスを展開することをお勧めします。
- NetScaler Gateway をデフォルトゲートウェイまたは内部ネットワークへの静的ルートで構成し、ユーザーがネットワーク内のリソースにアクセスできるようにします。NetScaler Gateway は、デフォルトで静的ルートを使用するように構成されています。
- 認証と認可に使用される外部サーバは設定され、実行されています。詳細については、「認証と承認」を参照してください。
- ネットワークには、正しいNetScaler Gateway ユーザー機能を提供するための名前解決用のドメインネームサーバー（DNS）またはWindowsインターネットネームサービス（WINS）サーバーがあります。
- NetScaler Gateway プラグインを使用したユーザー接続用のユニバーサルライセンスをCitrix Webサイトからダウンロードし、ライセンスをNetScaler Gateway にインストールする準備ができました。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- NetScaler Gateway には、信頼できる認証局（CA）によって署名された証明書があります。詳しくは、「Installing and Managing Certificates」を参照してください。

NetScaler Gateway をインストールする前に、インストール前チェックリストを使用して設定を書き留めます。

セキュリティの計画

NetScaler Gateway の展開を計画するときは、証明書、および認証と承認に関連する基本的なセキュリティ問題を理解する必要があります。

セキュアな証明書管理を構成する

デフォルトでは、NetScaler Gateway には、アプライアンスがSSLハンドシェイクを完了できるようにする自己署名Secure Sockets Layer（SSL）サーバー証明書が含まれています。自己署名証明書は、テストやサンプル展開には十分ですが、本番環境での使用はお勧めしません。NetScaler Gateway を実稼働環境に展開する前に、既知の認証局（CA）から署名付きSSLサーバー証明書を要求して受信し、NetScaler Gateway にアップロードすることをお勧めします。

NetScaler Gateway がSSLハンドシェイクでクライアントとして動作する必要がある環境（別のサーバーとの暗号化された接続を開始する）にNetScaler Gateway を展開する場合は、NetScaler Gateway にも信頼されたルート証明書をインストールする必要があります。たとえば、Citrix Virtual AppsとWeb Interfaceを備えたNetScaler Gateway を展開する場合、NetScaler Gateway からWeb Interfaceへの接続をSSLで暗号化できます。この構成では、NetScaler Gateway に信頼されたルート証明書をインストールする必要があります。

認証サポート

ユーザーを認証し、内部ネットワーク上のネットワークリソースに対するユーザーのアクセス（または承認）のレベルを制御するようにNetScaler Gateway を構成できます。

NetScaler Gateway を展開する前に、ネットワーク環境に次の認証タイプのいずれかをサポートするためのディレクトリと認証サーバーが配置されている必要があります。

- LDAP
- RADIUS
- TACACS+
- 監査およびスマートカードをサポートするクライアント証明書
- RADIUS構成のRSA
- SAML認証

© 1997–2026 Citrix Systems, Inc. All rights reserved.

環境がこれらの認証タイプをサポートしていない場合、またはリモートユーザーの人口が少ない場合は、NetScaler Gateway でローカルユーザーのリストを作成できます。次に、このローカルリストに対してユーザーを認証するようにNetScaler Gateway を構成できます。この構成では、ユーザーアカウントを別の外部ディレクトリに保持する必要はありません。

NetScaler Gateway 展開環境のセキュリティ保護

展開が異なれば、セキュリティに関する考慮事項も異なる場合があります。NetScaler ADCの安全な導入ガイドラインは、特定のセキュリティ要件に基づいて適切な安全な導入を決定するのに役立つ一般的なセキュリティガイダンスを提供します。

詳しくは、「NetScaler ADC 安全な展開ガイドライン」を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Gatewayインストール前のチェックリスト

チェックリストは、NetScaler Gateway をインストールする前に完了する必要があるタスクと計画情報のリストで構成されています。

各タスクを完了してメモを作成すると、各タスクをチェックオフできるスペースが用意されています。インストールプロセス中およびNetScaler Gateway の構成中に入力する必要がある構成値をメモしておくことをお勧めします。

NetScaler Gateway をインストールおよび構成する手順については、「NetScaler Gateway のインストール」を参照してください。

ユーザーデバイス

- ユーザーデバイスが、 NetScaler Gateway プラグインのシステム要件に記載されているインストールの前提条件を満たしていることを確認します
- ユーザーが接続するモバイルデバイスを特定します。**注**：ユーザーがiOSデバイスに接続する場合は、セッションプロファイルでSecure Browse を有効にする必要があります。

NetScaler Gateway の基本的なネットワーク接続

アプライアンスの構成を開始する前に、ライセンスと署名付きサーバー証明書を取得することをお勧めします。

- NetScaler Gateway ホスト名を特定して書き留めます。**注**:これは完全修飾ドメイン名 (FQDN) ではありません。FQDN は、仮想サーバーにバインドされた署名付きサーバー証明書に含まれています。
- Citrix Webサイトからユニバーサルライセンスを取得する
- 証明書署名要求 (CSR) を生成し、認証局 (CA) に送信します。CSR を認証局に送信する日付を入力します。
- システム IP アドレスとサブネットマスクを書き留めます。
- サブネット IP アドレスとサブネットマスクを書き留めます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 管理者パスワードを書き留めます。NetScaler Gateway に付属するデフォルトのパスワードは `nsroot` です。
- NetScaler Gateway がセキュリティで保護されたユーザー接続をリッスンするポート番号を書き留めます。デフォルトは TCP ポート 443 です。このポートは、セキュリティで保護されていないネットワーク (インターネット) と DMZ の間のファイアウォールで開いている必要があります。
- デフォルトゲートウェイの IP アドレスを書き留めます。
- DNS サーバの IP アドレスとポート番号を書き留めます。デフォルトのポート番号は 53 です。さらに、DNS サーバを直接追加する場合は、アプライアンスで ICMP（ping）も設定する必要があります。
- 最初の仮想サーバの IP アドレスとホスト名を書き留めます。
- 2 番目の仮想サーバの IP アドレスとホスト名（該当する場合）を書き留めます。
- WINS サーバの IP アドレスを書き留めます（該当する場合）。

NetScaler Gateway を介してアクセス可能な内部ネットワーク

- ユーザーがNetScaler Gateway を介してアクセスできる内部ネットワークを書き留めます。例：10.10.0.0/24
- ユーザーがNetScaler Gateway プラグインを使用してNetScaler Gateway 経由で接続するときにアクセスする必要があるすべての内部ネットワークおよびネットワークセグメントを入力します。

高可用性

2つのNetScaler Gateway アプライアンスがある場合は、1つのNetScaler Gateway が接続を受け入れて管理し、2番目のNetScaler Gateway が最初のアプライアンスを監視する高可用性構成でそれらを展開できます。最初のNetScaler Gateway が何らかの理由で接続の受け入れを停止した場合、2番目のNetScaler Gateway が引き継ぎ、アクティブな接続の受け入れを開始します。

- NetScaler Gateway ソフトウェアのバージョン番号を書き留めます。
- バージョン番号は、両方のNetScaler Gateway アプライアンスで同じである必要があります。
- 管理者パスワードを書き留めます (`nsroot`)。パスワードは両方のアプライアンスで同じである必要があります。
- プライマリNetScaler Gateway IPアドレスとIDを書き留めます。最大 ID 番号は 64 です。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- セカンダリNetScaler Gateway IPアドレスとIDを書き留めます。
- ユニバーサルライセンスを取得し、両方のアプライアンスにインストールします。
- 両方のアプライアンスに同じユニバーサルライセンスをインストールします。
- RPC ノードのパスワードを書き留めます。

認証と承認

NetScaler Gateway は、さまざまな組み合わせで使用できるいくつかの異なる認証および承認タイプをサポートしています。認証と認可の詳細については、「 認証と承認」を参照してください。

LDAP認証

環境に LDAP サーバが含まれている場合は、認証に LDAP を使用できます。

- LDAP サーバの IP アドレスとポートを書き留めます。

  LDAP サーバへのセキュアでない接続を許可する場合、デフォルトのポートは 389 です。LDAP サーバーへの接続を SSL で暗号化する場合、デフォルトのポートは 636 です。
- セキュリティの種類を書き留めます。

  セキュリティは、暗号化の有無にかかわらず構成できます。
- 管理者バインド DN を書き留めます。

  LDAPサーバーで認証が必要な場合は、NetScaler Gateway がLDAPディレクトリにクエリを実行するときに認証に使用する必要がある管理者DNを入力します。例として、cn=管理者、cn=Users、dc=ace、dc=comがある。
- 管理者パスワードを書き留めます。

  パスワードは、管理者バインド DN に関連付けられています。
- ベース DN を書き留めます。

  ユーザが配置されている DN（またはディレクトリレベル）。たとえば、ou=users、dc=ace、dc=com などです。
- サーバのログオン名属性を書き留めます。

  ユーザーのログオン名を指定する LDAP ディレクトリのユーザーオブジェクト属性を入力します。デフォルトはsAMAccountNameです。Active Directory を使用していない場合、この設定

© 1997–2026 Citrix Systems, Inc. All rights reserved.

の一般的な値は cn または uid です。 LDAP ディレクトリ設定の詳細については、 LDAP 認証の設定を参照してください。

- グループ属性を書き留めます。 ユーザが属するグループを指定する LDAP ディレクトリの Person オブジェクト属性を入力します。デフォルトは memberOf です。この属性により、NetScaler Gateway はユーザーが属するディレクトリグループを識別できます。
- サブ属性名を書き留めます。

RADIUS 認証および認可

環境に RADIUS サーバが含まれている場合は、認証に RADIUS を使用できます。 RADIUS認証には、RSA SecurID、SafeWord、Gemalto Protiva製品が含まれる。

- プライマリ RADIUS サーバの IP アドレスとポートを書き留めます。デフォルトのポートは 1812 です。
- プライマリ RADIUS サーバシークレット（共有シークレット）を書き留めます。
- セカンダリ RADIUS サーバの IP アドレスとポートを書き留めます。デフォルトのポートは 1812 です。
- セカンダリ RADIUS サーバシークレット（共有シークレット）を書き留めます。
- パスワードエンコーディングのタイプ（PAP、CHAP、MS-CHAP v1、MSCHAP v2）を書き留めます。

SAML認証

セキュリティアサーションマークアップ言語 (SAML) は、ID プロバイダ (IdP) とサービスプロバイダの間で認証と承認を交換するための XML ベースの標準です。

- NetScaler Gateway にセキュアなIdP証明書を取得してインストールします。
- リダイレクト URL を書き留めます。
- ユーザーフィールドを書き留めます。
- 署名証明書の名前を書き留めます。
- SAML 発行者名を書き留めます。
- デフォルトの認証グループを書き留めます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ファイアウォールを介してポートを開く（シングルホップDMZ）

組織が単一のDMZで内部ネットワークを保護し、DMZにNetScaler Gateway を展開する場合は、ファイアウォールを介して次のポートを開きます。ダブルホップDMZ展開に2つのNetScaler Gateway アプライアンスをインストールする場合は、 ファイアウォールで適切なポートを開くを参照してください。

セキュリティで保護されていないネットワークと DMZ の間のファイアウォール上

- インターネットとNetScaler Gateway の間のファイアウォールでTCP/SSLポート（デフォルトは443）を開きます。ユーザーデバイスは、このポートでNetScaler Gateway に接続します。

セキュリティで保護されたネットワーク間のファイアウォール上

- DMZ とセキュリティで保護されたネットワーク間のファイアウォールで、1 つ以上の適切なポートを開きます。NetScaler Gateway は、1つ以上の認証サーバー、またはこれらのポート上のセキュリティで保護されたネットワーク内のCitrix Virtual Apps and Desktopsを実行しているコンピューターに接続します。
- 認証ポートを書き留めます。

  NetScaler Gateway 構成に適したポートのみを開きます。

  - LDAP 接続の場合、デフォルトは TCP ポート 389 です。
  - RADIUS 接続の場合、デフォルトは UDP ポート 1812 です。Citrix Virtual Apps and Desktops のポートを書き留めます。
- NetScaler GatewayをCitrix Virtual Apps and Desktopsで使用している場合は、TCPポート1494を開きます。セッション画面の保持を有効にする場合は、1494 ではなく TCP ポート 2598 を開きます。これらのポートは両方とも開いたままにしておくことをお勧めします。

Citrix Virtual Desktops、Citrix Virtual Apps、Web Interface、またはStoreFront

NetScaler Gateway を展開して、Web InterfaceまたはStoreFront を介してCitrix Virtual Apps and Desktops へのアクセスを提供する場合は、次のタスクを実行します。この展開では、NetScaler Gateway プラグインは必要ありません。ユーザーは、WebブラウザーとCitrix Receiverのみを使用して、NetScaler Gateway を介して公開アプリケーションおよびデスクトップにアクセスします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Web InterfaceまたはStoreFrontを実行しているサーバーのFQDNまたはIPアドレスを書き留めます。
- Secure Ticket Authority（STA）を実行しているサーバの FQDN または IP アドレスを書き留めます（Web インターフェイスの場合のみ）。

Citrix Endpoint Management

内部ネットワークにCitrix Endpoint Managementを展開する場合は、次のタスクを実行します。ユーザーがインターネットなどの外部ネットワークからEndpoint Managementに接続する場合、ユーザーはモバイル、Web、およびSaaSアプリにアクセスする前にNetScaler Gateway に接続する必要があります。

- Endpoint Management 完全修飾ドメイン名または IP アドレスを書き留めます。
- ユーザーがアクセスできるウェブ、SaaS、モバイル iOS または Android アプリケーションを特定します。

Citrix Virtual Apps を使用したダブルホップ DMZ 展開

Citrix Virtual Appsを実行しているサーバーへのアクセスをサポートするために、ダブルホップDMZ構成で2つのNetScaler Gateway アプライアンスを展開する場合は、次のタスクを実行します。

最初のDMZのNetScaler Gateway

最初の DMZ は、内部ネットワークの最も外側のエッジ（インターネットまたはセキュリティ保護されていないネットワークに最も近い）にある DMZ です。クライアントは、DMZからインターネットを分離するファイアウォールを介して最初のDMZのNetScaler Gateway に接続します。最初のDMZにNetScaler Gateway をインストールする前に、この情報を収集してください。

- このNetScaler Gateway のこのチェックリストの「NetScaler Gateway の基本ネットワーク接続」セクションの項目を完了します。

  これらの項目を完了すると、インターフェイス0はこのNetScaler Gatewayをインターネットに接続し、インターフェイス1はこのNetScaler Gatewayを2番目のDMZのNetScaler Gatewayに接続します。
- プライマリアプライアンスで 2 番目の DMZ アプライアンス情報を設定します。

  NetScaler Gateway をダブルホップDMZの最初のホップとして構成するには、最初のDMZのアプライアンスの2番目のDMZでNetScaler Gateway のホスト名またはIPアドレスを指定する必要があります。最初のホップでアプライアンスでNetScaler Gateway プロキシが構成されるタ

© 1997–2026 Citrix Systems, Inc. All rights reserved.

イミングを指定したら、NetScaler Gateway にグローバルにバインドするか、仮想サーバーにバインドします。

- アプライアンス間の接続プロトコルとポートを書き留めます。

  NetScaler Gateway をダブルDMZの最初のホップとして構成するには、2番目のDMZの NetScaler Gateway が接続をリッスンする接続プロトコルとポートを指定する必要があります。接続プロトコルとポートは SSL を使用した SOCKS（デフォルトポート 443）です。プロトコルとポートは、最初の DMZ と 2 番目の DMZ を分離するファイアウォールを介して開く必要があります。

2番目のDMZのNetScaler Gateway

2 番目の DMZ は、内部のセキュアネットワークに最も近い DMZ です。2番目のDMZに展開されたNetScaler Gateway は、ICAトラフィックのプロキシとして機能し、外部ユーザーデバイスと内部ネットワーク上のサーバー間で2番目のDMZを通過します。

- このNetScaler Gateway のこのチェックリストの「NetScaler Gateway 基本的なネットワーク接続」セクションのタスクを完了します。

  これらの項目を完了すると、インターフェイス0は、最初のDMZでこのNetScaler GatewayをNetScaler Gatewayに接続します。インターフェイス1は、このNetScaler Gateway をセキュリティで保護されたネットワークに接続します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler Gatewayアプライアンスのインストールと構成

NetScaler Gateway アプライアンスを受け取ったら、アプライアンスを開梱し、サイトとラックを準備します。アプライアンスを設置する場所が環境基準を満たし、指示に従ってサーバラックが配置されていることを確認したら、ハードウェアを取り付けます。アプライアンスをマウントしたら、アプライアンスをネットワーク、電源、および初期設定に使用するコンソール端末に接続します。アプライアンスの電源を入れた後、初期設定を行い、管理およびネットワーク IP アドレスを割り当てます。インストール手順に記載されている注意事項と警告を必ず守ってください。

NetScaler ADC VPX仮想アプライアンスをインストールするときは、まず仮想アプライアンスイメージを取得し、ハイパーバイザーまたは他の仮想マシンモニターにインストールする必要があります。

NetScaler Gateway アプライアンスを構成する前に、設定を記録できるように、NetScaler Gateway インストール前チェックリストのトピックを使用することをお勧めします 。チェックリストには、NetScaler Gateway とアプライアンスのインストールに関する情報が含まれています。

ウィザードを使用してNetScaler Gateway アプライアンスを構成する

NetScaler Gateway には、アプライアンスの設定を構成するために使用できる次の6つのウィザードがあります：

- NetScaler Gateway アプライアンスに初めてログオンすると、初回セットアップウィザードが表示されます。
- クイック構成ウィザードを使用すると、Citrix Endpoint Management、StoreFront、およびWeb Interfaceへの接続に関する正しいポリシー、式、および設定を構成できます。
- NetScaler Gateway ウィザードでは、NetScaler Gateway 固有の設定を構成できます。
- セットアップウィザードを使用すると、NetScaler Gateway の基本的な設定を初めて構成できます。
- Citrix Endpoint Managementの統合構成は、NetScaler Gateway およびCitrix Endpoint Management環境の構成に役立ちます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 公開アプリケーションウィザードでは、Citrix Workspace アプリを使用してユーザー接続の設定を構成できます。

初回セットアップウィザード

NetScaler Gateway アプライアンスの初期設定のインストールと構成を完了し、構成ユーティリティに初めてログオンするときに、次の条件が満たされない場合は、初回セットアップウィザードが表示されます：

- アプライアンスにライセンスをインストールしていない。
- サブネットまたはマッピング IP アドレスが設定されていません。
- アプライアンスのデフォルトの IP アドレスが 192.168.100.1 の場合。

初回セットアップウィザードでNetScaler Gateway を構成する

NetScaler Gateway（物理アプライアンスまたはVPX仮想アプライアンス）を初めて構成するには、アプライアンスと同じネットワーク上に構成された管理用コンピューターが必要です。

アプライアンスの管理IPアドレスとしてNetScaler Gateway IP（NSIP）アドレスと、サーバーが接続できるサブネットIP（SNIP）アドレスを割り当てます。NetScaler Gateway アドレスとSNIP アドレスの両方に適用されるサブネットマスクを割り当てます。タイムゾーンも設定します。ホスト名を割り当てる場合は、NSIP アドレスの代わりに名前を指定してアプライアンスにアクセスできます。

には 2 つのセクションがあります。最初のセクションでは、NetScaler Gateway アプライアンスの次の基本システム設定を構成します：

NSIP アドレス、SNIP アドレス、 サブネットマスクアプライアンスホスト名 DNS

サーバータイムゾーン管理者パスワード 2 番目のセクションでは、ライセンスをインストールします。DNS サーバのアドレスを指定すると、ローカルコンピュータからアプライアンスにライセンスをアップロードする代わりに、ハードウェアシリアル番号（HSN）またはライセンスキーを使用してライセンスを割り当てることができます。

注：ライセンスをローカルコンピューターに保存することをお勧めします。

これらの設定の構成が完了すると、NetScaler Gateway でアプライアンスを再起動するように求められます。アプライアンスに再度ログオンすると、他のウィザードおよび構成ユーティリティを使用して他の設定を構成できます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

クイック構成ウィザード

クイック構成ウィザードを使用すると、NetScaler Gateway で複数の仮想サーバーを構成できます。仮想サーバを追加、編集、および削除できます。

クイック構成ウィザードを使用すると、次の展開をシームレスに構成できます。

- Secure Ticket Authority（STA）の複数のインスタンスを構成できる、Citrix Virtual Apps and Desktops へのWeb Interface接続
- Citrix Endpoint Management のみ
- StoreFront のみ
- Citrix Endpoint Management とStoreFront を一緒に

クイック構成ウィザードでは、アプライアンスで次の設定を構成できます。

- 仮想サーバ名、IP アドレス、ポート
- 非セキュアポートからセキュアポートへのリダイレクト
- LDAP サーバ
- RADIUSサーバー
- 証明書
- DNS サーバー
- Citrix Endpoint Management およびCitrix Virtual Apps and Desktops

  注：SSOを有効にするには、セッションアクションの［**NetScaler Gateway セッションプロファイルの作成**］**>**［**クライアントエクスペリエンス**］タブの［**Webアプリケーションへのシングルサインオン**］オプションを手動で有効にする必要があります。

NetScaler Gateway は、Citrix Endpoint Managementへの直接ユーザー接続をサポートしています。これにより、ユーザーはShareFileへのアクセスとともに、Web、SaaS、およびモバイルアプリにアクセスできます。また、StoreFront の設定を構成して、ユーザーがWindowsベースのアプリケーションと仮想デスクトップにアクセスできるようにすることもできます。

クイック構成ウィザードを実行すると、Citrix Endpoint Management、StoreFront、およびWeb Interfaceの設定に基づいて、次のポリシーが作成されます。

- セッションポリシー（Receiver、Receiver for Web、NetScaler Gateway プラグイン、プログラムネイバーフッドエージェントのポリシーとプロファイルを含む）
- クライアントレスアクセス
- LDAPおよびRADIUS認証

© 1997–2026 Citrix Systems, Inc. All rights reserved.

クイック構成ウィザードで設定を構成する

NetScaler Gateway の設定を構成して、Citrix Endpoint Management、StoreFront、またはWeb Interfaceとの通信を有効にするには、クイック構成ウィザードを使用します。構成が完了すると、ウィザードにより、NetScaler Gateway、Endpoint Management、StoreFront、またはWeb Interface間の通信に関する正しいポリシーが作成されます。これらのポリシーには、認証、セッション、およびクライアントレスアクセスポリシーが含まれます。ウィザードが完了すると、ポリシーは仮想サーバにバインドされます。

クイック構成ウィザードを完了すると、NetScaler Gateway はEndpoint Managementまたは StoreFront と通信でき、ユーザーはWindowsベースのアプリケーション、仮想デスクトップ、Web、SaaS、モバイルアプリにアクセスできます。その後、ユーザーはEndpoint Managementに直接接続できます。

ウィザードでは、次の設定を構成します。

- 仮想サーバ名、IP アドレス、ポート
- 非セキュアポートからセキュアポートへのリダイレクト
- 証明書
- LDAP サーバ
- RADIUSサーバー
- 認証用のクライアント証明書 (2 要素認証のみ)
- Endpoint Management、StoreFront、またはWeb Interface

クイック構成ウィザードは、LDAP、RADIUS、およびクライアント証明書認証をサポートしています。ウィザードで 2 要素認証を構成するには、次のガイドラインに従います。

- プライマリ認証タイプとして LDAP を選択した場合、セカンダリ認証タイプとして RADIUS を設定できます。
- プライマリ認証タイプとして RADIUS を選択した場合、セカンダリ認証タイプとして LDAP を設定できます。
- プライマリ認証タイプとしてクライアント証明書を選択した場合、セカンダリ認証タイプとして LDAP または RADIUS を設定できます。

クイック構成ウィザードを使用して複数の LDAP 認証ポリシーを作成することはできません。 **たとえば、 フィールドで samAccountName を使用するポリシーを 1 つ構成し、 フィールドでユーザープリンシパル名 (UPN) を使用する 2 つ目の LDAP ポリシーを構成するとします。** これら

© 1997–2026 Citrix Systems, Inc. All rights reserved.

の個別のポリシーを構成するには、NetScaler Gateway 構成ユーティリティを使用して認証ポリシーを作成します。詳細については、 LDAP 認証の設定を参照してください。

次の方法を使用して、NetScaler Gateway の証明書をクイック構成ウィザードで構成できます。

- アプライアンスにインストールされている証明書を選択します。
- 証明書と秘密キーをインストールします。
- テスト証明書を選択します。 **注**:テスト証明書を使用する場合は、証明書に含まれる完全修飾ドメイン名 (FQDN) を追加する必要があります。

クイック構成ウィザードは 、次の 2 つの方法のいずれかで開くことができます。

- NetScaler Gateway のログオンページを表示し、［ **展開の種類** ］で［ **NetScaler Gateway**］を選択すると、［ **ホーム** ］タブが表示されます。 で他のオプションを選択した場合、 タブは表示されません。
- NetScaler Gateway**の詳細ペインの［NetScaler Gateway の作成/監視** ］リンクから。このリンクは、NetScaler ADC機能を有効にするライセンスをインストールすると表示されます。アプライアンスのライセンスをNetScaler Gateway 専用にした場合、リンクは表示されません。

ウィザードを最初に実行した後、ウィザードをもう一度実行して、さらに仮想サーバーと設定を作成できます。

重要：クイック構成ウィザードを使用して追加のNetScaler Gateway 仮想サーバーを構成する場合は、一意のIPアドレスを使用する必要があります。既存の仮想サーバーで使用されているものと同じ IP アドレスは使用できません。たとえば、ポート番号が 80 の IP アドレス 192.168.10.5 の仮想サーバーがあるとします。クイック構成ウィザードを実行して、ポート番号 443 の IP アドレス 192.168.10.5 を持つ 2 番目の仮想サーバーを作成します。設定を保存しようとすると、エラーが発生します。

クイック構成ウィザードで設定を構成するには

1. 構成ユーティリティで、次のいずれかを実行します。
    a. アプライアンスにNetScaler Gateway のみのライセンスが付与されている場合は、［ **ホーム** ］タブをクリックします。
    b. アプライアンスにNetScaler ADC機能を含めるためのライセンスが付与されている場合は、［構成］タブのナビゲーションペインで［ **NetScaler Gateway** ］をクリックし、詳細ペインの［ **はじめに**］の下の［ **エンタープライズストアのNetScaler Gateway の構成**］をクリックします。
2. ダッシュボードで、［ **新しいNetScaler Gateway の作成**］をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. **NetScaler Gateway 設定で**、以下を構成します。
    a. に、仮想サーバーの名前を入力します。
    b. に、仮想サーバーの IP アドレスを入力します。
    c. **［Port］**ボックスにポート番号を入力します。デフォルトのポート番号は 443 です。
    d. ポート 80 からポート 443 へのユーザー接続を許可するには、 を選択します。
4. **［続行］** をクリックします。
5. ページで、次のいずれかの操作を行います。
    a. をクリックし、 で証明書を選択します。
    b. をクリックし、** の で、 をクリックして証明書と秘密キーに移動します。
    c. をクリックし、 に、テスト証明書に含まれる完全修飾ドメイン名 (FQDN) を入力します。
6. **［続行］** をクリックします。
7. で、次の操作を行います。
    a. **プライマリ認証で**、LDAP、RADIUS、または証明書を選択します。
    b. 認証サーバーを選択するか、前の手順で選択した認証タイプの設定を構成します。 を選択した場合は、クライアント証明書を選択するか、新しいクライアント証明書をインストールします。
    c. で、認証の種類を選択し、認証サーバーの設定を構成します。
8. **［続行］** をクリックします。

ネットワーク設定と認証設定の構成が完了したら、Citrix Endpoint ManagementまたはCitrix Virtual Apps and Desktops（StoreFront またはWeb Interface）の設定を構成できます。

エンタープライズストアの設定を構成する

NetScaler Gateway は、Web、SaaS、モバイルアプリ、およびShareFileへのユーザーアクセスをEndpoint Management経由でのみサポートしています。StoreFront またはWeb Interfaceも展開する場合、ユーザーはWindowsベースのアプリと仮想デスクトップにアクセスできます。次のオプションの設定を構成できます。

- Endpoint Management のみ
- StoreFront のみ
- Endpoint Management とStoreFront 一緒に
- Web インターフェイスのみ

© 1997–2026 Citrix Systems, Inc. All rights reserved.

前の手順で をクリックすると、展開シナリオの設定を構成できます。次の手順は、［Citrix 統合設定］ページから開始します。

仮想サーバーを作成した後、クイック構成ウィザードで仮想サーバーを編集しても、Citrix Endpoint ManagementまたはCitrix Virtual Apps and Desktopsの設定を変更することはできません。

たとえば、 **Citrix Enterprise Storeの設定を構成する前に仮想サーバーの構成をキャンセルすると** 、ウィザードは設定を構成せずにWebインターフェイスを自動的に選択します。この状況が発生した場合、Web Interfaceを構成するための仮想サーバーの詳細を編集できますが、Citrix Endpoint Managementに切り替えることはできません。切り替えるには、新しい仮想サーバーを作成する必要があり、構成中にウィザードをキャンセルしてはいけません。Web Interface 仮想サーバーが必要ない場合は、クイック構成ウィザードを使用して削除できます。

StoreFront のみの設定を構成するには

1. ［ **Citrix Virtual Apps and Desktops**］をクリックします。
2. ［ **展開の種類**］で［ **StoreFront**］を選択します。
3. ［ **StoreFront完全修飾ドメイン名**］に、StoreFrontサーバーの完全修飾ドメイン名（FQDN）を入力します。
4. **Receiver for Web Pathでは**、デフォルトのパスをそのまま使用するか、独自のパスを入力します。
5. 安全なユーザー接続には **HTTPS** を選択します。
6. ［ **シングルサインオンドメイン**］で、StoreFront のドメインを入力します。
7. StoreFrontを展開し、Citrix Virtual Appsの公開アプリケーションまたはCitrix Virtual Desktopsの仮想デスクトップへのアクセスを提供する場合は、［ **STA URL**］に、Secure Ticket Authority（STA）を実行しているサーバーの完全なIPアドレスまたはFQDNを入力します。
8. **［完了］** をクリックします。

ユーザーがNetScaler Gateway を介してStoreFront に接続すると、ユーザーはReceiver for WebまたはReceiverのいずれかからアプリケーションおよびデスクトップを起動できます。

Endpoint Managementのみの設定を構成するには

1. 「 **Citrix Endpoint Management**」をクリックします。
2. に、Endpoint Management の FQDN を入力します。
3. **［完了］** をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Web インターフェイスの設定を構成するには

1. クイック構成ウィザードで、「**Citrix Virtual Apps and Desktops**」をクリックします。
2. で、 を選択し、次の項目を構成します。
   a. **Citrix Virtual Apps サイトURL**］に、Web Interfaceの完全なIPアドレスまたはFQDNを入力します。
   b. 「**Citrix Virtual Apps ServicesサイトURL」に、Citrix Workspaceアプリパスを含むWebインターフェイスの完全なIPアドレスまたは完全修飾ドメイン名**（FQDN）を入力します。デフォルトのパスを入力することも、独自のパスを入力することもできます。
   c. に、使用するドメインを入力します。
   d. に、STA を実行しているサーバーの完全な IP アドレスまたは FQDN を入力します。
3. ［**完了**］ をクリックします。

NetScaler Gateway ウィザード

NetScaler Gateway ウィザードを使用して、アプライアンスで次の設定を構成します：

- 仮想サーバー
- 証明書
- ネームサービスプロバイダー
- 認証
- 承認
- ポートリダイレクト
- クライアントレスアクセス
- SharePoint のクライアントレスアクセス

NetScaler Gateway ウィザードを使用して設定を構成する

セットアップウィザードを実行した後、NetScaler Gateway ウィザードを実行してNetScaler Gateway の他の設定を構成できます。NetScaler Gateway ウィザードは、構成ユーティリティから実行します。

NetScaler Gateway にはテスト証明書が付属しています。認証局（CA）からの署名付き証明書がない場合は、NetScaler Gateway ウィザードを使用するときにテスト証明書を使用できます。署名付き証明書を受け取ったら、テスト証明書を削除し、署名付き証明書をインストールできます。NetScaler Gateway をユーザーに公開する前に、署名付き証明書を取得することをお勧めします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注：NetScaler Gateway ウィザード内から証明書署名要求（CSR）を作成できます。NetScaler Gateway ウィザードを使用してCSRを作成する場合は、ウィザードを終了し、証明機関から署名付き証明書を受け取ったときにウィザードを再度開始する必要があります。証明書の詳細については、「 証明書のインストールと管理」を参照してください。

仮想サーバーを構成するときに、NetScaler Gateway ウィザードでインターネットプロトコルバージョン6（IPv6）のユーザー接続を構成できます。ユーザー接続に IPv6 を使用する方法の詳細については、「 ユーザー接続用の IPv6 の構成」を参照してください。

NetScaler Gateway ウィザードを起動するには

1. 構成ユーティリティで、［構成］タブをクリックし、ナビゲーションペインで［ NetScaler Gateway］をクリックします。
2. 詳細ペインの［はじめに］で、［ NetScaler Gateway ウィザード］をクリックします。
3. ［Next］をクリックして、ウィザードの指示に従います。

セットアップウィザード

セットアップウィザードを使用して、アプライアンスで次の初期設定を構成します：

- システム IP アドレスとサブネットマスク
- マップされた IP アドレスとサブネットマスク
- ホスト名
- デフォルトゲートウェイ
- ライセンス

注：セットアップウィザードを実行する前に、Citrix Webサイトからライセンスをダウンロードしてください。詳しくは、「 NetScaler Gateway のライセンス」を参照してください

公開アプリケーションウィザード

公開アプリケーションウィザードを使用して、内部ネットワークでCitrix Virtual Apps and Desktopsを実行しているサーバーに接続するようにNetScaler Gateway を構成します。公開アプリケーションウィザードでは、次の操作を実行できます。

- サーバーファームに接続する仮想サーバーを選択します。
- Web InterfaceまたはStoreFront のユーザー接続、シングルサインオン、およびSecure Ticket Authority の設定を構成します。
- SmartAccess のセッションポリシーを作成または選択します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ウィザード内では、ユーザー接続のセッションポリシー式を作成することもできます。サーバーファームに接続するようにNetScaler Gateway を構成する方法の詳細については、「Web Interfaceを介した公開アプリケーションおよび仮想デスクトップへのアクセスの提供」を参照してください。

統合されたCitrix Endpoint Management 構成

Citrix Endpoint Management MDMを使用してNetScaler Gateway を展開すると、スケーリング、アプリの高可用性の確保、セキュリティの維持が可能になります。Citrix Endpoint Management構成を使用するには、バージョン10.1、ビルド120.1316.eをインストールする必要があります。

統合Citrix Endpoint Management 構成では、次の項目が作成されます。

- デバイスマネージャ用の負荷分散サーバー。
- 電子メールフィルタリング機能を備えた Microsoft Exchange 用のサーバーの負荷分散。
- ShareFile の負荷分散サーバー。

統合Citrix Endpoint Management構成を使用した設定の作成について詳しくは、「Citrix Endpoint Management環境の設定を構成する」を参照してください

NetScaler Gatewayを構成します

NetScaler Gateway で基本ネットワーク設定を構成したら、ユーザーがセキュリティで保護されたネットワークのネットワークリソースに接続できるように詳細設定を構成します。これらの設定には次のものが含まれます。

- 仮想サーバー。NetScaler Gateway で複数の仮想サーバーを構成できます。これにより、実装する必要があるユーザーシナリオに応じて異なるポリシーを作成できます。各仮想サーバには、独自の IP アドレス、証明書、およびポリシーセットがあります。たとえば、仮想サーバーを構成し、グループのメンバーシップと仮想サーバーにバインドするポリシーに応じて、ユーザーを内部ネットワークのネットワークリソースに制限できます。次の方法を使用して、仮想サーバーを作成できます。
  - クイック構成ウィザード
  - NetScaler Gateway ウィザード
  - 構成ユーティリティ
- 高可用性。ネットワークに2つのNetScaler Gateway アプライアンスを展開すると、高可用性を構成できます。プライマリアプライアンスに障害が発生した場合、セカンダリアプライアンスはユーザセッションに影響を与えることなく引き継ぐことができます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 証明書。証明書を使用して、NetScaler Gateway へのユーザー接続をセキュリティで保護できます。証明書署名要求 (CSR) を作成するときは、証明書に完全修飾ドメイン名を追加します。証明書を仮想サーバーにバインドできます。
- 認証。NetScaler Gateway は、ローカルLDAP、RADIUS、SAML、クライアント証明書、TACACS+など、いくつかの認証タイプをサポートしています。さらに、カスケード認証と 2 要素認証を構成できます。 注:認証に RSA、Safeword、または Gemalto Protiva を使用する場合は、RADIUS を使用してこれらのタイプを構成します。
- ユーザー接続。セッションプロファイルを使用して、ユーザー接続を構成できます。プロファイル内では、ユーザーがログオンできるプラグインと、ユーザーが必要とする可能性のある制限を決定できます。次に、1 つのプロファイルでポリシーを作成できます。セッションポリシーは、ユーザー、グループ、および仮想サーバーにバインドできます。
- ホームページ。デフォルトのAccess Interfaceをホームページとして使用することも、カスタムホームページを作成することもできます。ユーザーがNetScaler Gateway に正常にログオンすると、ホームページが表示されます。
- エンドポイント分析。NetScaler Gateway では、ユーザーのログオン時にユーザーデバイスのソフトウェア、ファイル、レジストリエントリ、プロセス、およびオペレーティングシステムをチェックするポリシーを構成できます。エンドポイント分析では、ユーザーデバイスに必要なソフトウェアが必要になるため、ネットワークのセキュリティを強化できます。

構成ユーティリティの使用

構成ユーティリティを使用すると、ほとんどのNetScaler Gateway 設定を構成できます。Web ブラウザを使用して、構成ユーティリティにアクセスします。

構成ユーティリティにログオンします

1. Webブラウザーで、NetScaler Gateway のシステムIPアドレス（`http://192.168.100.1`など）を入力します。 注：NetScaler Gateway は、 デフォルトのIPアドレス192.168.100.1、 サブネットマスクが255.255.0.0であらかじめ構成されています。
2. と に次のように入力します。 `nsroot.`
3. ［展開の種類］で［NetScaler Gateway］を選択し、［ログイン］をクリックします。

構成ユーティリティに初めてログオンすると、デフォルトで タブに が開きます。［ **ホーム** ］タブでは、クイック構成ウィザードを使用して、仮想サーバー、認証、証明書、およびCitrix Endpoint Managementの設定を構成できます。クイック構成ウィザードでは、StoreFront またはWeb Interfaceの設定を構成することもできます。

NetScaler Gateway の構成について詳しくは、以下を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- セットアップウィザードを使用した初期設定の構成。
- Configuring Settings with the Quick Configuration Wizard
- NetScaler Gateway ウィザードを使用した設定の構成

仮想サーバーを作成する

仮想サーバは、ユーザがログオンするアクセスポイントです。各仮想サーバには、独自の IP アドレス、証明書、およびポリシーセットがあります。仮想サーバーは、着信トラフィックを受け入れるIPアドレス、ポート、およびプロトコルの組み合わせで構成されます。仮想サーバーには、ユーザーがアプライアンスにログオンするときの接続設定が含まれています。仮想サーバーでは、次の設定を構成できます。

- 証明書
- 認証
- ポリシー
- ブックマーク
- アドレスプール (IP プールまたはイントラネット IP とも呼ばれます)
- NetScaler Gateway を使用したダブルホップDMZ展開
- Secure Ticket Authority
- SmartAccess ICA プロキシセッション転送

NetScaler Gateway ウィザードを実行すると、ウィザード中に仮想サーバーを作成できます。次の方法で、より多くの仮想サーバーを構成できます。

- **仮想サーバノードから**。このノードは、構成ユーティリティのナビゲーションペインにあります。構成ユーティリティを使用して、仮想サーバーを追加、編集、および削除できます。
- **クイック構成ウィザード**。Citrix Endpoint Management、StoreFront、またはWeb Interfaceを環境に展開する場合は、クイック構成ウィザードを使用して、展開に必要な仮想サーバーとすべてのポリシーを作成できます。

ユーザーがログオンし、RADIUS などの特定の認証タイプを使用できるようにする場合は、仮想サーバを設定し、サーバに一意の IP アドレスを割り当てることができます。ユーザーがログオンすると、仮想サーバーに転送され、RADIUS 資格情報の入力を求められます。

また、ユーザーがNetScaler Gateway にログオンする方法を構成することもできます。セッションポリシーを使用して、ユーザーソフトウェアの種類、アクセス方法、およびログオン後にユーザーに表示されるホームページを構成できます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

仮想サーバーを作成するには

仮想サーバーを追加、変更、有効化、無効化、および削除するには、NetScaler Gateway GUIまたはクイック構成ウィザードを使用します。クイック構成ウィザードを使用した仮想サーバーの構成の詳細については、「クイック構成ウィザードを使用した設定の構成」を参照してください。

注：

VPN 仮想サーバーは、デフォルトで DTLS バージョン 1.0 をサポートしています。DTLS バージョン 1.2 を有効にするには、「SSL VPN 仮想サーバーを使用した DTLS VPN 仮想サーバーの設定」を参照してください。

GUI を使用して仮想サーバーを作成するには

1. ［**NetScaler Gateway**］>［**仮想サーバー**］に移動します。
2. 詳細ペインで、 をクリックします。
3. 要件に従って設定を構成します。
4. ［**Create**］ をクリックしてから、 ［**Close**］ をクリックします。

CLI を使用して仮想サーバーを作成するには

コマンドプロンプトで次を入力します：

```
add vpn vserver <name> <serviceType> [<IPAddress> [<port>]
```

例:

```
add vpn vserver gatewayserver SSL 1.1.1.1 443
```

ネットプロファイルを VPN 仮想サーバーにバインドする際の注意点

ネットプロファイル（ネットワークプロファイル）を作成して、指定した送信元 IP アドレスを使用するようにアプライアンスを設定し、ネットプロファイルを VPN 仮想サーバーにバインドできます。ただし、ネットプロファイルを VPN 仮想サーバーにバインドする場合は、次の点に注意してください。

- ネットプロファイルをNetScaler Gateway 仮想サーバーにバインドすると、ネットプロファイルは、バックエンドサーバーへのトラフィック用に仮想サーバーまたはサービスによって使用される特定のSNIPを選択しません。代わりに、Gateway Appliance はネットプロファイルバインディングを無視し、ラウンドロビン方式を使用して SNIP を選択します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- ネットプロファイルは、動的に生成されたサービス（STA、SF モニタ）では機能しません。STA およびその他の動的に生成されるサービスの場合、ネットプロファイルをそれらのモニタに直接バインドでき、その時点でそれらのモニタが使用されます。ただし、同じアプライアンスに複数のゲートウェイがある場合、すべてのゲートウェイは、設定されたモニタに対して同じネットプロファイルを使用します。

ネットプロファイルの詳細については、 バックエンド通信に指定されたソース IP を使用するを参照してください。

仮想サーバ上の現在のユーザーと接続しているユーザーの総数

現在のユーザー: 特定の仮想サーバーにログオンしているユーザーの数。CCU を追跡するために現在のユーザを監視することをお勧めします。

接続しているユーザーの合計: 特定の仮想サーバーを介して 1 つ以上のアクティブな接続を持つユーザーの数。接続しているユーザーの総数は、主にICAプロキシで使用されます。

接続ユーザーの合計数カウンタは、次のシナリオで使用できます。

- ICA接続は確立されているが、対応する認証、承認、および監査セッションが確立されていないとします。このシナリオでは、ユーザーがアプリケーションまたはデスクトップを起動してブラウザを閉じ、起動したアプリケーションまたはデスクトップで作業を続行します。認証、承認、および監査セッションはタイムアウトしますが、接続はまだアクティブです。接続しているユーザーの合計数を使用して、まだ接続しているユーザーを識別できます。
- HDX最適ルーティングでは、認証ゲートウェイとICAゲートウェイを異なるアプライアンス上に置くことができます。この場合の接続ユーザーの合計は、ICAゲートウェイ上の接続ユーザーの数を識別するために使用できます。

注意事項：

- アクティブなセッションがある（まだタイムアウトしていない）が、これらのセッションにアクティブな接続がない場合、現在のユーザは合計接続ユーザ数を超えています。たとえば、ユーザーがアプリケーションまたはデスクトップを起動してすぐに閉じたものの、認証、承認、および監査セッションからログアウトしなかった場合などです。
- 認証、承認、および監査セッションがタイムアウトしても、ICA接続がアクティブな場合、接続しているユーザーの合計が現在のユーザーを超えています。
- 純粋なVPN設定（ICAは関与しない）では、現在のユーザー数と接続ユーザーの総数は等しくなります。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

仮想サーバーで接続タイプを構成する

仮想サーバーを作成および構成するときに、次の接続オプションを構成できます：

- Citrix Workspace アプリとの接続は、SmartAccess、エンドポイント分析、またはネットワーク層トンネリング機能を使用せずに、Citrix Virtual Apps and Desktops にのみ接続します。
- NetScaler Gateway プラグインおよびSmartAccessとの接続。これにより、SmartAccess、エンドポイント分析、およびネットワーク層トンネリング機能を使用できます。
- モバイルデバイスからNetScaler Gateway へのマイクロVPN接続を確立するSecure Hub との接続。
- 複数のデバイスからユーザーがICAセッションプロトコルを介して行われる並列接続。複数のユニバーサルライセンスを使用しないように、接続は 1 つのセッションに移行されます。

ユーザがユーザソフトウェアなしでログオンできるようにする場合は、クライアントレスアクセスポリシーを設定し、それを仮想サーバにバインドできます。

仮想サーバーで基本接続または SmartAccess 接続を構成するには

1. ［**NetScaler Gateway**］に移動し、［**仮想サーバー**］をクリックします。
2. 詳細ペインで、 をクリックします。
3. に、仮想サーバーの名前を入力します。
4. に、仮想サーバーのIPアドレスとポート番号を入力します。
5. 次のいずれかを行います：
    - ICA 接続のみを許可するには、 をクリックします。
    - Secure Hub、NetScaler Gateway プラグイン、およびSmartAccessを使用したユーザーログオンを許可するには、［**SmartAccess モード**］をクリックします。
    - SmartAccessが複数のユーザー接続のICAプロキシセッションを管理できるようにするには、「**ICAプロキシセッション移行**」をクリックします。
6. 仮想サーバーのその他の設定を構成し、、 の順にクリックします。

ワイルドカード仮想サーバー用のリッスンポリシーを構成する

NetScaler Gateway 仮想サーバーを構成して、仮想サーバーが特定のVLANでリッスンする機能を制限できます。指定された VLAN 上のトラフィックの処理に制限するリッスンポリシーを使用して、ワイルドカード仮想サーバを作成できます。

設定パラメータは次のとおりです。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

パラメーター	説明
名前	仮想サーバーの名前。この名前は必須であり、仮想サーバーの作成後に名前を変更することはできません。名前は 127 文字を超えることはできません。また、最初の文字は数字または文字である必要があります。また、アットマーク (@)、アンダースコア (_)、ダッシュ (-)、ピリオド (.)、コロン (:)、シャープ記号 (#)、およびスペースを使用することもできます。
IP	仮想サーバの IP アドレス。VLAN にバインドされたワイルドカード仮想サーバの場合、値は常に* です。
種類	サービスの動作。選択肢は、HTTP、SSL、FTP、TCP、SSL_TCP、UDP、SSL_BRIDGE、NNTP、DNS、ANY、SIP-UDP、DNS-TCP、RTSPです。
ポート	仮想サーバーがユーザー接続をリッスンするポート。ポート番号は 0 ～ 65535 の範囲で指定する必要があります。VLAN にバインドされたワイルドカード仮想サーバの場合、値は通常* です。
リスニング優先度	リッスンポリシーに割り当てられている優先順位。プライオリティは逆の順序で評価されます。数字が小さいほど、リッスンポリシーに割り当てられるプライオリティが高くなります。
リッスンポリシールール	仮想サーバがリッスンする必要がある VLAN の識別に使用するポリシールール。ルールは次のとおりです。CLIENT.VLAN.ID.EQ (`<ipaddressat>`) `<ipaddressat>`の場合は、VLAN に割り当てられた ID 番号を置き換えます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

リッスンポリシーを使用してワイルドカード仮想サーバーを作成するには

1. ナビゲーションペインで［**NetScaler Gateway**］を展開し、［**仮想サーバー**］をクリックします。
2. 詳細ペインで、 をクリックします。
3. に、仮想サーバーの名前を入力します。
4. で、プロトコルを選択します。
5. に、仮想サーバーの IP アドレスを入力します。
6. に、仮想サーバーのポートを入力します。
7. タブの の に、リッスンポリシーの優先度を入力します。
8. の横にある をクリックします。
9. 「**式の作成**」ダイアログで、「**追加**」をクリックして式を設定し、「**OK」**をクリックします。
10. ［**Create**］をクリックしてから、［**CIose**］をクリックします。

NetScaler Gateway でIPアドレスを構成する

構成ユーティリティにログオンし、ユーザー接続用の IP アドレスを構成できます。NetScaler Gateway は、管理アクセス用のデフォルトIPアドレス192.168.100.1、サブネットマスク255.255.0.0で構成されています。デフォルトの IP アドレスは、システム IP (NSIP) アドレスのユーザーが構成した値が存在しない場合に使用されます。

- NSIP アドレス。アプライアンスへのすべての管理関連アクセスに使用されるNetScaler Gateway の管理IPアドレス。NetScaler Gateway は、認証にNSIPアドレスも使用します。
- **デフォルトゲートウェイ**。セキュリティで保護されたネットワークの外部からNetScaler Gateway にトラフィックを転送するルーター。
- **サブネット IP (SNIP) アドレス**。セカンダリネットワーク上のサーバと通信することによってユーザデバイスを表す IP アドレス。

SNIP アドレスは、ポート 1024 ～ 64000 を使用します。

NetScaler GatewayがIPアドレスを使用する方法

NetScaler Gateway は、発生している機能に基づいてIPアドレスからトラフィックをソースします。次のリストでは、一般的なガイドラインとして、いくつかの機能と、NetScaler Gateway がそれぞれのIPアドレスを使用する方法について説明します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **認証。**NetScaler Gateway が使用するIPアドレスは、認証サーバーの種類によって異なります。
  - LDAP/RADIUS/TACACS サーバ。AAAD が認証仮想サーバーと直接通信する場合、NSIP アドレスが使用されます。
  - ロードバランサをプロキシとして使用する場合、ロードバランサは認証に SNIP アドレスを使用します。AAAD は NSIP アドレスを使用してロードバランサと通信します。NetScaler ADCが使用するIPアドレスは、認証仮想サーバーと通信しているエンティティによって異なります。
  - SAML/OAUTH/WEBAUTH サーバー:これらのサーバーは SNIP アドレスを使用して通信します。
- **ホームページからのファイル転送。**NetScaler Gateway はSNIPアドレスを使用します。
- **DNS および WINS クエリ。**NetScaler Gateway はSNIPアドレスを使用します。
- **セキュリティで保護されたネットワーク内のリソースへのネットワークトラフィック。**NetScaler Gateway は、NetScaler Gateway の構成に応じて、SNIPアドレスまたはIPプールを使用します。
- **ICA プロキシ設定。**NetScaler Gateway はSNIPアドレスを使用します。

サブネット IP アドレス

サブネットIPアドレスを使用すると、ユーザーは別のサブネット上にある外部ホストから NetScaler Gateway に接続できます。サブネット IP アドレスを追加すると、対応するルートエントリがルートテーブルに作成されます。サブネットごとに作成されるエントリは 1 つだけです。ルートエントリは、サブネットに追加された最初の IP アドレスに対応します。

システムIPアドレスとマッピングされたIPアドレスとは異なり、NetScaler Gateway の初期構成時にサブネットIPアドレスを指定することは必須ではありません。

マッピング IP アドレスとサブネット IP アドレスは、ポート 1024 ～ 64000 を使用します。

サブネット IP アドレスを追加するには

1. 構成ユーティリティの タブのナビゲーションウィンドウで、\ > を展開し、 をクリックします。
2. 詳細ペインで、 をクリックします。
3. ダイアログボックスの に IP アドレスを入力します。
4. に、サブネットマスクを入力します。
5. で、 を選択し、、** の順にクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ユーザー接続用の IPv6 を構成する

インターネットプロトコルバージョン6（IPv6）を使用してユーザー接続をリッスンするように NetScaler Gateway を構成できます。次のいずれかの設定を構成する場合は、 チェックボックスをオンにして、ダイアログボックスに IPv6 アドレスを入力できます。

- グローバル設定-公開アプリケーション-ICAプロキシ
- グローバル認証-RADIUS
- グローバル認証-LDAP
- グローバル認証-TACACS
- セッションプロファイル-公開アプリケーション-ICAプロキシ
- NetScaler Gateway 仮想サーバー
- 認証サーバの作成-RADIUS
- 認証サーバーの作成-LDAP
- 認証サーバの作成-TACACS
- 監査サーバーの作成
- 高可用性セットアップ
- 高可用性のためのルートモニターのバインド/バインド解除
- 仮想サーバー (負荷分散)

IPv6アドレスでリッスンするようにNetScaler Gateway 仮想サーバーを構成すると、ユーザーは Citrix Workspace アプリでのみ接続できます。NetScaler Gateway プラグインとのユーザー接続は、IPv6ではサポートされていません。

NetScaler Gateway でIPv6を構成するには、次のガイドラインを使用できます：

- Citrix Virtual Apps とWeb Interface。ユーザー接続用にIPv6を構成し、IPv6を使用するマッピングIPアドレスがある場合、Citrix Virtual Apps およびWeb InterfaceサーバーもIPv6を使用できます。Web Interfaceは、NetScaler Gateway の背後にインストールする必要があります。ユーザーがNetScaler Gateway 経由で接続すると、IPv6アドレスはIPv4に変換されます。接続が戻ると、IPv4 アドレスは IPv6 に変換されます。
- 仮想サーバー。NetScaler Gateway ウィザードを実行すると、仮想サーバーのIPv6を構成できます。NetScaler Gateway ウィザードの［仮想サーバー］ページで、［IPv6］をクリックしてIPアドレスを入力します。仮想サーバーのIPv6アドレスを構成するには、NetScaler Gateway ウィザードを使用する必要があります。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- その他。ICAプロキシ、認証、監査、および高可用性用にIPv6を構成するには、ダイアログボックスで チェックボックスをオンにし、IPアドレスを入力します。

セキュリティで保護されたネットワークにある DNS サーバーを解決する

DNS サーバーがファイアウォールの背後にあるセキュリティで保護されたネットワークにあり、ファイアウォールが ICMP トラフィックをブロックしている場合、ファイアウォールが要求をブロックしているため、サーバーへの接続をテストできません。この問題は、次の手順で解決できます。

- 既知の完全修飾ドメイン名 (FQDN) に解決されるカスタム DNS モニターを使用して DNS サービスを作成する。
- NetScaler Gateway 上に直接アドレス指定できないDNS仮想サーバーを作成する。
- サービスを仮想サーバーにバインドします。

注：

- DNS 仮想サーバーと DNS サービスを構成するのは、DNS サーバーがファイアウォールの内側にある場合のみです。
- アプライアンスにNetScaler ADC負荷分散ライセンスをインストールすると、ナビゲーションペインに［仮想サーバーとサービス］ノードが表示されません。この手順を実行するには、 を展開し、 をクリックします。

DNS サービスと DNS モニターを構成するには

1. 構成ユーティリティの タブのナビゲーションペインで、 を展開し、 をクリックします。
2. 詳細ペインで、［Add］ をクリックします。
3. に、サービスの名前を入力します。
4. で、 を選択します。
5. に、DNS サーバーの IP アドレスを入力します。
6. ［Port］ボックスにポート番号を入力します。
7. タブで、 をクリックします。
8. タブの で、 を選択し、、、 の順にクリックします。
9. ダイアログボックスで、、 の順にクリックします。

次に、「DNS 仮想サーバーを構成し、DNS サービスを仮想サーバーにバインドするには 」の手順を使用して DNS 仮想サーバーを作成します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

DNS サービスを DNS 仮想サーバーにバインドするには

1. ダイアログボックスの タブで、 をクリックし、DNS サービスを選択し、、 の順にクリックします。

DNS 仮想サーバーを構成する

DNS 仮想サーバーを構成するには、名前と IP アドレスを指定します。NetScaler Gateway 仮想サーバーと同様に、DNS仮想サーバーにIPアドレスを割り当てる必要があります。ただし、この IP アドレスは、ユーザデバイスがすべての内部アドレスを解決できるように、ターゲットネットワークの内部側にある必要があります。また、DNS ポートを指定します。

注：アプライアンスにNetScaler ADC負荷分散ライセンスをインストールすると、ナビゲーションペインに［仮想サーバーとサービス］ノードが表示されません。この機能は、負荷分散仮想サーバーを使用して構成できます。詳しくは、NetScaler ADCドキュメントの「Citrix 製品ドキュメント」を参照してください。

DNS 仮想サーバーを構成するには

1. 構成ユーティリティの タブのナビゲーションペインで、 を展開し、 をクリックします。
2. 詳細ペインで、［Add］ をクリックします。
3. に、仮想サーバーの名前を入力します。
4. に、DNS サーバーの IP アドレスを入力します。
5. に、DNS サーバーがリッスンするポートを入力します。
6. で を選択し、 をクリックします。

最後に、展開のニーズに応じて、次の2つの方法のいずれかを使用して、DNS仮想サーバーを NetScaler Gateway に関連付けます。

- サーバーをNetScaler Gateway にグローバルにバインドします。
- DNS 仮想サーバーを仮想サーバーごとにバインドします。

DNS 仮想サーバーをグローバルに展開すると、すべてのユーザーがそのサーバーにアクセスできます。次に、DNS 仮想サーバーを仮想サーバーにバインドして、ユーザーを制限できます。

ネームサービスプロバイダーの設定

NetScaler Gateway は、ネームサービスプロバイダーを使用してWebアドレスをIPアドレスに変換します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler Gateway ウィザードを実行すると、DNSサーバーまたはWINSサーバーのいずれかを構成できます。構成ユーティリティを使用して、他の DNS サーバーまたは WINS サーバーを構成することもできます。

NetScaler Gateway にDNSサーバーを追加するには

1. ナビゲーションペインにある、［Configuration］タブの構成ユーティリティで、［NetScaler Gateway］を展開し、［Global Settings］をクリックします。
2. 詳細ペインの で、 をクリックします。
3. タブで、 をクリックします。
4. ダイアログボックスの に DNS サーバーの IP アドレスを入力し、、 の順にクリックします。
5. 構成ユーティリティで「OK」をクリックします。

WINSサーバーをNetScaler Gateway に追加するには

1. ナビゲーションペインにある、［Configuration］タブの構成ユーティリティで、［NetScaler Gateway］を展開し、［Global Settings］をクリックします。
2. 詳細ペインの で、 をクリックします。
3. タブの に WINS サーバーの IP アドレスを入力し、 をクリックします。

次に、DNS 仮想サーバー名と IP アドレスを指定します。NetScaler Gateway 仮想サーバーと同様に、仮想サーバーにはIPアドレスを割り当てる必要があります。ただし、この IP アドレスは、ユーザデバイスがすべての内部アドレスを適切に解決できるように、ターゲットネットワークの内部側にある必要があります。DNS ポートも指定する必要があります。

名前解決のためにDNSサーバーとWINSサーバーを構成する場合は、NetScaler Gateway ウィザードを使用して、最初に名前検索を実行するサーバーを選択できます。

名前ルックアップの優先度を指定するには

1. 構成ユーティリティで、［構成］タブをクリックし、ナビゲーションペインで［ NetScaler Gateway］をクリックします。
2. 詳細ペインの［はじめに］で、［ NetScaler Gateway ウィザード］をクリックします。
3. ［次へ］をクリックして、［ネームサービスプロバイダ］ページが表示されるまで現在の設定を受け入れます。
4. で、 または を選択し、ウィザードの最後に進みます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

サーバー起動接続を構成する

IPアドレスが有効なNetScaler Gateway にログオンしたユーザーごとに、DNSサフィックスがユーザー名に追加され、DNSアドレスレコードがアプライアンスのDNSキャッシュに追加されます。この手法は、ユーザの IP アドレスではなく DNS 名をユーザに提供するのに役立ちます。

IPアドレスがユーザーのセッションに割り当てられると、内部ネットワークからユーザーのデバイスに接続できます。たとえば、リモートデスクトップまたは仮想ネットワークコンピューティング (VNC) クライアントを使用して接続しているユーザーは、問題のあるアプリケーションを診断するためにユーザーデバイスにアクセスできます。また、リモートでログオンしている内部ネットワークIPアドレスを持つ2人のNetScaler Gateway ユーザーが、NetScaler Gateway を介して相互に通信することも可能です。アプライアンスでログオンしているユーザーの内部ネットワーク IP アドレスの検出を許可すると、この通信が補助されます。

リモートユーザーは、次のpingコマンドを使用して、NetScaler Gateway にログオンできるユーザーの内部ネットワークIPアドレスを検出できます：

```
ping \<username.domainname\>
```

サーバーは、次のさまざまな方法でユーザーデバイスへの接続を開始できます：

- TCP または UDP 接続。接続は、内部ネットワーク内の外部システム、またはNetScaler Gateway にログオンしている別のコンピューターから発生します。NetScaler Gateway にログオンした各ユーザーデバイスに割り当てられた内部ネットワークIPアドレスは、これらの接続に使用されます。NetScaler Gateway がサポートするさまざまな種類のサーバー起動接続について説明します。 TCP または UDP サーバー起動接続の場合、サーバーはユーザーデバイスの IP アドレスとポートに関する予備知識を持ち、それに接続します。NetScaler Gateway はこの接続を傍受します。

  次に、ユーザーデバイスはサーバーへの初期接続を行い、サーバーは、既知または最初に構成されたポートから派生したポートでユーザーデバイスに接続します。

  このシナリオでは、ユーザーデバイスはサーバーへの初期接続を行い、この情報が埋め込まれているアプリケーション固有のプロトコルを使用して、サーバーとポートと IP アドレスを交換します。これにより、NetScaler Gateway は、アクティブなFTP接続などのアプリケーションをサポートできるようになります。
- Port コマンド。これは、アクティブな FTP および特定の Voice over IP プロトコルで使用されます。
- プラグイン間の接続。NetScaler Gateway は、内部ネットワークIPアドレスを使用したプラグイン間の接続をサポートします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

このタイプの接続では、同じNetScaler Gateway を使用する2つのNetScaler Gateway ユーザーデバイスが相互に接続を開始できます。このタイプの例としては、Office Communicator や Yahoo! メッセンジャー。

ユーザーがNetScaler Gateway からログオフし、ログオフ要求がアプライアンスに到達しなかった場合、ユーザーは任意のデバイスを使用して再度ログオンし、以前のセッションを新しいセッションに置き換えることができます。この機能は、ユーザごとに 1 つの IP アドレスが割り当てられる展開で役立つ場合があります。

ユーザーがNetScaler Gateway に初めてログオンすると、セッションが作成され、IPアドレスがユーザーに割り当てられます。ユーザーがログオフしてもログオフ要求が失われた場合、またはユーザーデバイスがクリーンログオフを実行できない場合、セッションはシステム上で維持されます。ユーザーが同じデバイスまたは別のデバイスから再度ログオンしようとすると、認証が成功すると、［ログオン転送］ダイアログボックスが表示されます。ユーザーがログオンの転送を選択すると、NetScaler Gateway 上の以前のセッションが閉じられ、新しいセッションが作成されます。ログオンの転送は、ログオフ後 2 分間だけアクティブになります。複数のデバイスから同時にログオンを試みた場合は、最後のログオン試行で元のセッションが置き換えられます。

NetScaler Gateway でルーティングを構成する

内部ネットワークリソースへのアクセスを提供するために、NetScaler Gateway はデータを内部の安全なネットワークにルーティングします。デフォルトでは、NetScaler Gateway は静的ルートを使用します。

NetScaler Gateway がデータをルーティングできるネットワークは、NetScaler Gateway ルーティングテーブルの構成方法と、NetScaler Gateway に指定するデフォルトゲートウェイによって決まります。

NetScaler Gateway ルーティングテーブルには、ユーザーがアクセスする必要がある内部ネットワークリソースにデータをルーティングするために必要なルートが含まれている必要があります。

NetScaler Gateway は、次のルーティングプロトコルをサポートしています：

- ルーティング情報プロトコル（RIP v1 および v2）
- Open Shortest Path First (OSPF)
- ボーダーゲートウェイプロトコル (BGF)

スタティックルートの設定

別のホストまたはネットワークとの通信を設定するときに、動的ルーティングを使用しない場合は、NetScaler Gateway から新しい宛先への静的ルートを構成する必要があります。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

スタティックルートを設定するには

1. 構成ユーティリティの タブのナビゲーションペインで、 > > を展開し、 をクリックします。
2. 詳細ペインの タブで、 をクリックします。
3. ルートの設定を構成し、 をクリックします。

スタティックルートをテストするには

1. 構成ユーティリティのナビゲーションウィンドウで、 を展開し、** をクリックします。
2. 詳細ペインの で、 をクリックします。
3. の に、デバイスの名前を入力します。
4. の にデバイスの IP アドレスを入力し、 をクリックします。

   他のデバイスと正常に通信している場合、メッセージは、同じ数のパケットが送受信され、ゼロのパケットが失われたことを示します。

   他のデバイスと通信していない場合、ステータスメッセージは、受信されたパケットがゼロで、すべてのパケットが失われたことを示します。この通信不足を修正するには、手順を繰り返してスタティックルートを追加します。

テストを停止するには、 ダイアログボックスで、 をクリックし、** をクリックします。

オートネゴシエーションの設定

デフォルトでは、アプライアンスは自動ネゴシエーションを使用するように構成されています。このオートネゴシエーションでは、NetScaler Gateway がネットワークトラフィックを両方向同時に送信し、適切なアダプタ速度を決定します。 デフォルト設定を自動ネゴシエーションのままにすると、NetScaler Gateway は全二重操作を使用します。この動作では、ネットワークアダプターは双方向に同時にデータを送信できます。

自動ネゴシエーションを無効にすると、NetScaler Gateway は半二重操作を使用します。この動作では、アダプターは2つのノード間で両方向にデータを送信できますが、アダプターは一度に一方向または他方のみを使用できます。

初回のインストールでは、アプライアンスに接続されているポートに自動ネゴシエーションを使用するようにNetScaler Gateway を構成することをお勧めします。最初にログオンしてNetScaler Gateway を構成したら、自動ネゴシエーションを無効にすることができます。オートネゴシエーションをグローバルに設定することはできません。各インターフェイスの設定を有効または無効にする必要があります。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

オートネゴシエーションを有効または無効にするには

1. 構成ユーティリティの タブのナビゲーションウィンドウで、\ > を展開し、** をクリックします。
2. 詳細ウィンドウで、インターフェイスを選択し、 をクリックします。
3. 「 **インタフェースを設定」(Configure Interface**) ダイアログボックスで次のいずれかを実行します：

   - オートネゴシエーションを有効にするには、［オートネゴシエーション］の横にある［ **はい** ］をクリックし、［ **OK］**をクリックします。
   - オートネゴシエーションを無効にするには、［オートネゴシエーション］の横にある［ **いいえ** ］をクリックし、［ **OK］**をクリックします。

NetScaler Gateway でホスト名とFQDNを構成する

ホスト名は、ライセンスファイルに関連付けられているNetScaler Gateway アプライアンスの名前です。ホスト名はアプライアンスに固有で、ユニバーサルライセンスをダウンロードするときに使用されます。ホスト名は、セットアップウィザードを実行してNetScaler Gateway を初めて構成するときに定義します。

完全修飾ドメイン名 (FQDN) は、仮想サーバーにバインドされた署名付き証明書に含まれています。NetScaler Gateway ではFQDNを構成しません。1つのアプライアンスは、証明書を使用して NetScaler Gateway で構成された各仮想サーバーに割り当てられた一意のFQDNを持つことができます。

証明書の FQDN は、証明書の詳細を表示することで確認できます。FQDN は、証明書のサブジェクトフィールドにあります。

証明書の FQDN を表示するには

1. 構成ユーティリティの タブのナビゲーションウィンドウで、 を展開し、** をクリックします。
2. 詳細ウィンドウで、証明書を選択し、、** の順にクリックします。
3. 「証明書の詳細」ダイアログ・ボックスで、「 **件名**」をクリックします。証明書の FQDN がリストに表示されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler Gateway のポリシーとプロファイル

NetScaler Gateway のポリシーとプロファイルを使用すると、指定されたシナリオまたは条件の下で構成設定を管理および実装できます。個々のポリシーは、指定された条件セットが満たされたときに有効になる構成設定を指定または定義します。各ポリシーには一意の名前があり、ポリシーにバインドされたプロファイルを持つことができます。

ポリシーの仕組み

ポリシーは、ブール条件と、プロファイルと呼ばれる設定のコレクションで構成されます。条件は実行時に評価され、ポリシーを適用する必要があるかどうかが決定されます。

プロファイルは、特定のパラメータを使用する設定の集まりです。プロファイルには任意の名前を付けることができ、複数のポリシーで再利用できます。プロファイル内で複数の設定を構成できますが、ポリシーごとに含めることができるプロファイルは 1 つだけです。

ポリシーは、設定された条件とプロファイルを使用して、仮想サーバ、グループ、ユーザ、またはグローバルにバインドできます。ポリシーは、制御する構成設定のタイプによって参照されます。たとえば、セッションポリシーでは、ユーザーのログオン方法と、ユーザーがログオンしたままにできる時間を制御できます。

NetScaler Gateway をCitrix Virtual Apps で使用している場合、NetScaler Gateway ポリシー名はフィルターとしてCitrix Virtual Apps に送信されます。NetScaler GatewayをCitrix Virtual Apps およびSmartAccessと互換性があるように構成する場合は、Citrix Virtual Apps で次の設定を構成します。

- アプライアンスに構成されている仮想サーバーの名前。この名前は、NetScaler Gateway ファーム名としてCitrix Virtual Apps に送信されます。
- 事前認証ポリシーまたはセッションポリシーの名前は、フィルタ名として送信されます。

NetScaler Gateway をCitrix EndpointManagementと互換性を持たせるための構成について詳しくは、「Citrix Endpoint Management環境の設定を構成する」を参照してください。

NetScaler Gateway をCitrix Virtual Apps and Desktopsと互換性を持たせるための構成について詳しくは、「Web Interfaceを使用した Citrix Virtual AppsおよびCitrix Virtual Desktops のリソースへのアクセス」および「Citrix Endpoint ManagementまたはStoreFrontとの統合」を参照してください。

事前認証ポリシーの詳細については、 エンドポイントポリシーの設定を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

条件付きポリシー

ポリシーを設定するときは、任意のブール式を使用して、ポリシーが適用される条件を表すことができます。条件付きポリシーを設定する場合、次のような、使用可能な任意のシステム式を使用できます。

- クライアントセキュリティ文字列
- ネットワーク情報
- HTTP ヘッダーとクッキー
- 一日の時間
- クライアント証明書の値

また、ユーザーデバイスが特定の条件 (SmartAccess のセッションポリシーなど) を満たす場合にのみ適用するポリシーを作成することもできます。

条件付きポリシーを構成するもう 1 つの例は、ユーザーの認証ポリシーを変更することです。たとえば、自宅のコンピューターやモバイルデバイスからMicro VPNを使用するなど、内部ネットワークの外部からNetScaler Gateway プラグインを使用して接続するユーザーに、LDAPを使用して認証し、WAN経由で接続しているユーザーはRADIUSを使用して認証されるように要求できます。

注:ポリシー・ルールがセッション・プロファイルのセキュリティ設定の一部として構成されている場合、エンドポイント分析結果に基づくポリシー条件は使用できません。

ポリシーの優先順位

ポリシーは、ポリシーがバインドされている順序で優先順位付けおよび評価されます。

次の 2 つの方法により、ポリシーのプライオリティが決まります。

- ポリシーがバインドされるレベル（グローバル、仮想サーバー、グループ、またはユーザー）。ポリシーレベルは、次のように最高から最低にランク付けされます。
  - ユーザー (最優先度)
  - グループ
  - 仮想サーバー
  - グローバル (最低優先度)
- 数値のプライオリティは、ポリシーがバインドされているレベルに関係なく優先されます。グローバルにバインドされたポリシーのプライオリティ番号が 1 で、ユーザにバインドされた別

© 1997–2026 Citrix Systems, Inc. All rights reserved.

のポリシーのプライオリティ番号が 2 の場合、グローバルポリシーが優先されます。プライオリティ番号が小さいほど、ポリシーの優先順位が高くなります。

NetScaler Gateway でポリシーを作成する

構成ユーティリティを使用して、ポリシーを作成できます。ポリシーを作成したら、ポリシーを適切なレベル（ユーザー、グループ、仮想サーバー、グローバル）にバインドします。ポリシーをこれらのレベルのいずれかにバインドすると、ポリシー条件が満たされると、ユーザーはプロファイル内の設定を受け取ります。各ポリシーとプロファイルには一意の名前があります。

展開の一部としてCitrix Endpoint ManagementまたはStoreFront を使用している場合は、クイック構成ウィザードを使用してこの展開環境の設定を構成できます。ウィザードの詳細については、「 クイック構成ウィザードを使用した設定の構成」を参照してください。

システム式の設定

システム式は、ポリシーが適用される条件を指定します。たとえば、事前認証ポリシーの式は、ユーザーがログオンしている間に適用されます。セッションポリシーの式は、ユーザーが認証されてNetScaler Gateway にログオンした後に評価され、適用されます。

NetScaler Gateway での式は次のとおりです：

- NetScaler Gateway への接続を確立するときにユーザーが使用できるオブジェクトを制限する一般的な表現。たとえば、以下を参照してください：
  - セッションポリシー
- ユーザーデバイスにインストールして実行する必要があるソフトウェア、ファイル、プロセス、またはレジストリ値を定義するクライアントセキュリティ表現。たとえば、以下を参照してください：
  - エンドポイントポリシー
- ネットワーク設定に基づいてアクセスを制限するネットワークベースの式。たとえば、以下を参照してください：
  - トラフィックポリシー
  - 承認ポリシー

NetScaler Gateway は、NetScaler ADCアプライアンスとしても使用できます。アプライアンス上のいくつかの式は、NetScaler ADCにより適用されます。一般的な式とネットワークベースの式は、NetScaler ADCで一般的に使用され、NetScaler Gateway では一般的に使用されません。クラ

© 1997–2026 Citrix Systems, Inc. All rights reserved.

イアントセキュリティ式は、NetScaler Gateway で使用され、ユーザーデバイスに正しいアイテムがインストールされているかどうかを判断します。

クライアントセキュリティ式の設定

式はポリシーの構成要素です。式は、リクエストまたはレスポンスに対して評価される単一の条件を表します。次のような条件をチェックする単純な式のセキュリティ文字列を作成できます。

- サービスパックを含むユーザーデバイスのオペレーティングシステム
- ウイルス対策ソフトウェアのバージョンとウイルス定義
- ファイル
- プロセス
- レジストリ値
- ユーザー証明書

NetScaler Gateway での証明書管理

NetScaler Gateway では、証明書を使用して安全な接続を作成し、ユーザーを認証します。

セキュアな接続を確立するには、接続の一端にサーバー証明書が必要です。接続のもう一方の端には、サーバ証明書を発行した認証局 (CA) のルート証明書が必要です。

- サーバー証明書。サーバー証明書は、サーバーの ID を証明します。NetScaler Gateway には、このタイプのデジタル証明書が必要です。
- ルート証明書。ルート証明書は、サーバ証明書に署名した CA を識別します。ルート証明書は認証局に属します。ユーザーデバイスは、サーバー証明書を検証するために、このタイプのデジタル証明書を必要とします。

ユーザーデバイス上の Web ブラウザとのセキュアな接続を確立すると、サーバーは証明書をデバイスに送信します。

ユーザーデバイスがサーバー証明書を受信すると、Internet Explorer などの Web ブラウザーは、証明書を発行した CA と、その CA がユーザーデバイスによって信頼されているかどうかを確認します。CA が信頼されていない場合、またはテスト証明書の場合、Web ブラウザはユーザに証明書を受け入れるか拒否するかを尋ねます（事実上、サイトへのアクセス権限を承認または拒否します）。

NetScaler Gateway では、次の3種類の証明書がサポートされています。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 仮想サーバーにバインドされ、サーバーファームへの接続にも使用できるテスト証明書。NetScaler Gateway には、テスト証明書がプリインストールされています。
- CA によって署名され、秘密キーとペアになっている PEM または DER 形式の証明書。
- 証明書と秘密キーの格納または転送に使用される PKCS #12 形式の証明書。PKCS #12 証明書は、通常、既存のWindows証明書からPFXファイルとしてエクスポートされ、NetScaler Gateway にインストールされます。

ThawteやVerisignなど、信頼できるCAによって署名された証明書を使用することをお勧めします。

証明書署名要求を作成する

SSLまたはTLSを使用してセキュリティで保護された通信を提供するには、NetScaler Gateway でサーバー証明書が必要です。証明書をNetScaler Gateway にアップロードする前に、証明書署名要求（CSR）と秘密キーを生成する必要があります。NetScaler Gateway ウィザードまたは構成ユーティリティに含まれている［証明書要求の作成］を使用して、CSRを作成します。証明書要求の作成により、署名用に認証局（CA）に電子メールで送信される.csr ファイルと、アプライアンスに残る秘密キーが作成されます。CA が証明書に署名し、指定した電子メールアドレスに証明書を返します。署名付き証明書を受け取ったら、NetScaler Gateway にインストールできます。CA から証明書を受け取ったら、証明書と秘密キーをペアにします。

重要：NetScaler Gateway ウィザードを使用してCSRを作成する場合は、ウィザードを終了し、CAが署名付き証明書を送信するのを待つ必要があります。証明書を受け取ったら、NetScaler Gateway ウィザードを再度実行して設定を作成し、証明書をインストールできます。NetScaler Gateway ウィザードについて詳しくは、「NetScaler Gateway ウィザードを使用した設定の構成」を参照してください。

NetScaler Gateway ウィザードを使用してCSRを作成する

1. 構成ユーティリティで、「構成」タブをクリックし、ナビゲーションペインで「**Citrix ADC Gateway**」をクリックします。
2. 詳細ペインの［はじめに］で、［**NetScaler ADC Gateway** ウィザード］をクリックします。
3. ページが表示されるまで、ウィザードの指示に従います。
4. をクリックし、フィールドに入力します。 注：完全修飾ドメイン名（FQDN）は、NetScaler Gateway ホスト名と同じである必要はありません。FQDN はユーザーログオンに使用されます。
5. をクリックして証明書をコンピューターに保存し、 をクリックします。
6. 設定を保存せずにNetScaler Gateway ウィザードを終了します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler ADC GUIを使用してCSRを作成する

また、NetScaler Gateway ウィザードを実行せずに、NetScaler ADC GUIを使用してCSRを作成することもできます。

1. > > に移動し、 を選択します。
2. 証明書の設定を完了し、 をクリックします。

証明書と秘密キーを作成したら、Thawte や Verisign などの CA に証明書を電子メールで送信します。

詳細な手順については、「 証明書署名要求の作成」を参照してください。

NetScaler Gateway に署名付き証明書をインストールする

認証局（CA）から署名付き証明書を受け取ったら、それをアプライアンスの秘密キーとペアにして、NetScaler Gateway に証明書をインストールします。

GUI を使用して、署名付き証明書と秘密キーをペアリングします

1. WinSCPなどのセキュアシェル（SSH）プログラムを使用して、証明書をNetScaler Gatewayのフォルダーnsconfig/sslにコピーします。
2. 構成ユーティリティの タブのナビゲーションペインで、 > を展開します。
3. ページで、 をクリックします。
4. 詳細ペインで、 をクリックします。
5. **に、証明書の名前を入力します。
6. で、 をクリックします。
7. 証明書に移動し、 をクリックし、 をクリックします。
8. で、 をクリックします。秘密キーの名前は、証明書署名要求 (CSR) と同じ名前です。秘密キーは、NetScaler Gateway の\ nsconfig\ sslディレクトリにあります。
9. 秘密キーを選択し、 をクリックします。
10. 証明書が PEM 形式の場合は、 に秘密鍵のパスワードを入力します。
11. 証明書の有効期限が切れるときの通知を構成する場合は、 を選択します。
12. に日数を入力し、 をクリックし、 をクリックします。

GUI を使用して証明書と秘密キーを仮想サーバーにバインドする

証明書と秘密キーのペアを作成してリンクしたら、それを仮想サーバーにバインドします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. 構成ユーティリティの［構成］タブのナビゲーションペインで、［**NetScaler Gateway**］> ［**仮想サーバー**］の順に展開します。
2. 詳細ペインで仮想サーバーを選択して、［**Open**］ をクリックします。
3. 「証明書」タブの「**使用可能**」で証明書を選択し、「**追加**」をクリックして、「**OK」**をクリックします。

CLI を使用して、証明書と秘密キーを仮想サーバーにバインドします

コマンドプロンプトで次を入力します：

```
bind ssl vserver <vServerName> -certkeyName <string> -ocspCheck
( Mandatory | Optional )
```

例:

```
bind ssl vserver TestClient -CertkeyName ag51.xm.nsi.test.com -CA
-ocspCheck Mandatory
```

注: デバイス証明書に OCSP チェックが必要ない場合、oscpCheck はオプションです。

GUI を使用して仮想サーバーからテスト証明書をバインド解除します

署名付き証明書をインストールしたら、仮想サーバーにバインドされているすべてのテスト証明書をバインド解除します。構成ユーティリティを使用して、テスト証明書のバインドを解除できます。

1. 構成ユーティリティの［構成］タブのナビゲーションペインで、［**NetScaler Gateway**］> ［**仮想サーバー**］の順に展開します。
2. 詳細ペインで仮想サーバーを選択して、［**Open**］ をクリックします。
3. タブの で、テスト証明書を選択し、 をクリックします。

中間証明書を構成する

中間証明書は、NetScaler Gateway（サーバー証明書）とルート証明書（ユーザーデバイスにインストールされている）の間にある証明書です。中間証明書はチェーンの一部です。

組織によっては、組織単位間の地理的分離の問題を解決するため、または組織の異なるセクションに異なる発行ポリシーを適用するために、証明書を発行する責任を委任しています。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

証明書の発行責任は、下位の認証局 (CA) を設定することで委任できます。CA は、独自の証明書（自己署名）に署名することも、別の認証局によって署名することもできます。X.509 標準には、CA の階層を設定するためのモデルが含まれています。このモデルでは、次の図に示すように、ルート CA は階層の最上位にあり、認証局による自己署名証明書です。ルート CA に直接従属する CA には、ルート認証局によって署名された CA 証明書があります。階層内の下位 CA の下にある CA には、下位 CA によって署名された CA 証明書があります。

図1：典型的なデジタル証明書チェーンの階層構造を示す X.509 モデル



サーバ証明書が自己署名証明書を使用して CA によって署名されている場合、証明書チェーンは、エンドエンティティ証明書とルート認証局という 2 つの証明書で構成されます。ユーザー証明書またはサーバー証明書が中間認証局によって署名されている場合、証明書チェーンは長くなります。

次の図は、最初の 2 つの要素がエンドエンティティ証明書（この場合は gwy01.company.com）と中間認証局の証明書（この順序で）であることを示しています。中間認証局の証明書の後には、その認証局の証明書が続きます。このリストは、リストの最後の証明書がルート認証局の証明書になるまで続きます。チェーン内の各証明書は、以前の証明書の ID を証明します。

図2：一般的なデジタル証明書チェーン



中間証明書をインストールする

1. 構成ユーティリティの タブのナビゲーションウィンドウで、 を展開し、 をクリックします。
2. 詳細ペインで、［Install］をクリックします。
3. に、証明書の名前を入力します。
4. の で、 をクリックし、一覧から または を選択します。
5. コンピューター（ローカル）またはNetScaler Gateway（アプライアンス）の証明書に移動します。
6. で、 を選択します。
7. をクリックし、 をクリックします。

NetScaler Gateway に中間証明書をインストールするときは、秘密キーまたはパスワードを指定する必要はありません。

証明書をアプライアンスにインストールしたら、証明書をサーバー証明書にリンクする必要があります。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

中間証明書をサーバー証明書にリンクする

1. 構成ユーティリティの タブのナビゲーションウィンドウで、 を展開し、 をクリックします。
2. 詳細ペインでサーバー証明書を選択し、 で をクリックします。
3. ［CA 証明書名］の横にあるリストから中間証明書を選択し、［OK］をクリックします。

認証にデバイス証明書を使用する

NetScaler Gateway では、デバイスIDを証明書の秘密キーにバインドできるデバイス証明書チェックがサポートされています。デバイス証明書チェックは、従来のまたは高度なエンドポイント分析 (EPA) ポリシーの一部として構成できます。クラシック EPA ポリシーでは、デバイス証明書は事前認証 EPA に対してのみ構成できます。

NetScaler Gateway は、エンドポイント分析スキャンの実行前、またはログオンページが表示される前に、デバイス証明書を検証します。エンドポイント分析を設定すると、エンドポイントスキャンが実行され、ユーザーデバイスが検証されます。デバイスがスキャンに合格し、NetScaler Gateway がデバイス証明書を検証すると、ユーザーはNetScaler Gatewayにログオンできます。

重要：

- デフォルトでは、Windows はデバイス証明書にアクセスするための管理者権限を義務付けています。
- 管理者以外のユーザーのデバイス証明書チェックを追加するには、VPN プラグインをインストールする必要があります。VPN プラグインのバージョンは、デバイス上の EPA プラグインと同じバージョンである必要があります。
- 複数の CA 証明書をゲートウェイに追加し、デバイス証明書を検証できます。
- NetScaler Gateway に2つ以上のデバイス証明書をインストールする場合、ユーザーは NetScaler Gateway へのログオンを開始するとき、またはエンドポイント分析スキャンの実行前に正しい証明書を選択する必要があります。
- デバイス証明書を作成するときは、X.509 証明書である必要があります。
- 中間 CA によって発行されたデバイス証明書がある場合は、中間 CA 証明書とルート CA 証明書の両方をバインドする必要があります。
- EPA クライアントは、ユーザーがマシン証明書ストアにアクセスできるローカル管理者権限を持っている必要があります。これがまれにしか発生しないため、回避策として、ローカルストアにアクセスできる完全なNetScaler Gatewayプラグインをインストールします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

デバイス証明書の作成の詳細については、以下を参照してください。

- Microsoft Web サイトのActive Directory 証明書サービス (AD CS) のネットワークデバイス登録サービス (NDES) 。
- AppleサポートWebサイトのDCE/RPC および Active Directory 証明書プロファイルペイロードを使用して、Microsoft証明機関に証明書を要求する方法 。
- iPad/iPhone 証明書の発行 Microsoft サポートブログの「ディレクトリサービスチームに尋ねる」を参照してください。
- Windows IT Pro の Webサイトでネットワークデバイス登録サービスをセットアップします 。
- Configuration Manager用の PKI 証明書の展開のステップバイステップ例：Microsoft System CenterのWindows Server 2008認証局 。

デバイス証明書を構成する手順

デバイス証明書を設定するには、次の手順を完了する必要があります。

- デバイス証明書発行者の証明機関証明書をNetScaler Gateway にインストールします。詳しくは、「 NetScaler Gateway への署名付き証明書のインストール」を参照してください。
- デバイス証明書発行者の証明機関証明書をNetScaler Gateway 仮想サーバーにバインドし、OCSPチェックを有効にします。詳しくは、「 NetScaler Gateway への署名付き証明書のインストール」を参照してください。
- デバイス証明書発行者の認証局証明書に OCSP（レスポンダ）を作成し、バインドします。詳細については、「 OCSP による証明書ステータスの監視」を参照してください。

仮想サーバーでデバイス証明書のチェックを有効にし、デバイス証明書発行者の認証局証明書をデバイス証明書のチェックリストに追加します。詳細については、 クラシック EPA ポリシーの仮想サーバーでのデバイス証明書チェックの有効化を参照してください。

Windows マシンでクライアント側の設定とデバイス証明書の検証を完了します。詳細については、「 Windows マシンでのデバイス証明書の検証」を参照してください。

注:

デバイス証明書 EPA チェックを利用するすべてのクライアントでは、マシンのシステム証明書ストアにデバイス証明書がインストールされている必要があります。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

クラシック EPA ポリシーの仮想サーバーでデバイス証明書チェックを有効にする

デバイス証明書を作成したら、NetScaler Gateway への既存の証明書のインポートとインストールの手順に従って、NetScaler Gateway に証明書をインストールします。

1. 「構成」タブで、「 **Citrix Gateway」>「仮想サーバー**」に移動します。
2. **NetScaler Gateway 仮想サーバーページで 、既存の仮想サーバー**を選択し、「 **編集**」をクリックします。
3. 「 **VPN 仮想サーバー** 」ページの「 **基本設定** 」セクションで、「 **編集**」をクリックします。
4. 認証を無効にするには、 チェックボックスをオフにします。
5. ボックスを選択して、デバイス証明書を有効にします
6. をクリックして、使用可能なデバイス証明書発行者の CA 証明書名をリストに追加します。
7. CA 証明書を仮想サーバーにバインドするには、 セクションの をクリックし、 をクリックして証明書を選択し、 をクリックします。

注：

高度な EPA ポリシーの仮想サーバーでデバイス証明書を有効にしてバインドする方法については、 EPA コンポーネントとしての nFactor でのデバイス証明書を参照してください。

Windows マシンでのデバイス証明書の検証

1. ブラウザーを開き、NetScaler Gateway FQDNにアクセスします。
2. Citrix エンドポイント分析（EPA）クライアントの実行を許可します。EPA がインストールされていない場合は、EPA をインストールします。

   Citrix EPAはデバイス証明書を実行して検証し、デバイス証明書EPAチェックに合格すると認証ページにリダイレクトされ、合格しなかった場合はEPAエラーページにリダイレクトされます。他の EPA チェックがある場合、EPA スキャンの結果は、設定された EPA チェックによって異なります。

クライアントでさらにデバッグするには、クライアントで次の EPA ログを調べます。 C:\Users\<User name>\ AppData\ Local\ Citrix\ AGEE\ nsepa.txt

注：

CRL によるデバイス証明書の検証はサポートされていません。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

既存の証明書をインポートしてインストールする

既存の証明書は、インターネットインフォメーションサービス（IIS）を実行している Windows ベースのコンピューター、または Secure Gateway を実行しているコンピューターからインポートできます。

証明書をエクスポートするときは、必ず秘密キーもエクスポートしてください。秘密キーをエクスポートできないことがあります。つまり、NetScaler Gateway に証明書をインストールできません。この場合は、証明書署名要求 (CSR) を使用して証明書を作成します。詳細については、「証明書署名要求の作成」を参照してください。

Windows から証明書と秘密キーをエクスポートすると、コンピューターは個人情報交換 (.pfx) ファイルを作成します。このファイルは、PKCS #12 証明書としてNetScaler Gateway にインストールされます。

Secure GatewayをNetScaler Gatewayに置き換える場合は、Secure Gatewayから証明書と秘密キーをエクスポートできます。Secure GatewayからNetScaler Gateway へのインプレース移行を行う場合は、アプリケーションとアプライアンスの完全修飾ドメイン名（FQDN）が同じである必要があります。Secure Gatewayから証明書をエクスポートすると、すぐにSecure Gatewayを廃棄し、NetScaler Gateway に証明書をインストールして、構成をテストします。Secure GatewayとNetScaler Gateway が同じFQDNを持つ場合、ネットワーク上で同時に実行することはできません。

Windows Server 2003 または Windows Server 2008 を使用している場合は、Microsoft管理コンソールを使用して証明書をエクスポートできます。詳細については、Windows オンラインヘルプを参照してください。

他のすべてのオプションはデフォルト値のままにし、パスワードを定義して、.pfx ファイルをコンピュータに保存します。証明書がエクスポートされたら、NetScaler Gateway にインストールします。

NetScaler Gateway に証明書と秘密キーをインストールするには

1. 構成ユーティリティで、［構成］タブをクリックし、ナビゲーションペインで［**NetScaler Gateway**］をクリックします。
2. 詳細ペインの［はじめに］で、［**NetScaler Gateway ウィザード**］をクリックします。
3. をクリックし、既存の仮想サーバーを選択して、 をクリックします。
4. 「**証明書オプション**」で、「**PKCS #12 (.pfx) ファイルのインストール**」を選択します。
5. で、 をクリックし、証明書に移動して、 をクリックします。
6. ((パスワード)) に、秘密キーのパスワードを入力します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

これは、証明書を PEM 形式に変換するときに使用したパスワードです。

7. 「 **次へ** 」をクリックして、他の設定を変更せずにCitrix Gateway ウィザードを終了します。

証明書がNetScaler Gateway にインストールされると、構成ユーティリティの［ **SSL**］**\ >［証明書］ノードに証明書が表示されます** 。

秘密キーを作成するには

1. 構成ユーティリティの タブのナビゲーションペインで、 をクリックします。
2. 詳細ペインの で、 をクリック します。
3. に、秘密キーの名前を入力するか、 をクリックして既存のファイルに移動します。
4. に、秘密キーのサイズを入力します。
5. **「公開指数値」**で、「F4」または「3」を選択します。

   RSA キーの公開指数値。これは暗号アルゴリズムの一部であり、RSA キーの作成に必要です。値は F4 (16 進数:0x10001) または 3 (16 進数:0x3) です。デフォルトは F4 です。
6. で、 または を選択します。証明書にはPEM形式を推奨します。
7. **PEM エンコーディングアルゴリズムで** 、DES または DES3 を選択 します。
8. と にパスワードを入力し、、 の順にクリックします。

   注:パスフレーズを割り当てるには、 が PEM で、エンコードアルゴリズムを選択する必要があります。

**構成ユーティリティでDSA秘密キーを作成するには、 をクリックし、RSA秘密キーを作成する手順に従います。

証明書失効リスト

認証局 (CA) は、証明書失効リスト (CRL) を発行します。CRL には、信頼できなくなった証明書に関する情報が含まれています。たとえば、アンがXYZ Corporationを離れたとします。会社は、Ann の証明書を CRL に配置して、彼女がそのキーでメッセージに署名するのを防ぐことができます。

同様に、秘密キーが侵害された場合、または証明書の有効期限が切れて新しい証明書が使用されている場合は、証明書を取り消すことができます。公開キーを信頼する前に、証明書が CRL に表示されていないことを確認してください。

NetScaler Gateway は、次の2つのCRLタイプをサポートしています。

- 失効した証明書または無効になった証明書を一覧表示する CRL

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Online Certificate Status Protocol (OSCP)、X.509 証明書の失効ステータスを取得するために使用されるインターネットプロトコル

CRL を追加するには、次の手順を実行します。

NetScaler Gateway アプライアンスでCRLを構成する前に、CRLファイルがアプライアンスにローカルに保存されていることを確認します。高可用性セットアップの場合、CRLファイルは両方のNetScaler Gateway アプライアンスに存在し、ファイルへのディレクトリパスは両方のアプライアンスで同じである必要があります。

CRL を更新する必要がある場合は、次のパラメータを使用できます。

- CRL名：NetScaler ADCに追加されるCRLの名前。最大 31 文字です。
- CRLファイル：NetScaler ADCに追加されるCRLファイルの名前。NetScaler ADCは、デフォルトで/var/netscaler/sslディレクトリでCRLファイルを検索します。最大 63 文字です。
- URL: 最大 127 文字
- ベース DN: 最大 127 文字
- バインド DN: 最大 127 文字
- パスワード:最大 31 文字
- 日数:最大 31

1. 構成ユーティリティの タブで、 を展開し、 をクリックします。
2. 詳細ペインで、［Add］ をクリックします。
3. ダイアログボックスで、次の値を指定します。
    - CRL名
    - CRL ファイル
    - フォーマット (オプション)
    - CA 証明書 (オプション)
4. **［Create］** をクリックしてから、 **［Close］** をクリックします。CRL 詳細ペインで、構成した CRL を選択し、画面の下部に表示される設定が正しいことを確認します。

GUI で LDAP または HTTP を使用して CRL 自動更新を設定するには、次の手順を実行します。

CRL は、CA によって定期的に、または場合によっては特定の証明書が失効した直後に生成および発行されます。NetScaler Gateway アプライアンスのCRLを定期的に更新して、無効な証明書で接続しようとするクライアントから保護することをお勧めします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler Gateway アプライアンスは、Webの場所またはLDAPディレクトリからCRLを更新できます。更新パラメータと Web ロケーションまたは LDAP サーバを指定する場合、コマンドの実行時に CRL がローカルハードディスクドライブに存在している必要はありません。最初の更新では、CRL File パラメーターで指定されたパスのローカルハードディスクドライブにコピーが格納されます。CRL を格納するためのデフォルトのパスは /var/netscaler/SSL です。

CRL リフレッシュパラメータ

CRL名

> NetScaler Gateway で更新されるCRLの名前。

CRL 自動更新を有効にする

> CRL 自動更新を有効または無効にします。

CA 証明書

> CRL を発行した CA の証明書。この CA 証明書は、アプライアンスにインストールする必要があります。NetScaler ADCは、証明書がインストールされているCAからのみCRLを更新できます。

方法

> Web サーバ（HTTP）または LDAP サーバから CRL リフレッシュを取得するプロトコル。可能な値:HTTP、LDAP。デフォルト:HTTP。

スコープ

> LDAP サーバーでの検索操作の範囲。指定したスコープが
>
> Base の場合、検索はベース DN と同じレベルになります。指定した範囲が
>
> One の場合、検索はベース DN の 1 レベル下まで拡張されます。

サーバーIP

> CRL の取得元の LDAP サーバの IP アドレス。IPv6 IP アドレスを使用するには、[IPv6] を選択します。

-

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ポート

LDAP または HTTP サーバが通信するポート番号。

URL

CRL の取得元の Web ロケーションの URL。

ベース DN

LDAP サーバが CRL 属性を検索するために使用するベース DN。

注：LDAPサーバーでCRLを検索するには、CA証明書の発行者名の代わりにベースDN属性を使用することをお勧めします。Issuer-Name フィールドは、LDAP ディレクトリ構造の DN と正確に一致しない場合があります。

バインド DN

バインド DN 属性は、LDAP リポジトリ内の CRL オブジェクトにアクセスするために使用されます。バインド DN 属性は、LDAP サーバの管理者クレデンシャルです。LDAP サーバへの不正アクセスを制限するには、このパラメータを設定します。

パスワード

LDAP リポジトリ内の CRL オブジェクトへのアクセスに使用される管理者パスワード。LDAP リポジトリへのアクセスが制限されている場合、つまり匿名アクセスが許可されていない場合、パスワードが必要です。

間隔

CRL リフレッシュを実行する必要がある間隔。CRL を瞬時に更新する場合は、間隔を NOW として指定します。可能な値:MONTHLY, DAILY, WEEKLY, NOW, NONE.

日数

CRL リフレッシュを実行する必要がある日。間隔が DAILYに設定されている場合、このオプションは使用できません。

-

© 1997–2026 Citrix Systems, Inc. All rights reserved.

時間

CRL リフレッシュを実行する必要がある正確な時刻（24 時間形式）。

バイナリ

LDAP ベースの CRL 取得モードをバイナリに設定します。可能な値:はい、いいえ。デフォルト:いいえ。

1. ナビゲーションウィンドウで、 を展開し、 をクリックします。
2. 更新パラメータを更新する設定済みの CRL を選択し、 をクリックします。
3. オプションを選択します。
4. グループで、次のパラメータの値を指定します。 注:アスタリスク (*) は、必須パラメータを示します。
   - 方法
   - バイナリ
   - スコープ
   - サーバーIP
   - ポート*
   - URL
   - ベース DN*
   - バインド DN
   - パスワード
   - 間隔
   - 日数
   - 時間
5. ［Create］ をクリックします。 ペインで、構成した CRL を選択し、画面の下部に表示される設定が正しいことを確認します。

OCSPで証明書のステータスを監視する

Online Certificate Status Protocol (OCSP) は、クライアント SSL 証明書の状態を判断するために使用されるインターネットプロトコルです。NetScaler Gateway は RFC 2560 で定義されているように OCSP をサポートしています。OCSP には、タイムリーな情報の点で、証明書失効リスト

© 1997–2026 Citrix Systems, Inc. All rights reserved.

(CRL) よりも大きな利点があります。クライアント証明書の最新の失効ステータスは、多額の資金や高額株式取引を含む取引で特に役立ちます。また、使用するシステムリソースとネットワークリソースも少なくなります。NetScaler Gateway のOCSPの実装には、要求のバッチ処理と応答のキャッシュが含まれます。

OCSPのNetScaler Gateway 実装

NetScaler Gateway アプライアンスでのOCSP検証は、NetScaler Gateway がSSLハンドシェイク中にクライアント証明書を受信したときに開始されます。証明書を検証するために、NetScaler Gateway はOCSP要求を作成し、OCSPレスポンダーに転送します。そのために、NetScaler Gateway は、クライアント証明書からOCSPレスポンダーのURLを抽出するか、ローカルで構成されたURLを使用します。NetScaler Gateway がサーバーからの応答を評価し、トランザクションを許可するか拒否するかを決定するまで、トランザクションは一時停止状態になります。サーバーからの応答が構成された時間を超えて遅延し、他のレスポンダーが構成されていない場合、NetScaler Gateway は、OCSPチェックをオプションまたは必須に設定したかどうかに応じて、トランザクションを許可するかエラーを表示します。NetScaler Gateway は、OCSP要求のバッチ処理とOCSP応答のキャッシュをサポートして、OCSPレスポンダーの負荷を軽減し、応答を高速化します。

OCSP リクエストのバッチング

NetScaler Gateway は、クライアント証明書を受信するたびに、OCSPレスポンダーに要求を送信します。OCSPレスポンダーの過負荷を避けるために、NetScaler Gateway は同じ要求で複数のクライアント証明書の状態を照会できます。リクエストのバッチ処理を効率的に実行するには、バッチの形成を待っている間に単一の証明書の処理が遅れないようにタイムアウトを定義する必要があります。

OCSP 応答キャッシュ

OCSP レスポンダから受信した応答をキャッシュすると、ユーザへの応答が速くなり、OCSP レスポンダの負荷が軽減されます。OCSPレスポンダーからクライアント証明書の失効ステータスを受信すると、NetScaler Gateway は事前定義された時間応答をローカルにキャッシュします。SSL ハンドシェイク中にクライアント証明書を受信すると、NetScaler Gateway はまずローカルキャッシュでこの証明書のエントリを確認します。まだ有効な（キャッシュタイムアウト制限内で）エントリが見つかると、そのエントリが評価され、クライアント証明書が受け入れられるか拒否されます。証明書が見つからない場合、NetScaler Gateway はOCSPレスポンダーに要求を送信し、構成された期間応答をローカルキャッシュに保存します。

OCSP 証明書ステータスの設定

オンライン証明書状態プロトコル (OCSP) を構成するには、OCSP レスポンダの追加、OCSP レスポンダを認証局 (CA) からの署名付き証明書にバインドし、証明書と秘密キーを Secure

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Sockets Layer (SSL) 仮想サーバーにバインドします。構成済みの OCSP レスポンダーに別の証明書と秘密キーをバインドする必要がある場合は、まずレスポンダーをバインド解除してから、レスポンダーを別の証明書にバインドする必要があります。

OCSP を設定するには

1. タブのナビゲーションウィンドウで、 を展開し、 をクリックします。
2. 詳細ペインで、［Add］ をクリックします。
3. に、プロファイルの名前を入力します。
4. に、OCSP レスポンダの Web アドレスを入力します。

   このフィールドは必須です。Web アドレスは 32 文字を超えることはできません。
5. OCSP応答をキャッシュするには、［キャッシュ］をクリックし、［タイムアウト］に、NetScaler Gateway が応答を保持する分数を入力します。
6. で、 をクリックします。
7. で、OCSP 要求のグループをバッチ処理する時間をミリ秒単位で指定します。

   指定できる値は 0 ～ 10000 です。デフォルトは1です。
8. ［時間スキューで生成される時間］に、アプライアンスが応答を確認または受け入れる必要があるときにNetScaler Gateway が使用できる時間を入力します。
9. OCSP レスポンダによる署名チェックを無効にする場合は、 で を選択します。

   信頼応答を有効にする場合は、ステップ 8 とステップ 9 をスキップします。
10. で、OCSP 応答の署名に使用する証明書を選択します。

    証明書が選択されていない場合、OCSP レスポンダがバインドされている CA が応答の検証に使用されます。
11. に、OCSP 応答を待機するミリ秒数を入力します。

    この時間には、バッチ処理遅延時間も含まれます。値の範囲は 0 ～ 120000 です。デフォルトは 2000 です。
12. で、OCSP 要求の署名に使用する証明書と秘密キーを選択します。証明書と秘密キーを指定しない場合、リクエストは署名されません。
13. 一度使用した番号を有効にするには`(nonce) extension`、 を選択します。
14. クライアント証明書を使用するには、 をクリックします。
15. ［Create］ をクリックしてから、［Close］ をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler Gateway の構成設定の管理

NetScaler Gateway の構成を変更すると、その変更はログファイルに保存されます。いくつかのタイプの構成設定を表示できます。

- 設定を保存しました。NetScaler Gateway に保存した設定を表示できます。
- 実行構成。構成したが、NetScaler Gateway の保存済み構成として保存していないアクティブな設定（仮想サーバーや認証ポリシーなど）を表示できます。
- 実行構成と保存済み構成の比較。NetScaler Gateway で実行されている構成と保存されている構成を並べて比較できます。

NetScaler Gateway の構成設定をクリアすることもできます。

重要：NetScaler Gateway の設定をクリアすると、証明書、仮想サーバー、およびポリシーが削除されます。構成をクリアしないことをお勧めします。

NetScaler Gateway 構成を保存する

NetScaler Gateway 上の現在の構成をネットワーク内のコンピューターに保存し、現在の実行構成を表示し、保存済み構成と実行構成を比較できます。

NetScaler Gateway で構成を保存するには

1. 構成ユーティリティの詳細ペインの上にある アイコンをクリックし、 をクリックします。

NetScaler Gateway で構成ファイルを表示して保存するには

保存される構成は、仮想サーバー、ポリシー、IPアドレス、ユーザー、グループ、証明書の設定など、NetScaler Gateway のログファイルに保存される設定です。

NetScaler Gateway で設定を構成すると、コンピューター上のファイルにその設定を保存できます。NetScaler Gateway ソフトウェアを再インストールする必要がある場合や、誤って一部の設定を削除した場合は、このファイルを使用して構成を復元できます。設定を復元する必要がある場合は、ファイルをNetScaler Gateway にコピーし、コマンドラインインターフェイスまたはWinSCPなどのプログラムを使用してアプライアンスを再起動し、ファイルをNetScaler Gatewayにコピーします。

1. 構成ユーティリティの タブのナビゲーションウィンドウで、 を展開し、 をクリックします。
2. 詳細ウィンドウの で、 をクリックします。
3. ダイアログボックスで、 をクリックし、ファイルに名前を付けて、 をクリックします。 注：ns.confというファイル名を使用してファイルを保存することをお勧めします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

現在の実行構成を表示するには

NetScaler Gateway への変更を保存せずに行われた変更は、実行構成と呼ばれます。これらの設定はNetScaler Gateway でアクティブになりますが、アプライアンスには保存されません。ポリシー、仮想サーバ、ユーザ、またはグループなどの追加設定を構成した場合は、実行構成でこれらの設定を表示できます。

1. 構成ユーティリティの タブのナビゲーションウィンドウで、 を展開し、 をクリックします。
2. 詳細ペインの で、 をクリックします。

保存済み構成と実行構成を比較するには

アプライアンスに保存されている設定を確認し、それらの設定を実行構成と比較できます。実行構成を保存するか、構成を変更するかを選択できます。

1. 構成ユーティリティの タブのナビゲーションウィンドウで、 を展開し、 をクリックします。
2. 詳細ペインの で、 をクリックします。

NetScaler Gateway の構成をクリアする

NetScaler Gateway の構成設定をクリアできます。次の 3 つのレベルからクリアする設定を選択できます。

重要：NetScaler Gateway の構成設定をクリアする前に、構成を保存することをお勧めします。

- ベーシック。システムIPアドレス、デフォルトゲートウェイ、マッピングされたIPアドレス、サブネットIPアドレス、DNS設定、ネットワーク設定、高可用性設定、管理パスワード、および機能およびモード設定を除くアプライアンスのすべての設定をクリアします。
- 拡張。システム IP アドレス、マッピング IP アドレス、サブネット IP アドレス、DNS 設定、および高可用性定義を除くすべての設定をクリアします。
- フル。設定を工場出荷時の設定に復元します。ただし、アプライアンスへのネットワーク接続を維持するために必要なシステムIP（NSIP）アドレスとデフォルトルートは除きます。

設定のすべてまたは一部をクリアすると、機能設定は工場出荷時のデフォルト設定に設定されます。

構成をクリアしても、NetScaler Gateway に保存されている証明書、ライセンスなどのファイルは削除されません。ファイル ns.conf は変更されません。構成をクリアする前に構成を保存する場合は、まず構成をコンピューターに保存します。構成を保存すると、NetScaler Gateway でns.conf ファイルを復元できます。ファイルをアプライアンスに復元してNetScaler Gateway を再起動すると、ns.confの構成設定が復元されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

rc.conf などの設定ファイルへの変更は元に戻されません。

高可用性ペアがある場合、両方のNetScaler Gateway アプライアンスが同じように変更されます。たとえば、1 つのアプライアンスの基本設定をクリアすると、変更は 2 番目のアプライアンスに伝播されます。

NetScaler Gateway の構成設定をクリアするには

1. 構成ユーティリティの タブのナビゲーションウィンドウで、 を展開し、 をクリックします。
2. 詳細ペインの で、 をクリックします。
3. で、クリアするレベルを選択し、 をクリックします。

NetScaler Gateway での証明書管理

NetScaler Gateway では、証明書を使用して安全な接続を作成し、ユーザーを認証します。

セキュアな接続を確立するには、接続の一端にサーバー証明書が必要です。接続のもう一方の端には、サーバ証明書を発行した認証局 (CA) のルート証明書が必要です。

- サーバー証明書。サーバー証明書は、サーバーの ID を証明します。NetScaler Gateway には、このタイプのデジタル証明書が必要です。
- ルート証明書。ルート証明書は、サーバ証明書に署名した CA を識別します。ルート証明書は認証局に属します。ユーザーデバイスは、サーバー証明書を検証するために、このタイプのデジタル証明書を必要とします。

ユーザーデバイス上の Web ブラウザとのセキュアな接続を確立すると、サーバーは証明書をデバイスに送信します。

ユーザーデバイスがサーバー証明書を受信すると、Internet Explorer などの Web ブラウザーは、証明書を発行した CA と、その CA がユーザーデバイスによって信頼されているかどうかを確認します。CA が信頼されていない場合、またはテスト証明書の場合、Web ブラウザはユーザに証明書を受け入れるか拒否するかを尋ねます（事実上、サイトへのアクセス権限を承認または拒否します）。

NetScaler Gateway では、次の3種類の証明書がサポートされています。

- 仮想サーバーにバインドされ、サーバーファームへの接続にも使用できるテスト証明書。NetScaler Gateway には、テスト証明書がプリインストールされています。
- CA によって署名され、秘密キーとペアになっている PEM または DER 形式の証明書。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 証明書と秘密キーの格納または転送に使用される PKCS #12 形式の証明書。PKCS #12 証明書は、通常、既存のWindows証明書からPFXファイルとしてエクスポートされ、NetScaler Gateway にインストールされます。

ThawteやVerisignなど、信頼できるCAによって署名された証明書を使用することをお勧めします。

証明書署名要求を作成する

SSLまたはTLSを使用してセキュリティで保護された通信を提供するには、NetScaler Gateway でサーバー証明書が必要です。証明書をNetScaler Gateway にアップロードする前に、証明書署名要求（CSR）と秘密キーを生成する必要があります。NetScaler Gateway ウィザードまたは構成ユーティリティに含まれている［証明書要求の作成］を使用して、CSRを作成します。証明書要求の作成により、署名用に認証局（CA）に電子メールで送信される.csr ファイルと、アプライアンスに残る秘密キーが作成されます。CA が証明書に署名し、指定した電子メールアドレスに証明書を返します。署名付き証明書を受け取ったら、NetScaler Gateway にインストールできます。CA から証明書を受け取ったら、証明書と秘密キーをペアにします。

重要：NetScaler Gateway ウィザードを使用してCSRを作成する場合は、ウィザードを終了し、CAが署名付き証明書を送信するのを待つ必要があります。証明書を受け取ったら、NetScaler Gateway ウィザードを再度実行して設定を作成し、証明書をインストールできます。NetScaler Gateway ウィザードについて詳しくは、「NetScaler Gateway ウィザードを使用した設定の構成」を参照してください。

NetScaler Gateway ウィザードを使用してCSRを作成する

1. 構成ユーティリティで、「構成」タブをクリックし、ナビゲーションペインで「**Citrix ADC Gateway**」をクリックします。
2. 詳細ペインの［はじめに］で、［**NetScaler ADC Gateway** ウィザード］をクリックします。
3. ページが表示されるまで、ウィザードの指示に従います。
4. をクリックし、フィールドに入力します。 注：完全修飾ドメイン名（FQDN）は、NetScaler Gateway ホスト名と同じである必要はありません。FQDN はユーザーログオンに使用されます。
5. をクリックして証明書をコンピューターに保存し、 をクリックします。
6. 設定を保存せずにNetScaler Gateway ウィザードを終了します。

NetScaler ADC GUIを使用してCSRを作成する

また、NetScaler Gateway ウィザードを実行せずに、NetScaler ADC GUIを使用してCSRを作成することもできます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. > > に移動し、 を選択します。
2. 証明書の設定を完了し、 をクリックします。

証明書と秘密キーを作成したら、Thawte や Verisign などの CA に証明書を電子メールで送信します。

詳細な手順については、「 証明書署名要求の作成」を参照してください。

NetScaler Gateway に署名付き証明書をインストールする

認証局（CA）から署名付き証明書を受け取ったら、それをアプライアンスの秘密キーとペアにして、NetScaler Gateway に証明書をインストールします。

GUI を使用して、署名付き証明書と秘密キーをペアリングします

1. WinSCPなどのセキュアシェル（SSH）プログラムを使用して、証明書をNetScaler Gatewayのフォルダーnsconfig/sslにコピーします。
2. 構成ユーティリティの タブのナビゲーションペインで、 > を展開します。
3. ページで、 をクリックします。
4. 詳細ペインで、 をクリックします。
5. **に、証明書の名前を入力します。
6. で、 をクリックします。
7. 証明書に移動し、 をクリックし、 をクリックします。
8. で、 をクリックします。秘密キーの名前は、証明書署名要求 (CSR) と同じ名前です。秘密キーは、NetScaler Gateway の\ nsconfig\ sslディレクトリにあります。
9. 秘密キーを選択し、 をクリックします。
10. 証明書が PEM 形式の場合は、 に秘密鍵のパスワードを入力します。
11. 証明書の有効期限が切れるときの通知を構成する場合は、 を選択します。
12. に日数を入力し、 をクリックし、 をクリックします。

GUI を使用して証明書と秘密キーを仮想サーバーにバインドする

証明書と秘密キーのペアを作成してリンクしたら、それを仮想サーバーにバインドします。

1. 構成ユーティリティの［構成］タブのナビゲーションペインで、［**NetScaler Gateway**］>［**仮想サーバー**］の順に展開します。
2. 詳細ペインで仮想サーバーを選択して、［**Open**］ をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. 「証明書」タブの「**使用可能**」で証明書を選択し、「**追加**」をクリックして、「**OK」**をクリックします。

CLI を使用して、証明書と秘密キーを仮想サーバーにバインドします

コマンドプロンプトで次を入力します：

```
bind ssl vserver <vServerName> -certkeyName <string> -ocspCheck
( Mandatory | Optional )
```

例:

```
bind ssl vserver TestClient -CertkeyName ag51.xm.nsi.test.com -CA
-ocspCheck Mandatory
```

注: デバイス証明書に OCSP チェックが必要ない場合、oscpCheck はオプションです。

GUI を使用して仮想サーバーからテスト証明書をバインド解除します

署名付き証明書をインストールしたら、仮想サーバーにバインドされているすべてのテスト証明書をバインド解除します。構成ユーティリティを使用して、テスト証明書のバインドを解除できます。

1. 構成ユーティリティの［構成］タブのナビゲーションペインで、［**NetScaler Gateway**］**>** ［**仮想サーバー**］の順に展開します。
2. 詳細ペインで仮想サーバーを選択して、［**Open**］ をクリックします。
3. タブの で、テスト証明書を選択し、 をクリックします。

中間証明書を構成する

中間証明書は、NetScaler Gateway（サーバー証明書）とルート証明書（ユーザーデバイスにインストールされている）の間にある証明書です。中間証明書はチェーンの一部です。

組織によっては、組織単位間の地理的分離の問題を解決するため、または組織の異なるセクションに異なる発行ポリシーを適用するために、証明書を発行する責任を委任しています。

証明書の発行責任は、下位の認証局 (CA) を設定することで委任できます。CA は、独自の証明書（自己署名）に署名することも、別の認証局によって署名することもできます。X.509 標準には、CA の階層を設定するためのモデルが含まれています。このモデルでは、次の図に示すように、ルート CA は階層の最上位にあり、認証局による自己署名証明書です。ルート CA に直接従属する

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CA には、ルート認証局によって署名された CA 証明書があります。階層内の下位 CA の下にある CA には、下位 CA によって署名された CA 証明書があります。

図1：典型的なデジタル証明書チェーンの階層構造を示す X.509 モデル



サーバ証明書が自己署名証明書を使用して CA によって署名されている場合、証明書チェーンは、エンドエンティティ証明書とルート認証局という 2 つの証明書で構成されます。ユーザー証明書またはサーバー証明書が中間認証局によって署名されている場合、証明書チェーンは長くなります。

次の図は、最初の 2 つの要素がエンドエンティティ証明書（この場合は gwy01.company.com）と中間認証局の証明書（この順序で）であることを示しています。中間認証局の証明書の後には、その認証局の証明書が続きます。このリストは、リストの最後の証明書がルート認証局の証明書になるまで続きます。チェーン内の各証明書は、以前の証明書の ID を証明します。

図2：一般的なデジタル証明書チェーン



中間証明書をインストールする

1. 構成ユーティリティの タブのナビゲーションウィンドウで、 を展開し、 をクリックします。
2. 詳細ペインで、［Install］をクリックします。
3. に、証明書の名前を入力します。
4. の で、 をクリックし、一覧から または を選択します。
5. コンピューター（ローカル）またはNetScaler Gateway（アプライアンス）の証明書に移動します。
6. で、 を選択します。
7. をクリックし、 をクリックします。

NetScaler Gateway に中間証明書をインストールするときは、秘密キーまたはパスワードを指定する必要はありません。

証明書をアプライアンスにインストールしたら、証明書をサーバー証明書にリンクする必要があります。

中間証明書をサーバー証明書にリンクする

1. 構成ユーティリティの タブのナビゲーションウィンドウで、 を展開し、 をクリックします。
2. 詳細ペインでサーバー証明書を選択し、 で をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. ［CA 証明書名］の横にあるリストから中間証明書を選択し、［OK］をクリックします。

認証にデバイス証明書を使用する

NetScaler Gateway では、デバイスIDを証明書の秘密キーにバインドできるデバイス証明書チェックがサポートされています。デバイス証明書チェックは、従来のまたは高度なエンドポイント分析 (EPA) ポリシーの一部として構成できます。クラシック EPA ポリシーでは、デバイス証明書は事前認証 EPA に対してのみ構成できます。

NetScaler Gateway は、エンドポイント分析スキャンの実行前、またはログオンページが表示される前に、デバイス証明書を検証します。エンドポイント分析を設定すると、エンドポイントスキャンが実行され、ユーザーデバイスが検証されます。デバイスがスキャンに合格し、NetScaler Gateway がデバイス証明書を検証すると、ユーザーはNetScaler Gatewayにログオンできます。

重要：

- デフォルトでは、Windows はデバイス証明書にアクセスするための管理者権限を義務付けています。
- 管理者以外のユーザーのデバイス証明書チェックを追加するには、VPN プラグインをインストールする必要があります。VPN プラグインのバージョンは、デバイス上の EPA プラグインと同じバージョンである必要があります。
- 複数の CA 証明書をゲートウェイに追加し、デバイス証明書を検証できます。
- NetScaler Gateway に2つ以上のデバイス証明書をインストールする場合、ユーザーは NetScaler Gateway へのログオンを開始するとき、またはエンドポイント分析スキャンの実行前に正しい証明書を選択する必要があります。
- デバイス証明書を作成するときは、X.509 証明書である必要があります。
- 中間 CA によって発行されたデバイス証明書がある場合は、中間 CA 証明書とルート CA 証明書の両方をバインドする必要があります。
- EPA クライアントは、ユーザーがマシン証明書ストアにアクセスできるローカル管理者権限を持っている必要があります。これがまれにしか発生しないため、回避策として、ローカルストアにアクセスできる完全なNetScaler Gatewayプラグインをインストールします。

デバイス証明書の作成の詳細については、以下を参照してください。

- Microsoft Web サイトのActive Directory 証明書サービス (AD CS) のネットワークデバイス登録サービス (NDES) 。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- AppleサポートWebサイトのDCE/RPC および Active Directory 証明書プロファイルペイロードを使用して、Microsoft証明機関に証明書を要求する方法 。
- iPad/iPhone 証明書の発行 Microsoft サポートブログの「ディレクトリサービスチームに尋ねる」を参照してください。
- Windows IT Pro の Webサイトでネットワークデバイス登録サービスをセットアップします 。
- Configuration Manager用の PKI 証明書の展開のステップバイステップ例：Microsoft System CenterのWindows Server 2008認証局 。

デバイス証明書を構成する手順

デバイス証明書を設定するには、次の手順を完了する必要があります。

- デバイス証明書発行者の証明機関証明書をNetScaler Gateway にインストールします。詳しくは、「 NetScaler Gateway への署名付き証明書のインストール」を参照してください。
- デバイス証明書発行者の証明機関証明書をNetScaler Gateway 仮想サーバーにバインドし、OCSPチェックを有効にします。詳しくは、「 NetScaler Gateway への署名付き証明書のインストール」を参照してください。
- デバイス証明書発行者の認証局証明書に OCSP（レスポンダ）を作成し、バインドします。詳細については、「 OCSP による証明書ステータスの監視」を参照してください。

仮想サーバーでデバイス証明書のチェックを有効にし、デバイス証明書発行者の認証局証明書をデバイス証明書のチェックリストに追加します。詳細については、 クラシック EPA ポリシーの仮想サーバーでのデバイス証明書チェックの有効化を参照してください。

Windows マシンでクライアント側の設定とデバイス証明書の検証を完了します。詳細については、「 Windows マシンでのデバイス証明書の検証」を参照してください。

注:

デバイス証明書 EPA チェックを利用するすべてのクライアントでは、マシンのシステム証明書ストアにデバイス証明書がインストールされている必要があります。

クラシック EPA ポリシーの仮想サーバーでデバイス証明書チェックを有効にする

デバイス証明書を作成したら、NetScaler Gateway への既存の証明書のインポートとインストールの手順に従って、NetScaler Gateway に証明書をインストールします。

1. 「構成」タブで、「 **Citrix Gateway」>「仮想サーバー**」に移動します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. **NetScaler Gateway 仮想サーバーページで 、既存の仮想サーバー**を選択し、「**編集**」をクリックします。
3. 「**VPN 仮想サーバー** 」ページの「**基本設定** 」セクションで、「**編集**」をクリックします。
4. 認証を無効にするには、 チェックボックスをオフにします。
5. ボックスを選択して、デバイス証明書を有効にします
6. をクリックして、使用可能なデバイス証明書発行者の CA 証明書名をリストに追加します。
7. CA 証明書を仮想サーバーにバインドするには、 セクションの をクリックし、 をクリックして証明書を選択し、 をクリックします。

注：

高度な EPA ポリシーの仮想サーバーでデバイス証明書を有効にしてバインドする方法については、 EPA コンポーネントとしての nFactor でのデバイス証明書を参照してください。

Windows マシンでのデバイス証明書の検証

1. ブラウザーを開き、NetScaler Gateway FQDNにアクセスします。
2. Citrix エンドポイント分析（EPA）クライアントの実行を許可します。EPA がインストールされていない場合は、EPA をインストールします。

   Citrix EPAはデバイス証明書を実行して検証し、デバイス証明書EPAチェックに合格すると認証ページにリダイレクトされ、合格しなかった場合はEPAエラーページにリダイレクトされます。他の EPA チェックがある場合、EPA スキャンの結果は、設定された EPA チェックによって異なります。

クライアントでさらにデバッグするには、クライアントで次の EPA ログを調べます。 C:\Users\<User name>\ AppData\ Local\ Citrix\ AGEE\ nsepa.txt

注：

CRL によるデバイス証明書の検証はサポートされていません。

既存の証明書をインポートしてインストールする

既存の証明書は、インターネットインフォメーションサービス（IIS）を実行している Windows ベースのコンピューター、または Secure Gateway を実行しているコンピューターからインポートできます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

証明書をエクスポートするときは、必ず秘密キーもエクスポートしてください。秘密キーをエクスポートできないことがあります。つまり、NetScaler Gateway に証明書をインストールできません。この場合は、証明書署名要求 (CSR) を使用して証明書を作成します。詳細については、「証明書署名要求の作成」を参照してください。

Windows から証明書と秘密キーをエクスポートすると、コンピューターは個人情報交換 (.pfx) ファイルを作成します。このファイルは、PKCS #12 証明書としてNetScaler Gateway にインストールされます。

Secure GatewayをNetScaler Gatewayに置き換える場合は、Secure Gatewayから証明書と秘密キーをエクスポートできます。Secure GatewayからNetScaler Gateway へのインプレース移行を行う場合は、アプリケーションとアプライアンスの完全修飾ドメイン名（FQDN）が同じである必要があります。Secure Gatewayから証明書をエクスポートすると、すぐにSecure Gatewayを廃棄し、NetScaler Gateway に証明書をインストールして、構成をテストします。Secure GatewayとNetScaler Gateway が同じFQDNを持つ場合、ネットワーク上で同時に実行することはできません。

Windows Server 2003 または Windows Server 2008 を使用している場合は、Microsoft管理コンソールを使用して証明書をエクスポートできます。詳細については、Windows オンラインヘルプを参照してください。

他のすべてのオプションはデフォルト値のままにし、パスワードを定義して、.pfx ファイルをコンピュータに保存します。証明書がエクスポートされたら、NetScaler Gateway にインストールします。

NetScaler Gateway に証明書と秘密キーをインストールするには

1. 構成ユーティリティで、［構成］タブをクリックし、ナビゲーションペインで［**NetScaler Gateway**］をクリックします。
2. 詳細ペインの［はじめに］で、［**NetScaler Gateway ウィザード**］をクリックします。
3. をクリックし、既存の仮想サーバーを選択して、 をクリックします。
4. 「**証明書オプション**」で、「**PKCS #12 (.pfx) ファイルのインストール**」を選択します。
5. で、 をクリックし、証明書に移動して、 をクリックします。
6. ((パスワード)) に、秘密キーのパスワードを入力します。

   これは、証明書を PEM 形式に変換するときに使用したパスワードです。
7. 「**次へ**」をクリックして、他の設定を変更せずにCitrix Gateway ウィザードを終了します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

証明書がNetScaler Gateway にインストールされると、構成ユーティリティの［**SSL**］**\ >［証明書］ノードに証明書が表示されます** 。

秘密キーを作成するには

1. 構成ユーティリティの タブのナビゲーションペインで、 をクリックします。
2. 詳細ペインの で、 をクリック します。
3. に、秘密キーの名前を入力するか、 をクリックして既存のファイルに移動します。
4. に、秘密キーのサイズを入力します。
5. **「公開指数値」**で、「F4」または「3」を選択します。

   RSA キーの公開指数値。これは暗号アルゴリズムの一部であり、RSA キーの作成に必要です。値は F4 (16 進数:0x10001) または 3 (16 進数:0x3) です。デフォルトは F4 です。
6. で、 または を選択します。証明書にはPEM形式を推奨します。
7. **PEM エンコーディングアルゴリズムで** 、DES または DES3 を選択 します。
8. と にパスワードを入力し、、 の順にクリックします。

   注:パスフレーズを割り当てるには、 が PEM で、エンコードアルゴリズムを選択する必要があります。

**構成ユーティリティでDSA秘密キーを作成するには、 をクリックし、RSA秘密キーを作成する手順に従います。

証明書失効リスト

認証局 (CA) は、証明書失効リスト (CRL) を発行します。CRL には、信頼できなくなった証明書に関する情報が含まれています。たとえば、アンがXYZ Corporationを離れたとします。会社は、Ann の証明書を CRL に配置して、彼女がそのキーでメッセージに署名するのを防ぐことができます。

同様に、秘密キーが侵害された場合、または証明書の有効期限が切れて新しい証明書が使用されている場合は、証明書を取り消すことができます。公開キーを信頼する前に、証明書が CRL に表示されていないことを確認してください。

NetScaler Gateway は、次の2つのCRLタイプをサポートしています。

- 失効した証明書または無効になった証明書を一覧表示する CRL
- Online Certificate Status Protocol (OSCP)、X.509 証明書の失効ステータスを取得するために使用されるインターネットプロトコル

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CRL を追加するには、次の手順を実行します。

NetScaler Gateway アプライアンスでCRLを構成する前に、CRLファイルがアプライアンスにローカルに保存されていることを確認します。高可用性セットアップの場合、CRLファイルは両方のNetScaler Gateway アプライアンスに存在し、ファイルへのディレクトリパスは両方のアプライアンスで同じである必要があります。

CRL を更新する必要がある場合は、次のパラメータを使用できます。

- CRL名：NetScaler ADCに追加されるCRLの名前。最大 31 文字です。
- CRLファイル：NetScaler ADCに追加されるCRLファイルの名前。NetScaler ADCは、デフォルトで/var/netscaler/sslディレクトリでCRLファイルを検索します。最大 63 文字です。
- URL: 最大 127 文字
- ベース DN: 最大 127 文字
- バインド DN: 最大 127 文字
- パスワード:最大 31 文字
- 日数:最大 31

1. 構成ユーティリティの タブで、 を展開し、 をクリックします。
2. 詳細ペインで、［Add］ をクリックします。
3. ダイアログボックスで、次の値を指定します。
    - CRL名
    - CRL ファイル
    - フォーマット (オプション)
    - CA 証明書 (オプション)
4. **［Create］** をクリックしてから、 **［Close］** をクリックします。CRL 詳細ペインで、構成した CRL を選択し、画面の下部に表示される設定が正しいことを確認します。

GUI で LDAP または HTTP を使用して CRL 自動更新を設定するには、次の手順を実行します。

CRL は、CA によって定期的に、または場合によっては特定の証明書が失効した直後に生成および発行されます。NetScaler Gateway アプライアンスのCRLを定期的に更新して、無効な証明書で接続しようとするクライアントから保護することをお勧めします。

NetScaler Gateway アプライアンスは、Webの場所またはLDAPディレクトリからCRLを更新できます。更新パラメータと Web ロケーションまたは LDAP サーバを指定する場合、コマンドの実行時に CRL がローカルハードディスクドライブに存在している必要はありません。最初の更新で

© 1997–2026 Citrix Systems, Inc. All rights reserved.

は、CRL File パラメーターで指定されたパスのローカルハードディスクドライブにコピーが格納されます。CRL を格納するためのデフォルトのパスは /var/netscaler/SSL です。

CRL リフレッシュパラメータ

CRL名

> NetScaler Gateway で更新されるCRLの名前。

CRL 自動更新を有効にする

> CRL 自動更新を有効または無効にします。

CA 証明書

> CRL を発行した CA の証明書。この CA 証明書は、アプライアンスにインストールする必要があります。NetScaler ADCは、証明書がインストールされているCAからのみCRLを更新できます。

方法

> Web サーバ（HTTP）または LDAP サーバから CRL リフレッシュを取得するプロトコル。可能な値:HTTP、LDAP。デフォルト:HTTP。

スコープ

> LDAP サーバーでの検索操作の範囲。指定したスコープが
>
> Base の場合、検索はベース DN と同じレベルになります。指定した範囲が
>
> One の場合、検索はベース DN の 1 レベル下まで拡張されます。

サーバーIP

> CRL の取得元の LDAP サーバの IP アドレス。IPv6 IP アドレスを使用するには、[IPv6] を選択します。

ポート

© 1997–2026 Citrix Systems, Inc. All rights reserved.

LDAP または HTTP サーバが通信するポート番号。

URL

CRL の取得元の Web ロケーションの URL。

ベース DN

LDAP サーバが CRL 属性を検索するために使用するベース DN。

注：LDAPサーバーでCRLを検索するには、CA証明書の発行者名の代わりにベースDN属性を使用することをお勧めします。Issuer-Name フィールドは、LDAP ディレクトリ構造の DN と正確に一致しない場合があります。

バインド DN

バインド DN 属性は、LDAP リポジトリ内の CRL オブジェクトにアクセスするために使用されます。バインド DN 属性は、LDAP サーバの管理者クレデンシャルです。LDAP サーバへの不正アクセスを制限するには、このパラメータを設定します。

パスワード

LDAP リポジトリ内の CRL オブジェクトへのアクセスに使用される管理者パスワード。LDAP リポジトリへのアクセスが制限されている場合、つまり匿名アクセスが許可されていない場合、パスワードが必要です。

間隔

CRL リフレッシュを実行する必要がある間隔。CRL を瞬時に更新する場合は、間隔を NOW として指定します。可能な値:MONTHLY, DAILY, WEEKLY, NOW, NONE.

日数

CRL リフレッシュを実行する必要がある日。間隔が DAILYに設定されている場合、このオプションは使用できません。

時間

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> CRL リフレッシュを実行する必要がある正確な時刻（24 時間形式）。

バイナリ

> LDAP ベースの CRL 取得モードをバイナリに設定します。可能な値:はい、いいえ。デフォルト:いいえ。

1. ナビゲーションウィンドウで、 を展開し、 をクリックします。
2. 更新パラメータを更新する設定済みの CRL を選択し、 をクリックします。
3. オプションを選択します。
4. グループで、次のパラメータの値を指定します。 注:アスタリスク (*) は、必須パラメータを示します。
   - 方法
   - バイナリ
   - スコープ
   - サーバーIP
   - ポート*
   - URL
   - ベース DN*
   - バインド DN
   - パスワード
   - 間隔
   - 日数
   - 時間
5. ［Create］ をクリックします。 ペインで、構成した CRL を選択し、画面の下部に表示される設定が正しいことを確認します。

OCSPで証明書のステータスを監視する

Online Certificate Status Protocol (OCSP) は、クライアント SSL 証明書の状態を判断するために使用されるインターネットプロトコルです。NetScaler Gateway は RFC 2560 で定義されているように OCSP をサポートしています。OCSP には、タイムリーな情報の点で、証明書失効リスト (CRL) よりも大きな利点があります。クライアント証明書の最新の失効ステータスは、多額の資金

© 1997–2026 Citrix Systems, Inc. All rights reserved.

や高額株式取引を含む取引で特に役立ちます。また、使用するシステムリソースとネットワークリソースも少なくなります。NetScaler Gateway のOCSPの実装には、要求のバッチ処理と応答のキャッシュが含まれます。

OCSPのNetScaler Gateway 実装

NetScaler Gateway アプライアンスでのOCSP検証は、NetScaler Gateway がSSLハンドシェイク中にクライアント証明書を受信したときに開始されます。証明書を検証するために、NetScaler Gateway はOCSP要求を作成し、OCSPレスポンダーに転送します。そのために、NetScaler Gateway は、クライアント証明書からOCSPレスポンダーのURLを抽出するか、ローカルで構成されたURLを使用します。NetScaler Gateway がサーバーからの応答を評価し、トランザクションを許可するか拒否するかを決定するまで、トランザクションは一時停止状態になります。サーバーからの応答が構成された時間を超えて遅延し、他のレスポンダーが構成されていない場合、NetScaler Gateway は、OCSPチェックをオプションまたは必須に設定したかどうかに応じて、トランザクションを許可するかエラーを表示します。NetScaler Gateway は、OCSP要求のバッチ処理とOCSP応答のキャッシュをサポートして、OCSPレスポンダーの負荷を軽減し、応答を高速化します。

OCSP リクエストのバッチング

NetScaler Gateway は、クライアント証明書を受信するたびに、OCSPレスポンダーに要求を送信します。OCSPレスポンダーの過負荷を避けるために、NetScaler Gateway は同じ要求で複数のクライアント証明書の状態を照会できます。リクエストのバッチ処理を効率的に実行するには、バッチの形成を待っている間に単一の証明書の処理が遅れないようにタイムアウトを定義する必要があります。

OCSP 応答キャッシュ

OCSP レスポンダから受信した応答をキャッシュすると、ユーザへの応答が速くなり、OCSP レスポンダの負荷が軽減されます。OCSPレスポンダーからクライアント証明書の失効ステータスを受信すると、NetScaler Gateway は事前定義された時間応答をローカルにキャッシュします。SSL ハンドシェイク中にクライアント証明書を受信すると、NetScaler Gateway はまずローカルキャッシュでこの証明書のエントリを確認します。まだ有効な（キャッシュタイムアウト制限内で）エントリが見つかると、そのエントリが評価され、クライアント証明書が受け入れられるか拒否されます。証明書が見つからない場合、NetScaler Gateway はOCSPレスポンダーに要求を送信し、構成された期間応答をローカルキャッシュに保存します。

OCSP 証明書ステータスの設定

オンライン証明書状態プロトコル (OCSP) を構成するには、OCSP レスポンダの追加、OCSP レスポンダを認証局 (CA) からの署名付き証明書にバインドし、証明書と秘密キーを Secure Sockets Layer (SSL) 仮想サーバーにバインドします。構成済みの OCSP レスポンダーに別の証明

© 1997–2026 Citrix Systems, Inc. All rights reserved.

書と秘密キーをバインドする必要がある場合は、まずレスポンダーをバインド解除してから、レスポンダーを別の証明書にバインドする必要があります。

OCSP を設定するには

1. タブのナビゲーションウィンドウで、 を展開し、 をクリックします。
2. 詳細ペインで、［Add］ をクリックします。
3. に、プロファイルの名前を入力します。
4. に、OCSP レスポンダの Web アドレスを入力します。

   このフィールドは必須です。Web アドレスは 32 文字を超えることはできません。
5. OCSP応答をキャッシュするには、［キャッシュ］をクリックし、［タイムアウト］に、NetScaler Gateway が応答を保持する分数を入力します。
6. で、 をクリックします。
7. で、OCSP 要求のグループをバッチ処理する時間をミリ秒単位で指定します。

   指定できる値は 0 ～ 10000 です。デフォルトは1です。
8. ［時間スキューで生成される時間］に、アプライアンスが応答を確認または受け入れる必要があるときにNetScaler Gateway が使用できる時間を入力します。
9. OCSP レスポンダによる署名チェックを無効にする場合は、 で を選択します。

   信頼応答を有効にする場合は、ステップ 8 とステップ 9 をスキップします。
10. で、OCSP 応答の署名に使用する証明書を選択します。

    証明書が選択されていない場合、OCSP レスポンダがバインドされている CA が応答の検証に使用されます。
11. に、OCSP 応答を待機するミリ秒数を入力します。

    この時間には、バッチ処理遅延時間も含まれます。値の範囲は 0 ～ 120000 です。デフォルトは 2000 です。
12. で、OCSP 要求の署名に使用する証明書と秘密キーを選択します。証明書と秘密キーを指定しない場合、リクエストは署名されません。
13. 一度使用した番号を有効にするには`(nonce) extension`、 を選択します。
14. クライアント証明書を使用するには、 をクリックします。
15. ［Create］ をクリックしてから、［Close］ をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler Gateway の構成をテストする

NetScaler Gateway で初期設定を構成したら、アプライアンスに接続して設定をテストできます。

NetScaler Gateway の設定をテストするには、ローカルユーザーアカウントを作成します。次に、仮想サーバの IP アドレスまたはアプライアンスの完全修飾ドメイン名（FQDN）のいずれかを使用して、Web ブラウザを開き、Web アドレスを入力します。たとえば、アドレスバーに「`https://my.company.com`」 または「`https://192.168.96.183`」と入力します 。

ログオン画面で、前に作成したユーザーアカウントのユーザー名とパスワードを入力します。ログオンすると、NetScaler Gateway プラグインをダウンロードしてインストールするように求められます。

NetScaler Gateway プラグインをインストールし、正常に接続すると、Access Interfaceが表示されます。Access Interfaceは、NetScaler Gateway のデフォルトのホームページです。

GUI を使用してユーザアカウントを作成する

1. 構成ユーティリティの タブのナビゲーションペインで、 > を展開し、 をクリックします。
2. 詳細ペインで、［Add］ をクリックします。
3. に、ユーザー名を入力します。
4. ローカル認証を使用する場合は、 チェックボックスをオフにします。LDAP や RADIUS などの外部認証タイプを使用したユーザの認証がデフォルトです。このチェックボックスをオフにすると、NetScaler Gateway はユーザーを認証します。
5. と に、ユーザーのパスワードを入力し、 をクリックし、 をクリックします。

構成ユーティリティを使用してユーザーを追加する場合、次のポリシーをユーザーにバインドできます：

- 承認
- トラフィック、セッション、監査
- ブックマーク
- イントラネットアプリケーション
- イントラネット IP アドレス

テストユーザーアカウントでのログオンに問題がある場合は、次の点を確認してください。

- 証明書の警告が表示された場合は、テスト証明書または無効な証明書がNetScaler Gateway にインストールされています。認証局（CA）によって署名された証明書がアプライアンスにイン

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ストールされている場合は、対応するルート証明書がユーザーデバイスにあることを確認します。

- CA 署名付き証明書を使用した場合は、署名付き証明書署名要求 (CSR) を使用してサイト証明書を正しく生成したこと、および CSR に入力された識別名 (DN) データが正確であることを確認します。また、ホスト名が署名付き証明書の IP アドレスと一致しないという問題もあります。構成された証明書の共通名が、構成された仮想サーバの IP アドレス情報に対応していることを確認します。
- ログオン画面が表示されない場合、または他のエラーメッセージが表示された場合は、セットアッププロセスを確認し、すべての手順を正しく実行し、すべてのパラメータを正確に入力したことを確認します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler Gatewayソフトウェアのアップグレード

新しいリリースが利用可能になったら、NetScaler Gateway にあるソフトウェアをアップグレードできます。アップデートは、Citrix Webサイトで確認できます。新しいリリースにアップグレードできるのは、アップデートのリリース時にNetScaler Gateway ライセンスがSubscription Advantage プログラムの下にある場合のみです。Subscription Advantage はいつでも更新できます。詳しくは、 Citrix サポートWebサイトを参照してください 。

アップグレードパスと互換性のある製品情報は、『 Citrix アップグレードガイド』にも記載されています。

最新のNetScaler Gateway メンテナンスリリースの詳細については、 Citrixナレッジセンターを参照してください。

ソフトウェアアップデートの確認

1. CitrixのWebサイトに移動します。
2. をクリックしてログオンします。
3. **［Downloads］**をクリックします。
4. ［ダウンロードの検索］で［ **NetScaler Gateway］**を選択します
5. **「ダウンロード・タイプの選択」**で、**「 製品ソフトウェア 」**を選択し、**「 検索」**をクリックします。 **仮想アプライアンスを選択して** 、NetScaler ADC VPXをダウンロードすることもできます。この場合、対象のハイパーバイザーを選択するためのページが開きます。
6. NetScaler Gateway ページで、［ **NetScaler ADC ゲートウェイ］または［アクセスゲートウェイ**］を展開します。
7. ダウンロードするアプライアンスソフトウェアのバージョンをクリックします。
8. ダウンロードするバージョンのアプライアンスソフトウェアページで、仮想アプライアンスを選択し、 をクリックします。
9. 画面の指示に従ってソフトウェアをダウンロードしてください。

ソフトウェアがコンピュータにダウンロードされたら、アップグレードウィザードまたはコマンドプロンプトを使用してソフトウェアをインストールできます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

アップグレードウィザードを使用してNetScaler Gatewayをアップグレードする

1. **構成ユーティリティの タブのナビゲーションペインで、** をクリックします。
2. 詳細ウィンドウで、 をクリックします。
3. **［Next］**をクリックして、ウィザードの指示に従います。

コマンドプロンプトを使用してNetScaler Gateway をアップグレードする

1. ソフトウェアをNetScaler Gateway にアップロードするには、WinSCPなどのセキュアFTPクライアントを使用してアプライアンスに接続します。
2. ソフトウェアをコンピュータからアプライアンスの /var/`nsinstall` ディレクトリにコピーします。
3. PuTTY などのセキュアシェル（SSH）クライアントを使用して、アプライアンスへの SSH 接続を開きます。
4. NetScaler Gateway にログオンします。
5. コマンドプロンプトで、次のように入力します。 `shell`
6. `nsinstall`ディレクトリに移動するには、コマンドプロンプトで次のように入力します。 `cd /var/nsinstall`
7. ディレクトリの内容を表示するには、次のように入力します。 `ls`
8. ソフトウェアをアンパックするには、tar —xvzf build_x_xx.tgz と入力します。build_x_xx.tgz は、アップグレードするビルドの名前です。
9. インストールを開始するには、コマンドプロンプトで次のように入力します。 `./installns`
10. インストールが完了したら、NetScaler Gateway を再起動します。

NetScaler Gateway の再起動後、インストールが正常に完了したことを確認するには、構成ユーティリティを起動します。アプライアンス上のNetScaler Gateway のバージョンが右上隅に表示されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler Gateway をダブルホップDMZに展開する

内部ネットワークを保護するために、3つのファイアウォールを使用する場合があります。3つのファイアウォールは、DMZを2つの段階にわけて、内部ネットワークにさらなるセキュリティを提供します。このネットワーク構成を、ダブルホップDMZと呼びます。

図1：ダブルホップDMZに展開されたNetScaler Gateway アプライアンス



注：

説明のため、前の例では、StoreFront、Web Interface、およびCitrix Virtual Apps を備えた3つのファイアウォールを使用したダブルホップ構成について説明していますが、DMZに1つのアプライアンスとセキュリティで保護されたネットワーク内の1つのアプライアンスを持つダブルホップDMZを使用することもできます。DMZ に 1 つのアプライアンスとセキュアネットワークに 1 つのアプライアンスを持つダブルホップ構成を設定する場合、第 3 のファイアウォールでポートを開く手順は無視できます。

ダブルホップDMZを構成して、Citrix StoreFront またはNetScaler Gateway プロキシと並行してインストールされたWeb Interfaceをサポートできます。ユーザーはCitrix Workspace アプリを使用して接続します。

注：

StoreFront を使用してダブルホップDMZにNetScaler Gateway を展開すると、Citrix Workspace アプリ用の電子メールベースの自動検出は機能しません。

ダブルホップ展開の仕組み

NetScaler Gateway アプライアンスをダブルホップDMZに展開して、Citrix Virtual Apps を実行しているサーバーへのアクセスを制御できます。ダブルホップ展開の接続は、次のように発生します：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- ユーザーは、Webブラウザーを使用し、Citrix Workspaceアプリを使用して公開アプリケーションを選択して、最初のDMZでNetScaler Gateway に接続します。
- Citrix Workspace アプリがユーザーデバイスで起動します。ユーザーはNetScaler Gateway に接続して、セキュリティで保護されたネットワークのサーバーファームで実行されている公開アプリケーションにアクセスします。

  注： Secure HubとNetScaler Gateway プラグインは、ダブルホップDMZ展開ではサポートされていません。Citrix Workspace アプリのみがユーザー接続に使用されます。
- 最初のDMZのNetScaler Gateway は、ユーザー接続を処理し、SSL VPNのセキュリティ機能を実行します。このNetScaler Gateway は、ユーザー接続を暗号化し、ユーザーの認証方法を決定し、内部ネットワーク内のサーバーへのアクセスを制御します。
- 2番目のDMZのNetScaler Gatewayは、NetScaler Gatewayプロキシデバイスとして機能します。このNetScaler Gateway により、ICAトラフィックが2番目のDMZを通過して、サーバーファームへのユーザー接続を完了できます。最初のDMZのNetScaler Gateway と内部ネットワークのSecure Ticket Authority（STA）間の通信も、2番目のDMZのNetScaler Gatewayを介してプロキシされます。

NetScaler Gateway は、IPv4接続とIPv6接続をサポートしています。構成ユーティリティを使用して IPv6 アドレスを構成できます。

次の表に、さまざまなICA機能のダブルホップ展開サポートを示します。

ICA機能	ダブルホップサポート
SmartAccess	はい
SmartControl	はい
Enlightened Data Transport（EDT）	はい
HDX Insight	はい
ICA セッション信頼性 (ポート 2598)	はい
ICA セッションの移行	はい
ICA セッションタイムアウト	はい
マルチストリームICA	はい (TCP のみ)
Framehawk	いいえ

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ICA機能	ダブルホップサポート
UDP オーディオ	いいえ

ダブルホップ DMZ 展開の準備

ダブルホップ DMZ 配置を設定するときに適切に準備し、不要な問題を回避するには、次の質問に答える必要があります：

- 負荷分散をサポートしたいですか?
- ファイアウォールではどのポートを開く必要がありますか。
- SSL証明書はいくつ必要ですか？
- 展開を開始する前に必要なコンポーネントは何ですか?

このセクションのトピックには、環境に応じてこれらの質問に答えるのに役立つ情報が含まれています。

展開を開始するために必要なコンポーネント

ダブルホップ DMZ 展開を開始する前に、次のコンポーネントがあることを確認します：

- 少なくとも2つのNetScaler Gateway アプライアンス（DMZごとに1つ）が使用可能である必要があります。
- Citrix Virtual Apps を実行するサーバーは、内部ネットワークにインストールされ、動作している必要があります。
- Web InterfaceまたはStoreFront を2番目のDMZにインストールし、内部ネットワークのサーバーファームで動作するように構成する必要があります。
- 少なくとも、最初のDMZのNetScaler Gateway に1つのSSLサーバー証明書がインストールされている必要があります。この証明書により、WebブラウザーとNetScaler Gateway へのユーザー接続が暗号化されます。

  ダブルホップ DMZ 展開内の他のコンポーネント間で発生する接続を暗号化する場合は、追加の証明書が必要です：

ダブルホップ DMZ 展開での通信フロー

ダブルホップDMZ展開に関連する構成の問題を理解するには、ダブルホップDMZ展開内のさまざまなNetScaler Gateway およびCitrix Virtual Apps コンポーネントがユーザー接続をサポートする

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ためにどのように通信するかについての基本的な理解が必要です。StoreFrontとWeb Interfaceの接続プロセスは同じです。

ユーザー接続プロセスは 1 つの連続したフローで行われますが、このプロセスには次の高レベルのステップが含まれます。

- ユーザーを認証する
- セッションチケットを作成する
- Citrix Workspace アプリを起動する
- 接続を完了する

次の図は、StoreFront またはWeb Interfaceへのユーザー接続プロセスで発生する手順を示しています。セキュリティで保護されたネットワークでは、Citrix Virtual Apps を実行しているコンピューターは、Secure Ticket Authority（STA）、XMLサービス、および公開アプリケーションも実行しています。



接続プロセス

ユーザの認証は、ダブルホップ DMZ 展開におけるユーザ接続プロセスの最初のステップです。

次の図は、この展開でのユーザー接続プロセスを示しています。



ユーザー認証段階では、次の基本プロセスが発生します。

1. ユーザーがNetScaler Gatewayの `<https://www.ng.wxyco.com>` などのアドレスをWebブラウザーで入力して、最初のDMZでNetScaler Gateway に接続します。NetScaler Gateway でログオンページ認証を有効にした場合、NetScaler Gateway はユーザーを認証します。
2. 最初のDMZのNetScaler Gateway が要求を受信します。
3. NetScaler Gateway は、Webブラウザー接続をWeb Interfaceにリダイレクトします。
4. Web Interfaceは、内部ネットワークのサーバーファームで実行されているCitrix XMLサービスにユーザー資格情報を送信します。
5. Citrix XMLサービスはユーザーを認証します。
6. XML サービスは、ユーザーがアクセスを許可されている公開アプリケーションのリストを作成し、このリストを Web Interface に送信します。

   注：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- NetScaler Gateway で認証を有効にすると、アプライアンスはNetScaler Gateway のログオンページをユーザーに送信します。ユーザーがログオンページで認証情報を入力すると、アプライアンスがユーザーを認証します。その後、NetScaler Gateway はユーザーの資格情報をWeb Interfaceに返します。
- 認証を有効にしない場合、NetScaler Gateway は認証を実行しません。アプライアンスは Web インターフェイスに接続し、Web インターフェイスのログオンページを取得し、Web インターフェイスのログオンページをユーザーに送信します。ユーザーはWeb Interfaceのログオンページで認証資格情報を入力し、NetScaler Gateway はユーザーの資格情報を Web Interfaceに返します。

セッションチケットの作成は、ダブルホップ DMZ 展開におけるユーザ接続プロセスの第 2 段階です。

セッションチケットの作成段階では、次の基本プロセスが発生します。

7. Web Interfaceは、内部ネットワーク内のXMLサービスおよびSecure Ticket Authority（STA）の両方と通信し、ユーザーがアクセスを許可されている公開アプリケーションごとにセッションチケットを生成します。セッションチケットには、公開アプリケーションをホストするCitrix Virtual Apps を実行しているコンピューターのエイリアスアドレスが含まれています。
8. STA は、公開アプリケーションをホストするサーバーの IP アドレスを保存します。次に、STA は要求されたセッションチケットを Web Interface に送信します。各セッションチケットには、公開アプリケーションをホストするサーバーのIPアドレスを表すエイリアスが含まれていますが、実際のIPアドレスは含まれません。
9. Web Interface は、公開アプリケーションごとに ICA ファイルを生成します。ICA ファイルには、STA によって発行されたチケットが含まれています。次に、Web Interface は、公開アプリケーションへのリンクの一覧を Web ページを作成して入力し、この Web ページをユーザーデバイス上の Web ブラウザに送信します。

   Citrix Workspace アプリの起動は、ダブルホップDMZ展開におけるユーザー接続プロセスの第3段階です。基本的なプロセスは次のとおりです。

10. ユーザーが Web Interface で公開アプリケーションへのリンクをクリックします。Web Interfaceは、その公開アプリケーションのICAファイルをユーザーデバイスのブラウザに送信します。

    ICAファイルには、WebブラウザーにReceiverを起動するように指示するデータが含まれています。

    ICAファイルには、最初のDMZのNetScaler Gateway の完全修飾ドメイン名（FQDN）またはドメインネームシステム（DNS）名も含まれています。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

11. WebブラウザでReceiverが起動し、ユーザーはICAファイル内のNetScaler Gateway名を使用して、最初のDMZでNetScaler Gatewayに接続します。最初のSSL/TLSハンドシェークは、NetScaler Gateway を実行しているサーバーのアイデンティティを確立するために発生します。

    接続の完了は、ダブルホップ DMZ 展開におけるユーザ接続プロセスの第 4 段階であり、最後の段階です。

    接続完了段階では、次の基本プロセスが発生します。

    - ユーザーが Web Interface で公開アプリケーションへのリンクをクリックします。
    - Webブラウザーは、Web Interfaceによって生成されたICAファイルを受信し、Citrix Workspace アプリを起動します。 注：ICAファイルには、Citrix Workspace アプリを起動するようにWebブラウザーに指示するコードが含まれています。
    - Citrix Workspace アプリは、最初のDMZでNetScaler GatewayへのICA接続を開始します。
    - 最初のDMZのNetScaler Gatewayは、内部ネットワーク内のSecure Ticket Authority（STA）と通信して、セッションチケットのエイリアスアドレスを、Citrix Virtual Apps またはStoreFront を実行しているコンピューターの実際のIPアドレスに解決します。この通信は、NetScaler Gateway プロキシによって2番目のDMZを介してプロキシされます。
    - 最初のDMZのNetScaler Gatewayは、Citrix Workspace アプリへのICA接続を完了します。
    - Citrix Workspace アプリは、両方のNetScaler Gateway アプライアンスを介して、内部ネットワーク上のCitrix Virtual Apps を実行しているコンピューターと通信できるようになりました。

    ユーザー接続プロセスを完了するための詳細な手順は次のとおりです。

12. Citrix Workspace アプリは、公開アプリケーションのSTAチケットを最初のDMZでNetScaler Gateway に送信します。
13. 最初のDMZのNetScaler Gateway は、チケットの検証のために内部ネットワークのSTAに接続します。STAに接続するために、NetScaler Gatewayは、2番目のDMZのNetScaler Gatewayプロキシへの SSL接続を備えたSOCKSまたはSOCKSを確立します。
14. 2番目のDMZのNetScaler Gateway プロキシは、内部ネットワークのSTAにチケット検証要求を渡します。STAはチケットを検証し、公開アプリケーションをホストするCitrix Virtual Apps を実行しているコンピューターにチケットをマッピングします。
15. STAは、2番目のDMZのNetScaler Gatewayプロキシに応答を送信します。この応答は、最初のDMZでNetScaler Gatewayに渡されます。この応答により、チケットの検証が完了し、公開アプリケーションをホストするコンピュータのIPアドレスが含まれます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

16. 最初のDMZのNetScaler Gateway は、Citrix Virtual Apps サーバーのアドレスをユーザー接続パケットに組み込み、このパケットを2番目のDMZのNetScaler Gateway プロキシに送信します。
17. 2番目のDMZのNetScaler Gateway プロキシは、接続パケットで指定されたサーバーに接続要求を行います。
18. サーバーは、2番目のDMZのNetScaler Gateway プロキシに応答します。2番目のDMZのNetScaler Gateway プロキシは、この応答を最初のDMZのNetScaler Gateway に渡して、最初のDMZのサーバーとNetScaler Gatewayの間の接続を完了します。
19. 最初のDMZのNetScaler Gateway は、最終的な接続パケットをユーザーデバイスに渡すことによって、ユーザーデバイスとのSSL/TLSハンドシェイクを完了します。ユーザーデバイスからサーバーへの接続が確立されます。
20. ICAトラフィックは、ユーザーデバイスとサーバーの間で、最初のDMZのNetScaler Gateway、2番目のDMZのNetScaler Gatewayプロキシを介して流れます。

ダブルホップDMZでのNetScaler Gateway のインストールと構成

ダブルホップDMZにNetScaler Gateway を展開するには、いくつかの手順を完了する必要があります。手順には、両方の DMZ へのアプライアンスのインストールと、アプライアンスのユーザーデバイス接続の設定が含まれます。

最初のDMZにNetScaler Gatewayをインストールする

最初のDMZにNetScaler Gateway をインストールするには、「ハードウェアのインストール」の手順に従います。

最初のDMZに複数のNetScaler Gateway アプライアンスをインストールする場合は、ロードバランサーの背後にアプライアンスを展開できます。

最初のDMZでNetScaler Gatewayを構成する

ダブルホップDMZ展開では、最初のDMZの各NetScaler Gateway を構成して、2番目のDMZのStoreFront またはWeb Interfaceのいずれかに接続をリダイレクトする必要があります。

StoreFront またはWeb Interfaceへのリダイレクトは、NetScaler Gateway グローバルサーバーレベルまたは仮想サーバーレベルで実行されます。NetScaler Gateway を介してWeb Interfaceに接続するには、Web Interfaceへのリダイレクトが有効になっているNetScaler Gateway ユーザーグループにユーザーを関連付ける必要があります。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

第2のDMZにNetScaler Gatewayをインストールする

2番目のDMZのNetScaler Gateway アプライアンスは、ICAおよびSecure Ticket Authority（STA）トラフィックを2番目のDMZでプロキシするため、NetScaler Gateway プロキシと呼ばれます。ハードウェアをインストールして、 各NetScaler Gateway アプライアンスを2番目のDMZにインストールします。

このインストール手順を使用して、2 番目の DMZ に他のアプライアンスをインストールできます。

2番目のDMZにNetScaler Gateway アプライアンスをインストールした後、次の設定を構成します：

- NetScaler Gateway プロキシで仮想サーバーを構成します。
- 第1および第2DMZのNetScaler Gateway アプライアンスが相互に通信するように構成します。
- 2番目のDMZのNetScaler Gateway をグローバルに、または仮想サーバーにバインドします。
- 第1 DMZのアプランスでSTAを構成します。
- ファイアウォールでDMZを分離して、ポートを開きます。
- アプライアンスに証明書をインストールします。

NetScaler Gateway プロキシの仮想サーバーの設定を構成する

NetScaler Gateway アプライアンス間の接続を許可するには、NetScaler Gateway プロキシ上の仮想サーバーでダブルホップを有効にします。

ユーザーが接続すると、NetScaler Gateway アプライアンスはユーザーを認証し、プロキシアプライアンスへの接続をプロキシします。最初のDMZのNetScaler Gateway で、2番目のDMZのNetScaler Gatewayと通信するように仮想サーバーを構成します。NetScaler Gateway プロキシで認証またはポリシーを構成しないでください。仮想サーバーで認証を無効にすることをお勧めします。

GUIを使用してNetScaler Gateway プロキシ上の仮想サーバーでダブルホップを有効にするには

1. **構成 > NetScaler Gateway > 仮想サーバーに移動します。**
2. 仮想サーバを選択し、 をクリックします。
3. セクションで、 アイコンをクリックし、 をクリックします。
4. を選択します。



© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. ［OK］ をクリックします。

GUIを使用してNetScaler Gateway プロキシ上の仮想サーバーで認証を無効にするには

1. **構成 > NetScaler Gateway > 仮想サーバーに移動します。**
2. 仮想サーバを選択し、 をクリックします。
3. セクションで、 アイコンをクリックし、 をクリックします。



4. ** チェックボックスをオフにします。



5. ［OK］ をクリックします。

アプライアンスのプロキシと通信するようにアプライアンスを設定する

ダブルホップDMZにNetScaler Gateway を展開する場合は、最初のDMZでNetScaler Gateway を構成して、2番目のDMZのNetScaler Gateway プロキシと通信する必要があります。

2 番目の DMZ に複数のアプライアンスを展開する場合は、最初の DMZ の各アプライアンスが 2 番目の DMZ のすべてのプロキシアプライアンスと通信するように設定します。

注:IPv6 を使用する場合は、構成ユーティリティを使用してネクストホップサーバーを構成します。これを行うには、 ［NetScaler Gateway］>［リソース］の順に展開し、［ ネクストホップサーバー］をクリックします。次の手順の手順に従って、 チェックボックスをオンにします。

NetScaler Gateway プロキシと通信するようにNetScaler Gateway を構成するには

1. 構成ユーティリティの［構成］タブで、［NetScaler Gateway］>［リソース］の順に展開し、［ネクストホップサーバー］をクリックします。
2. 詳細ペインで、［Add］ をクリックします。
3. に、最初のNetScaler Gateway の名前を入力します。
4. に、2番目のDMZにあるNetScaler Gateway プロキシの仮想サーバーIPアドレスを入力します。
5. にポート番号を入力し、、 の順にクリックします。443 などのセキュアなポートを使用している場合は、 を選択します。

最初のDMZにインストールされている各NetScaler Gateway を、2番目のDMZにインストールされているすべてのNetScaler Gateway プロキシアプライアンスと通信するように構成する必要があります。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler Gateway プロキシの設定を構成したら、NetScaler Gateway グローバルのネクストホップサーバーまたは仮想サーバーにポリシーをバインドします。

NetScaler Gateway ネクストホップサーバーをグローバルにバインドするには

1. 構成ユーティリティの［構成］タブで、［NetScaler Gateway］>［リソース］の順に展開し、［ネクストホップサーバー］をクリックします。
2. 詳細ウィンドウで、ネクストホップサーバーを選択し、 で を選択します。
3. ［ネクストホップサーバーのグローバルバインドの構成］ダイアログボックスの［ネクストホップサーバー名］でプロキシアプライアンスを選択し、［OK］をクリックします。

NetScaler Gateway ネクストホップサーバーを仮想サーバーにバインドするには

1. 構成ユーティリティの［構成］タブで、［NetScaler Gateway］を展開し、［仮想サーバー］をクリックします。
2. 詳細ペインで仮想サーバーを選択し、 をクリックします。
3. ［公開アプリケーション］タブの［ネクストホップサーバー］で項目をクリックし、［OK］をクリックします。

タブからネクストホップサーバーを追加することもできます。

STAおよびICAトラフィックを処理するようにNetScaler Gatewayを構成する

ダブルホップDMZにNetScaler Gateway を展開する場合は、最初のDMZでNetScaler Gateway を構成して、Secure Ticket Authority（STA）およびICAトラフィックとの通信を適切に処理する必要があります。STA を実行しているサーバは、グローバルにバインドすることも、仮想サーバにバインドすることもできます。

STA を構成したら、STA をグローバルにバインドすることも、仮想サーバにバインドすることもできます。

STA をグローバルに設定してバインドするには、次の手順を実行します。

1. GUIの［構成］タブで、［ **NetScaler Gateway** ］を展開し、［ **グローバル設定**］をクリックします。
2. 詳細ペインの で、 **Secure Ticket Authority が使用する STA サーバーのバインド/バインド解除をクリックします。**
3. ダイアログボックスで、 をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. ダイアログボックスの に、STAを実行しているサーバーへのパス (http://mycompany.comまたは`<http://ipAddress>`など) を入力し、 をクリックします。

STA を構成して仮想サーバにバインドするには

1. GUIの［構成］タブで、［ **NetScaler Gateway** ］を展開し、［ **仮想サーバー**］をクリックします。
2. 詳細ペインで仮想サーバーを選択し、 をクリックします。
3. 「 **公開アプリケーション** 」タブの「 **Secure Ticket Authority**」で、「 **追加**」をクリックします。
4. ダイアログボックスの に、STAを実行しているサーバーへのパス (`<http://mycompany.com>`または`<http://ipAddress>`など) を入力し、 をクリックします。

注：

VPN 仮想サーバーが同じネクストホップ仮想サーバーと STA サーバーを共有している場合、同じネクストホップ仮想サーバーを共有する仮想サーバーから共通 STA サーバーがバインド解除されると、接続がリセットされます。

ファイアウォールの適切なポートを開きます

ダブルホップ DMZ 展開に関連するさまざまなコンポーネント間で発生するさまざまな接続をサポートするために、ファイアウォールで適切なポートが開いていることを確認する必要があります。接続プロセスの詳細については、 ダブルホップ DMZ 展開での通信フローを参照してください 。

次の図は、ダブルホップ DMZ 展開で使用できる一般的なポートを示しています。



次の表に、最初のファイアウォールを介して発生する接続と、その接続をサポートするために開く必要があるポートを示します。

最初のファイアウォールを介した接続	使用ポート
インターネットからのWebブラウザは、最初のDMZでNetScaler Gateway に接続します。 **注：** NetScaler Gateway には、ポート80で確立された接続をセキュアポートにリダイレクトするオプションがあります。NetScaler Gateway でこのオプションを有効にすると、最初のファイアウォールを介してポート80を開くことができます。ユーザーがポート80で	最初のファイアウォールを介して TCP ポート 443 を開きます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

最初のファイアウォールを介した接続	使用ポート
NetScaler Gateway に暗号化されていない接続を行うと、NetScaler Gateway は自動的に安全なポートに接続をリダイレクトします。	
インターネットからのCitrix Workspace アプリは、最初のDMZでNetScaler Gatewayに接続します。	最初のファイアウォールを介して TCP ポート 443 を開きます。

次の表は、2 番目のファイアウォールを介して発生する接続と、接続をサポートするために開く必要があるポートを示しています。

第 2 ファイアウォール経由の接続	使用ポート
最初のDMZのNetScaler Gateway は、2番目のDMZのWeb Interfaceに接続します。	セキュリティで保護されていない接続の場合は TCP ポート 80、2 番目のファイアウォールを介したセキュアな接続の場合は TCP ポート 443 を開きます。
最初のDMZのNetScaler Gatewayは、2番目のDMZのNetScaler Gatewayに接続します。	TCP ポート 443 を開いて、2 番目のファイアウォールを介した安全な SOCKS 接続を確立します。
最初のDMZでNetScaler Gateway で認証を有効にした場合、このアプライアンスは内部ネットワークの認証サーバーに接続する必要がある場合があります。	認証サーバが接続をリッスンする TCP ポートを開きます。例としては、RADIUS 用のポート 1812、LDAP 用のポート 389 などがあります。

次の表に、第 3 のファイアウォールを介して発生する接続と、接続をサポートするために開く必要があるポートを示します。

第 3 ファイアウォール経由の接続	使用ポート
StoreFront または2番目のDMZのWeb Interfaceは、内部ネットワークのサーバーでホストされているXMLサービスに接続します。	セキュアでない接続の場合はポート 80 を、3 番目のファイアウォールを介したセキュアな接続にはポート 443 を開きます。
2番目のDMZのStoreFront またはWeb Interfaceは、内部ネットワークのサーバーでホストされているSecure Ticket Authority（STA）に接続します。	セキュアでない接続の場合はポート 80 を、3 番目のファイアウォールを介したセキュアな接続にはポート 443 を開きます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

第 3 ファイアウォール経由の接続	使用ポート
2番目のDMZのNetScaler Gateway は、セキュアネットワークに存在するSTAに接続します。	セキュアでない接続の場合はポート 80 を、3番目のファイアウォールを介したセキュアな接続にはポート 443 を開きます。
2番目のDMZのNetScaler Gateway は、内部ネットワークのサーバー上の公開アプリケーションまたは仮想デスクトップへのICA接続を確立します。	TCP ポート 1494 を開いて、第 3 のファイアウォールを介した ICA 接続をサポートします。Citrix Virtual Apps でセッション画面の保持を有効にした場合は、1494ではなくTCPポート2598を開きます。
最初のDMZでNetScaler Gateway で認証を有効にした場合、このアプライアンスは内部ネットワークの認証サーバーに接続する必要がある場合があります。	認証サーバが接続をリッスンする TCP ポートを開きます。例としては、RADIUS 用のポート 1812、LDAP 用のポート 389 などがあります。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

システムのメンテナンスとモニタリング

NetScaler Gateway の構成が完了したら、アプライアンスを保守および監視する必要があります。次の方法でこれを行うことができます。

- NetScaler Gateway を最新バージョンのソフトウェアにアップグレードできます。Citrix Web サイトにログオンすると、NetScaler Gateway ダウンロードサイトに移動してソフトウェアをダウンロードできます。メンテナンスビルドのReadmeは、Citrix ナレッジセンターで参照できます。
- NetScaler Gateway の構成タスクと管理タスクをグループの異なるメンバーに割り当てることができます。委任管理では、個人にアクセスレベルを割り当てて、NetScaler Gateway での特定のタスクの実行を制限できます。
- NetScaler Gateway 構成は、アプライアンスまたはコンピューター上のファイルに保存できます。現在の実行構成と保存済み構成を比較できます。NetScaler Gateway から構成を消去することもできます。
- NetScaler Gateway 構成ユーティリティでは、ユーザーセッションを表示、更新、およびエンドユーザーセッションできます。
- NetScaler Gateway でログを構成できます。ログはアプライアンスに関する重要な情報を提供し、問題が発生した場合に役立ちます。

委任管理者の構成

NetScaler Gateway には、デフォルトの管理者ユーザー名とパスワードがあります。デフォルトのユーザー名とパスワードは`nsroot`です。セットアップウィザードを初めて実行するときは、管理者パスワードを変更できます。

さらに管理者アカウントを作成し、各アカウントにNetScaler Gateway への異なるアクセスレベルを割り当てることができます。これらの追加アカウントは、委任管理者と呼ばれます。たとえば、NetScaler Gateway の接続とログを監視する担当者が1人、NetScaler Gateway の特定の設定を構成する別の担当者が割り当てられているとします。最初の管理者は読み取り専用アクセス権を持ち、2 番目の管理者はアプライアンスへのアクセスが制限されています。

委任された管理者を設定するには、コマンドポリシー、およびシステムユーザーとグループを使用します。

委任管理者を設定する場合、構成プロセスは次のとおりです。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- システムユーザーを追加します。システムユーザは、指定された権限を持つ管理者です。すべての管理者は、所属するグループのポリシーを継承します。
- システムグループを追加します。システムグループには、特定の権限を持つシステムユーザーが含まれます。システムグループのメンバーは、所属するグループのポリシーを継承します。
- コマンドポリシーを作成します。コマンドポリシーを使用すると、ユーザーまたはグループがアクセスおよび変更できるNetScaler Gateway 構成の部分を定義できます。また、コマンドグループ、仮想サーバ、および管理者とグループが設定できるその他の要素などのコマンドを制御することもできます。
- 優先度を設定して、コマンドポリシーをユーザーまたはグループにバインドします。委任管理を構成するときは、管理者またはグループに優先順位を割り当て、NetScaler Gateway が優先するポリシーを判断できるようにします。

NetScaler Gateway には、デフォルトの拒否システムコマンドポリシーがあります。コマンドポリシーはグローバルにバインドできません。ポリシーをシステム管理者（ユーザー）またはグループに直接バインドします。ユーザーおよびグループにコマンドポリシーが関連付けられていない場合、デフォルトの拒否ポリシーが適用され、ユーザーはコマンドを実行したり、NetScaler Gateway を構成したりできません。

カスタムコマンドポリシーを設定して、ユーザー権利の割り当てに関する詳細レベルをより詳細に定義できます。たとえば、セッションポリシーをNetScaler Gateway に追加する権限をあるユーザーに付与し、そのユーザーに他の構成の実行を許可することはできません。

委任管理者のコマンドポリシーの設定

NetScaler Gateway には、委任管理に使用できる4つの組み込みコマンドポリシーがあります：

- **読み取り専用では**、システムコマンドグループおよび`ns.conf show`コマンドを除くすべてのコマンドを表示するための読み取り専用アクセスが許可されます。
- **Operator** は読み取り専用アクセスを許可し、サービスでコマンドを有効または無効にするアクセスも許可します。このポリシーでは、サービスおよびサーバーを「アクセスダウン」に設定するためのアクセスも許可します。
- **ネットワークは** 、システムコマンドとシェルコマンドを除いて、ほぼ完全なシステムアクセスを許可します。
- **スーパーユーザは** 、デフォルトの管理者`nsroot`に付与される権限など、完全なシステム権限を付与します。

コマンドポリシーには、組み込みの式が含まれています。構成ユーティリティを使用して、システムユーザー、システムグループ、コマンドポリシーを作成し、権限を定義します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler Gateway で管理ユーザーを作成するには

1. 構成ユーティリティのナビゲーションペインの タブで、 > を展開し、 をクリックします。
2. 詳細ペインで、 をクリックします。
3. **に、ユーザー名を入力します。
4. フィールドと フィールドに、パスワードを入力します。
5. グループにユーザーを追加するには、「 **メンバー**」で「 **追加**」をクリックします。
6. でグループを選択し、右矢印をクリックします。
7. **コマンドポリシー > アクション > 挿入をクリックします。**
8. 「コマンドポリシーの挿入」ダイアログ・ボックスで、コマンドを選択し、「 **OK」>「作成」>「閉じる」**をクリックします。

管理グループの作成

管理グループには、NetScaler Gateway の管理権限を持つユーザーが含まれます。構成ユーティリティで管理グループを作成できます。

構成ユーティリティを使用して管理グループを構成するには

1. 構成ユーティリティのナビゲーションペインの タブで、 > を展開し、 をクリックします。
2. 詳細ペインで、 をクリックします。
3. に、グループの名前を入力します。
4. 既存のユーザーをグループに追加するには、 で をクリックします。
5. でユーザーを選択し、右矢印をクリックします。
6. の で、 をクリックし、1 つまたは複数のポリシーを選択し、、、 の順にクリックします。

委任管理者用のカスタムコマンドポリシーの設定

カスタムコマンドポリシーを設定する場合は、ポリシー名を指定し、ポリシーコンポーネントを設定してコマンド仕様を作成します。コマンド仕様により、管理者が使用できるコマンドを制限できます。たとえば、管理者が remove コマンドを使用する権限を拒否するとします。ポリシーを設定するときは、アクションを deny に設定し、パラメータを設定します。

単純なコマンドポリシーまたは高度なコマンドポリシーを設定できます。単純なポリシーを構成するときは、NetScaler Gateway や認証などのアプライアンス上のコンポーネントを構成します。詳細ポリシーを設定するときは、エンティティグループと呼ばれるコンポーネントを選択し、そのグループで管理者が実行できるコマンドを選択します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

簡単なカスタムコマンドポリシーを作成するには

1. 構成ユーティリティの タブのナビゲーションペインで、 > を展開し、 をクリックします。**
2. 詳細ペインで、 をクリックします。**
3. に、ポリシーの名前を入力します。
4. **［アクション］で、［許可］** または**［拒否］** を選択します。
5. で、 をクリックします。
6. ダイアログボックスの タブの で、委任された管理者が実行できる操作を選択します。
7. で、1 つ以上のグループを選択します。

   Ctrl キーを押すと、複数のグループを選択できます。
8. **［Create］** をクリックしてから、**［Close］** をクリックします。

高度なカスタムコマンドポリシーを作成するには

1. 構成ユーティリティのナビゲーションペインの タブで、 > を展開し、 をクリックします。
2. 詳細ペインで、 をクリックします。
3. に、ポリシーの名前を入力します。
4. **［アクション］で、［許可］** または**［拒否］** を選択します。
5. で、 をクリックします。
6. ダイアログボックスで、 タブをクリックします。
7. で、認証や高可用性など、コマンドが属するグループを選択します。
8. で、ポリシーを選択します。

   Ctrl キーを押すと、リスト内の複数の項目を選択できます。
9. でコマンドを選択し、、** の順にクリックします。

   Ctrl キーを押すと、リスト内の複数の項目を選択できます。
10. をクリックし、** をクリックします。
11. ダイアログボックスで、、** の順にクリックします。

「 作成」をクリックすると、**「 コマンドポリシーの作成」ダイアログボックスの「コマンド仕様 」**の下に式が表示されます。

カスタムコマンドポリシーを作成したら、ユーザーまたはグループにバインドできます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注: カスタムコマンドポリシーは、作成したユーザーまたはグループにのみバインドできます。カスタムコマンドポリシーをユーザー `nsroot` にバインドすることはできません。

カスタムコマンドポリシーをユーザーまたはグループにバインドするには

1. 構成ユーティリティの タブのナビゲーションペインで、 > を展開し、 をクリックするか、 をクリックします。
2. 詳細情報のウィンドウ領域で、一覧からユーザーまたはグループを選択し、 をクリックします。
3. 「 **コマンドポリシー**」でポリシーを選択し、 **「OK」**をクリックします。

NetScaler Gateway での監査の構成

NetScaler Gateway では、アプライアンスが収集する状態とステータス情報をログに記録できます。監査ログを使用して、イベント履歴を時系列で表示できます。ログ内のメッセージには、メッセージを生成したイベントに関する情報、タイムスタンプ、メッセージタイプ、および定義済みのログレベルとメッセージ情報が含まれます。ログに記録される情報とメッセージが保存される場所を決定する設定を構成できます。

NetScaler Gateway は現在、ローカルログ用の独自のログ形式と、syslogサーバーで使用するsyslog形式の2つのログ形式をサポートしています。監査ログを構成して、次の情報を提供できます。

レベル	説明
緊急	重大なエラーのみをログに記録します。ログのエントリは、NetScaler Gateway が使用できなくなる重大な問題が発生していることを示しています。
アラート	NetScaler Gateway が正しく機能しない可能性があるが、その操作にとって重要ではない問題をログに記録します。NetScaler Gateway で重大な問題が発生するのを防ぐために、できるだけ早く是正措置を講じることができます。
クリティカル	NetScaler Gateway の操作を制限しないが、より大きな問題にエスカレートする可能性のある重大な状態を記録します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

レベル	説明
エラー	NetScaler Gateway で失敗した操作の結果として生じるエントリを記録します。
警告	エラーまたは重大なエラーにつながる可能性のある潜在的な問題をログに記録します。
通知	情報レベルのログよりも詳細な問題を記録しますが、通知と同じ目的を果たします。
情報	NetScaler Gateway によって実行されたアクションを記録します。このレベルは、問題のトラブルシューティングに役立ちます。

TCP圧縮を構成した場合、NetScaler Gateway 監査ログには、NetScaler Gateway の圧縮統計も格納されます。異なるデータに対して達成された圧縮率は、各ユーザーセッションのログファイルに格納されます。

NetScaler Gateway はログ署名セッションIDを使用します。これにより、ユーザーごとではなくセッションごとにログを追跡できます。セッションの一部として生成されるログは、同じ sessionID を持ちます。ユーザが同じユーザデバイスから同じ IP アドレスを持つ 2 つのセッションを確立する場合、各セッションは一意の sessionID を持ちます。

重要:

カスタムログ解析スクリプトを作成した場合は、カスタム解析スクリプト内でこのシグニチャを変更する必要があります。

NetScaler Gateway でのログの構成

NetScaler Gateway でログを構成するときは、監査ログをNetScaler Gateway に保存するか、syslogサーバーに送信するかを選択できます。構成ユーティリティを使用して、監査ポリシーを作成し、監査ログを格納するための設定を構成します。

監査ポリシーを作成するには

1. 構成ユーティリティの［構成］タブで、［ **NetScaler Gateway** ］>［ **ポリシー** ］>［ **監査**］の順に展開します。
2. ** に、ポリシーの名前を入力します。
3. 次のいずれかを選択します：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- syslog は、ログを Syslog サーバに送信する場合に使用します。
- `Nslog`でNetScaler Gateway にログを保存します。

  注：
  このオプションを選択すると、ログはアプライアンスの /var/log フォルダに保存されます。

4. 詳細ペインで、 をクリックします。
5. ログが保存されているサーバー情報について、次の情報を入力します。
   - に、サーバーの名前を入力します。
   - に、ログサーバーの名前または IP アドレスを入力します。
6. をクリックし、 をクリックします。

監査ポリシーを作成したら、次の任意の組み合わせにポリシーをバインドできます。

- グローバルに
- 仮想サーバー
- グループ
- ユーザー

監査ポリシーをグローバルにバインドするには

1. 構成ユーティリティの［構成］タブで、［ **NetScaler Gateway** ］>［ **ポリシー** ］>［ **監査**］の順に展開します。
2. ** `Syslog` **または** `Nslog` **を選択します。
3. 詳細ウィンドウで、 をクリックし、 をクリックします。
4. ダイアログボックスの で、 をクリックします。
5. 「 **ポリシー名**」でポリシーを選択し、 **「OK」**をクリックします。

監査ポリシーを変更するには

既存の監査ポリシーを変更して、ログの送信先サーバーを変更できます。

1. 構成ユーティリティの［ **構成** ］タブで、［ **NetScaler Gateway** ］>［ **ポリシー** ］>［ **監査**］の順に展開します
2. ** `Syslog` **または** `Nslog` **を選択します。
3. 詳細ウィンドウで、ポリシーをクリックし、 をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. 「サーバー」で新しいサーバーを選択し、 **「OK」**をクリックします。

監査ポリシーを削除するには

NetScaler Gateway から監査ポリシーを削除できます。監査ポリシーを削除すると、ポリシーは自動的にバインド解除されます。

1. 構成ユーティリティの［構成］タブで、［ **NetScaler Gateway** ］>［ **ポリシー** ］>［ **監査**］の順に展開します。
2. または を選択します。
3. 詳細ウィンドウで、ポリシーをクリックし、 をクリックします。

ACL ロギングの設定

拡張アクセス制御リスト（ACL）と一致するパケットの詳細を記録するようにNetScaler Gatewayを構成できます。ACL 名に加えて、ログに記録される詳細には、送信元および宛先 IP アドレスなどのパケット固有の情報が含まれます。情報は、有効にしたロギングのタイプ（syslog または `nslog`）に応じて、syslogまたは`nslog`ファイルのいずれかに保存されます。

ロギングは、グローバルレベルと ACL レベルの両方で有効にできます。ただし、ACL レベルでロギングを有効にするには、グローバルレベルでも有効にする必要があります。グローバル設定が優先されます。

ロギングを最適化するために、同じフローからの複数のパケットが ACL に一致する場合、最初のパケットの詳細だけがロギングされます。カウンタは、同じフローに属する他のすべてのパケットに対して増分されます。フローは、次のパラメータに対して同じ値を持つパケットのセットとして定義されます。

- 接続元IP
- 接続先IP
- 送信元ポート
- Destination port
- プロトコル (TCP または UDP)

パケットが同じフローからのものではない場合、または期間が平均時間を超えている場合は、新しいフローが作成されます。平均時間は、同じフローのパケットが追加のメッセージを生成しない時間です（ただし、カウンタは増加します）。

注:

任意の時点でログに記録できる異なるフローの合計数は 10,000 に制限されています。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

次の表に、拡張 ACL のルールレベルで ACL ロギングを設定するためのパラメータを示します。

パラメーター名	説明
`Logstate`	ACL のロギング機能の状態。有効な値:有効および無効。デフォルト:無効。
`Ratelimit`	特定の ACL が生成できるログメッセージの数。デフォルトは 100 です。

構成ユーティリティを使用して ACL ロギングを構成するには

ACL のロギングを設定し、ルールが生成できるログメッセージの数を指定できます。

1. 構成ユーティリティのナビゲーションペインで、 > を展開し、 をクリックします。
2. 詳細ウィンドウで、 タブをクリックし、 をクリックします。
3. ダイアログボックスの に、ポリシーの名前を入力します。
4. チェックボックスをオンにします。
5. テキストボックスに、ルールに指定するレート制限を入力し、 をクリックします。

ACLロギングを構成したら、NetScaler Gateway で有効にすることができます。監査ポリシーを作成し、ユーザー、グループ、仮想サーバー、またはグローバルにバインドします。

NetScaler Gateway でACLまたはTCPのログを有効にするには

1. 構成ユーティリティのナビゲーションペインで、［**NetScaler Gateway**］>［**ポリシー**］>［**監査**］の順に展開します。
2. syslogまたは`nslog`を選択します。
3. 「**サーバー**」タブで、「**追加**」をクリックします。
4. ダイアログボックスの にサーバーの名前を入力し、サーバーの設定を構成します。
5. または をクリックし、 をクリックします。

NetScaler Gateway プラグインログの有効化

NetScaler Gateway プラグインを構成して、ユーザーデバイスに保存されているテキストファイルにすべてのエラーを記録できます。ユーザーは、NetScaler Gateway プラグインを構成して、ユーザーデバイス上のログオンレベルを設定して、特定のユーザーアクティビティを記録できます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ユーザーがログを構成すると、プラグインはユーザーデバイスに次の 2 つのファイルを作成します。

- hooklog \\.txt。<num\ > NetScaler Gateway プラグインが生成する傍受メッセージをログに記録します。
- nssslvpn.txt。プラグインのエラーが一覧表示されます。

注:

hooklog.txt ファイルは自動的には削除されません。Citrix では、ファイルを定期的に削除することをお勧めします。

ユーザーログは、ユーザーデバイス上の Windows の次のディレクトリにあります。

- Windows XP (すべてのユーザー): %SystemDrive%:\Documents and Settings\All Users\Application Data\Citrix\AGEE
- Windows XP (ユーザー固有): %SystemDrive%:\Documents and Settings\\%username%\Local Settings\Application Data\Citrix\AGEE
- Windows Vista (すべてのユーザー): %SystemDrive%:\ProgramData\Citrix\AGEE
- Windows Vista (ユーザー固有): %SystemDrive%:\Users\\%username% \AppData\Local\Citrix\AGEE
- Windows 7 (すべてのユーザー): %SystemDrive%:\ProgramData\Citrix\AGEE
- Windows 7 (ユーザー固有): %SystemDrive%:\Users\\%username% \AppData\Local\Citrix\AGEE
- Windows 8（すべてのユーザー）：%SystemDrive%:\ProgramData\Citrix\AGEE
- Windows 8（ユーザー固有）：%SystemDrive%:\Users\\%username% \AppData\Local\Citrix\AGEE

これらのログファイルを使用して、NetScaler Gateway プラグインのトラブルシューティングを行うことができます。ユーザーは、ログファイルをテクニカルサポートに電子メールで送信できます。

［構成］ダイアログボックスで、ユーザーはNetScaler Gateway プラグインのログ記録レベルを設定できます。ログレベルは次のとおりです。

- エラーメッセージを記録する
- イベントメッセージを記録する
- NetScaler Gateway プラグイン統計を記録する
- すべてのエラー、イベントメッセージ、および統計を記録する

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Windows向けCitrix Secure Accessクライアントのログ機能について詳しくは、「Windowsクライアントのログ収集の改善」を参照してください。

ICA 接続を監視するには

サーバーファームのアクティブなユーザーセッションは、 ダイアログボックスを使用して監視できます。このダイアログボックスには、次の情報が表示されます。

- サーバーファームに接続しているユーザーのユーザー名
- サーバーファームのドメイン名
- ユーザーデバイスの IP アドレス
- ユーザーデバイスのポート番号
- Citrix Virtual Apps and Desktops を実行しているサーバーのIPアドレス
- Citrix Virtual Apps and Desktops を実行しているサーバーのポート番号

1. 構成ユーティリティのナビゲーションペインで、 をクリックします。
2. 詳細ウィンドウの で、 をクリックして、監視ダイアログボックスを表示します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

認証と承認

NetScaler Gateway は、NetScaler Gateway のユーザー認証を広範囲にカスタマイズできる柔軟な認証設計を採用しています。業界標準の認証サーバーを使用し、サーバーでユーザーを認証するようにNetScaler Gateway を構成できます。NetScaler Gateway は、クライアント証明書に存在する属性に基づく認証もサポートしています。NetScaler Gateway 認証は、ユーザー認証に単一のソースを使用する単純な認証手順と、複数の認証タイプに依存するより複雑なカスケード認証手順に対応するように設計されています。

NetScaler Gateway 認証には、ローカルユーザーとグループを作成するためのローカル認証が組み込まれています。この設計は、構成する認証手順を制御するためのポリシーの使用を中心にしています。作成したポリシーは、NetScaler Gateway グローバルまたは仮想サーバーレベルで適用でき、ユーザーのソースネットワークに基づいて条件付きで認証サーバーパラメータを設定するために使用できます。

ポリシーはグローバルまたは仮想サーバにバインドされるため、ポリシーに優先順位を割り当て、認証の一部として複数の認証サーバのカスケードを作成することもできます。

NetScaler Gatewayには、次の認証タイプがサポートされています。

- ローカル
- ライトウェイトディレクトリアクセスプロトコル（LDAP）
- RADIUS
- SAML
- TACACS+
- クライアント証明書認証（スマートカード認証を含む）

NetScaler Gateway はRSA SecurID、Gemalto Protiva、SafeWordにも対応している。これらの認証の種類を構成するには、RADIUSサーバーを使用します。

認証によってユーザーはNetScaler Gateway にログオンして内部ネットワークに接続できますが、承認はユーザーがアクセスできるセキュアネットワーク内のリソースを定義します。LDAP ポリシーと RADIUS ポリシーを使用して認可を設定します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

デフォルトのグローバル認証タイプの設定

NetScaler Gateway をインストールしてNetScaler Gateway ウィザードを実行すると、ウィザード内で認証を構成しました。この認証ポリシーは、NetScaler Gateway グローバルレベルに自動的にバインドされます。NetScaler Gateway ウィザードで構成する認証の種類は、デフォルトの認証の種類です。デフォルトの認証の種類を変更するには、NetScaler Gateway ウィザードを再度実行するか、構成ユーティリティでグローバル認証設定を変更します。

追加の認証の種類を追加する必要がある場合は、NetScaler Gateway で認証ポリシーを構成し、構成ユーティリティを使用してポリシーをNetScaler Gateway にバインドできます。認証をグローバルに設定する場合は、認証のタイプを定義し、設定を構成し、認証できる最大ユーザ数を設定します。

ポリシーを設定してバインドしたら、優先度を設定して、優先する認証タイプを定義できます。たとえば、LDAP および RADIUS 認証ポリシーを設定します。LDAP ポリシーのプライオリティ番号が 10 で、RADIUS ポリシーのプライオリティ番号が 15 の場合、各ポリシーをバインドする場所に関係なく、LDAP ポリシーが優先されます。これをカスケード認証と呼びます。

ログオンページは、NetScaler Gateway のメモリ内キャッシュまたはNetScaler Gateway で実行されているHTTPサーバーから配信するように選択できます。メモリ内キャッシュからログオンページを配信することを選択した場合、NetScaler Gateway からのログオンページの配信は、HTTP サーバーからの配信よりも大幅に高速です。インメモリキャッシュからログオンページを配信するように選択すると、多数のユーザーが同時にログオンするときの待機時間が短縮されます。
キャッシュからのログオンページの配信は、グローバル認証ポリシーの一部としてのみ構成できます。

また、認証用の特定の IP アドレスであるネットワークアドレス変換（NAT）IP アドレスを設定することもできます。このIPアドレスは認証用に一意であり、NetScaler Gateway のサブネット、マッピング、または仮想IPアドレスではありません。この設定はオプションです。

注：NetScaler Gateway ウィザードを使用してSAML認証を構成することはできません。

クイック構成ウィザードを使用して、LDAP、RADIUS、およびクライアント証明書認証を構成できます。ウィザードを実行すると、NetScaler Gateway で構成された既存のLDAPサーバーまたはRADIUSサーバーから選択できます。LDAP または RADIUS の設定を構成することもできます。2要素認証を使用する場合は、プライマリ認証タイプとしてLDAPを使用することをお勧めします。

認証をグローバルに設定するには

1. ナビゲーションペインにある、［Configuration］タブの構成ユーティリティで、［NetScaler Gateway］を展開し、［Global Settings］をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. 詳細ウィンドウの で、 をクリックします。
3. に、この認証の種類を使用して認証できるユーザーの数を入力します。
4. に、認証用の一意の IP アドレスを入力します。
5. を選択すると、ログオンページが高速に配信されます。
6. 認証が失敗した場合にユーザーにメッセージを表示するには、 を選択します。ユーザーが受け取るメッセージには、パスワードエラー、アカウントが無効またはロックされている、またはユーザーが見つからない、などが含まれます。
7. で、認証タイプを選択します。
8. 認証タイプの設定を構成し、をクリックします。

認可なしの認証の設定

承認は、ユーザーがNetScaler Gateway を介して接続できるリソースを定義します。式を使用して承認ポリシーを構成し、ポリシーを許可または拒否するように設定します。NetScaler Gateway は、承認なしで認証のみを使用するように構成できます。

承認なしで認証を構成すると、NetScaler Gateway はグループ承認チェックを実行しません。ユーザーまたはグループに設定したポリシーは、ユーザーに割り当てられます。

認可の設定の詳細については、 認可の設定を参照してください。

認可の設定

承認では、ユーザーがNetScaler Gateway にログオンするときにアクセスできるネットワークリソースを指定します。承認のデフォルト設定では、すべてのネットワークリソースへのアクセスを拒否します。デフォルトのグローバル設定を使用し、承認ポリシーを作成して、ユーザーがアクセスできるネットワークリソースを定義することをお勧めします。

NetScaler Gateway での承認は、承認ポリシーと式を使用して構成します。承認ポリシーを作成したら、アプライアンスで構成したユーザーまたはグループに承認ポリシーをバインドできます。

承認ポリシーの構成

認可ポリシーを設定するときに、内部ネットワークのネットワークリソースへのアクセスを許可または拒否するように設定できます。たとえば、ユーザが 10.3.3.0 ネットワークにアクセスできるようにするには、次の式を使用します。

CLIENT.IP.DST.IN_SUBNET (10.3.0.0/16)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

承認ポリシーは、ユーザーおよびグループに適用されます。ユーザーが認証された後、NetScaler Gateway は、RADIUS、LDAP、またはTACACS+サーバーのいずれかからユーザーのグループ情報を取得することにより、グループ認証チェックを実行します。ユーザーがグループ情報を使用できる場合、NetScaler Gateway はグループに許可されているネットワークリソースをチェックします。

ユーザーがアクセスできるリソースを制御するには、承認ポリシーを作成する必要があります。認可ポリシーを作成する必要がない場合は、デフォルトのグローバル認可を設定できます。

ファイルパスへのアクセスを拒否する式を認可ポリシー内に作成する場合は、サブディレクトリパスだけを使用でき、ルートディレクトリは使用できません。たとえば、fs.path には「\\\ rootdir\\\ dir1\\\ dir2」が含まれているのではなく、fs.path には「\\\ dir1\\\ dir2」が含まれています。この例で 2 番目のバージョンを使用すると、ポリシーは失敗します。

認可ポリシーを設定したら、次のタスクに示すように、それをユーザーまたはグループにバインドします。

デフォルトでは、認可ポリシーは、仮想サーバにバインドされたポリシーに対して最初に検証され、次にグローバルにバインドされたポリシーに対して検証されます。ポリシーをグローバルにバインドし、ユーザー、グループ、または仮想サーバにバインドするポリシーよりもグローバルポリシーを優先する場合は、ポリシーのプライオリティ番号を変更できます。プライオリティ番号は 0 から始まります。プライオリティ番号が小さいほど、ポリシーの優先順位が高くなります。

たとえば、グローバルポリシーのプライオリティ番号が 1 で、ユーザのプライオリティが 2 の場合、グローバル認証ポリシーが最初に適用されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

重要：

- 従来の認可ポリシーは、TCP トラフィックにのみ適用されます。
- 高度な承認ポリシーは、すべてのタイプのトラフィックに適用できます (TCP/UDP/ICMP/DNS).
  - To apply policy on UDP/ICMP/DNS traffic, policies must be bound at type UDP_REQUEST, ICMP_REQUEST, and DNS_REQUEST respectively.
  - While binding, if "type" is not explicitly mentioned or "type" is set to REQUEST, the behavior does not change from earlier builds, that is these policies are applied only to TCP traffic.
  - The policies bound at UDP_REQUEST do not apply for DNS traffic. For DNS, policies must be explicitly bound to DNS_REQUEST TCP_DNS is similar to other TCP requests.

高度な承認ポリシーの詳細については、記事`<https://support.citrix.com/article/CTX232237>`を参照してください。

承認ポリシー表現の例

権限付与ポリシーの表現例を以下に示します。

- `add authorization policy athzPol1 "HTTP.REQ.USER.IS_MEMBER_OF(\"allowedGroup\")" ALLOW`
- `add authorization policy athzPol2 "CLIENT.IP.DST.BETWEEN(10.102.75.10,10.102.75.20)" DENY`
- `add authorization policy athzPol3 "HTTP.REQ.HOSTNAME.CONTAINS(\"portal-srv") || CLIENT.IP.DST.IN_SUBNET(10.102.75.0/25)" ALLOW`

GUI を使用して認可ポリシーを設定するには

1. **NetScaler Gateway > ポリシー > 認証に移動します。**
2. 詳細ペインで、 をクリックします。
3. ** に、ポリシーの名前を入力します。
4. **［アクション］で、［許可］** または**［拒否］** を選択します。
5. 「エクスプレッション」で**、**「エクスプレッションエディタ」をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

6. 式の設定を開始するには、 をクリックし、必要な要素を選択します。
7. 式が完成したら、 をクリックします。
8. ［**Create**］ をクリックします。

GUI を使用して認可ポリシーをユーザにバインドするには

1. **Citrix Gateway > ユーザー管理に移動します。**
2. をクリックします。
3. 詳細ペインで、ユーザーを選択し、 をクリックします。
4. で、 をクリックします。
5. ページで、ポリシーを選択するか、ポリシーを作成します。
6. で、優先度番号を設定します。
7. 「 **タイプ**」でリクエストのタイプを選択し、 **「OK」**をクリックします。

GUI を使用して認可ポリシーをグループにバインドするには

1. ［ **NetScaler Gateway］ >［ユーザー管理］**に移動します。
2. をクリックします。
3. 詳細ペインでグループを選択し、 をクリックします。
4. で、 をクリックします。
5. ページで、ポリシーを選択するか、ポリシーを作成します。
6. で、優先度番号を設定します。
7. 「 **タイプ**」でリクエストのタイプを選択し、 **「OK」**をクリックします。

デフォルトのグローバル認証の設定

ユーザが内部ネットワークでアクセスできるリソースを定義するには、デフォルトのグローバル認可を設定します。グローバル認可を設定するには、内部ネットワーク上のネットワークリソースへのアクセスをグローバルに許可または拒否します。

作成したグローバル認可アクションは、直接またはグループを介して、関連付けられた認可ポリシーをまだ持っていないすべてのユーザに適用されます。ユーザまたはグループの認可ポリシーは、常にグローバル認可アクションを上書きします。デフォルトの認可アクションが に設定されている場合は、すべてのユーザまたはグループに許可ポリシーを適用して、それらのユーザまたはグループがネットワークリソースにアクセスできるようにする必要があります。この要件は、セキュリティの向上に役立ちます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

デフォルトのグローバル認証を設定するには、次の手順を実行します。

1. ナビゲーションペインにある、［Configuration］タブの構成ユーティリティで、［NetScaler Gateway］を展開し、［Global Settings］をクリックします。
2. 詳細ペインの で、 をクリックします。
3. タブのの横にあるまたはを選択し、をクリックします。

認証の無効化

展開で認証が不要な場合は、認証を無効にできます。認証を必要としない仮想サーバーごとに、認証を無効にできます。

重要：認証は慎重に無効にすることをお勧めします。外部認証サーバーを使用していない場合は、ローカルユーザーとグループを作成して、NetScaler Gateway でユーザーを認証できるようにします。認証を無効にすると、NetScaler Gateway への接続を制御および監視する認証、承認、およびアカウンティング機能の使用が停止します。ユーザーがWebアドレスを入力してNetScaler Gateway に接続すると、ログオンページは表示されません。

認証を無効にするには

1. 構成ユーティリティのナビゲーションペインで、［NetScaler Gateway］を展開し、［仮想サーバー］をクリックします。
2. 詳細ペインで仮想サーバーをクリックし、 をクリックします。
3. タブの で、 をクリックしてオフにします。

特定の時刻の認証の設定

認証ポリシーを設定して、ユーザが特定の時間（通常の勤務時間内など）に内部ネットワークにアクセスできるようにすることができます。ユーザーが別の時間にログオンしようとすると、ログオンは拒否されます。

ユーザーがNetScaler Gateway にログオンするタイミングを制限するには、認証ポリシー内に式を作成し、それを仮想サーバーまたはグローバルにバインドします。

時刻、日付、または曜日の認証を設定するには

1. 構成ユーティリティの［構成］タブで、［NetScaler Gateway］>［ポリシー］>［認証］の順に展開します。
2. で、認証の種類を選択します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. 詳細ペインで、 タブをクリックし、認証ポリシーを選択して、 をクリックします。
4. ダイアログボックスの で、 の横にある をクリックします。
5. ダイアログボックスの で、 を選択します。
6. 「修飾子」で、次のいずれかを選択します。

   - TIME は、ユーザーがログオンできない時間を設定します。
   - DATE: ユーザーがログオンできない日付を設定します。
   - DAYOFWEEK は、ユーザーがログオンできない日を設定します。

   例:時間:2020-10-12-02:30:00 GMT 日付:2020-10-12 DAYOFWEEK: Monday
7. 「演算子」で、値を選択します。
8. で、テキストボックスの横にあるカレンダーをクリックし、日、日付、または時刻を選択します。
9. 「OK」を 2 回クリックし、「閉じる」をクリックして「OK」をクリックします

認証ポリシーの仕組み

ユーザーがNetScaler Gateway にログオンすると、作成したポリシーに従って認証されます。ポリシーは、認証タイプを定義します。単一の認証ポリシーは、単純な認証のニーズに使用でき、通常はグローバルレベルでバインドされます。デフォルトの認証タイプ (ローカル) を使用することもできます。ローカル認証を構成する場合は、NetScaler Gateway のユーザーとグループも構成する必要があります。

複数の認証ポリシーを設定し、それらをバインドして、詳細な認証手順と仮想サーバーを作成できます。たとえば、複数のポリシーを設定して、カスケード認証と 2 要素認証を設定できます。また、認証ポリシーの優先順位を設定して、NetScaler Gateway がユーザー資格情報をチェックするサーバーと順序を決定することもできます。認証ポリシーには、式とアクションが含まれます。たとえば、式を True 値に設定した場合、ユーザーのログオン時にアクションによってユーザーログオンが true と評価され、ユーザーはネットワークリソースにアクセスできます。

認証ポリシーを作成したら、ポリシーをグローバルレベルまたは仮想サーバにバインドします。少なくとも1つの認証ポリシーを仮想サーバーにバインドすると、グローバル認証タイプの優先順位が仮想サーバーにバインドされたポリシーよりも高い場合を除き、ユーザーが仮想サーバーにログオンするときに、グローバルレベルにバインドされた認証ポリシーは使用されません。

ユーザーがNetScaler Gateway にログオンすると、認証は次の順序で評価されます。

- 仮想サーバは、バインドされた認証ポリシーがあるかどうかがチェックされます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 認証ポリシーが仮想サーバーにバインドされていない場合、NetScaler Gateway はグローバル認証ポリシーを確認します。
- 認証ポリシーが仮想サーバまたはグローバルにバインドされていない場合、ユーザはデフォルトの認証タイプで認証されます。

LDAP および RADIUS 認証ポリシーを構成し、2 要素認証用にポリシーをグローバルにバインドする場合は、構成ユーティリティでポリシーを選択し、ポリシーがプライマリ認証タイプかセカンダリ認証タイプかを選択できます。グループ抽出ポリシーを構成することもできます。

認証プロファイルの設定

認証プロファイルは、NetScaler Gateway ウィザードまたは構成ユーティリティを使用して作成できます。プロファイルには、認証ポリシーのすべての設定が含まれています。プロファイルは、認証ポリシーの作成時に設定します。

NetScaler Gateway ウィザードでは、選択した認証タイプを使用して認証を構成できます。ウィザードの実行後に追加の認証ポリシーを構成する場合は、構成ユーティリティを使用できます。NetScaler Gateway ウィザードについて詳しくは、「NetScaler Gateway ウィザードを使用した設定の構成」を参照してください。

構成ユーティリティを使用して認証ポリシーを作成するには

1. 構成ユーティリティの［構成］タブで、［NetScaler Gateway］>［ポリシー］>［認証］の順に展開します。
2. ナビゲーションペインの で、認証の種類を選択します。
3. 詳細ペインの タブで、 をクリックします。
4. 外部認証タイプを使用している場合は、 の横にある をクリックします。
5. ダイアログボックスで、認証タイプの設定を構成し、、 の順にクリックします。
6. ダイアログボックスで、 の横にある を選択し、、、 の順にクリックします。 注:認証タイプを選択して認証プロファイルを保存する場合、認証タイプを変更することはできません。別の認証タイプを使用するには、新しいポリシーを作成する必要があります。

構成ユーティリティを使用して認証ポリシーを変更するには

認証サーバの IP アドレスや式など、設定済みの認証ポリシーおよびプロファイルを変更できます。

1. 構成ユーティリティの［構成］タブで、［NetScaler Gateway］>［ポリシー］>［認証］の順に展開します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. ナビゲーションペインの で、認証の種類を選択します。
3. 詳細ウィンドウの タブで、サーバーを選択し、 をクリックします。

認証ポリシーを削除するには

ネットワークから認証サーバーを変更または削除した場合は、対応する認証ポリシーをNetScaler Gateway から削除します。

1. 構成ユーティリティの［構成］タブで、［NetScaler Gateway］>［ポリシー］>［認証］の順に展開します。
2. ナビゲーションペインの で、認証の種類を選択します。
3. 詳細ペインの タブで、ポリシーを選択し、 をクリックします。

認証ポリシーのバインド

認証ポリシーを設定したら、ポリシーをグローバルにバインドするか、仮想サーバにバインドします。いずれかの構成ユーティリティを使用して、認証ポリシーをバインドできます。

GUI を使用して認証ポリシーをグローバルにバインドするには

1. 構成ユーティリティの［構成］タブで、［ **Citrix Gateway**］>［**ポリシー**］>［**認証**］を展開します。
2. 認証タイプをクリックします。
3. 詳細ウィンドウの タブで、サーバーをクリックし、 の をクリックします。
4. タブまたは タブの で、 をクリックします。
5. 「 **ポリシー名**」でポリシーを選択し、 **「OK」**をクリックします。

   注： ポリシーを選択すると、NetScaler Gateway によって式が自動的に真値に設定されます。

GUI を使用してグローバル認証ポリシーをバインド解除するには

1. 構成ユーティリティの［構成］タブで、［ **Citrix Gateway**］>［**ポリシー**］>［**認証**］を展開します。
2. 「 **ポリシー** 」タブの「 **アクション**」で、「 **グローバルバインディング**」をクリックします。
3. **「認証ポリシーをグローバルにバインド/バインド解除」ダイアログボックスの「プライマリ」タブまたは「セカンダリ」タブで、「ポリシー名」でポリシーを選択し、「ポリシーをバインド解除」をクリックして、「OK」をクリックします。**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

認証ポリシーの優先度の設定

デフォルトでは、認証ポリシーは、仮想サーバにバインドされたポリシーに対して最初に検証され、次にグローバルにバインドされたポリシーに対して検証されます。認証ポリシーをグローバルにバインドし、仮想サーバにバインドするポリシーよりもグローバルポリシーを優先させる場合は、ポリシーのプライオリティ番号を変更できます。プライオリティ番号は 0 から始まります。プライオリティ番号が小さいほど、認証ポリシーの優先順位が高くなります。

たとえば、グローバルポリシーのプライオリティ番号が 1 で、仮想サーバのプライオリティが 2 の場合、グローバル認証ポリシーが最初に適用されます。

グローバル認証ポリシーのプライオリティを設定または変更するには

1. 構成ユーティリティの［構成］タブで、［NetScaler Gateway］>［ポリシー］>［認証］の順に展開します。
2. 「 ポリシー 」タブの「 アクション」で、「 グローバルバインディング」をクリックします。
3. ［認証グローバルポリシーのバインド/バインド解除］ダイアログボックスの［プライマリ］タブまたは［セカンダリ］タブの［優先度］に番号を入力し、［OK］をクリックします。

仮想サーバーにバインドされた認証ポリシーの優先順位を変更するには

仮想サーバーにバインドされている認証ポリシーを変更することもできます。

1. 構成ユーティリティの［構成］タブのナビゲーションペインで、［ NetScaler Gateway ］を展開し、［ 仮想サーバー］をクリックします。
2. 仮想サーバーを選択し、 をクリックします。
3. タブをクリックし、 または を選択します。
4. ポリシーを選択し、［優先度］に優先度の番号を入力し、［OK］をクリックします。

ローカルユーザの設定

NetScaler Gateway でローカルにユーザーアカウントを作成して、認証サーバー上のユーザーを補完することができます。たとえば、社外のコンサルタントや来訪者などの一時的なユーザー用のアカウントを、認証サーバー上ではなくAccess Gateway上にローカルに作成します。

ローカル認証を使用している場合は、ユーザーを作成し、NetScaler Gateway で作成したグループに追加します。ユーザーとグループを構成したら、承認およびセッションポリシーを適用し、ブックマークを作成し、アプリケーションを指定し、ユーザーがアクセスできるファイル共有とサーバーのIPアドレスを指定できます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ローカルユーザーを作成するには

1. 構成ユーティリティで、「 **構成** 」タブをクリックし、ナビゲーションペインで「 **Citrix Gateway」>「ユーザー管理**」を展開して、「 **AAAユーザー**」をクリックします。
2. 詳細ペインで、 をクリックします。
3. ** に、ユーザー名を入力します。
4. ローカル認証を使用している場合は、**をオフにします。 注**:LDAP や RADIUS などの外部認証サーバに対してユーザを認証するには、 を選択します。** NetScaler Gateway がローカルユーザーデータベースに対して認証されるようにするには、このチェックボックスをオフにします。
5. と に、ユーザーのパスワードを入力し、 をクリックし、 をクリックします。

ユーザーパスワードを変更するには

ローカルユーザーの作成後、ユーザーのパスワードを変更するか、外部認証サーバーに対して認証されるユーザーアカウントを構成できます。

1. 構成ユーティリティで、「 **構成** 」タブをクリックし、ナビゲーションペインで「 **Citrix Gateway」>「ユーザー管理**」を展開して、「 **AAAユーザー**」をクリックします。
2. 詳細ウィンドウで、ユーザーを選択し、 をクリックします。
3. 「 **パスワード** 」と「 **パスワードの確認**」に、ユーザーの新しいパスワードを入力し、「 **OK」**をクリックします。

ユーザーの認証方法を変更するには

ローカル認証用に設定されているユーザがいる場合は、認証を外部認証サーバに変更できます。これを行うには、外部認証を有効にします。

1. 構成ユーティリティで、「 **構成** 」タブをクリックし、ナビゲーションペインで「 **Citrix Gateway」>「ユーザー管理**」を展開して、「 **AAAユーザー**」をクリックします。
2. 詳細ウィンドウで、ユーザーを選択し、 をクリックします。
3. 「 **外部認証**」を選択し、「 **OK」**をクリックします。

ユーザーを削除するには

NetScaler Gateway からユーザーを削除することもできます。

1. 構成ユーティリティで、「 **構成** 」タブをクリックし、ナビゲーションペインで「 **Citrix Gateway」>「ユーザー管理**」を展開して、「 **AAAユーザー**」をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. 詳細ウィンドウで、ユーザーを選択し、 をクリックします。

NetScaler Gateway からユーザーを削除すると、関連付けられているすべてのポリシーもユーザープロファイルから削除されます。

グループの設定

NetScaler Gateway には、ローカルグループであり、ローカル認証でユーザーを認証できるグループを持つことができます。認証に外部サーバーを使用している場合、NetScaler Gateway 上のグループは、内部ネットワークの認証サーバーで構成されたグループと一致するように構成されます。ユーザーがログオンして認証されると、グループ名が認証サーバー上のグループと一致する場合、ユーザーはNetScaler Gateway 上のグループの設定を継承します。

グループを設定したら、認可ポリシーとセッションポリシーの適用、ブックマークの作成、アプリケーションの指定、およびユーザがアクセスできるファイル共有およびサーバの IP アドレスの指定を行うことができます。

ローカル認証を使用している場合は、ユーザーを作成し、NetScaler Gateway で構成されているグループに追加します。その後、ユーザはそのグループの設定を継承します。

重要：ユーザーがAcActive Directory グループのメンバーである場合、NetScaler Gateway 上のグループの名前はActive Directory グループと同じである必要があります。

グループを作成するには

1. 構成ユーティリティで、「 **構成** 」タブをクリックし、ナビゲーションペインで「 **Citrix Gateway」>「ユーザー管理** 」を展開して、「 **AAAグループ**」をクリックします。
2. 詳細ペインで、 をクリックします。
3. にグループの名前を入力し、 をクリックし、 をクリックします。

グループを削除するには

NetScaler Gateway からユーザーグループを削除することもできます。

1. 構成ユーティリティで、「 **構成** 」タブをクリックし、ナビゲーションペインで「 **Citrix Gateway」>「ユーザー管理** 」を展開して、「 **AAAグループ**」をクリックします。
2. 詳細ペインでグループを選択し、 をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

グループへのユーザーの追加

グループの作成時または後で、グループにユーザーを追加できます。複数のグループにユーザーを追加すると、ユーザーはそれらのグループにバインドされているポリシーと設定を継承できます。

ユーザーをグループに追加するには、次の手順に従います：

1. 構成ユーティリティで、「構成」タブをクリックし、ナビゲーションペインで「**NetScaler Gateway」>「ユーザー管理」を展開して、「AAAユーザー**」をクリックします。
2. 詳細ウィンドウで、グループを選択し、 をクリックします。
3. 「**ユーザー**」タブの「**使用可能なユーザー**」でユーザーを選択し、「**追加**」をクリックして、「**OK」**をクリックします。

グループを使用したポリシーの設定

グループを構成したら、 グループダイアログボックスを使用して 、ユーザーアクセスを指定するポリシーと設定を適用できます。ローカル認証を使用している場合は、ユーザーを作成し、NetScaler Gateway で構成されているグループに追加します。その後、ユーザはそのグループの設定を継承します。

「グループ」ダイアログ・ボックスでは、ユーザー・グループに対して次のポリシーまたは設定を構成できます。

- ユーザー
- 承認ポリシー
- 監査ポリシー
- セッションポリシー
- トラフィックポリシー
- ブックマーク
- イントラネットアプリケーション
- イントラネット IP アドレス

構成では、複数のグループに属するユーザーがいる場合があります。さらに、各グループには、異なるパラメータが設定された 1 つ以上のバインドされたセッションポリシーがある場合があります。複数のグループに属するユーザーは、そのユーザーが属するすべてのグループに割り当てられたセッションポリシーを継承します。どのセッションポリシー評価が他方よりも優先されるかを確認するには、セッションポリシーの優先順位を設定する必要があります。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

たとえば、group1 がホームページ www.homepage1.com で設定されたセッションポリシーにバインドされているとします。Group2 は、ホームページ www.homepage2.com で設定されたセッションポリシーにバインドされています。これらのポリシーが、優先度番号のない、または同じ優先度番号を持つ各グループにバインドされている場合、両方のグループに属するユーザーに表示されるホームページは、最初に処理されるポリシーによって異なります。ホームページ www.homepage1.com のセッションポリシーに低い優先度の番号を設定すると、両方のグループに属するユーザーがホームページ www.homepage1.com を受信できるようになります。

セッションポリシーにプライオリティ番号が割り当てられていない場合、またはプライオリティ番号が同じ場合、precedence は次の順序で評価されます。

- ユーザー
- グループ
- 仮想サーバー
- グローバル

ポリシーがプライオリティ番号なしで同じレベルにバインドされている場合、またはポリシーのプライオリティ番号が同じ場合、評価の順序はポリシーのバインド順序に従います。最初にレベルにバインドされたポリシーは、後でバインドされたポリシーよりも優先されます。

ユーザーが複数のグループにバインドされ、各グループに IIP がバインドされている場合、そのユーザーはバインドされたグループから自由な IP を取得できます。

LDAP認証の構成

1つまたは複数のLDAPサーバーでユーザーアクセスを認証するようにNetScaler Gateway を構成できます。

LDAP認証には、Active Directory、LDAPサーバー、およびNetScaler Gateway で同じグループ名が必要です。グループ名は、大文字小文字の使い分けを含め、一字一句正確に一致させる必要があります。

既定では、LDAP 認証は、セキュア・ソケット・レイヤー (SSL) またはトランスポート・レイヤー・セキュリティ (TLS) を使用して安全です。セキュア LDAP 接続には 2 つのタイプがあります。1 つのタイプでは、LDAP サーバは、LDAP サーバがクリア LDAP 接続を受け入れるために使用するポートとは別のポートで SSL または TLS 接続を受け入れます。ユーザが SSL または TLS 接続を確立すると、LDAP トラフィックは接続を介して送信できます。

LDAP 接続のポート番号は次のとおりです。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- セキュリティで保護されていない LDAP 接続の場合は 389
- 636 セキュアな LDAP 接続の場合
- Microsoftのセキュアでない LDAP 接続の場合は 3268
- MicrosoftのセキュアLDAP接続の場合は 3269

2 番目のタイプのセキュア LDAP 接続では、StartTLS コマンドを使用し、ポート番号 389 を使用します。NetScaler Gateway でポート番号389または3268を構成すると、サーバーはStartTLSを使用して接続を試みます。他のポート番号を使用すると、サーバーは SSL または TLS を使用して接続を試みます。サーバーが StartTLS、SSL、または TLS を使用できない場合、接続は失敗します。

LDAPサーバーのルートディレクトリを指定すると、NetScaler Gateway はすべてのサブディレクトリを検索してユーザー属性を検索します。大きなディレクトリでは、このアプローチはパフォーマンスに影響する可能性があります。このため、特定の組織単位（OU）を使用することをお勧めします。

次の表に、LDAP サーバのユーザ属性フィールドの例を示します。

LDAP サーバ	ユーザー属性	大文字と小文字を区別
Microsoft Active Directory サーバー	sAMAccountName	いいえ
Novell eDirectory	ou	はい
IBM Directory Server	uid	はい
Lotus Domino	CN	はい
Sun ONE ディレクトリ (旧 iPlanet)	uidかcn	はい

次の表に、ベース DN の例を示します。

LDAP サーバ	ベース DN
Microsoft Active Directory サーバー	DC=`citrix`、DC=ローカル
Novell eDirectory	ou=users、ou=dev
IBM Directory Server	cn=users

© 1997–2026 Citrix Systems, Inc. All rights reserved.

LDAP サーバ	ベース DN
Lotus Domino	OU=City、O=`Citrix`、C=US
Sun ONE ディレクトリ (旧iPlanet)	OU=People、dc=`citrix`、dc=com

次の表に、バインド DN の例を示します。

LDAP サーバ	バインド DN
Microsoft Active Directory サーバー	cn=Administrator、cn=Users、DC=`citrix`、DC=local
Novell eDirectory	cn=admin、o=`citrix`
IBM Directory Server	LDAP_dn
Lotus Domino	cn=Notes Administrator、O=`Citrix`、C=US
Sun ONE ディレクトリ (旧iPlanet)	uid=admin,ou=Administrators, ou=TopologyManagement,o=NetscapeRoot

注:LDAP サーバー設定の詳細については、 LDAP ディレクトリの属性の決定を参照してください。

構成ユーティリティを使用して LDAP 認証を構成するには

1. **NetScaler Gateway** >**ポリシー** > **認証に移動します。**
2. **LDAP**をクリックします。
3. 詳細ペインの タブで、 をクリックします。
4. ** に、ポリシーの名前を入力します。
5. 「 **サーバー**」の横にある「 **新規**」をクリックします。
6. ** に、サーバーの名前を入力します。
7. の に、LDAP サーバーの IP アドレスとポート番号を入力します。
8. で、Active Directory の場合は **AD** 、 **Novell ディレクトリサービスの場合は NDS** のいずれかを選択します。
9. **で、以下を完了します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

a. に、ユーザーが配置されているベース DN を入力します。ベース DN は、選択したディレクトリ（AD または NDS）の下にあるユーザを検索します。

   ベース DN は、ユーザー名を削除し、ユーザーが配置されているグループを指定することによって、バインド DN から取得されます。ベース DN の構文の例は次のとおりです。

   ```
   ou=users,dc=ace,dc=com

   cn=Users,dc=ace,dc=com
   ```

b. に、LDAP ディレクトリへのクエリの管理者バインド DN を入力します。バインド DN の構文の例は次のとおりです。

   ```
   domain/user name

   ou=administrator,dc=ace,dc=com

   user@domain.name (for Active Directory)

   cn=Administrator,cn=Users,dc=ace,dc=com
   ```

   Active Directory の場合は、cn=groupname として指定されたグループ名が必要です。NetScaler Gateway で定義するグループ名とLDAPサーバー上のグループ名は同一である必要があります。

   その他の LDAP ディレクトリでは、グループ名は必要ないか、必要に応じて ou=groupname として指定します。

   NetScaler Gateway は、管理者の資格情報を使用してLDAPサーバーにバインドし、ユーザーを検索します。ユーザーを特定した後、NetScaler Gateway は管理者の資格情報をバインド解除し、ユーザーの資格情報で再バインドします。

c. と に、LDAP サーバーの管理者パスワードを入力します。

10. その他の LDAP 設定を自動的に取得するには、 をクリックします。

    をクリックすると、 の下のフィールドが自動的に入力されます。この手順を無視する場合は、手順 12 と 13 に進みます。それ以外の場合は、ステップ 14 に進みます。

11. ［**その他の設定］**の［サーバーログオン名の属性］に、構成するLDAPサーバーのユーザーログオン名をNetScaler Gateway が検索するときに使用する属性を入力します。デフォルトは `samAccountName` です。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

12. ** に、1 つまたは複数の Active Directory グループに関連付けられているユーザーを検索する値を入力します。

    たとえば、「memberOf=CN=GatewayAccess、OU=Groups、DC=Users、DC=LAB」などです。

    注：

    前の例を使用して、特定のADグループのメンバーにのみNetScaler Gateway アクセスを制限できます。

13. **で、Active Directory のデフォルトの memberOf のままにするか、属性を使用している LDAP サーバタイプの属性に変更します。この属性により、NetScaler Gateway は、承認中にユーザーに関連付けられたグループを取得できます。
14. で、セキュリティの種類を選択し、 をクリックします。
15. ユーザに LDAP パスワードの変更を許可するには、 を選択します。

    注：

    - セキュリティの種類として **PLAINTEXT** を選択した場合、ユーザーがパスワードを変更できるようにすることはサポートされません。
    - セキュリティのために **PLAINTEXT****または **TLS**を選択する場合は、ポート番号 389 を使用します。**SSL**を選択する場合は、ポート番号 636 を使用します。

LDAP ディレクトリ内の属性を決定する

NetScaler Gatewayで認証設定を構成できるように、LDAPディレクトリ属性の決定についてサポートが必要な場合は、Softerraの無償のLDAPブラウザーを使用して簡単に検索できます。

LDAP ブラウザは、 Softerra LDAP アドミニストレータの Web サイトからダウンロードできます 。ブラウザをインストールしたら、次の属性を設定します。

- LDAP サーバーのホスト名または IP アドレス。
- LDAP サーバーのポート。デフォルトは 389 です。
- ベース DN フィールド。空白のままにできます。LDAPブラウザーによって提供される情報は、NetScaler Gateway でこの設定を構成する必要があるベースDNを決定するのに役立ちます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 匿名バインドチェックは、LDAP サーバーに接続するためにユーザー資格情報が必要かどうかを判断します。LDAP サーバがクレデンシャルを必要とする場合は、チェックボックスをオフのままにします。

設定が完了すると、LDAP ブラウザは左ペインにプロファイル名を表示し、LDAP サーバに接続します。

LDAP グループ抽出の設定

2 要素認証を使用している場合、プライマリ認証ソースとセカンダリ認証ソースの両方から抽出されたグループが連結されます。認可ポリシーは、プライマリまたはセカンダリ認証サーバから抽出されたグループに適用できます。

LDAPサーバーから取得したグループ名は、NetScaler Gateway でローカルに作成されたグループ名と比較されます。2 つのグループ名が一致する場合、ローカルグループのプロパティは LDAP サーバから取得したグループに適用されます。

ユーザーが複数のLDAPグループに属している場合、NetScaler Gateway はユーザーが属するすべてのグループからユーザー情報を抽出します。ユーザーがNetScaler Gateway の2つのグループのメンバーであり、各グループにバインドされたセッションポリシーがある場合、ユーザーは両方のグループからセッションポリシーを継承します。ユーザーが正しいセッションポリシーを受け取るようにするには、セッションポリシーの優先度を設定します。

LDAP グループメンバーシップ属性の詳細については、以下を参照してください。

- LDAP グループ抽出がユーザオブジェクトから直接動作する仕組み
- LDAP グループ抽出がグループオブジェクトから間接的に動作する仕組み

LDAP グループ抽出がユーザオブジェクトから直接動作する仕組み

グループオブジェクトからグループメンバーシップを評価するLDAPサーバーは、NetScaler Gateway 認証をサポートします。

一部の LDAP サーバーでは、Active Directory (memberOf 属性を使用) や IBM eDirectory (groupMembership 属性を使用) など、オブジェクトが属するグループに関する情報をユーザーオブジェクトに含めることができます。ユーザーのグループメンバーシップは、IBM ディレクトリサーバー (IBM-AllGroups を使用) や Sun ONE ディレクトリサーバー (nsRole を使用) など、ユーザーオブジェクトの属性にすることができます。これらのタイプのLDAPサーバーはどちらも、NetScaler Gateway グループの抽出をサポートしています。

たとえば、IBM Directory Server では、静的グループ、動的グループ、およびネストされたグループを含むすべてのグループメンバーシップを、IBM-AllGroups 属性を使用して返すことができま

© 1997–2026 Citrix Systems, Inc. All rights reserved.

す。Sun ONE では、管理対象、フィルタ処理、ネストを含むすべてのロールは nsRole 属性を使用して計算されます。

LDAP グループ抽出がグループオブジェクトから間接的に動作する仕組み

グループオブジェクトからグループメンバーシップを間接的に評価するLDAPサーバーは、NetScaler Gateway 認証と互換性がありません。

Lotus Domino などの一部の LDAP サーバーでは、グループ・オブジェクトのみがユーザーに関する情報を格納できます。これらのLDAPサーバーでは、ユーザーオブジェクトにグループに関する情報を含めることができないため、NetScaler Gateway グループ抽出と互換性がありません。この LDAP サーバータイプでは、グループのメンバーリストでユーザーを検索することにより、グループメンバーシップの検索が実行されます。

LDAP 認可グループ属性フィールド

次の表に、LDAP グループ属性フィールドの例を示します。

LDAP サーバ	LDAP 属性
Microsoft Active Directory サーバー	memberOf
Novell eDirectory	groupMembership
IBM Directory Server	ibm-allGroups
Sun ONE ディレクトリ (旧iPlanet)	nsRole

LDAP 認証を設定するには

認証ポリシーで LDAP 認可を設定するには、グループ属性名とサブ属性を設定します。

1. 構成ユーティリティの［構成］タブで、［NetScaler Gateway］>［ポリシー］>［認証］の順に展開します。
2. で、認証の種類をクリックします。
3. 詳細ペインで、［Add］ をクリックします。
4. に、ポリシーの名前を入力します。
5. 「サーバー」の横にある「新規」をクリックします。
6. に、サーバーの名前を入力します。
7. に、LDAP サーバーの IP アドレスとポートを入力します。
8. に memberOf と入力します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

9. に CN と入力し、 をクリックします。
10. 「 認証ポリシーの作成 」ダイアログ・ボックスの「 名前付き表現」の横にある式を選択し、「 式の追加」をクリックし、「 作成 」をクリックして「 閉じる」をクリックします。

LDAP ネストされたグループ抽出の設定

NetScaler Gateway は、LDAPグループにクエリを実行し、認証サーバーで構成した祖先グループからグループおよびユーザー情報を抽出できます。たとえば、group1 を作成し、そのグループ内に group2 と group3 を作成したとします。ユーザーがグループ3に属している場合、NetScaler Gateway は、ネストされたすべての祖先グループ（group2、group1）から指定されたレベルまでの情報を抽出します。

認証ポリシーを使用して、LDAP ネストされたグループ抽出を設定できます。クエリが実行されると、NetScaler Gateway は、最大ネストレベルに達するまで、または使用可能なすべてのグループを検索するまでグループを検索します。

LDAP ネストされたグループ抽出を設定するには

1. 構成ユーティリティのナビゲーションペインで、［**NetScaler Gateway**］>［**ポリシー**］>［**認証/承認**］>［**認証** ］の順に展開し、［ **LDAP**］をクリックします。
2. 詳細ペインの タブで、 をクリックします。
3. に、ポリシーの名前を入力します。
4. 「サーバー」の横にある「 **新規**」をクリックします。
5. に、サーバーの名前を入力します。
6. LDAP サーバの設定を構成します。
7. を展開し、 をクリックします。
8. ［ **最大ネストレベル**］に、NetScaler Gateway がチェックするレベルの数を入力します。
9. ** に、LDAP サーバ上のグループ名を一意に識別する LDAP 属性名（`sAMAccountName` など）を入力します。
10. ** に、任意のグループの親グループを決定するために検索応答で取得する LDAP 属性名を入力します。例：`memberOf`。
11. **に、グループの親グループを決定するために、グループ検索属性の一部として検索する LDAP サブ属性名を入力します。たとえば、「CN」と入力します。
12. **に、クエリ文字列を入力します。たとえば、フィルタは`&(samaccountname=test)(objectClass=*)`です。
13. をクリックし、 をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

14. ダイアログボックスの の横で式を選択し、 をクリックし、 をクリックして をクリックします。

複数ドメインの LDAP グループ抽出の設定

認証に複数のドメインがあり、StoreFront またはWeb Interfaceを使用している場合は、グループ抽出を使用して正しいドメイン名をWeb Interfaceに送信するようにNetScaler Gateway を構成できます。

Active Directory では、ネットワーク内のドメインごとにグループを作成する必要があります。グループを作成したら、グループおよび指定したドメインに属するユーザーを追加します。Active Directory でグループを構成したら、NetScaler Gateway 上の複数のドメインのLDAPグループ抽出を構成します。

複数のドメインのグループ抽出用にNetScaler Gateway を構成するには、ネットワーク内のドメインの数と同じ数のセッションポリシーと認証ポリシーを作成する必要があります。たとえば、`Sampa`とChild という名前の2 つのドメインがあるとします。各ドメインは、1 つのセッションポリシーと 1 つの認証ポリシーを受け取ります。

ポリシーを作成したら、NetScaler Gateway でグループを作成し、セッションポリシーをグループにバインドします。次に、認証ポリシーを仮想サーバーにバインドします。

StoreFront を複数のドメインに展開する場合は、ドメイン間に信頼関係が必要です。

Citrix Endpoint ManagementまたはWeb Interfaceを複数のドメインに展開する場合、ドメインは相互に信頼する必要はありません。

グループ抽出のためのセッションポリシーの作成

グループ抽出のセッションポリシーを作成する最初の手順は、2 つのセッションプロファイルを作成し、次のパラメータを設定することです：

- ICA プロキシを有効にします。
- Web インターフェイス Web アドレスを追加します。
- Windows ドメインを追加します。
- プロファイルをセッションポリシーに追加し、式を true に設定します。

グループ抽出用のセッションプロファイルを作成するには

1. 構成ユーティリティの［構成］タブのナビゲーションペインで、［**Citrix Gateway**］>［**ポリシー**］を展開し、［**セッション**］をクリックします。
2. 詳細ペインで、 タブをクリックし、 をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. ** に、プロファイルの名前を入力します。たとえば、`Sampa`と入力します。
4. タブで、次の操作を行います：
   a. **ICAプロキシの横にある「 グローバル上書き 」**をクリックし、**「 オン」**を選択します。
   b. の横にある をクリックし、Web インターフェイスの Web アドレスを入力します。
   c. の横にある をクリックし、Windows ドメインの名前を入力して、 をクリックします。
5. ****で、最初のドメインの名前をクリアし、2 番目のドメインの名前 (Child など) を入力します。
6. の横で、最初の Windows ドメインの名前をクリアし、2 番目のドメインの名前を入力し、、の順にクリックします。

セッションプロファイルを作成したら、2 つのセッションポリシーを作成します。各セッションポリシーは、プロファイルの 1 つを使用します。

セッションポリシーを作成するには

1. 構成ユーティリティの［構成］タブのナビゲーションペインで、［**Citrix Gateway**］**>**［**ポリシー** ］を展開し、［**セッション**］をクリックします。
2. 詳細ペインの タブで、 をクリックします。
3. ** に、ポリシーの名前を入力します。
4. **「 リクエスト・プロファイル」**で、最初のドメインのプロファイルを選択します。
5. の横にある をクリックし、 を選択し、 をクリックして、** をクリックします。
6. ****で、名前を 2 番目のドメインに変更します。
7. **「 要求プロファイル」**で、2 番目のドメインのプロファイルを選択し、**「 作成」**、**「 閉じる** 」の順にクリックします。

複数ドメインの LDAP 認証ポリシーの作成

NetScaler Gateway でセッションポリシーを作成したら、ほぼ同じLDAP認証ポリシーを作成します。認証ポリシーを設定する場合、 重要なフィールドは検索フィルタです。このフィールドには、Active Directory で作成したグループの名前を入力する必要があります。

最初に認証プロファイルを作成し、次に認証ポリシーを作成します。

複数のドメイングループ抽出用の認証プロファイルを作成するには

1. 構成ユーティリティの［構成］タブで、［NetScaler Gateway**］>［ポリシー］>［認証］の順に展開します**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. ナビゲーションペインで ［**LADP**］ をクリックします。
3. 詳細ペインで、 タブをクリックし、 をクリックします。
4. に、最初のドメインの名前 (`Sampa` など) を入力します。
5. LDAP サーバーの設定を構成し、 をクリックします。
6. ステップ 3、4、5 を繰り返して 2 番目のドメインの認証プロファイルを設定し、 をクリックします。

プロファイルを作成して保存したら、認証ポリシーを作成します。

複数のドメイングループ抽出の認証ポリシーを作成するには

1. 構成ユーティリティの［構成］タブで、［ **Citrix Gateway**］ > ［**ポリシー**］ > ［**認証**］を展開します。
2. 詳細ウィンドウで、 タブをクリックし、 をクリックします。
3. に、最初のドメインの名前を入力します。
4. で を選択します。
5. 「 **サーバー**」で、最初のドメインの認証プロファイルを選択します。
6. の横にある をクリックし、 を選択し、 をクリックして、** をクリックします。
7. に、2 番目のドメインの名前を入力します。
8. で、2 番目のドメインの認証プロファイルを選択し、、** の順にクリックします。

複数ドメインの LDAP グループ抽出のためのグループおよびバインディングポリシーの作成

認証ポリシーを作成したら、NetScaler Gateway にグループを作成します。グループを作成したら、認証ポリシーを仮想サーバーにバインドします。

NetScaler Gateway でグループを作成するには

1. 構成ユーティリティの［ **構成** ］タブのナビゲーションペインで、［ **NetScaler Gateway**］ > ［**ユーザー管理** ］の順に展開し、［ **AAAグループ**］をクリックします。
2. 詳細ペインで、 をクリックします。
3. ****に、最初の Active Directory グループの名前を入力します。 **重要**：複数のドメインからグループを抽出するためにNetScaler Gateway でグループを作成する場合、グループ名はActive Directory で定義したグループと同じである必要があります。グループ名でも大文字と小文字が区別され、大文字と小文字は Active Directory で入力した大文字と小文字が一致する必要があります。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. 「 **ポリシー** 」タブで「 **セッション**」をクリックし、「 **ポリシーの挿入**」をクリックします。
5. でポリシーをダブルクリックし、 をクリックします。

認証ポリシーを仮想サーバーにバインドするには

1. 構成ユーティリティの［ **構成** ］タブのナビゲーションペインで、［ **Citrix Gateway** ］を展開し、［ **仮想サーバー**］をクリックします。
2. 詳細ペインで仮想サーバーを選択して、［**Open**］ をクリックします。
3. タブで をクリックし、 で をダブルクリックして、最初の認証ポリシーを選択します。
4. 「 **ポリシー名**」で、「 **ポリシーの挿入**」をクリックし、2 番目の認証ポリシーをダブルクリックして、「 **OK」**をクリックします。

LDAP認証の14日間パスワード有効期限通知

NetScaler Gatewayアプライアンスは、LDAPベース認証の14日間パスワード有効期限通知をサポートしています。この機能を使用することで、管理者はパスワード有効期限のしきい値（日数）についてエンドユーザーに通知できます。詳細については、「LDAP認証のパスワード有効期限通知」を参照してください。

クライアント証明書認証の構成

NetScaler Gateway 仮想サーバーにログオンするユーザーは、仮想サーバーに提示されるクライアント証明書の属性に基づいて認証することもできます。クライアント証明書認証は、LDAP や RADIUS などの他の認証タイプと一緒に使用して、2 要素認証を提供することもできます。

クライアント側の証明書属性に基づいてユーザーを認証するには、仮想サーバーでクライアント認証を有効にし、クライアント証明書を要求する必要があります。さらに、NetScaler Gateway上でルート証明書をその仮想サーバーにバインドする必要があります。

ユーザーがNetScaler Gateway 仮想サーバーにログオンすると、認証後、証明書の指定されたフィールドからユーザー名情報が抽出されます。通常、このフィールドはSubject:CNです。ユーザー名の抽出に成功すると、ユーザーの認証が完了します。認証は、次の場合に失敗します。

- セキュアソケットレイヤー (SSL) ハンドシェイク中にユーザーが有効な証明書を提供しない場合。
- ユーザー名の抽出が失敗し、認証が失敗します。

クライアント証明書に基づいて認証するには、既定の認証の種類としてクライアント証明書を指定します。また、「証明書アクション」を作成して、クライアントのSSL証明書に基づいた認証時の動作を定義することもできます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

GUI を使用してクライアント証明書をデフォルトの認証タイプとして設定するには

1. ［**構成**］>［**NetScaler Gateway**］の順に選択し、 ［**グローバル設定**］をクリックします。
2. 詳細ウィンドウの で、 をクリックします。
3. 要件に従って証明書を使用して 2 要素認証を有効にするには、 を選択します。
4. で、ユーザー名を保持する証明書フィールドの種類を選択します。
5. で、グループ名を保持する証明書フィールドのタイプを選択します。
6. に既定のグループの名前を入力し、 をクリックします。

クライアント証明書からのユーザー名の抽出

NetScaler Gatewayでクライアント証明書による認証を有効にすると、クライアント証明書の属性に基づいてユーザーが認証されます。認証が成功すると、証明書からユーザー名またはユーザーのユーザー名とグループ名が抽出されます。また、そのユーザーに指定されたポリシーが適用されます。

クライアント証明書認証ポリシーの構成およびバインド

クライアント証明書認証ポリシーを作成し、仮想サーバーにバインドできます。このポリシーを使用して、特定のグループまたはユーザーへのアクセスを制限できます。このポリシーは、グローバルポリシーよりも優先されます。

クライアント証明書認証ポリシーを構成するには、次の手順を実行します。

1. 構成ユーティリティの［構成］タブで、［**Citrix Gateway**］>［**ポリシー**］>［**認証**］を展開します。
2. ナビゲーションペインの で、 をクリックします。
3. 詳細ペインで、 をクリックします。
4. フィールドに、ポリシーの名前を入力します。
5. 「**サーバー**」の横にある「**新規**」をクリックします。
6. ** に、プロファイルの名前を入力します。
7. ［**2 要素**］ の横にある ［**オフ**］ を選択します。
8. フィールドと フィールドで値を選択し、 をクリックします。 注：以前にクライアント証明書をデフォルトの認証タイプとして構成した場合は、ポリシーに使用したものと同じ名前を使用します。デフォルトの認証タイプの フィールドと フィールドに入力した場合は、プロファイルにも同じ値を使用します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

9. 「**認証ポリシーの作成**」ダイアログ・ボックスの「**名前付き表現**」の横にある式を選択し、「**式の追加**」をクリックし、「**作成**」をクリックして「**閉じる**」をクリックします。

クライアント証明書ポリシーを仮想サーバーにバインドするには、次の手順を実行します。

クライアント証明書認証ポリシーを構成したら、そのポリシーを仮想サーバーにバインドできます。

1. 構成ユーティリティの［構成］タブのナビゲーションペインで、［**NetScaler Gateway**］を展開し、［**仮想サーバー**］をクリックします。
2. 詳細ペインで仮想サーバーをクリックし、 をクリックします。
3. **NetScaler Gateway 仮想サーバー**の構成ダイアログボックスで 、「**認証**」タブをクリックします。
4. **プライマリまたはセカンダリをクリックします**。
5. で、 をクリックします。
6. 「**ポリシー名**」でポリシーを選択し、「**OK**」をクリックします。

クライアント証明書を要求するように仮想サーバーを構成するには、次の手順を実行します。

認証にクライアント証明書を使用する場合は、SSL ハンドシェイク中にクライアント証明書が要求されるように仮想サーバーを構成する必要があります。

1. 構成ユーティリティの［構成］タブのナビゲーションペインで、［**NetScaler Gateway**］を展開し、［**仮想サーバー**］をクリックします。
2. 詳細ウィンドウで、 **仮想サーバーをクリックし** 、 をクリックします。
3. タブで、 をクリックします。
4. で、 をクリックします。
5. 「**クライアント証明書**」で「**オプション**」または「**必須**」を選択し、「OK」を 2 回クリックします。同じ仮想サーバーで他の認証タイプを許可し、クライアント証明書の使用を必要としない場合は、 を選択します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注

- コールバックURLについて詳しくは、「NetScaler Gateway のインポート」を参照してください。
- 証明書の詳細については、「証明書のインストール、リンク、および更新」を参照してください。

2 要素クライアント証明書認証の設定

最初にユーザを認証し、次に LDAP や RADIUS などのセカンダリ認証タイプでログオンするようにユーザに要求するようにクライアント証明書を設定できます。このシナリオでは、クライアント証明書が最初にユーザーを認証します。次に、ログオンページが表示され、ユーザー名とパスワードを入力できます。Secure Sockets Layer (SSL) ハンドシェイクが完了すると、ログオンシーケンスは次の 2 つのパスのいずれかを取ることができます。

- ユーザー名もグループも証明書から抽出されません。ログオンページがユーザーに表示され、有効なログオン資格情報の入力を求めるプロンプトが表示されます。NetScaler Gateway は、通常のパスワード認証の場合と同様に、ユーザーの資格情報を認証します。
- ユーザー名とグループ名は、クライアント証明書から抽出されます。ユーザー名のみが抽出された場合、ログオン名が存在するユーザーにログオンページが表示され、ユーザーは名前を変更できません。パスワードフィールドのみが空白です。

NetScaler Gateway が2回目の認証ラウンド中に抽出したグループ情報は、NetScaler Gateway が証明書から抽出したグループ情報（存在する場合）に追加されます。

スマートカード認証の構成

暗号化スマートカードを使用してユーザーを認証するようにNetScaler Gateway を構成できます。

NetScaler Gateway でスマートカードを構成するには、次の操作を行う必要があります。

- 証明書認証ポリシーを作成します。詳細については、「クライアント証明書認証の構成」を参照してください。
- 認証ポリシーを仮想サーバーにバインドします。
- クライアント証明書を発行する認証局（CA）のルート証明書をNetScaler Gateway に追加します。詳しくは、「To install a root certificate on NetScaler Gateway」を参照してください。

  重要：スマートカード認証のためにルート証明書を仮想サーバーに追加する場合は、 リストから証明書を選択する必要があります** 。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



クライアント証明書を作成したら、フラッシュと呼ばれる証明書をスマートカードに書き込むことができます。この手順を完了すると、スマートカードをテストできます。

スマートカードパススルー認証用に Web Interface を構成する場合、次のいずれかの条件が存在する場合、Web Interface へのシングルサインオンは失敗します：

- タブのドメインを`mydomain`の代わりに`mydomain`.comとして設定した場合 。
- タブでドメイン名を設定せず、値を1に設定するコマンド`wi-sso-split-upn`を実行した場合。この例では、userPrincipalName にはドメイン名「`mydomain`.com」が含まれています。

スマートカード認証を使用すると、ユーザーのログオンプロセスを合理化すると同時に、インフラストラクチャへのユーザーアクセスのセキュリティを強化できます。社内ネットワークへのアクセスは、公開キーインフラストラクチャを使用した証明書ベースの 2 要素認証によって保護されます。秘密キーは、ハードウェアで保護されるため、スマートカードの外に漏れることはありません。ユーザーは、スマートカードとPINを使用してさまざまなコーポレートデバイスからデスクトップとアプリケーションにアクセスできるようになります。

スマートカードは、Citrix Virtual Apps and Desktopsで提供されるデスクトップとアプリケーションのユーザー認証をStoreFront経由で行うために使用できます。StoreFront にログオンするスマートカードユーザーは、Citrix Endpoint Managementが提供するアプリケーションにもアクセスできます。ただし、クライアント証明書認証を使用するEndpoint Management Webアプリケーションにアクセスするには、再度認証する必要があります。

詳しくは、StoreFront ドキュメントの「 スマートカード認証の構成 」を参照してください。

セキュアな ICA 接続を使用したスマートカード認証の構成

NetScaler Gateway でシングルサインオンが構成されたスマートカードを使用してログオンし、安全なICA接続を確立するユーザーは、個人識別番号（PIN）の入力を求められることがあります。

- ログオン時、および公開リソースを起動しようとしたとき。この状況は、Webブラウザーと Citrix Workspace アプリが、クライアント証明書を使用するように構成された同じ仮想サーバーを使用している場合に発生します。
- Citrix Workspace アプリは、プロセスまたはセキュアソケットレイヤー（SSL）接続をWebブラウザーと共有しません。したがって、ICA接続がNetScaler GatewayとのSSLハンドシェイクを完了すると、クライアント証明書がもう一度必要になります。

ユーザーに 2 つ目の PIN プロンプトが表示されないようにするには、次の 2 つの設定を変更する必要があります。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- VPN 仮想サーバーでのクライアント認証は無効にする必要があります。
- SSL 再ネゴシエーションを有効にする必要があります。

仮想サーバーを構成したら、 Web Interface 5.3でのNetScaler Gateway 設定の構成の説明に従って、1つ以上のSTAサーバーを仮想サーバーにバインドします。

スマートカード認証をテストすることもできます。

クライアント認証を無効にするには、次の手順を実行します。

1. 構成ユーティリティの［構成］タブのナビゲーションペインで、［ NetScaler Gateway ］を展開し、［ 仮想サーバー］をクリックします。
2. メインの詳細ペインで関連する仮想サーバーを選択し、 をクリックします。
3. ウィンドウで、 をクリックします。
4. チェックボックスをオフにします。
5. ［完了］ をクリックします。

SSL 再ネゴシエーションを有効にするには、次の手順を実行します。

1. 構成ユーティリティを使用して、 タブから に移動し、 をクリックします。
2. メインパネルで、 をクリックします。
3. メニューから、 を選択します。

スマートカード認証をテストするには:

1. スマートカードをユーザーデバイスに接続します。
2. Webブラウザーを開き、NetScaler Gateway にログオンします。

RADIUS認証の構成

1つまたは複数のRADIUSサーバーでユーザーアクセスを認証するようにNetScaler Gateway を構成できます。RSA SecurID、SafeWord、または Gemalto Protiva 製品を使用している場合、これらの各製品は RADIUS サーバを使用して構成されます。

構成によっては、ネットワークアクセスサーバの IP アドレス (NAS IP) またはネットワークアクセスサーバ識別子 (NAS ID) の使用が必要になる場合があります。RADIUS認証サーバーを使用するようにNetScaler Gateway を構成する場合は、次のガイドラインに従ってください。

- NAS IPの使用を有効にすると、アプライアンスは、RADIUS接続の確立に使用されるソースIPアドレスではなく、構成済みのIPアドレスをRADIUSサーバに送信します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- NAS IDを構成すると、アプライアンスはRADIUSサーバーにこの識別子を送信します。NAS IDを構成しないと、アプライアンスはRADIUSサーバーにホスト名を送信します。
- NAS IP を有効にすると、アプライアンスは RADIUS サーバと通信するために NAS IP を使用して設定された NAS ID を無視します。

ジェムアルトプロティバの設定

Protiva は、Gemalto のスマートカード認証の長所を利用するために開発した、強力な認証プラットフォームです。Protiva では、ユーザーは Protiva デバイスによって生成されるユーザー名、パスワード、ワンタイムパスワードを使用してログオンします。RSA SecurID と同様に、認証要求は Protiva 認証サーバーに送信され、サーバーはパスワードを検証または拒否します。Gemalto Protiva をNetScaler Gateway と互換性があるように構成するには、次のガイドラインを使用します。

- Protiva サーバーをインストールします。
- インターネット認証サーバー (IAS) を拡張する Protiva SAS エージェントソフトウェアを Microsoft IAS RADIUS サーバーにインストールします。IAS サーバーの IP アドレスとポート番号を書き留めておいてください。
- NetScaler Gateway でRADIUS認証プロファイルを構成し、Protivaサーバーの設定を入力します。

セーフワードを構成する

SafeWord 製品ラインは、トークンベースのパスコードを使用した安全な認証を提供します。ユーザーがパスコードを入力すると、SafeWord は直ちにパスコードを無効にし、再度使用することはできません。SafeWord サーバーを構成するときは、次の情報が必要です。

- NetScaler Gateway のIPアドレス。IP アドレスは、RADIUS サーバクライアントの設定で設定した IP アドレスと同じ IP アドレスである必要があります。NetScaler Gateway は、内部IPアドレスを使用してRADIUSサーバーと通信します。共有シークレットを構成するときは、内部IPアドレスを使用します。2 つのアプライアンスを高可用性に設定する場合は、仮想内部 IP アドレスを使用します。
- 共有シークレット。
- SafeWord サーバーの IP アドレスとポート。デフォルトのポート番号は 1812 です。

RADIUS認証を構成するには

1. 構成ユーティリティの［構成］タブで、［NetScaler Gateway］>［ポリシー］>［認証］の順に展開します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. をクリックし、詳細ウィンドウの タブで、 をクリックします。
3. ダイアログボックスの に、ポリシーの名前を入力します。
4. に、ポリシーの名前を入力します。
5. 「 サーバー」の横にある「 新規」をクリックします。
6. ダイアログボックスの に、サーバーの名前を入力します。
7. の に、RADIUS サーバーの IP アドレスを入力します。
8. に、ポートを入力します。デフォルトは 1812 です。
9. の と に、RADIUS サーバーシークレットを入力します。
10. に ID 番号を入力し、 をクリックします。
11. 「 認証ポリシーの作成 」ダイアログ・ボックスの「 名前付き表現」の横にある式を選択し、「 式の追加」をクリックし、「 作成 」をクリックして「 閉じる」をクリックします。

RADIUS 認証プロトコルの選択

NetScaler Gateway は、ユーザー認証に次のようないくつかのプロトコルを使用するように構成されたRADIUSの実装をサポートしています。

- パスワード認証プロトコル (PAP)
- チャレンジハンドシェイク認証プロトコル (CHAP)
- Microsoftのチャレンジハンドシェイク認証プロトコル (MS-CHAP バージョン 1 およびバージョン 2)

NetScaler Gateway の展開環境がRADIUS認証を使用するように構成されており、RADIUSサーバーがPAPを使用するように構成されている場合は、強力な共有シークレットをRADIUSサーバーに割り当てることでユーザー認証を強化できます。強力な RADIUS 共有シークレットは、大文字、小文字、数字、および句読点のランダムなシーケンスで構成され、少なくとも 22 文字の長さです。可能であれば、ランダムな文字生成プログラムを使用して RADIUS 共有シークレットを判別します。

RADIUSトラフィックをさらに保護するには、各NetScaler Gateway アプライアンスまたは仮想サーバーに異なる共有シークレットを割り当てます。RADIUS サーバでクライアントを定義する場合、各クライアントに個別の共有秘密を割り当てることもできます。その場合は、RADIUS認証を使用する各NetScaler Gateway ポリシーを個別に構成する必要があります。

RADIUSポリシーを作成するときは、ポリシーの一部としてNetScaler Gateway で共有シークレットを構成します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

IP アドレス抽出の設定

RADIUSサーバーからIPアドレスを抽出するようにNetScaler Gateway を構成できます。ユーザがRADIUS サーバで認証されると、サーバは、ユーザに割り当てられているフレーム付き IP アドレスを返します。フレーム付き IP アドレスは、アクセス要求では RADIUS 属性 8 フレームド IP アドレスとも呼ばれます。

IP アドレス抽出のコンポーネントは次のとおりです：

- リモートRADIUSサーバーが、NetScaler Gateway にログオンしたユーザーの内部ネットワークからIPアドレスを提供できるようにします。
- **ipaddress**タイプを使用する任意の RADIUS 属性（ベンダーエンコードされた属性を含む）の設定を許可します。

IP アドレス抽出用に RADIUS サーバを設定する場合は、ベンダー ID と属性タイプを設定します。ベンダー ID と属性は、RADIUS クライアントと RADIUS サーバ間の関連付けを作成するために使用されます。

- ベンダー識別子（ID）により、RADIUS サーバは、RADIUS サーバで設定された IP アドレスのプールから、クライアントに IP アドレスを割り当てることができます。ベンダー ID は、内部ネットワークの IP アドレスを提供する RADIUS 応答の属性です。ゼロの値は、属性がベンダーエンコードされていないことを示します。
- 属性タイプは、RADIUS 応答のリモート IP アドレス属性です。最小値は 1 で、最大値は 255 です。

一般的な設定は、RADIUS **属性フレームの IP アドレスを抽出することです**。ベンダー ID が 0 に設定されているか、指定されていません。属性タイプは 8 に設定されます。

GUI を使用して RADIUS サーバからの IP アドレス抽出を設定するには、次の手順を実行します。

1. > > に移動し、
2. **詳細ペインの** タブで、RADIUS ポリシーを選択し、 をクリックします。
3. ダイアログボックスの の横にある をクリックします。
4. の に値を入力します。
5. 「 **グループ属性タイプ**」に値を入力し、 **「OK」** を 2 回クリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

RADIUS グループ抽出の設定

RADIUS 許可は、グループ抽出と呼ばれる方式を使用して設定できます。グループ抽出を構成すると、NetScaler Gateway にユーザーを追加するのではなく、RADIUSサーバー上のユーザーを管理できます。

RADIUS 許可を設定するには、認証ポリシーを使用し、グループベンダー ID（ID）、グループ属性タイプ、グループプレフィクス、およびグループセパレータを設定します。ポリシーを構成するときは、式を追加し、ポリシーをグローバルにバインドするか、仮想サーバにバインドします。

Windows Server 2003 での RADIUS の設定

Windows Server 2003でRADIUS認証にMicrosoftインターネット認証サービス（IAS）を使用している場合は、NetScaler Gateway の構成中に次の情報を提供する必要があります。

- ベンダー ID は、IAS で入力したベンダー固有のコードです。
- Type は、ベンダーによって割り当てられた属性番号です。
- 属性名は IAS で定義した属性名のタイプです。デフォルトの名前はctxUserGroups=

IAS が RADIUS サーバーにインストールされていない場合は、コントロールパネルの からインストールできます。詳細については、Windows オンラインヘルプを参照してください。

IAS を構成するには、Microsoft 管理コンソール (MMC) を使用して IAS のスナップインをインストールします。ウィザードの指示に従って、次の設定を選択してください。

- を選択します。
- を選択し、カスタムポリシーを作成します。
- ポリシーの を選択します。
- 次のいずれかのプロトコルを選択します。
  - Microsoftチャレンジハンドシェイク認証プロトコルバージョン 2（MS-CHAP v2）
  - Microsoftチャレンジハンドシェイク認証プロトコル（MS-CHAP）
  - チャレンジハンドシェイク認証プロトコル (CHAP)
  - 暗号化されていない認証 (PAP、SPAP)
- を選択します。

  ベンダー固有属性は、サーバー上のグループで定義したユーザーとNetScaler Gateway のユーザーを一致させる必要があります。この要件を満たすには、ベンダー固有の属性をNetScaler Gateway に送信します。必ず を選択してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- RADIUS のデフォルトは 0 です。この番号をベンダーコードに使用します。
- ベンダー割り当ての属性番号は 0 です。

  これは、 属性に割り当てられた番号です。属性は文字列形式です。
- に を選択します。

  Attribute 値には、属性名とグループが必要です。

  アクセスゲートウェイの場合、属性値は ctxUserGroups=GroupName です。売上と財務などの 2 つのグループが定義されている場合、属性値は ctxUserGroups=Sales; finance になります。各グループはセミコロンで区切ります。
- ダイアログボックスの他のすべてのエントリを削除し、 と表示されているエントリを残します。

IASでリモートアクセスポリシーを構成したら、NetScaler Gateway でRADIUS認証と承認を構成します。

RADIUS 認証を構成するときは、IAS サーバーで構成した設定を使用します。

Windows Server 2008 での認証用の RADIUS の設定

Windows Server 2008 では、インターネット認証サービス (IAS) に代わるネットワークポリシーサーバー (NPS) を使用して、RADIUS の認証と承認を構成します。サーバーマネージャーを使用して役割としてNPSを追加することで、NPSをインストールできます。

NPS をインストールするときに、ネットワークポリシーサービスを選択します。インストール後、ネットワークの RADIUS 設定を構成するには、 メニューの から NPS を起動します。NPSを開くと、NetScaler Gateway をRADIUSクライアントとして追加し、サーバーグループを構成します。

RADIUS クライアントを構成するときは、次の設定を選択してください。

- ベンダー名には、 を選択します。
- NetScaler Gateway で同じ共有シークレットを構成する必要があるため、共有シークレットを書き留めておきます。

RADIUS グループの場合、RADIUS サーバの IP アドレスまたはホスト名が必要です。デフォルト設定は変更しないでください。

RADIUS クライアントとグループを構成したら、次の 2 つのポリシーで設定を構成します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 接続要求ポリシー：ネットワークサーバーの種類、ネットワークポリシーの条件、ポリシーの設定など、NetScaler Gateway 接続の設定を構成します。
- 拡張認証プロトコル (EAP) 認証とベンダー固有の属性を設定するネットワークポリシー。

接続要求ポリシーを構成するときに、ネットワークサーバーの種類として を選択します。次に、条件として を選択し、値として を選択して、条件を設定します。

ネットワークポリシーを構成するときは、次の設定を構成する必要があります。

- ネットワークアクセスサーバーの種類として を選択します。
- EAP の と を選択します。
- に を選択します。

  デフォルトの属性番号は 26 です。この属性は、RADIUS 認可に使用されます。

  NetScaler Gateway には、サーバー上のグループで定義されたユーザーとNetScaler Gateway 上のユーザーを一致させるために、ベンダー固有の属性が必要です。これは、ベンダー固有の属性をNetScaler Gateway に送信することによって行われます。
- 属性形式として を選択します。

  Attribute 値には、属性名とグループが必要です。

  NetScaler Gateway の場合、属性値はctxUserGroups= グループ名です。売上と財務などの 2 つのグループが定義されている場合、属性値は ctxUserGroups=Sales; finance になります。各グループはセミコロンで区切ります。
- 区切り文字は、セミコロン、コロン、スペース、ピリオドなどのグループを区切るために NPS で使用した区切り文字です。

IASでのリモートアクセスポリシーの構成が完了したら、NetScaler Gateway でRADIUS認証と承認を構成できます。

RADIUS 認可を設定するには

1. 構成ユーティリティの［構成］タブで、［NetScaler Gateway］>［ポリシー］>［認証］の順に展開します。
2. をクリックします。
3. タブで、 をクリックします。
4. に、ポリシーの名前を入力します。
5. サーバーの下* をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

6. に、RADIUS サーバーの名前を入力します。
7. に、RADIUS サーバーの IP アドレスとポートを入力します。
8. で、 と の値を入力します。
9. で、認証プロトコルを選択し、 をクリックします。
10. 「 認証ポリシーの作成 」ダイアログ・ボックスの「 名前付き表現」の横にある式を選択し、「 式の追加」をクリックし、「 作成 」をクリックして「 閉じる」をクリックします。

RADIUS ユーザアカウンティングの設定

NetScaler Gateway は、ユーザーセッションの開始および停止メッセージをRADIUSアカウンティングサーバーに送信できます。各ユーザセッションで送信されるメッセージには、RFC2866 で定義されている属性のサブセットが含まれます。表 1 に、サポートされている属性と、送信される RADIUS アカウンティングメッセージ（RAD_START および RAD_STOP）のタイプを示します。表2に、`Acct-Terminate-Cause`属性に割り当てることができる定義済みの値と、対応する NetScaler Gateway イベントを示します。

表1. サポートされている RADIUS 属性

属性	意味	RAD_START	RAD_STOP
User-Name	セッションに関連付けられているユーザーの名前。	X	X
セッション ID	NetScalerセッション ID。	X	X
Acct-Session-Time	セッション継続時間 (秒)。	X	
Acct-Terminate-Cause	アカウント終了の理由。	X	

表2. RADIUS 終了の原因

NETSCALERのログアウト方法	RADIUS 終了の原因
LOGOUT_SESSN_TIMEDOUT	RAD_TERM_SESSION_TIMEOUT
LOGOUT_SESSN_INITIATEDBYUSER	RAD_TERM_USER_REQUEST

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NETSCALERのログアウト方法	RADIUS 終了の原因
LOGOUT_SESSN_KILLEDBYADMIN	RAD_TERM_ADMIN_RESET
LOGOUT_SESSN_TLOGIN	RAD_TERM_NAS_REQUEST
LOGOUT_SESSN_MAXLICRCHD	RAD_TERM_NAS_REQUEST
LOGOUT_SESSN_CLISECCHK_FAILED	RAD_TERM_NAS_REQUEST
LOGOUT_SESSN_PREAUTH_CHANGED	RAD_TERM_NAS_REQUEST
LOGOUT_SESSN_COOKIE_MISMATCH	RAD_TERM_NAS_REQUEST
LOGOUT_SESSS_DHT	RAD_TERM_NAS_REQUEST
LOGOUT_SESSS_2FACTOR_FAIL	RAD_TERM_NAS_REQUEST
LOGOUT_SESSN_ICALIC	RAD_TERM_NAS_REQUEST
LOGOUT_SESSN_INTERNALERR	RAD_TERM_NAS_ERROR

RADIUS ユーザアカウンティングの設定には、ポリシーのペアを作成する必要があります。最初のポリシーは、アカウンティングメッセージの送信先となる RADIUS サーバを指定する RADIUS 認証ポリシーです。2 つ目は、RADIUS アカウンティングポリシーをアクションとして使用するセッションポリシーです。

RADIUS ユーザアカウンティングを設定するには、次の手順を実行する必要があります。

1. RADIUS ポリシーを作成して、RADIUS アカウンティングサーバを定義します。アカウンティングサーバは、RADIUS 認証に使用するサーバと同じサーバにすることができます。
2. RADIUS ユーザアカウンティングサーバを指定するアクションとして RADIUS ポリシーを使用して、セッションポリシーを作成します。
3. セッションポリシーをグローバルにバインドしてすべてのトラフィックに適用するか、NetScaler Gateway 仮想サーバーにバインドして、その仮想サーバーを通過するトラフィックにのみ適用します。

RADIUS ポリシーを作成するには

1. 構成ユーティリティのナビゲーションペインで、［NetScaler Gateway］ノードを展開し、［ポリシー］を展開します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. 認証を展開し、RADIUS を選択します。
3. 詳細ペインの タブで、 をクリックします。
4. ポリシーの名前を入力します。
5. メニューからサーバを選択するか、 アイコンをクリックし、プロンプトに従って新しい RADIUS サーバを追加します。
6. ペインの メニューから、 を選択します。
7. ［Create］ をクリックします。

セッションポリシーを作成するには

RADIUS アカウンティングサーバを指定する RADIUS ポリシーを設定したら、次のように、アクションでこのアカウンティングサーバを適用するセッションポリシーを作成します。

1. 構成ユーティリティのナビゲーションペインで、［NetScaler Gateway］ノードを展開し、［ポリシー］を展開します。
2. を選択します。
3. メインの詳細ペインで、 を選択します。
4. ポリシーの名前を入力します。
5. メニューで、 アイコンをクリックして新しいセッションアクションを追加します。
6. セッションアクションの名前を入力します。
7. タブをクリックします。
8. メニューで、前に作成した RADIUS ポリシーを選択します。
9. ［Create］ をクリックします。
10. ペインの メニューから、 を選択します。
11. ［Create］ をクリックします。

セッションポリシーをグローバルにバインドするには

1. 構成ユーティリティのナビゲーションペインで、［NetScaler Gateway］ノードを展開し、［ポリシー］を展開します。
2. を選択します。
3. メインの詳細ペインの メニューから、 を選択します。
4. ［Bind］ をクリックします。
5. ペインで、前に作成したセッションポリシーを選択し、 をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

6. リストで、セッションポリシーの エントリをクリックし、0 ～ 64000 の値を入力します。
7. ［OK］ をクリックします。

セッションポリシーをNetScaler Gateway 仮想サーバーにバインドするには

1. 構成ユーティリティのナビゲーションペインで、［NetScaler Gateway］ノードを展開し、［仮想サーバー］を選択します。
2. メインの詳細ペインで、仮想サーバーを選択し、 をクリックします。
3. ペインで、 アイコンをクリックしてポリシーを選択します。
4. メニューから を選択し、 メニューで が選択されていることを確認します。
5. ［続行］ をクリックします。
6. ［Bind］ をクリックします。
7. ペインで、前に作成したセッションポリシーを選択し、 をクリックします。
8. ［OK］ をクリックします。

SAML認証の構成

セキュリティアサーションマークアップ言語 (SAML) は、ID プロバイダ (IdP) とサービスプロバイダの間で認証と承認を交換するための XML ベースの標準です。NetScaler Gateway はSAML認証をサポートしています。

SAML 認証を構成するときは、次の設定を作成します。

- IdP 証明書名。これは、IdP の秘密キーに対応するパブリックキーです。
- リダイレクト URL。これは認証 IdP の URL です。認証されていないユーザーは、この URL にリダイレクトされます。
- ユーザーフィールド。IdP が Subject タグの NameIdentifier タグとは異なる形式でユーザー名を送信する場合、このフィールドを使用してユーザー名を抽出できます。この設定はオプションです。
- 署名証明書名。これは、IdPへの認証要求に署名するために使用されるNetScaler Gateway サーバーの秘密キーです。証明書名を設定しない場合、アサーションは署名されずに送信されるか、認証要求が拒否されます。
- SAML 発行者名。この値は、認証要求が送信されるときに使用されます。issuer フィールドには、アサーションの送信元の機関を示す一意の名前が必要です。これはオプションのフィールドです。
- デフォルトの認証グループ。これは、ユーザが認証される認証サーバー上のグループです。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 2要素。この設定では、2 要素認証を有効または無効にします。
- 署名なしアサーションを拒否します。有効にすると、署名証明書名が構成されていない場合、NetScaler Gateway はユーザー認証を拒否します。

NetScaler Gateway はHTTPポストバインディングをサポートしています。このバインディングでは、送信側は、必要な情報を含むフォーム自動投稿を含む 200 OK でユーザーに返信します。具体的には、デフォルトフォームには、フォームがリクエストかレスポンスかに応じて `SAMLResponse`、`SAMLRequest`という名前の2つの非表示フィールドを含める必要があります。このフォームには relayState も含まれます。relayState は、送信側によって処理されない任意の情報を送信するために使用される状態または情報です。依存側が情報を送り返すので、送信側がRelayStateとともにアサーションを取得したときに、送信側が次に何をすべきかを知ることができます。RelayStateを暗号化または難読化することをお勧めします。

注

- NetScaler GatewayをCitrix CloudへのIdPとして使用する場合、NetScaler Gatewayで**RelayState**ルールを構成する必要はありません。
- IdPチェーンの場合は、最初のSAMLポリシーでのみ**RelayState**ルールを設定すれば十分です。このコンテキストでは、IdPチェーンとは、設定されたSAMLアクションが、別のSAMLアクションを含む認証仮想サーバーIdPを参照するシナリオです。

Active Directory フェデレーションサービス 2.0 の構成

Active Directory フェデレーションサービス (AD FS) 2.0 は、フェデレーションサーバーの役割で使用する任意の Windows Server 2008 または Windows Server 2012 コンピューターで構成できます。ADFSサーバーをNetScaler Gateway と互換性があるように構成する場合は、Windows Server 2008またはWindows Server 2012の証明書利用者信頼ウィザードを使用して、次のパラメーターを構成する必要があります。

Windows Server 2008 のパラメーター：

- 依存パーティ信頼。NetScaler Gateway メタデータファイルの場所（`https://vserver.fqdn.com/ns.metadata.xml`など）を指定します。vserver.fqdn.comは、NetScaler Gateway 仮想サーバーの完全修飾ドメイン名（FQDN）です。FQDN は、仮想サーバーにバインドされたサーバー証明書に記載されています。
- 承認規則。証明書利用者へのユーザーのアクセスを許可または拒否できます。

Windows Server 2012 年の変数:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 依存パーティ信頼。NetScaler Gateway メタデータファイルの場所（`https://vserver.fqdn.com/ns.metadata.xml`など）を指定します。vserver.fqdn.comは、NetScaler Gateway 仮想サーバーの完全修飾ドメイン名（FQDN）です。FQDN は、仮想サーバーにバインドされたサーバー証明書に記載されています。
- AD FS プロファイル。AD FS プロファイルを選択します。
- 証明書。NetScaler Gateway は暗号化をサポートしていません。証明書を選択する必要はありません。
- SAML 2.0 WebSSO プロトコルのサポートを有効にします。これにより、SAML 2.0 SSO のサポートが有効になります。NetScaler Gateway 仮想サーバーのURL（`https:netScaler.virtualServerName.com/cgi/samlauth`など）を指定します。

  このURLは、NetScaler Gateway アプライアンスのアサーションコンシューマサービスURLです。これは定数パラメーターであり、NetScaler Gateway はこのURLでSAMLレスポンスを期待します。
- 証明書利用者信頼識別子。NetScaler Gateway という名前を入力します。これは、`https://netscalerGateway.virtualServerName.com/adfs/services/trust`などの証明書利用者を識別する URLです。
- 承認規則。証明書利用者へのユーザーのアクセスを許可または拒否できます。
- 要求ルールを構成します。発行トランスフォームルールを使用して LDAP 属性の値を設定し、テンプレートを使用できます。次に、以下を含む LDAP 設定を構成します。
  - メールアドレス
  - sAMAccountName
  - ユーザー プリンシパル名 (UPN)
  - MemberOf
- 証明書の署名。署名検証証明書を指定するには、リレーパーティのプロパティを選択し、証明書を追加します。

  署名証明書が 2048 ビット未満の場合は、警告メッセージが表示されます。警告を無視して続行できます。テスト展開を設定している場合は、リレーパーティの証明書失効リスト（CRL）を無効にします。このチェックを無効にしない場合、AD FS は CRL で証明書を検証しようとします。

  CRLを無効にするには、次のコマンドを実行します。set-adfwRelayingPartyTrust-signingCertfiCateRvocatonNone-TargetName NetScaler

© 1997–2026 Citrix Systems, Inc. All rights reserved.

設定を構成したら、リレーパーティの信頼ウィザードを完了する前に、証明書利用者データを確認します。NetScaler Gateway 仮想サーバー証明書をエンドポイントURL（`https://vserver.fqdn.com/cgi/samlauth`など）で確認します。

リレーパーティの信頼ウィザードでの設定の構成が完了したら、構成済みの信頼を選択し、プロパティを編集します。以下の手順に従います：

- セキュアハッシュアルゴリズムを SHA-1 に設定します。

  注：Citrix はSHA-1のみをサポートしています。
- 暗号化証明書を削除します。暗号化されたアサーションはサポートされていません。
- 次の項目を含む要求ルールを編集します。
  - トランスフォームルールの選択
  - クレームルールの追加
  - 要求規則テンプレートの選択:LDAP 属性を要求として送信する
  - 名前を挙げて
  - 属性ストアの選択:Active Directory
  - LDAP 属性を選択:\<Active Directory parameters>
  - 「名前 ID」として「アウトゴーイングクレームルール」を選択します

  注:属性名の XML タグはサポートされていません。
- シングルサインオフのログアウト URL を設定します。要求ルールは です。カスタムルールは、次のとおりである必要があります。

```
=> issue(Type = "logoutURL", Value = "https://<adfs.fqdn.com>/adfs/
ls/", Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/
claimproperties/attributename"] =
"urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified");
```

AD FSの設定を構成したら、AD FS署名証明書をダウンロードし、NetScaler Gateway で証明書キーを作成します。その後、証明書とキーを使用して、NetScaler Gateway でSAML認証を構成できます。

SAML 二要素認証の設定

SAML の 2 要素認証を設定できます。LDAP 認証を使用した SAML 認証を設定する場合は、次のガイドラインに従ってください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- SAML がプライマリ認証タイプの場合、LDAP ポリシーで認証を無効にし、グループ抽出を設定します。次に、LDAP ポリシーをセカンダリ認証タイプとしてバインドします。
- SAML 認証はパスワードを使用せず、ユーザー名のみを使用します。また、SAML 認証は、認証が成功した場合にのみユーザーに通知します。SAML 認証が失敗した場合、ユーザーには通知されません。失敗応答は送信されないため、SAML はカスケードの最後のポリシーであるか、唯一のポリシーである必要があります。
- 不透明な文字列ではなく、実際のユーザー名を構成することをお勧めします。
- SAML をセカンダリ認証タイプとしてバインドすることはできません。

SAML 認証を設定するには

1. 構成ユーティリティの［構成］タブで、［**Citrix Gateway**］>［**ポリシー**］>［**認証**］を展開します。
2. ナビゲーションペインで、 をクリックします。
3. 詳細ペインで、 をクリックします。
4. ダイアログボックスの に、ポリシーの名前を入力します。



1. 「サーバー」の横にある「**新規**」をクリックします。
2. に、サーバープロファイルの名前を入力します。
3. で証明書を選択するか、 をクリックします。これは、SAML または IdP サーバーにインストールされる証明書です。

   をクリックした場合は、証明書と秘密キーを追加します。詳しくは、「Installing and Managing Certificates」を参照してください。
4. に、認証 ID プロバイダ (IdP) の URL を入力します。

   これは、SAML サーバーへのユーザーログオンの URL です。これは、NetScaler Gateway が最初の要求をリダイレクトするサーバーです。
5. で、サインアウトプロセスを完了するためにクライアントを IdP に返送するタイミングをアプライアンスが認識できるように、URL を指定します。
6. で、クライアントを SP から IdP に移動するために使用する方法を選択します。これは、IdP でクライアントがどのように接続するかを理解できるように、IdP で同じである必要があります。アプライアンスがSPとして動作する場合、POST、REDIRECT、およびARTIFACTバインディングをサポートします。
7. 「**ログアウトバインド**」で「**リダイレクト**」を選択します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

8. で、SAML 署名証明書の下にある IdPCert 証明書 (Base64) を選択します。

   注:

   をクリックして、メタデータ構成が格納されている** URL を選択することもできます。

9. **ユーザーフィールドに**、抽出するユーザー名を入力します。
10. で、アプライアンスが IdP への認証要求に署名するために使用する SAML SP 証明書（秘密キーを含む）を選択します。IdP が認証要求署名を検証できるように、同じ証明書（秘密キーなし）を IdP にインポートする必要があります。このフィールドは、ほとんどの IdP では必要ありません。

    これは、NetScaler Gateway 仮想IPアドレスにバインドされている証明書です。SAML 発行者名は、lb.example.com や ng.example.com など、ユーザーがログオンする完全修飾ドメイン名 (FQDN) です。
11. **発行者名に**、アプライアンスが初期認証（GET）要求を送信する負荷分散またはNetScaler Gateway 仮想IPアドレスのFQDNを入力します。
12. で、IdP からのアサーションに署名を要求するかどうかを指定します。アサーションのみを署名する (ON) か、アサーションと IdP からの応答の両方に署名する (STRICT) 必要があります。
13. に、IdP によって送信されたアサーションを適用できるオーディエンスを入力します。これは通常、サービスプロバイダーを表すエンティティ名または URL です。
14. 「 **署名アルゴリズム**」で、「RSA-SHA256」を選択します。
15. **ダイジェスト方式で**、SHA256 を選択します。
16. に、抽出されたグループに加えて、認証が成功した場合に選択されるデフォルトグループを入力します。
17. に、ユーザグループを含むアサーション内のタグの名前を入力します。
18. に、サービスプロバイダーが着信アサーションで許可する許容クロックスキューを分単位で指定します。
19. をクリックし、** をクリックします。
20. ダイアログボックスの の横にある を選択し、 を選択し、 をクリックして をクリックし、 をクリックします。

参照ドキュメント

- SAMLサービスプロバイダーとしてのNetScaler

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- SAML IDプロバイダーとしてのNetScaler
- SAMLでサポートされる追加機能

SAML認証を使用してNetScaler Gateway にログインする

SAML認証を使用して、Citrix VPNクライアントとワークスペースアプリを使用してNetScaler Gateway にログインできます。プラグインは、認証仮想サーバーにバインドされた高度な SAML ポリシー、つまり nFactor 認証を通じてのみ SAML 認証をサポートします。

重要：SAML ポリシーが VPN 仮想サーバーに直接バインドされている場合、プラグインは SAML 認証、つまり非 nFactor 認証をサポートしません。

サポートされているプラットフォームとアプリ

次の表に、NetScaler Gateway にログインするためのSAML認証をサポートするプラットフォームとアプリケーションを示します。

PRODUCT	バージョン
Citrix Gateway	バージョン 12.0 ビルド 41.16 以降
VPN クライアント	バージョン 12.1 ビルド 49.37 以降。**サポートされているプラットフォーム**：Windows 7、Windows 8、Windows 8.1、Windows 10
ワークスペースアプリのバージョン	Windows: 1808; Mac: 1808

高度な SAML ポリシーを使用した SAML 認証の設定

高度なSAMLポリシーを使用したSAML認証の構成について詳しくは、SAML IdPとしてのNetScaler ADCを参照してください。

SAML 認証の改善

この機能を使用するには、この情報を使用するには、SAML の知識、基本的な認証の習熟度、および FIPS の理解が必要です。

SAML 2.0仕様と互換性のあるサードパーティのアプリケーションおよびサーバーでは、次のNetScaler ADC機能を使用できます。

- SAML サービスプロバイダー (SP)
- SAML アイデンティティプロバイダ (IdP)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SP と IdP は、クラウドサービス間でシングルサインオン (SSO) を許可します。SAML SP 機能は、IdP からのユーザクレームに対処する方法を提供します。IdPは、サードパーティのサービスまたは別のNetScaler ADCアプライアンスにすることができます。SAML IdP 機能は、ユーザーログオンをアサートし、SP によって消費されるクレームを提供するために使用されます。

SAML サポートの一環として、IdP モジュールと SP モジュールの両方が、ピアに送信されるデータにデジタル署名します。デジタル署名には、SP からの認証要求、IdP からのアサーション、およびこれらの 2 つのエンティティ間のログアウトメッセージが含まれます。デジタル署名は、メッセージの信頼性を検証します。

SAML SP および IdP の現在の実装は、パケットエンジンでシグニチャ計算を実行します。これらのモジュールは SSL 証明書を使用してデータに署名します。FIPS準拠のNetScaler ADCでは、SSL証明書の秘密キーはパケットエンジンまたはユーザー空間で利用できないため、今日のSAMLモジュールはFIPSハードウェアに対応していません。

このドキュメントでは、シグニチャ計算を FIPS カードにオフロードするメカニズムについて説明します。署名の検証は、公開鍵が利用可能であるため、ソフトウェアで行われます。

解決策

SAML 機能セットは、シグニチャオフロードに SSL API を使用するように拡張されました。影響を受けるこれらのSAMLサブ機能について詳しくは、Citrix 製品ドキュメントを参照してください。

1. SAML SP ポストバインディング — 認証リクエストの署名
2. SAML IdP ポストバインディング — アサーション/レスポンス/両方の署名
3. SAML SP シングルログアウトシナリオ — SP 開始モデルでのログアウトリクエストの署名と IdP 開始モデルでのログアウトレスポンスの署名
4. SAML SP アーティファクトバインディング — ArtifactResolve リクエストの署名
5. SAML SP リダイレクトバインディング — 認証リクエストの署名
6. SAML IdP リダイレクトバインディング — レスポンス/アサーション/両方の署名
7. SAML SP 暗号化のサポート — アサーションの復号化

プラットフォーム

API は FIPS プラットフォームにのみオフロードできます。

構成

オフロード設定は FIPS プラットフォームで自動的に実行されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ただし、SSL 秘密キーは FIPS ハードウェアのユーザー空間では使用できないため、FIPS ハードウェアでの SSL 証明書の作成には若干の構成変更があります。

設定情報は次のとおりです。

- `add ssl fipsKey fips-key`

  CSR を作成し、CA サーバで使用して証明書を生成します。その後、その証明書を`/nsconfig/ssl`にコピーできます。ファイルが fips3cert.cerだと仮定しましょう。

- `add ssl certKey fips-cert -cert fips3cert.cer -fipsKey fips-key`

  次に、SAML SP モジュールの SAML アクションでこの証明書を指定します。

- `set samlAction <name> -samlSigningCertName fips-cert`

  同様に、SAML IdP モジュールの`samlIdpProfile`でこれを使用します。

- `set samlidpprofile fipstest –samlIdpCertName fips-cert`

最初に、前のセクションで説明された`fips-key`がありません。FIPS キーがない場合は、「FIPS キーの作成」 の説明に従って作成します。

```
create ssl fipskey <fipsKeyName> -modulus <positive_integer> [-exponent (3
| F4)]



create certreq <reqFileName> -fipskeyName <string>
```

TACACS+ 認証の設定

TACACS+ サーバを認証用に設定できます。RADIUS 認証と同様に、TACACS+ は秘密キー、IP アドレス、およびポート番号を使用します。デフォルトのポート番号は 49 です。

TACACS+サーバーを使用するようにNetScaler Gateway を構成するには、サーバーのIPアドレスとTACACS+シークレットを指定します。ポートを指定する必要があるのは、使用中のサーバーポート番号がデフォルトのポート番号である 49 以外の場合のみです。

ユーザインターフェイスを使用して TACACS+ 認証を設定するには、次の手順を実行します。

1. 構成ユーティリティの［構成］タブで、［**Citrix Gateway**］>［**ポリシー**］>［**認証**］を展開します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. をクリックします。
3. 詳細ペインで、 をクリックします。
4. フィールドに、ポリシーの名前を入力します。
5. フィールドの横にある をクリックして新しい TACACS サーバを作成するか、 をクリックして既存の TACACS サーバに変更を加えます。
6. フィールドに、サーバーの名前を入力します。
7. に IP アドレスを入力します。
8. で、デフォルトのポート番号 49 を使用します。
9. フィールドにキーを入力します。 フィールドに、同じキーを入力して確認します。
10. **［詳細］** クリックします。
11. で、 を選択し、 をクリックします。
12. ダイアログボックスで、式を選択し、、 の順にクリックします。

コマンドラインインターフェイスを使用して TACACS+ 認証を設定するには、次のコマンドを入力します。

```
add authentication tacacsAction <name> [-serverIP <ip_addr|ipv6_addr|*>][-
serverPort <port>] [-authTimeout <positive_integer>] {-tacacsSecret }

[-authorization ( ON | OFF )] [-accounting ( ON | OFF )][-auditFailedCmds
( ON | OFF )] [-groupAttrName <string>][-defaultAuthenticationGroup
<string>] [-Attribute1 <string>] [-Attribute2 <string>] [-Attribute3
<string>] [-Attribute4 <string>]

[-Attribute5 <string>] [-Attribute6 <string>] [-Attribute7 <string>] [-
Attribute8 <string>] [-Attribute9 <string>] [-Attribute10 <string>]

[-Attribute11 <string>] [-Attribute12 <string>] [-Attribute13 <string>] [-
Attribute14 <string>] [-Attribute15 <string>] [-Attribute16 <string>]
```

NetScaler Gateway でTACACS+サーバー設定を構成したら、ポリシーをバインドしてアクティブにします。ポリシーは、グローバルまたは仮想サーバレベルのいずれかでバインドできます。認証ポリシーのバインドの詳細については、「 認証ポリシーのバインド」を参照してください。

設定のクリアベーシック TACACS の設定をクリアしてはならない

このトピックでは、clear config コマンドの実行時に、RBA（ロールベースアクセス）関連の設定をすべてクリアしないことに重点を置いています。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

現在の clear config コマンドは、次の 3 つのレベルのいずれかで実行されます：

- 基本
- 拡張
- フル

レベルに基づいて、NetScaler ADC構成はクリアされ、工場出荷時のデフォルトにリセットされます。

使用されるコマンドは、

```
clear ns config [-force] <level>
```

新しいコマンドは、すべての RBA 関連設定の削除を許可または拒否するノブを追加します。

新しいコマンド

RBA 設定のクリア機能について説明します。

1. はい/いいえノブ。デフォルト:はい。

   管理者は、RBA 構成を保持するかどうかを決定します。
2. クリアコンフィグの基本レベルのみがサポートされています。
3. 次の設定はクリアされません。

   - システムユーザー/グループを追加/バインドします。
   - cmd ポリシーを追加します。
   - TACACS コマンド（TACACS アクション/ポリシーの追加）
   - システムグローバルをバインドする

   注: TACACS 関連の設定（アクション/ポリシー）は、ポリシーがシステムグローバルにバインドされている場合、またはクリアされた場合に保持されます。

CLI 構成

使用されるコマンドは、

```
clear config [–force] <level> [-RBAconfig]
```

デフォルトでは YES に設定され、レベルに基づいて設定がクリアされます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

— `RBAconfig`がNOに設定されている場合、RBA 関連の設定は保持されます。以下が含まれます：

- /bind システムユーザー /グループの追加
- システムグローバルをバインドする
- TACACS 関連コマンド（TACACS アクション/ポリシーの追加）
- cmd ポリシーの追加

多要素認証の設定

NetScaler Gateway では、次の2種類の多要素認証を構成できます。

- 認証優先度レベルを設定するカスケード認証
- 2 種類の認証を使用してユーザーがログオンする必要がある 2 要素認証

複数の認証サーバーがある場合は、認証ポリシーの優先順位を設定できます。設定した優先度レベルによって、認証サーバーがユーザーの資格情報を検証する順序が決まります。プライオリティ番号の小さいポリシーは、番号が大きいポリシーよりも優先されます。

2 つの異なる認証サーバに対してユーザを認証させることができます。たとえば、LDAP 認証ポリシーと RSA 認証ポリシーを設定できます。ユーザーがログオンすると、最初にユーザー名とパスワードで認証されます。次に、個人識別番号 (PIN) と RSA トークンのコードを使用して認証します。

カスケード認証の設定

認証では、ポリシーの優先順位付けを使用して、複数の認証サーバのカスケードを作成できます。カスケードを設定すると、システムはカスケードされたポリシーの定義に従って各認証サーバを走査して、ユーザのクレデンシャルを検証します。優先順位付けされた認証ポリシーは昇順でカスケードされ、1 ～ 9999 の範囲のプライオリティ値を持つことができます。これらの優先順位は、グローバルまたは仮想サーバレベルでポリシーをバインドするときに定義します。

認証中、ユーザーがログオンすると、最初に仮想サーバーがチェックされ、次にグローバル認証ポリシーがチェックされます。ユーザーが仮想サーバとグローバルの両方の認証ポリシーに属している場合は、最初に仮想サーバのポリシーが適用され、次にグローバル認証ポリシーが適用されます。グローバルにバインドされた認証ポリシーをユーザに受信させる場合は、ポリシーのプライオリティを変更します。グローバル認証ポリシーのプライオリティ番号が 1 で、仮想サーバにバインドされた認証ポリシーのプライオリティ番号が 2 の場合、グローバル認証ポリシーが優先さ

© 1997–2026 Citrix Systems, Inc. All rights reserved.

れます。たとえば、仮想サーバーにバインドされた 3 つの認証ポリシーがあり、各ポリシーの優先順位を設定できます。

ユーザがプライマリカスケードのポリシーに対する認証に失敗した場合、またはそのユーザがプライマリカスケードのポリシーに対する認証に成功しても、セカンダリカスケードのポリシーに対する認証に失敗した場合、認証プロセスは停止し、ユーザはエラーページにリダイレクトされます。

注：複数のポリシーを仮想サーバーまたはグローバルにバインドする場合は、すべての認証ポリシーに一意の優先順位を定義することをお勧めします。

グローバル認証ポリシーのプライオリティを設定するには

1. 構成ユーティリティの［構成］タブで、［ **Citrix Gateway**］**>**［**ポリシー** ］**>**［**認証**］を展開します。
2. グローバルにバインドされているポリシーを選択し、 で をクリックします。
3. ［ **認証グローバルポリシーのバインド/バインド解除** ］ダイアログボックスの［優先度］に番号を入力し、［ **OK］**をクリックします。

仮想サーバーにバインドされた認証ポリシーの優先順位を変更するには

仮想サーバーにバインドされている認証ポリシーを変更することもできます。

1. 構成ユーティリティの［構成］タブのナビゲーションペインで、［ **NetScaler Gateway**］を展開し、［ **仮想サーバー**］をクリックします。
2. 詳細ペインで仮想サーバーを選択して、**［Open］**をクリックします。
3. タブをクリックし、 または をクリックします。
4. 認証ポリシーの横にある に番号を入力し、 をクリックします。

2 要素認証の設定

NetScaler Gateway は2要素認証をサポートしています。通常、ユーザーを認証するとき、NetScaler Gateway は、構成された認証方法のいずれかを使用してユーザーを正常に認証するとすぐに認証プロセスを停止します。場合によっては、あるサーバーでユーザーを認証し、別のサーバーからグループを抽出する必要がある場合があります。たとえば、ネットワークでRADIUSサーバに対してユーザーを認証するが、RSA SecurIDトークン認証も使用しており、ユーザー・グループがそのサーバに格納されている場合、グループを抽出するために、そのサーバに対するユーザーの認証が必要になることがあります。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ユーザが 2 つの認証タイプを使用して認証され、そのうちの 1 つがクライアント証明書認証である場合、2 番目の認証方法として証明書認証ポリシーを構成できます。たとえば、プライマリ認証タイプとして LDAP を使用し、セカンダリ認証としてクライアント証明書を使用します。ユーザーがユーザー名とパスワードでログオンすると、ネットワークリソースにアクセスできます。

2 要素認証を構成する場合、認証タイプがプライマリまたはセカンダリのどちらであるかを選択します。

2 要素認証を構成するには

1. 構成ユーティリティの［構成］タブで、［NetScaler Gateway］>［ポリシー］>［認証］の順に展開します。
2. タブで、 をクリックします。
3. ダイアログボックスで、 をクリックします。
4. をクリックします。
5. で、認証ポリシーを選択します。
6. 「セカンダリ」をクリックし、ステップ 4 と 5 を繰り返して「OK」をクリックします。

シングルサインオンの認証タイプの選択

NetScaler Gateway でシングルサインオンと2要素認証を構成している場合は、シングルサインオンに使用するパスワードを選択できます。たとえば、LDAP がプライマリ認証タイプとして設定され、RADIUS がセカンダリ認証タイプとして設定されているとします。ユーザーがシングルサインオンを必要とするリソースにアクセスすると、デフォルトでユーザー名とプライマリパスワードが送信されます。セッションプロファイル内の Web アプリケーションへのシングルサインオンに使用するパスワードを設定します。

シングルサインオンの認証を構成するには

1. 構成ユーティリティの［構成］タブのナビゲーションペインで、［**NetScaler Gateway**］>［**ポリシー**］>［**セッション**］**の順に展開します**。
2. 詳細ウィンドウで、 タブをクリックし、次のいずれかの操作を行います。
   - 新しいプロファイルを作成するには、「**追加**」をクリックします。
   - 既存のプロファイルを変更するには、 をクリックします。
3. 「クライアントエクスペリエンス」タブの「認証情報インデックス」の横にある「**グローバル上書き**」をクリックし、「**プライマリ** 」または「**セカンダリ**」を選択します。
4. これが新しいプロファイルの場合は、 をクリックし、 をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. 既存のプロファイルを変更する場合は、「 **OK」**をクリックします。

クライアント証明書と LDAP の 2 要素認証の設定

LDAP でのスマートカード認証の使用など、LDAP 認証および承認でセキュアクライアント証明書を使用できます。ユーザーがログオンすると、クライアント証明書からユーザー名が抽出されます。クライアント証明書は認証のプライマリ形式で、LDAP はセカンダリ形式です。クライアント証明書認証は、LDAP 認証ポリシーよりも優先される必要があります。ポリシーのプライオリティを設定する場合、クライアント証明書認証ポリシーには、LDAP 認証ポリシーに割り当てる番号よりも小さい番号を割り当てます。

クライアント証明書を使用するには、Windows Server 2008 の証明書サービスなどのエンタープライズ認証局 (CA) が、Active Directory を実行しているのと同じコンピューターで実行されている必要があります。CA を使用してクライアント証明書を作成できます。

LDAP 認証および承認でクライアント証明書を使用するには、SSL（Secure Sockets Layer）を使用するセキュアな証明書である必要があります。LDAPでセキュアクライアント証明書を使用するには、クライアント証明書をユーザーデバイスにインストールし、対応するルート証明書を NetScaler Gateway にインストールします。

クライアント証明書を設定する前に、次の操作を行います。

- 仮想サーバーを作成します。
- LDAP サーバの LDAP 認証ポリシーを作成します。
- LDAP ポリシーの式を True 値に設定します。

LDAP を使用したクライアント証明書認証を構成するには

1. 構成ユーティリティの［構成］タブで、［**NetScaler Gateway**］>［**ポリシー**］>［**認証**］**の順に展開します**。
2. ナビゲーションペインの で、 をクリックします。
3. 詳細ペインで、［Add］ をクリックします。
4. に、ポリシーの名前を入力します。
5. で、 を選択します。
6. 「 サーバー」の横にある「 新規」をクリックします。
7. にサーバーの名前を入力し、 をクリックします。
8. ダイアログボックスの に、サーバーの名前を入力します。
9. の横にある を選択します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

10. フィールドで、 を選択し、 をクリックします。
11. ダイアログボックスで、 の横にある を選択し、、、 の順にクリックします。

証明書認証ポリシーを作成したら、ポリシーを仮想サーバーにバインドします。証明書認証ポリシーをバインドした後、LDAP 認証ポリシーを仮想サーバーにバインドします。

重要：LDAP認証ポリシーを仮想サーバーにバインドする前に、証明書認証ポリシーを仮想サーバーにバインドする必要があります。

NetScaler Gatewayにルート証明書をインストールするには

証明書認証ポリシーを作成したら、CA から Base64 形式でルート証明書をダウンロードしてインストールし、コンピュータに保存します。その後、ルート証明書をNetScaler Gateway にアップロードできます。

1. 構成ユーティリティの タブのナビゲーションウィンドウで、 を展開し、 をクリックします。
2. 詳細ペインで、［Install］をクリックします。
3. に、証明書の名前を入力します。
4. 「証明書ファイル名」で「参照」をクリックし、リストから「アプライアンス」または「ローカル」を選択します。
5. ルート証明書に移動し、、 の順にクリックします。

ルート証明書を仮想サーバーに追加するには

NetScaler Gateway にルート証明書をインストールしたら、仮想サーバーの証明書ストアに証明書を追加します。

重要：スマートカード認証のためにルート証明書を仮想サーバーに追加する場合は、次の図に示すように、 リストボックスから証明書を選択する必要があります。

図1：ルート証明書を CA として追加する



1. 構成ユーティリティの［構成］タブのナビゲーションペインで、［ NetScaler Gateway ］を展開し、［ 仮想サーバー］をクリックします。
2. 詳細ペインで仮想サーバーを選択し、 をクリックします。
3. ［証明書］タブの［使用可能］で証明書を選択し、［追加］の横の一覧で［CA］をクリックし、［OK］をクリックします。
4. ステップ 2 を繰り返します。
5. タブで、 をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

6. で、 を選択します。
7. ［その他］の［クライアント証明書］の横にある［オプション］を選択し、［OK］を 2 回クリックします。
8. クライアント証明書を構成したら、NetScaler Gateway プラグインを使用してNetScaler Gateway にログオンして認証をテストします。複数の証明書がインストールされている場合は、正しい証明書を選択するように求めるプロンプトが表示されます。証明書を選択すると、ログオン画面が表示され、証明書から取得した情報が入力されたユーザー名が表示されます。パスワードを入力し、 をクリックします。

ログオン画面の フィールドに正しいユーザ名が表示されない場合は、LDAP ディレクトリ内のユーザアカウントとグループを確認します。NetScaler Gateway で定義されているグループは、LDAPディレクトリのグループと同じである必要があります。Active Directory で、ドメインルートレベルでグループを構成します。ドメインルートレベルにない Active Directory グループを作成すると、クライアント証明書が正しく読み取られないことがあります。

ユーザーおよびグループがドメインルートレベルにない場合、NetScaler Gateway のログオンページには、Active Directory で構成されているユーザー名が表示されます。たとえば、Active Directory に「ユーザー」という名前のフォルダーがあり、証明書には CN=Users と記載されています。ログオンページの に という単語が表示されます。

グループおよびユーザーアカウントをルートドメインレベルに移動しない場合は、NetScaler Gateway で証明書認証サーバーを構成するときに、［ユーザー名］フィールドと［グループ名］フィールドを空白のままにします。

認証のためのネイティブOTPサポート

NetScaler Gateway は、サードパーティのサーバーを使用せずにワンタイムパスワード（OTP）をサポートします。ワンタイムパスワードは、生成される番号またはパスコードがランダムであるため、セキュリティで保護されたサーバーを認証するための非常に安全なオプションです。以前は、乱数を生成する特定のデバイスを持つRSAなどの専門企業が、OTPを提供していました。このシステムは、サーバーが期待する数値を生成するために、クライアントと常に通信している必要があります。

この機能は、設備コストと運用コストの削減に加えて、NetScalerアプライアンスの構成全体を維持することで、管理者の管理を強化します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注：

サードパーティのサーバーは不要になったため、NetScaler管理者はユーザーデバイスを管理および検証するためのインターフェイスを構成する必要があります。

OTPソリューションを使用するには、NetScaler Gateway 仮想サーバーに登録されている必要があります。登録は一意のデバイスごとに一度だけ必要で、特定の環境に制限することができます。登録ユーザーの設定と検証は、追加の認証ポリシーの設定と似ています。

ネイティブOTPサポートの利点

- Active Directory に加えて、認証サーバー上に追加のインフラストラクチャを用意する必要がなくなるため、運用コストが削減されます。
- 構成をNetScalerアプライアンスにのみ統合し、管理者に優れた制御を提供します。
- クライアントが期待する数値を生成するために、追加の認証サーバーへのクライアントの依存を排除します。

ネイティブ OTP ワークフロー

ネイティブ OTP ソリューションは 2 つのプロセスであり、ワークフローは次のように分類されます。

- デバイス登録
- エンドユーザログイン

重要： サードパーティのソリューションを使用している場合、またはNetScaler ADCアプライアンス以外のデバイスを管理している場合は、登録プロセスをスキップできます。追加する最後の文字列は、NetScalerで指定された形式である必要があります。

次の図は、OTP を受信する新しいデバイスを登録するためのデバイス登録フローを示しています。



注:

デバイスの登録は、さまざまな要素を使用して行うことができます。デバイス登録プロセスを説明するために、1 つの要素（前の図で指定）を例として使用します。

次の図は、登録済みデバイスを介した OTP の検証を示しています。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

前提条件

ネイティブ OTP 機能を使用するには、次の前提条件が満たされていることを確認してください。

- NetScaler機能のリリースバージョンは12.0ビルド51.24以降です。
- AdvancedエディションまたはPremiumエディションのライセンスがNetScaler Gateway にインストールされている。
- NetScaler Gateway は管理IPで構成されており、管理コンソールにはブラウザとコマンドラインの両方を使用してアクセスできます。
- NetScalerは、ユーザーを認証するための認証、承認、監査仮想サーバーで構成されています。
- NetScalerアプライアンスはUnified Gateway で構成され、認証、承認、監査プロファイルがGateway仮想サーバーに割り当てられます。
- ネイティブ OTP ソリューションは、nFactor 認証フローに制限されています。ソリューションを構成するには、高度なポリシーが必要です。詳細については、 CTX222713の文書を参照してください。

また、Active Directory については、次の点を確認してください：

- 属性の最小長は 256 文字です。
- 属性タイプは、ユーザパラメータなどの 'DirectoryString' でなければなりません。これらの属性は文字列値を保持できます。
- デバイス名が英語以外の文字である場合、属性文字列タイプは Unicode である必要があります。
- NetScaler LDAP管理者は、選択したAD属性への書き込みアクセス権を持っている必要があります。
- NetScalerアプライアンスとクライアントマシンは、共通のネットワークタイムサーバーと同期する必要があります。

GUI を使用したネイティブ OTP の設定

ネイティブ OTP 登録は、単要素認証だけではありません。次のセクションでは、シングルファクタ認証とセカンドファクタ認証の設定について説明します。

第 1 ファクタのログインスキーマの作成

1. **セキュリティ AAA > アプリケーショントラフィック > ログインスキーマに移動します。**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. に移動し、 をクリックします。
3. ページで、 フィールドに *lschema_single_auth_manage_otp* と入力し、 **noschema** の横にある をクリックします。
4. フォルダをクリックします。
5. 下にスクロールして **SingleAuth.xml** を選択し、 をクリックします。
6. ［**Create**］ をクリックします。
7. をクリックし、 をクリックします。
8. ** 画面で、次の値を入力します。

   名前: `lpol_single_auth_manage_otp_by_url` **プロファイル:**リストから l`pol_single_auth_manage_otp_by_url`を選択します。 **ルール:** `HTTP.REQ.COOKIE.VALUE("NSC_TASS").EQ("` manageotp `")`

認証、承認、および監査仮想サーバーの構成

1. > > に移動します。既存の仮想サーバーを編集する場合にクリックします。
2. 右側のペインの ** の の横にある アイコンをクリックします。
3. **「 ログインスキーマなし」を選択します。**
4. 矢印をクリックし、 **lpol_single_auth_manage_otp_by_url** ポリシーを選択します。
5. **lpol_single_auth_manage_otp_by_url****ポリシーを選択し、 をクリックします。
6. ［**Bind**］ をクリックします。
7. 上にスクロールし、 の下の を 1** つ選択します。
8. **nFactor ポリシーを** 右クリックし、** を選択します。
9. の下にある アイコンをクリックし、** を作成して をクリックします。
10. 画面で、次のように入力し、 をクリックします。

    名前: manage_otp_flow_label

    ログインスキーマ: Lschema_Int
11. 画面で、 アイコンをクリックしてポリシーを作成します。
12. ** 画面で、次のように入力します。

    名前: auth_pol_ldap_otp_action
13. リストを使用して、 を選択します。
14. フィールドで、 アイコンをクリックしてアクションを作成します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

15. ページで、 ラジオボタンを選択し、 の横にあるチェックボックスの選択を解除し、次の値を入力して、 を選択します。

    名前: ldap_otp_action

    IPアドレス:192.168.10.11

    ベース DN: DC = トレーニング、DC = ラボ

    管理者:Administrator@training.lab

    パスワード: `xxxxx`

16. **セクションまでスクロールします。ドロップダウンメニューを使用して、次のオプションを選択します。 **サーバーログオン名属性として「新規」**と入力し、**userprincipalname**と入力します。
17. ドロップダウンメニューを使用して を として選択し、 **userprincipalname**と入力します。
18. フィールドに「UserParameters」と入力し、 をクリックします。
19. 次の属性を入力します。

    属性 1 = **メール属性 2** = objectGUID **属性 3** = immutableID

20. ［**OK**］ をクリックします。
21. ページで、 を **true** に設定し、 をクリックします。
22. ページで、 をクリックし、 をクリックします。**
23. ページで、 をクリックします。
24. ページで、 をクリックし、 をクリックします。

注：

認証仮想サーバーは、RfWebUI ポータルテーマにバインドする必要があります。サーバー証明書をサーバーにバインドします。サーバー IP '1.2.3.5' には、後で使用するために対応する FQDN (otpauth.server.com) が必要です。

第 2 要素 OTP のログインスキーマの作成

1. > > に移動します。編集する仮想サーバーを選択します。
2. 下にスクロールして、 を選択します。
3. ［**Add Binding**］ をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. セクションで、 アイコンをクリックしてポリシーを追加します。
5. ページで、 に OTP と入力し、 アイコンをクリックしてプロファイルを作成します。
6. 「 **認証ログインスキーマの作成** 」ページで、「名前」に「OTP」と入力し、「 **noschema**」の横にあるアイコンをクリックします。
7. **LoginSchemaフォルダ** をクリックし 、**DualAuthManageOTP.xmlを**選択し **、をクリックします。
8. ［**Create**］ をクリックします。
9. セクションで、 **True**と入力します。 ［**Create**］ をクリックします。
10. ［**Bind**］ をクリックします。
11. 認証の 2 つの要素に注目してください。 をクリックし、 をクリックします。

OTP を管理するためのコンテンツスイッチングポリシーを構成する

Unified Gateway を使用している場合は、次の構成が必要です。

1. **Traffic Management > Content Switching > Policies**に移動します。コンテンツスイッチングポリシーを選択し、右クリックして を選択します。
2. 式を編集して次の OR ステートメントを評価し、 **「OK」**をクリックします。

vpn_url||HTTP.REQ.URL.CONTAINS(“`manageotp`”)

CLI を使用したネイティブ OTP の設定

OTP デバイス管理ページを設定するには、次の情報が必要です。

- 認証仮想サーバーに割り当てられた IP
- 割り当てられた IP に対応する FQDN
- 認証仮想サーバーのサーバー証明書

注:

ネイティブ OTP は Web ベースのソリューションのみです。

OTP デバイスの登録および管理ページを設定するには

認証仮想サーバーの作成

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
add authentication vserver authvs SSL 1.2.3.5 443

bind authentication vserver authvs -portaltheme RFWebUI

bind ssl vserver authvs -certkeyname otpauthcert
```

注:

認証仮想サーバーは RfWebUI ポータルテーマにバインドする必要があります。サーバー証明書をサーバーにバインドします。サーバー IP '1.2.3.5' には、後で使用するために対応する FQDN (otpauth.server.com) が必要です。

LDAP ログオンアクションを作成するには

```
add authentication ldapAction <LDAP ACTION NAME> -serverIP <SERVER IP> -
 serverPort <SERVER PORT> -ldapBase <BASE> -ldapBindDn <AD USER>
-ldapBindDnPassword <PASSWO> -ldapLoginName <USER FORMAT>
```

例：

```
add authentication ldapAction ldap_logon_action -serverIP 1.2.3.4
-serverPort 636 -ldapBase "OU=Users,DC=server,DC=com" -ldapBindDn
administrator@ctxnsdev.com -ldapBindDnPassword PASSWORD -ldapLoginName
userprincipalname
```

LDAP ログオンの認証ポリシーを追加するには

```
add authentication Policy auth_pol_ldap_logon -rule true -action
ldap_logon_action
```

Loginschemaを使用して UI を表示するには

ログオン時にユーザー名フィールドとパスワードフィールドをユーザーに表示する

```
add authentication loginSchema lschema_single_auth_manage_otp
-authenticationSchema "/nsconfig/loginschema/LoginSchema/
SingleAuthManageOTP.xml"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

デバイスの登録と管理ページを表示する

デバイスの登録画面と管理画面を表示するには、URLまたはホスト名の2つの方法をお勧めします。

- **URL を使う**

  URL に '/manageotp' が含まれている場合

  - `add authentication loginSchemaPolicy lpol_single_auth_manage_otp_by_url -rule "http.req.cookie.value("NSC_TASS").contains("manageotp")" -action lschema_single_auth_manage_otp`
  - `bind authentication vserver authvs -policy lpol_single_auth_manage_otp_by_url -priority 10 -gotoPriorityExpression END`

- **ホスト名を使う**

  ホスト名が「alt.server.com」の場合

  - `add authentication loginSchemaPolicy lpol_single_auth_manage_otp_by_host -rule "http.req.header("host").eq("alt.server.com")" -action lschema_single_auth_manage_otp`
  - `bind authentication vserver authvs -policy lpol_single_auth_manage_otp_by_host -priority 20 -gotoPriorityExpression END`

CLI を使用してユーザログインページを設定するには

ページを設定するには、次の情報が必要です。

- 負荷分散仮想サーバーの IP
- 負荷分散仮想サーバーの対応する FQDN
- 負荷分散仮想サーバーのサーバー証明書

```
bind ssl vserver lbvs_https -certkeyname lbvs_server_cert
```

負荷分散におけるバックエンドサービスは、次のように表されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
add service iis_backendsso_server_com 1.2.3.210 HTTP 80

bind lb vserver lbvs_https iis_backendsso_server_com
```

OTP パスコード検証アクションを作成するには

```
add authentication ldapAction <LDAP ACTION NAME> -serverIP <SERVER IP>
-serverPort <SERVER PORT> -ldapBase <BASE> -ldapBindDn <AD USER>
-ldapBindDnPassword <PASSWORD> -ldapLoginName <USER FORMAT>
-authentication DISABLED -OTPSecret <LDAP ATTRIBUTE>
```

例:

```
add authentication ldapAction ldap_otp_action -serverIP 1.2.3.4
-serverPort 636 -ldapBase "OU=Users,DC=server,DC=com" -ldapBindDn
administrator@ctxnsdev.com -ldapBindDnPassword PASSWORD -ldapLoginName
userprincipalname -authentication DISABLED -OTPSecret userParameters
```

重要:

LDAPログオンとOTPアクションの違いは、認証を無効にして新しいパラメータ `OTPSecret` を導入する必要があることです。AD 属性値は使用しないでください。

OTP パスコード検証の認証ポリシーを追加するには

```
add authentication Policy auth_pol_otp_validation -rule true -action
ldap_otp_action
```

LoginSchema を介して 2 要素認証を提示するには

2 要素認証用の UI を追加します。

```
add authentication loginSchema lscheme_dual_factor -authenticationSchema
"/nsconfig/loginschema/LoginSchema/DualAuth.xml"

add authentication loginSchemaPolicy lpol_dual_factor -rule true -action
lscheme_dual_factor
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ポリシーラベルを介してパスコード検証係数を作成するには

次の要素の管理OTPフローポリシーラベルを作成します（最初の要素はLDAPログオンです）

```
add authentication loginSchema lschema_noschema -authenticationSchema
noschema

add authentication policylabel manage_otp_flow_label -loginSchema
lschema_noschema
```

OTPポリシーをポリシー・ラベルにバインドするには

```
bind authentication policylabel manage_otp_flow_label -policyName
 auth_pol_otp_validation -priority 10 -gotoPriorityExpression NEXT
```

UI フローをバインドするには

LDAPログオンに続いて、認証仮想サーバーを使用したOTP検証をバインドします。

```
bind authentication vserver authvs -policy auth_pol_ldap_logon -priority
10 -nextFactor  manage_otp_flow_label -gotoPriorityExpression NEXT

bind authentication vserver authvs -policy lpol_dual_factor -priority 30
-gotoPriorityExpression END
```

NetScalerでデバイスを登録する

1. /manageotp サフィックスを付けて、NetScaler ADC FQDN（最初のパブリック向きのIP）に移動します。たとえば、 `<https://otpauth.server.com/manageotp>`。ユーザーの資格情報を使用してログインします。
2. アイコンをクリックしてデバイスを追加します。

   
3. デバイス名を入力して **Go**を押します。画面にバーコードが表示されます。
4. をクリックし、 をクリックします。
5. デバイスのカメラを QR コードの上に置きます。オプションでコードを入力できます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注:

表示された QR コードは 3 分間有効です。

6. スキャンが成功すると、ログインに使用できる 6 桁の時刻依存コードが表示されます。



7. テストするには、QR 画面で をクリックし、右側の緑色のチェックマークをクリックします。
8. ドロップダウンメニューからデバイスを選択し、Google Authenticator のコード（赤ではなく青である必要があります）を入力し、 をクリックします。
9. ページの右上隅にあるドロップダウンメニューを使用して、必ずログアウトしてください。

OTPを使用してNetScalerにログインします

1. 最初に公開されている URL に移動し、Google Authenticator から OTP を入力してログオンします。
2. NetScalerスプラッシュページに認証します。



OTP のプッシュ通知

Citrix Gateway は、OTPのプッシュ通知をサポートしています。ユーザーは、Citrix Gateway にログインするために、登録されたデバイスで受信したOTPを手動で入力する必要はありません。管理者は、プッシュ通知サービスを使用してユーザーの登録デバイスにログイン通知が送信されるようにCitrix Gateway を設定できます。ユーザーが通知を受け取ったら、通知の \[許可\] をタップするだけでCitrix Gateway にログインできます。Gateway は、ユーザーからの確認応答を受信すると、要求の送信元を識別し、そのブラウザ接続に応答を送信します。

タイムアウト時間（30秒）内に通知応答が受信されない場合、ユーザーはCitrix Gateway のログインページにリダイレクトされます。その後、ユーザは OTP を手動で入力するか、\[**再送信（Resend Notification）** \] をクリックして、登録されたデバイスで再度通知を受信できます。

管理者は、プッシュ通知用に作成されたログインスキーマを使用して、プッシュ通知認証をデフォルト認証として行うことができます。

重要：

プッシュ通知機能は、Citrix ADC Premiumエディションライセンスで利用できます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

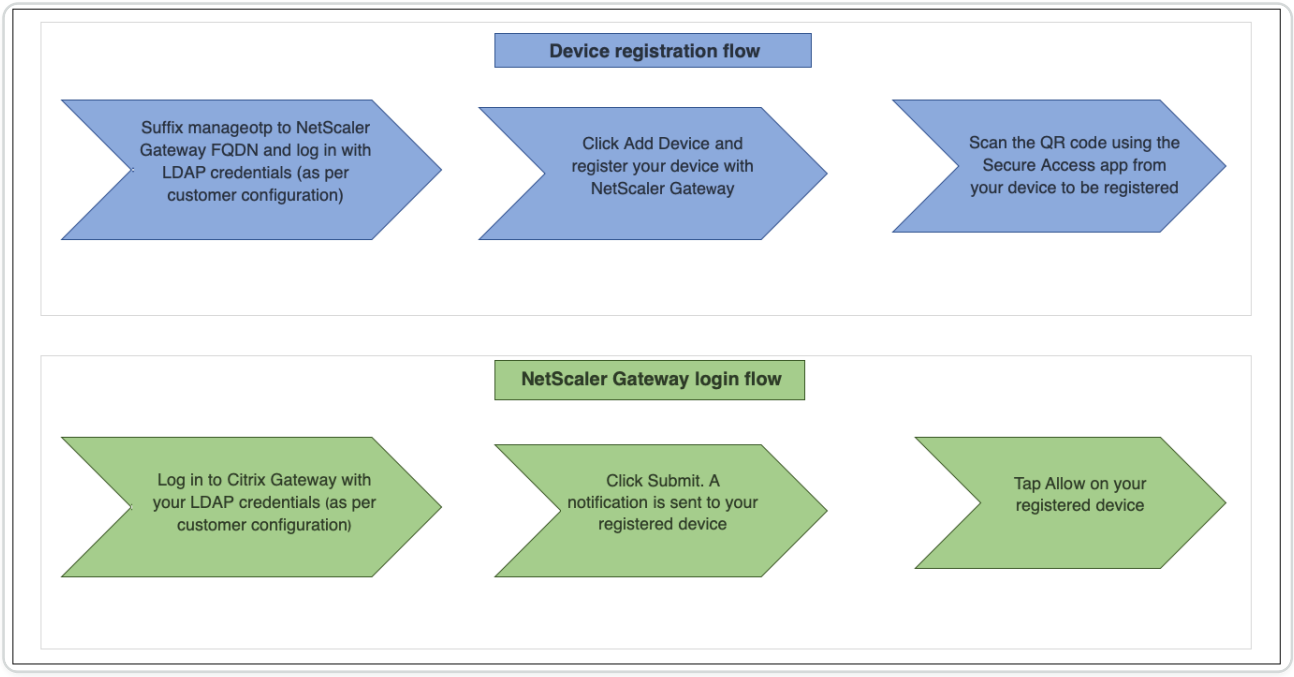
プッシュ通知の利点

- プッシュ通知は、より安全な多要素認証メカニズムを提供します。ユーザーがログイン試行を承認するまで、Citrix Gateway への認証は成功しません。
- プッシュ通知は、管理と使用が簡単です。ユーザーは、Citrix SSO モバイルアプリをダウンロードしてインストールする必要があります。管理者による支援は必要ありません。
- ユーザーはコードをコピーしたり覚えておく必要はありません。認証を受けるには、デバイスをタップするだけで済みます。
- ユーザーは複数のデバイスを登録できます。

プッシュ通知の動作

プッシュ通知ワークフローは、次の 2 つのカテゴリに分類できます。

- デバイス登録
- エンドユーザーログイン



プッシュ通知を使用するための前提条件

- Citrix Cloudのオンボーディングプロセスを完了します。

  a. Citrix Cloudの企業アカウントを作成するか、既存のアカウントに参加します。詳細なプロセスと手順については、「Citrix Cloudへのサインアップ」を参照してください。

  b. `<https://citrix.cloud.com>` にログインし、顧客を選択します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

c. 「メニュー」から「ID」と「アクセス管理」を選択し、「API Access」タブに移動して、顧客のクライアントを作成します。

d. ID、シークレット、カスタマー ID をコピーします。このIDとシークレットは、Citrix ADCでプッシュサービスを「ClientID」と「ClientSecret」として構成するために必要です。

重要：

- 同じ API 認証情報を複数のデータセンターで使用できます。
- オンプレミスのCitrix ADCアプライアンスは、サーバーアドレスのmfa.cloud.comとtrust.citrixWorkspacesapi.netを解決できる必要があり、アプライアンスからアクセスできる必要があります。これは、ポート 443 を介してこれらのサーバに対してファイアウォールまたは IP アドレスブロックがないことを保証するためです。

- iOSデバイスとAndroidデバイス用のアプリストアとPlayストアからCitrix SSO モバイルアプリをダウンロードします。プッシュ通知は、2.3.5からAndroid上のビルド1.1.13からiOSでサポートされています。
- Active Directory について次のことを確認します。
  - 属性の最小長は 256 文字以上にする必要があります。
  - 属性タイプは、ユーザーパラメータなどの 'ディレクトリ文字列' である必要があります。これらの属性は文字列値を保持できます。
  - デバイス名が英語以外の文字である場合、属性文字列タイプは Unicode である必要があります。
  - Citrix ADC LDAP管理者は、選択したAD属性への書き込みアクセス権を持っている必要があります。
  - Citrix ADCとクライアントマシンは、共通のネットワークタイムサーバーに同期する必要があります。

プッシュ通知の設定

プッシュ通知機能を使用するには、次の手順を完了する必要があります。

- Citrix Gateway 管理者は、ユーザーを管理および検証するためのインターフェイスを構成する必要があります。

a. プッシュ・サービスを構成します。

b. OTP管理とエンドユーザーログイン用にCitrix Gateway を構成します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix Gateway にログインするには、デバイスをGateway に登録する必要があります。

c. デバイスをCitrix Gateway に登録します。

d. Citrix Gateway にログインします

プッシュ・サービスの作成

1. \[**セキュリティ** \] > \[**AAA アプリケーショントラフィック** \] > \[**ポリシー** \] > \[**認証** \] > \[**高度なポリシー** \] > \[**アクション** \] > \[**プッシュサービス** \] に移動し、\[**追加** \] をクリックします。
2. 「 **名前」**に、プッシュ・サービスの名前を入力します。
3. 「 **クライアントID**」に、クラウド内のCitrix Pushサーバーと通信するための証明書利用者の一意のIDを入力します。
4. \[**クライアントシークレット**\] に、クラウド内のCitrix Pushサーバーと通信するための証明書利用者の一意のシークレットを入力します。
5. \[**顧客 ID**\] に、クライアント ID とクライアントシークレットのペアを作成するために使用するクラウド内のアカウントの顧客 ID または名前を入力します。

OTP管理とエンドユーザーログインのためのCitrix Gateway の構成

OTP 管理とエンドユーザログインを行うには、次の手順を実行します。

- OTP 管理用のログインスキーマの作成
- 認証、承認、監査仮想サーバーの構成
- VPN または負荷分散仮想サーバーの構成
- ポリシー・ラベルの構成
- エンド・ユーザー・ログイン用のログイン・スキーマの作成

設定の詳細については、ネイティブOTPサポートを参照してください。

重要: プッシュ通知の場合、管理者は以下を明示的に設定する必要があります。

- プッシュ・サービスを作成します。
- OTP管理用のログインスキーマを作成するときは、必要に応じてSingleAuthManageOTP.xmlログインスキーマまたは同等のログインスキーマを選択します。
- エンドユーザーログイン用のログインスキーマを作成するときは、必要に応じてDualAuthOrPush.xmlログインスキーマまたは同等のログインスキーマを選択します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

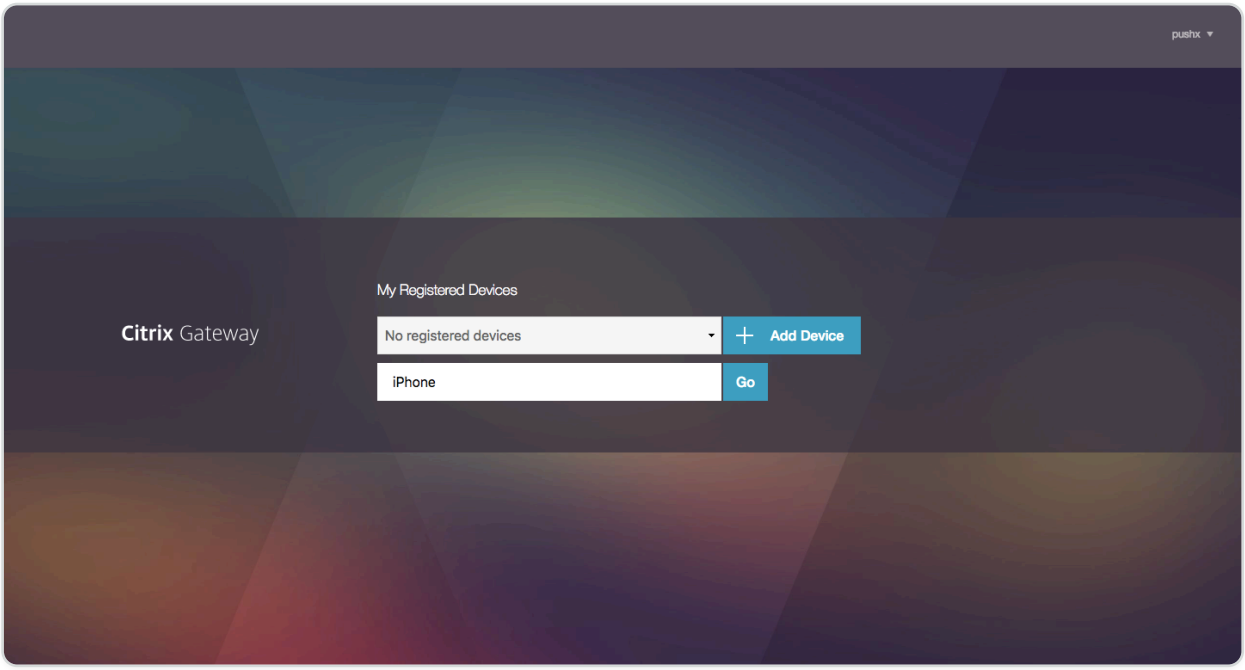
デバイスをCitrix Gateway に登録する

プッシュ通知機能を使用するには、デバイスをCitrix Gateway に登録する必要があります。

1. Webブラウザで、Citrix Gateway のFQDNを参照し、FQDNに **/manageotp** という接尾辞を付けます。

   認証ページが読み込まれます。 例： `<https://gateway.company.com/manageotp>`

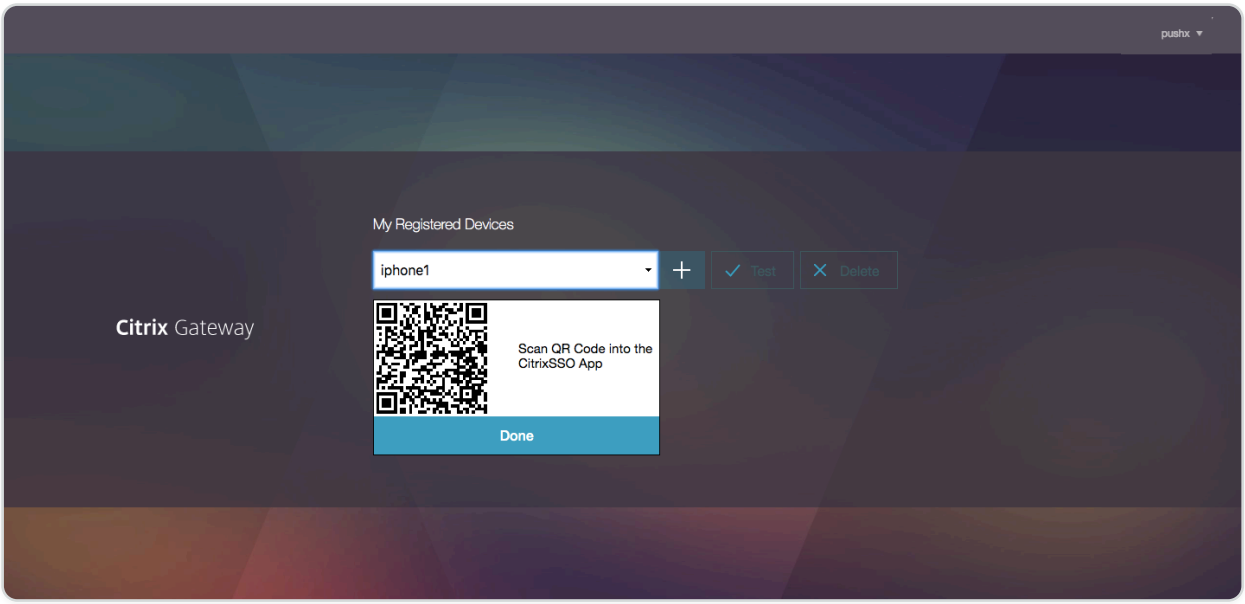
2. 必要に応じて、LDAP クレデンシャルまたは適切な 2 要素認証メカニズムを使用してログインします。



3. **［デバイスを追加］** をクリックします。
4. デバイスの名前を入力し、 **［実行］** をクリックします。

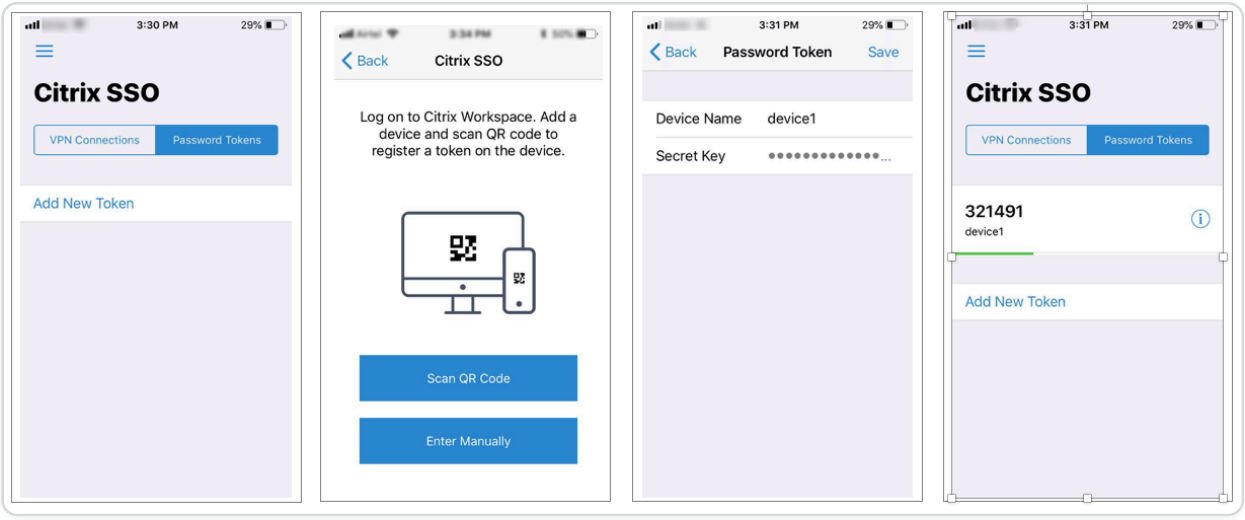
   Citrix Gateway のブラウザページにQRコードが表示されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



5. 登録するデバイスからCitrix SSO アプリを使用して、このQRコードをスキャンします。

   Citrix SSOはQRコードを検証し、プッシュ通知でゲートウェイに登録します。登録プロセスにエラーがない場合、トークンはパスワードトークンページに正常に追加されます。



6. 追加/管理するデバイスがない場合は、ページの右上隅にあるリストを使用してログアウトします。

ワンタイムパスワード認証のテスト

1. OTP をテストするには、リストからデバイスをクリックし、\[**Test**\] をクリックします。
2. デバイスで受信した OTP を入力し、\[**Go**\] をクリックします。

   「OTP 検証に成功しました」というメッセージが表示されます。
3. ページの右上隅のリストを使用してログアウトします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

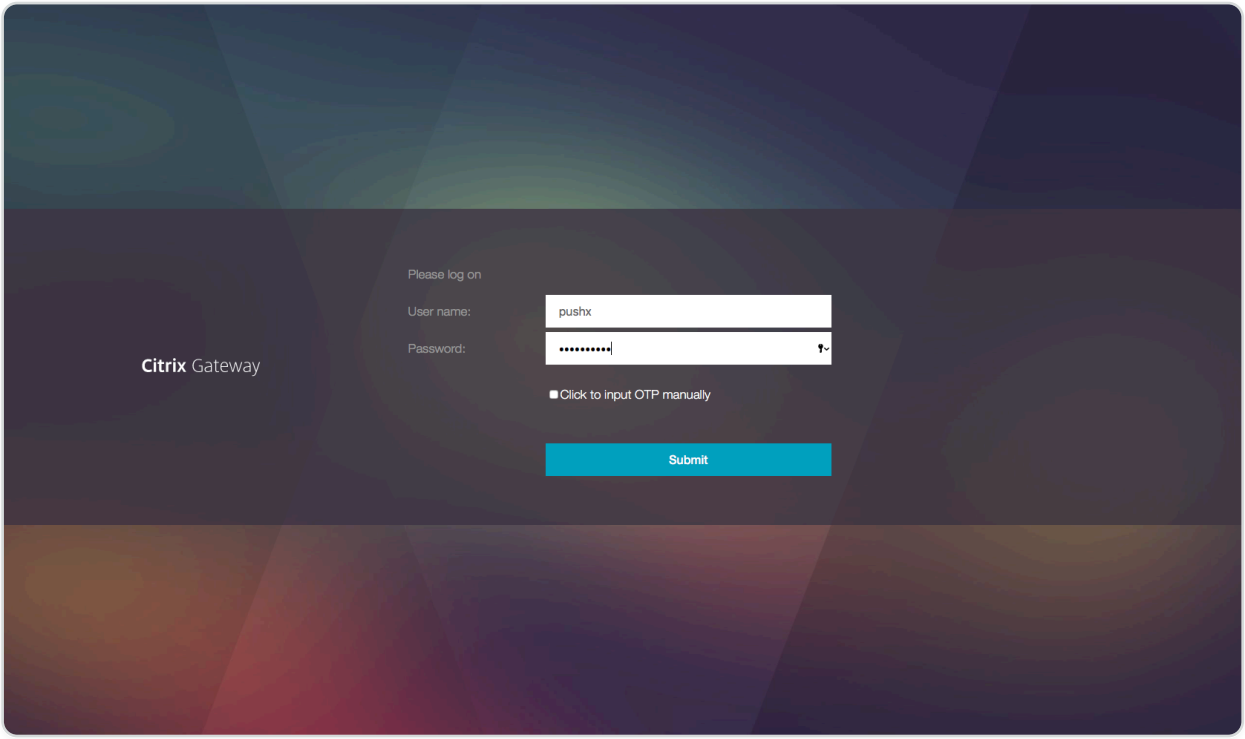
注：OTP 管理ポータルを使用して、認証のテスト、登録済みデバイスの削除、または追加のデバイスの登録をいつでも行うことができます。

Citrix Gateway にログインします

Citrix Gateway にデバイスを登録すると、ユーザーはプッシュ通知機能を使用して認証を行うことができます。

1. Citrix Gateway 認証ページに移動します（例：`<https://gateway.company.com>`）。

   ログインスキーマの構成に応じて、LDAP 認証情報のみを入力するように求められます。



2. LDAP ユーザー名とパスワードを入力し、\[**Submit**\] を選択します。

   登録済みのデバイスに通知が送信されます。

   注意: OTPを手動で入力する場合は、 **「クリックして** OTPを手動で入力する」を選択し、「**TOTP** 」フィールドにOTPを入力する必要があります。

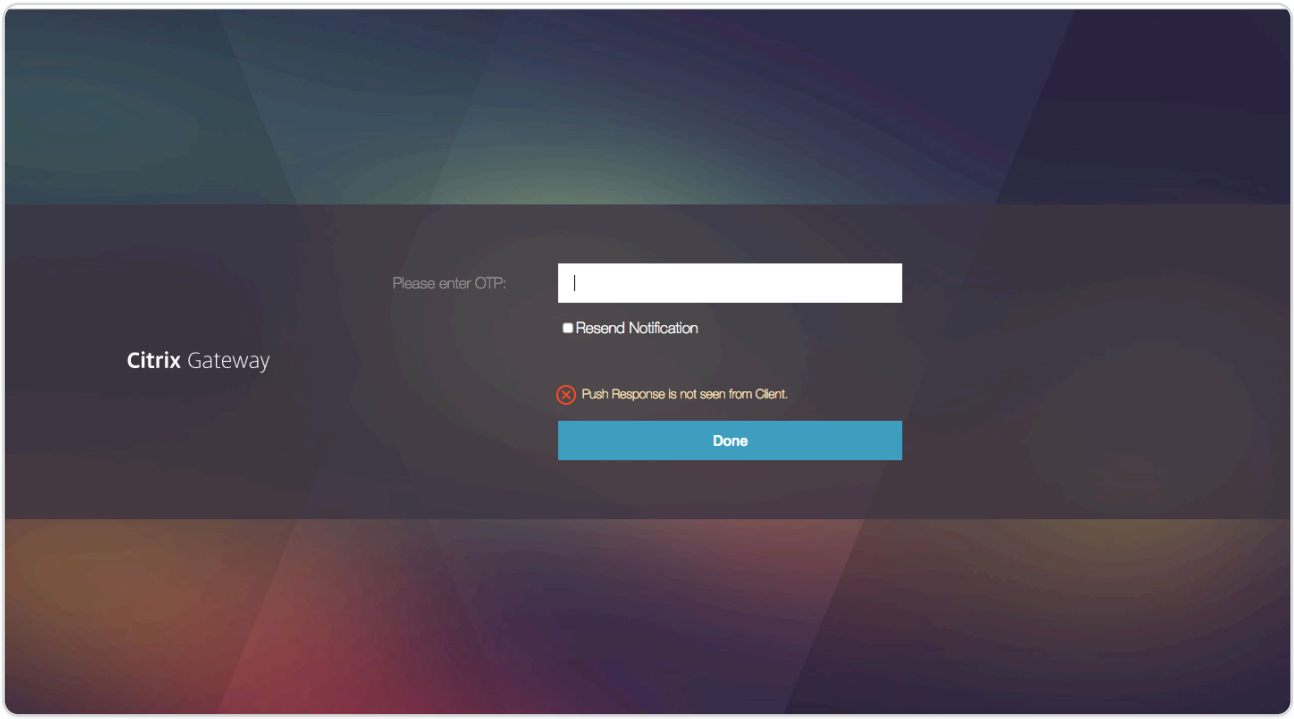
3. 登録したデバイスでCitrix SSO アプリを開き、 **［許可］**をタップします。

注：

- 認証サーバは、設定されたタイムアウト時間が経過するまで、プッシュサーバ通知応答を待機します。タイムアウト後、Citrix Gateway はログインページを表示します。その後、ユーザは OTP を手動で入力するか、\[**再送信（Resend Notification）** \] をクリックして、登録された

© 1997–2026 Citrix Systems, Inc. All rights reserved.

デバイスで再度通知を受信できます。選択したオプションに基づいて、Gateway は入力した OTP を検証するか、登録済みのデバイスに通知を再送信します。



- ログイン失敗に関する通知は、登録されたデバイスに送信されません。

障害状態

- 次の場合、デバイスの登録が失敗することがあります。
  - サーバー証明書がエンドユーザーのデバイスによって信頼されていない可能性があります。
  - OTPの登録に使用されたCitrix Gateway は、クライアントからアクセスできません。
- 通知は、次の場合に失敗することがあります。
  - ユーザーデバイスがインターネットに接続されていません
  - ユーザーデバイス上の通知がブロックされる
  - ユーザーがデバイス上の通知を承認しない

このような場合、認証サーバは、設定されたタイムアウト時間が経過するまで待機します。タイムアウト後、Citrix Gateway にはログインページが表示され、手動でOTPを入力するか、登録済みのデバイスに通知を再送信するかを選択できます。選択したオプションに基づいて、さらに検証が行われます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

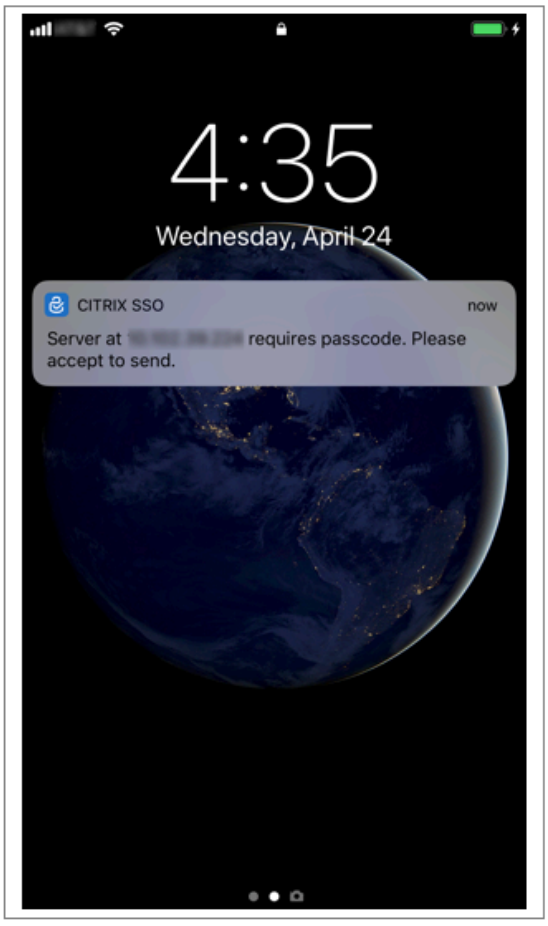
iOSでのCitrix SSO アプリケーションの動作 — 注意すべきポイント

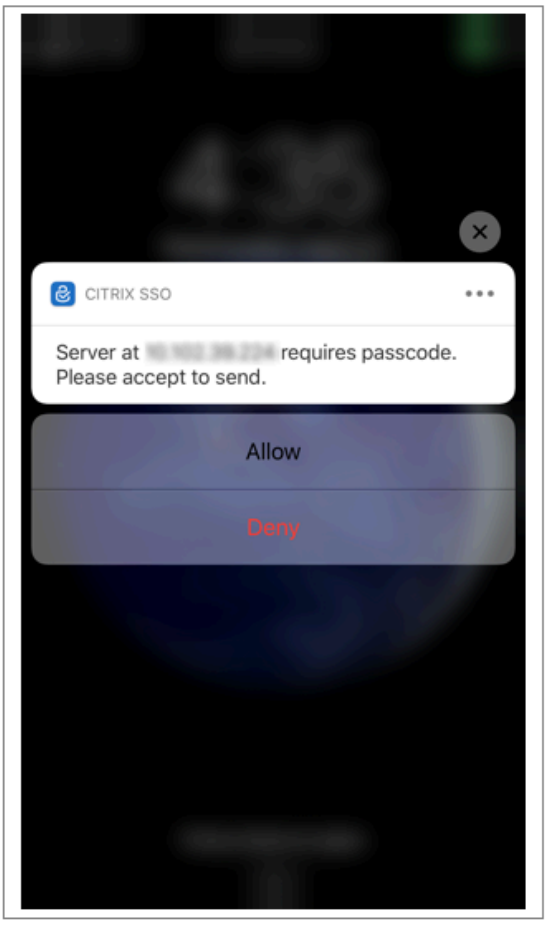
通知のショートカット

Citrix SSO iOSアプリには、ユーザーエクスペリエンスを向上させるためのアクション可能な通知のサポートが含まれています。iOSデバイスで通知を受信した後、デバイスがロックされているか、Citrix SSO アプリケーションがフォアグラウンドになっていない場合、ユーザーは通知に組み込まれたショートカットを使用してログイン要求を承認または拒否できます。

通知のショートカットにアクセスするには、デバイスのハードウェアに応じて、強制的にタッチ（3Dタッチ）または長押しする必要があります。［ショートカットの許可］アクションを選択すると、Citrix ADCにログイン要求が送信されます。認証、承認、および監査仮想サーバーでの認証ポリシーの構成方法に応じて、

- ログイン要求は、アプリをフォアグラウンドで起動したり、デバイスのロックを解除したりすることなく、バックグラウンドで送信されることがあります。
- アプリは、アプリがフォアグラウンドで起動される余分な要素として、Touch-ID/Face-ID/パスコードを要求することがあります。





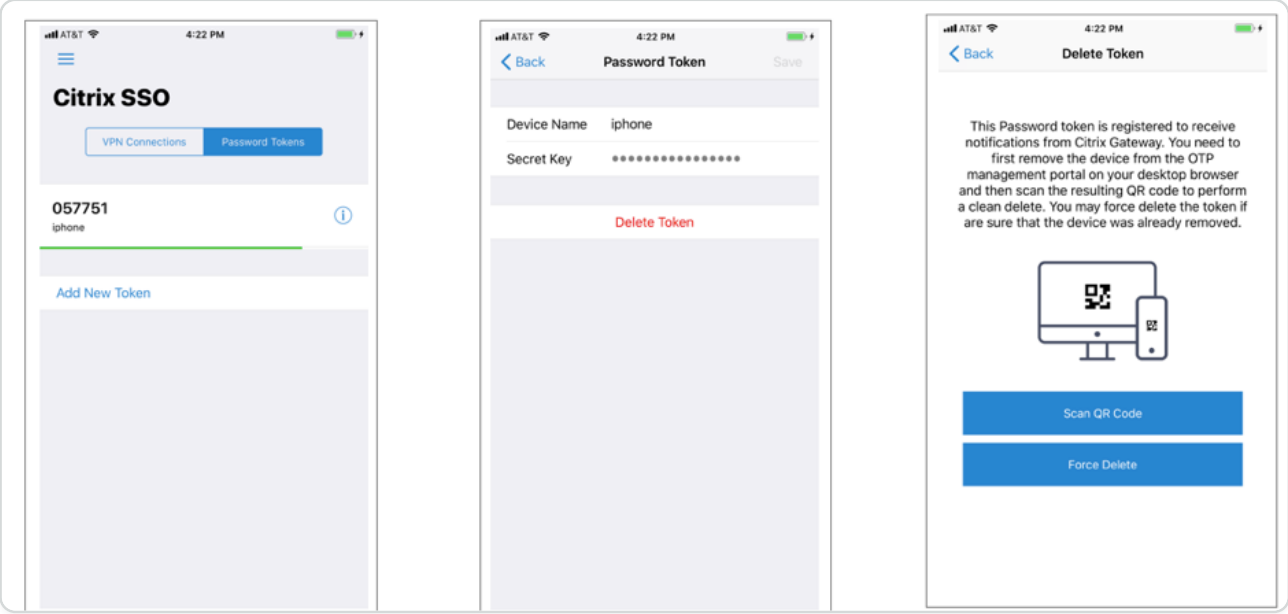
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix SSO からのパスワードトークンの削除

1. Citrix SSO アプリでプッシュ用に登録されたパスワードトークンを削除するには、以下の手順を実行する必要があります。
2. Gateway 上のiOS/Androidデバイスを登録解除（削除）します。デバイスから登録を削除するためのQRコードが表示されます。
3. Citrix SSO アプリを開き、削除するパスワードトークンの情報ボタンをタップします。
4. 「**トークンの削除**」をタップし、QRコードをスキャンします。

注：

- QRコードが有効な場合、トークンはCitrix SSO アプリから正常に削除されます。
- 端末がすでにGateway から削除されている場合は、QRコードをスキャンすることなく、「強制削除」をタップしてパスワードトークンを削除できます。強制削除を行うと、Citrix Gateway からデバイスが削除されていない場合でも、デバイスが通知を受信し続けることがあります。



シングルサインオンの設定

Windows、Webアプリケーション（SharePointなど）、ファイル共有、およびWeb InterfaceへのシングルサインオンをサポートするようにNetScaler Gateway を構成できます。シングルサインオンは、ユーザーがAccess Interfaceのファイル転送ユーティリティまたは通知領域のNetScaler Gateway アイコンメニューからアクセスできるファイル共有にも適用されます。

ユーザーがログオンするときにシングルサインオンを構成すると、ユーザーは資格情報をもう一度入力しなくても、自動的に再ログオンされます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Windows でのシングルサインオンの構成

ユーザーは、デスクトップからNetScaler Gateway プラグインを起動して接続を開きます。シングルサインオンを有効にすると、ユーザーがWindowsにログオンしたときにNetScaler Gateway プラグインが自動的に起動するように指定できます。シングルサインオンを構成すると、ユーザーのWindowsログオン資格情報が認証のためにNetScaler Gateway に渡されます。NetScaler Gateway プラグインのシングルサインオンを有効にすると、インストールスクリプトや自動ドライブマッピングなどのユーザーデバイスでの操作が容易になります。

シングルサインオンは、ユーザーデバイスが組織のドメインにログオンしている場合にのみ有効にします。シングルサインオンが有効で、ドメインに存在しないデバイスからユーザーが接続した場合、ユーザーはログオンするように求められます。

Windows でのシングルサインオンは、グローバルに、またはセッションポリシーにアタッチされたセッションプロファイルを使用して構成します。

Windows でシングルサインオンをグローバルに構成するには

1. 構成ユーティリティの［ **構成** ］タブのナビゲーションペインで、［ **Citrix Gateway** ］を展開し、［ **グローバル設定**］をクリックします。
2. 詳細ペインの で、 をクリックします。
3. ［ **クライアントエクスペリエンス** ］タブで、［ **Windows でのシングルサインオン**］をクリックし、［ **OK］**をクリックします。

セッションポリシーを使用して Windows でシングルサインオンを構成するには

1. 構成ユーティリティの［ **構成** ］タブのナビゲーションペインで、［ **Citrix Gateway**］ **>** ［**ポリシー**］を展開し、［ **セッション**］をクリックします。
2. 詳細ペインで、 をクリックします。
3. ** に、ポリシーの名前を入力します。
4. **「リクエストプロファイル」の横にある「 新規」**をクリックします。
5. ** に、プロファイルの名前を入力します。
6. ［ **クライアントエクスペリエンス** ］タブで、［ **Windowsでのシングルサインオン**］の横にある［ **グローバルを上書き**］、［ **Windowsでのシングルサインオン**］、［ **OK］**の順にクリックします。
7. ダイアログボックスで、 の横にある を選択し、 を選択し、 をクリックして をクリックし、 をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Web アプリケーションへのシングルサインオンの構成

Webベース認証を使用する内部ネットワーク内のサーバーにシングルサインオンを提供するようにNetScaler Gateway を構成できます。シングルサインオンを使用すると、ユーザーを SharePoint サイトなどのカスタムホームページや Web Interface にリダイレクトできます。また、ホームページで構成されたブックマークまたはユーザーがWebブラウザーに入力するWebアドレスから、NetScaler Gateway プラグインを使用してリソースへのシングルサインオンを構成することもできます。

ホームページを SharePoint サイトまたは Web Interface にリダイレクトする場合は、サイトの Web アドレスを指定します。ユーザーがNetScaler Gateway または外部認証サーバーによって認証されると、ユーザーは指定されたホームページにリダイレクトされます。ユーザクレデンシャルは Web サーバに透過的に渡されます。Web サーバーが資格情報を受け入れると、ユーザーは自動的にログオンします。Web サーバがクレデンシャルを拒否すると、ユーザはユーザ名とパスワードの入力を求める認証プロンプトを受け取ります。

Web アプリケーションへのシングルサインオンは、グローバルに構成することも、セッションポリシーを使用して構成することもできます。

Web アプリケーションへのシングルサインオンをグローバルに構成するには

1. ナビゲーションペインにある、［Configuration］タブの構成ユーティリティで、［NetScaler Gateway］を展開し、［Global Settings］をクリックします。
2. 詳細ペインの で、 をクリックします。
3. ［クライアントエクスペリエンス］タブで、［Web アプリケーションへのシングルサインオン］をクリックし、［OK］をクリックします。

セッションポリシーを使用して Web アプリケーションへのシングルサインオンを構成するには

1. 構成ユーティリティの［構成］タブのナビゲーションペインで、［ NetScaler Gateway］> ［ポリシー ］を展開し、［セッション］をクリックします。
2. 詳細ペインの タブで、セッションポリシーを選択し、 をクリックします。
3. 「 セッションポリシーの構成 」ダイアログ・ボックスの「 リクエスト・プロファイル」の横にある「 変更」をクリックします。
4. 「クライアントエクスペリエンス」タブで、「Web アプリケーションへのシングルサインオン」の横にある「グローバルオーバーライド」をクリックし、「Web アプリケーションへのシングルサインオン」をクリックして、「OK」をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Web アプリケーションへのシングルサインオン用の HTTP ポートを定義するには

シングルサインオンは、宛先ポートが HTTP ポートと見なされるネットワークトラフィックに対してのみ試行されます。HTTPトラフィックにポート80以外のポートを使用するアプリケーションへのシングルサインオンを許可するには、NetScaler Gateway で1つ以上のポート番号を追加します。複数のポートを有効にできます。ポートはグローバルに設定されます。

1. ナビゲーションペインにある、［Configuration］タブの構成ユーティリティで、［NetScaler Gateway］を展開し、［Global Settings］をクリックします。
2. 詳細ペインの で、 をクリックします。
3. タブで、 をクリックします。
4. ［HTTP ポート］にポート番号を入力し、［追加］をクリックし、［OK］を 2 回クリックします。

   追加するポートごとにステップ 4 を繰り返すことができます。

注:内部ネットワーク内の Web アプリケーションがパブリック IP アドレスを使用している場合、シングルサインオンは機能しません。シングルサインオンを有効にするには、クライアントレスアクセスまたはNetScaler Gateway プラグインがユーザーデバイス接続に使用されるかどうかにかかわらず、グローバルポリシー設定の一部として分割トンネリングを有効にする必要があります。グローバルレベルで分割トンネリングを有効にできない場合は、プライベートアドレス範囲を使用する仮想サーバを作成します。

LDAP を使用した Web アプリケーションへのシングルサインオンの構成

シングルサインオンを構成し、ユーザーが username@domain.com 形式のユーザープリンシパル名 (UPN) を使用してログオンすると、既定ではシングルサインオンが失敗し、ユーザーは 2 回認証する必要があります。ユーザーログオンにこの形式を使用する必要がある場合は、この形式のユーザー名を受け入れるように LDAP 認証ポリシーを変更します。

Web アプリケーションへのシングルサインオンを構成するには

1. 構成ユーティリティの［ **構成** ］タブで、［ **Citrix Gateway**］**>**［**ポリシー**］**>**［**認証**］を展開します。
2. 詳細ペインの タブで、LDAP ポリシーを選択し、 をクリックします。
3. ダイアログボックスの の横にある をクリックします。
4. **の に「DC=ドメイン名, DC=COM」と入力します。
5. に「LDAPaccount@domainname.com」と入力します。ここで、domainname.com はドメインの名前です。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

6. と に、パスワードを入力します。
7. **の に UserPrincipalName と入力します。
8. **に memberOf と入力します。
9. **に CN と入力します。
10. ［ **SSO 名属性］**に、ユーザーがログオンするときの形式を入力し、［ **OK**］ を 2 回クリックします。この値は `SamAccountName` または `UserPrincipalName` です 。

ドメインへのシングルサインオンの設定

ユーザーがCitrix Virtual Apps を実行しているサーバーに接続してSmartAccessを使用する場合は、サーバーファームに接続するユーザーのシングルサインオンを構成できます。セッションポリシーとプロファイルを使用して公開アプリケーションへのアクセスを構成する場合は、サーバーファームのドメイン名を使用します。

また、ネットワーク内のファイル共有へのシングルサインオンを構成することもできます。

ドメインへのシングルサインオンを構成するには

1. 構成ユーティリティの［構成］タブのナビゲーションペインで、［ NetScaler Gateway］> ［ポリシー ］を展開し、［セッション］をクリックします。
2. 詳細ペインの タブで、セッションポリシーを選択し、 をクリックします。
3. 「 セッションポリシーの構成 」ダイアログ・ボックスの「 リクエスト・プロファイル」の横にある「 変更」をクリックします。
4. 「 セッションプロファイルの設定 」ダイアログボックスの「 公開アプリケーション 」タブの「シングルサインオンドメイン」で、「 Override Global」をクリックし、ドメイン名を入力して「OK」を 2 回クリックします。

Citrix Virtual Appsを使用したNetScaler Gateway の構成について詳しくは、「NetScaler GatewayとCitrix Virtual Apps and Desktopsの統合」を参照してください。

Microsoft Exchange 2010 のシングルサインオンの構成

次のセクションでは、NetScaler Gateway でのMicrosoft Exchange 2010のシングルサインオン（SSO）の構成について説明します。Outlook Web Access (OWA) 2010 用の SSO は、次の条件では機能しません。

- Microsoft Exchange 2010 でのフォームベースの認証を使用する。
- 認証、承認、および監査トラフィック管理ポリシーを使用した仮想サーバの負荷分散。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注：

この設定は、認証、認可、および監査トラフィック管理ポリシーを持つ仮想サーバの負荷分散でのみ機能します。クライアントレス VPN を使用した OWA 2010 の SSO では機能しません。

次の手順は、NetScaler Gateway でMicrosoft Exchange 2010のSSOを構成する前に考慮する必要がある前提条件です。

- SSO フォームのアクション URL は OWA 2010 では異なります。トラフィック管理ポリシーを適宜変更します。
- logon.aspx リクエストで `PBack` Cookie を設定するには、書き換えポリシーが必要です。通常のシナリオでは、クライアントで `PBack` Cookie を設定し、 をクリックします。
- SSOを使用している場合、logon.aspx への応答が消費され、NetScaler Gateway によってフォーム要求が生成されます。クッキーはフォーム送信リクエストに添付されません。
- OWA サーバーは、フォーム送信要求で `PBack` Cookie を期待します。書き換えポリシーは、フォーム送信リクエストに `PBack` Cookie をアタッチするために必要です。

CLI を使用して、次の操作を実行します

1. 認証、認可、および監査のトラフィック管理の設定

   ```
   add tm formSSOAction OWA_Form_SSO_SSOPro -actionURL "/owa/auth.owa"
   -userField username -passwdField password -ssoSuccessRule
   "http.RES.SET_COOKIE.COOKIE(\"cadata\").VALUE(\"cadata\").LENGTH.GT(70"
   -responsesize 15000 -submitMethod POST
   ```

2. トラフィック管理ポリシーを設定し、ポリシーをバインドします。

   - `add tm trafficAction OWA_2010_Prof -appTimeout 1 -SSO ON -formSSO Action OWA_Form_SSO_SSOPro`
   - `add tm trafficPolicy owa2k10_pol "HTTP.REQ.URL.CONTAINS(\"owa/auth/logon.aspx\")" OWA_2010_Prof`
   - `bind tm global -policyName owa2k10_pol -priority 100`

CLI を使用した設定の書き換え

コマンドプロンプトで入力します：

- `add rewrite action set_pback_cookie insert_after "http.REQ.COOKIE.VALUE(\"OutlookSession\")" "\";PBack=0\"" -bypassSafetyCheck YES`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- `add rewrite policy set_pback_cookie "http.REQ.URL.CONTAINS(\"logon.aspx\")" set_pback_cookie`
- `bind rewrite global set_pback_cookie 100 END -type REQ_DEFAULT`

代替リライト構成

まれに、Microsoft Outlook が OWA セッションクッキーを発行せず、 `Pback` クッキーも挿入されないことがあります。この問題は、前述のコマンドを実行して書き換え設定を実装した後に発生する可能性があります。

このようなシナリオを克服し、回避策として、書き換え設定の代わりに次のコマンドを設定できます。

コマンドプロンプトで入力します：

- `add rewrite action set_pback_cookie insert_http_header "Cookie" '"PBack=0"'`
- `add rewrite policy set_pback_cookie "http.REQ.URL.CONTAINS(\"logon.aspx\")" set_pback_cookie`
- `set rewrite policy set_pback_cookie -action set_pback_cookie`
- `bind rewrite global set_pback_cookie 100 END -type REQ_DEFAULT`

ワンタイムパスワードの使用の設定

トークン個人識別番号（PIN）やパスコードなどのワンタイムパスワードを使用するように NetScaler Gateway を構成できます。ユーザーがパスコードまたは PIN を入力すると、認証サーバーはただちにワンタイムパスワードを無効にし、ユーザーは同じ PIN またはパスワードを再度入力できません。

ワンタイムパスワードの使用を含む製品には、次のものがあります。

- RSA SecurID
- Imprivata OneSign
- SafeWord
- Gemalto Protiva
- Nordic SMS PASSCODE

これらの各製品を使用するには、内部ネットワークの認証サーバを RADIUS を使用するように構成します。詳細については、 RADIUS 認証の設定を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

たとえば、RSA SecurIDトークンによって提供されるように、RADIUSでワンタイムパスワードを使用するようにNetScaler Gateway で認証を構成すると、NetScaler Gateway はキャッシュされたパスワードを使用してユーザーの再認証を試みます。この再認証は、NetScaler Gateway を変更した場合、またはNetScaler Gateway プラグインとNetScaler Gateway 間の接続が中断されてから復元された場合に発生します。

再認証の試行は、接続がCitrix Workspace アプリを使用するように構成されており、ユーザーがRADIUSまたはLDAPを使用してWeb Interfaceに接続する場合にも発生する可能性があります。ユーザーがアプリケーションを起動してアプリケーションを使用し、Receiverに戻って別のアプリケーションを起動すると、NetScaler Gateway はキャッシュされた情報を使用してユーザーを認証します。

RSA SecurID 認証の設定

RSA SecureID 認証用に RSA/ACE サーバを設定する場合は、次の手順を実行する必要があります。

次の情報を使用して RADIUS クライアントを設定します。

- NetScaler Gateway アプライアンスの名前を指定します。
- 説明を入力します (必須ではありません)。
- システム IP アドレスを指定します。
- NetScaler Gateway と RADIUS サーバー間の共有シークレットを指定します。
- メーカー/モデルを標準 RADIUS として設定します。

エージェントホスト構成では、次の情報が必要です。

- NetScaler Gateway の完全修飾ドメイン名（FQDN）を指定します（仮想サーバーにバインドされた証明書に表示される）。FQDN を入力したら、 キーをクリックすると、 ウィンドウが自動的に表示されます。

  FQDN を入力すると、ネットワークアドレスが自動的に表示されます。表示されない場合は、システム IP アドレスを入力します。
- コミュニケーションサーバを使用して、エージェントタイプを指定します。
- NetScaler Gateway を介した認証を許可されているすべてのユーザーまたはユーザーのセットをインポートするように構成します。

まだ設定されていない場合は、次の情報を含む RADIUS サーバのエージェントホストエントリを作成します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- RSA サーバの FQDN を入力します。

  FQDN を入力すると、ネットワークアドレスが自動的に表示されます。そうでない場合は、RSA サーバの IP アドレスを指定します。
- エージェントタイプ（RADIUS サーバ）を指定します。

RSA RADIUSサーバの構成の詳細については、製造元のマニュアルを参照してください。

RSA SecurID を構成するには、認証プロファイルとポリシーを作成し、ポリシーをグローバルに、または仮想サーバにバインドします。RSA SecurID を使用するための RADIUS ポリシーを作成するには、「RADIUS 認証の構成」を参照してください。

認証ポリシーを作成したら、仮想サーバまたはグローバルにバインドします。詳細については、「認証ポリシーのバインド」を参照してください。

RADIUS を使用したパスワードリターンの設定

ドメインパスワードは、トークンが RADIUS サーバから生成するワンタイムパスワードに置き換えることができます。ユーザーがNetScaler Gateway にログオンすると、トークンの暗証番号（PIN）とパスコードを入力します。NetScaler Gateway が資格情報を検証すると、RADIUSサーバーはユーザーのWindowsパスワードをNetScaler Gatewayに返します。NetScaler Gateway はサーバーからの応答を受け入れ、ログオン中にユーザーが入力したパスコードを使用する代わりに、返されたパスワードをシングルサインオンに使用します。RADIUS 機能によるこのパスワードの返却により、ユーザに Windows パスワードを思い出す必要なく、シングルサインオンを設定できます。

ユーザーがパスワードを返してログオンすると、Citrix Endpoint Management、StoreFront、Web Interfaceなど、内部ネットワークで許可されているすべてのネットワークリソースにアクセスできます。

返されたパスワードを使用してシングルサインオンを有効にするには、［パスワードベンダー識別子］パラメーターと［パスワード属性タイプ］パラメーターを使用して、NetScaler Gateway でRADIUS認証ポリシーを構成します。これらの2つのパラメーターは、ユーザーのWindowsパスワードをNetScaler Gateway に返します。

NetScaler Gateway は Imprivata OneSign をサポートしている。Imprivata OneSignの最低必要バージョンは、サービスパック3で4.0である。Imprivata OneSign のデフォルトのパスワードベンダー識別子は 398 です。Imprivata OneSign のデフォルトのパスワード属性タイプコードは 5 です。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

RSA、Cisco、Microsoft など、他の RADIUS サーバを使用してパスワードを返すことができます。ユーザのシングルサインオンパスワードをベンダー固有の属性値のペアで返すように RADIUS サーバを設定します。NetScaler Gateway 認証ポリシーでは、これらのサーバーの［**パスワードベンダー識別子］パラメーターと［パスワード属性の種類**］パラメーターを追加する必要があります。

ベンダー ID の完全なリストは、 インターネット割り当て番号局 (IANA) の Web サイトにあります。たとえば、RSA セキュリティのベンダー識別子は 2197、Microsoftでは 311、Cisco Systems の場合は9 です。ベンダーがサポートするベンダー固有の属性は、ベンダーに確認する必要があります。たとえば、Microsoftは、ベンダー固有属性のリストをMicrosoft ベンダー固有の RADIUS 属性で公開しています。

ベンダー固有の属性を選択して、ベンダーの RADIUS サーバ上のユーザのシングルサインオンパスワードを保存できます。ユーザーパスワードがRADIUSサーバーに格納されているベンダー識別子と属性を使用してNetScaler Gateway を構成すると、NetScaler Gateway は、RADIUSサーバーに送信されるアクセス要求パケットの属性の値を要求します。RADIUS サーバが access-accept パケット内の対応する属性と値のペアで応答する場合、使用する RADIUS サーバに関係なく、パスワードの返却は機能します。

返されたパスワードを使用してシングルサインオンを構成するには、次の手順を実行します：

1. 構成ユーティリティの［構成］タブで、［**NetScaler Gateway**］>［**ポリシー**］>［**認証**］**の順に展開します**。
2. ナビゲーションペインで、 をクリックします。
3. 詳細ペインで、 をクリックします。
4. ダイアログボックスの に、ポリシーの名前を入力します。
5. 「**サーバー**」の横にある「**新規**」をクリックします。
6. ** に、サーバーの名前を入力します。
7. RADIUS サーバの設定を構成します。
8. に、RADIUS サーバーから返されるベンダー ID を入力します。この識別子の最小値は 1 である必要があります。
9. **に、ベンダー固有の AVP コードで RADIUS サーバから返される属性タイプを入力します。値の範囲は 1 ～ 255 です。
10. ダイアログボックスの の横で式を選択し**、 をクリックし、 をクリックして をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Configuring SafeWord Authentication

SafeWord 製品ラインは、トークンベースのパスコードを使用して安全な認証を提供するのに役立ちます。ユーザーがパスコードを入力すると、そのパスコードは SafeWord によって無効になり、再度使用することはできません。

セキュアゲートウェイおよびWeb Interface展開でアクセスゲートウェイがSecure Gatewayを置き換える場合は、アクセスゲートウェイで認証を構成せず、Web Interfaceが着信HTTPトラフィックに対してSafeWord認証を提供することを引き続き許可することができます。

アクセスゲートウェイは、次の製品の SafeWord 認証をサポートしています。

- SafeWord 2008
- SafeWord プレミアアクセス
- SafeWord for Citrix
- SafeWord リモートアクセス

次の方法で、Access Gateway を SafeWord 製品を使用して認証するように構成できます。

- SafeWord PremierAccess の一部としてインストールされている PremierAccess RADIUS サーバーを使用するように認証を構成し、認証を処理できるようにします。
- SafeWord リモートアクセス、SafeWord for Citrix、および SafeWord PremierAccess 4.0 のコンポーネントである SafeWord IAS エージェントを使用するように認証を構成します。
- SafeWord Web Interfaceエージェントをインストールして、Citrix Web Interfaceをサポートします。Access Gatewayで認証を構成する必要はなく、Citrix Web Interfaceでこれを処理できます。この構成では、PremierAccess RADIUS サーバーまたは SafeWord IAS エージェントは使用されません。

SafeWord RADIUS サーバーを構成する場合は、次の情報が必要です。

- アクセスゲートウェイの IP アドレス。RADIUS サーバでクライアント設定を構成する場合は、アクセスゲートウェイ IP アドレスを使用します。
- 共有シークレット。
- SafeWord サーバーの IP アドレスとポート。

Gemalto プロティバ認証の設定

Protiva は、Gemalto のスマートカード認証の長所を利用するために開発された強力な認証プラットフォームです。Protiva では、ユーザーは Protiva デバイスによって生成されたユーザー名、パス

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ワード、ワンタイムパスワードを使用してログオンします。RSA SecurID と同様に、認証要求は Protiva 認証サーバに送信され、パスワードは検証または拒否されます。

NetScaler Gateway をサポートするようにGemalto Protivaを構成するには、次のガイドラインを使用します。

- Protiva サーバーをインストールします。
- Protiva インターネット認証サーバー (IAS) エージェントプラグインを Microsoft IAS RADIUS サーバーにインストールします。IAS サーバーの IP アドレスとポート番号を書き留めておいてください。

ゲートウェイ認証用の nFactor

nFactor 認証は、認証に関するまったく新しい可能性を可能にします。nFactor を使用する管理者は、仮想サーバーの認証要素を設定する際に、認証、承認、監査の柔軟性を享受できます。

2 つのポリシーバンクまたは 2 つの要因により、管理者は制限されなくなりました。政策銀行の数は、さまざまなニーズに合わせて拡張できます。以前の要素に基づいて、nFactor は認証方法を決定します。動的ログインフォームと障害発生時のアクションは、nFactor を使用することで可能です。

重要

- リリース13.0ビルド67.x以降、nFactor認証はゲートウェイ/VPN仮想サーバーでのみ標準ライセンスでサポートされ、認証仮想サーバーではサポートされません。Standard ライセンスでは、nFactor ビジュアライザー GUI を使用して nFactor フローで EPA を作成することはできません。また、ログインスキーマを編集することはできませんが、既成のログインスキーマをそのまま使用する必要があります。
- NetScaler ADCがnFactor認証をサポートするには、アドバンスドライセンスまたはプレミアムライセンスが必要です。NetScaler ADC での nFactor 認証について詳しくは、「nFactor 認証」を参照してください。

認証、認可、監査機能のライセンス要件

次の表に、使用可能な認証、承認、および監査機能のライセンス要件を示します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

	標準ライセンス	上級ライセンス	プレミアムライセンス
ローカル認証	はい	はい	はい
LDAP認証	はい	はい	はい
RADIUS認証	はい	はい	はい
TACACS認証	はい	はい	はい
Web認証	はい	はい	はい
クライアント証明書認証	はい	はい	はい
認証のネゴシエート	はい	はい	はい
SAML認証	はい	はい	はい
OAuth認証	いいえ	はい	はい
ネイティブOTP	いいえ	はい	はい
メールOTP	いいえ	はい	はい
OTPのプッシュ通知	いいえ	いいえ	はい
ナレッジベースの質問と回答 (KBA 認証)	いいえ	はい	はい
セルフサービスパスワードリセット (SSPR)	いいえ	はい	はい
nFactor ビジュアライザー	はい	はい	はい

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注

- NetScaler ADC 標準ライセンスで nFactor を構成する手順については、 NetScaler ADC 標準ライセンスで nFactor 認証用のゲートウェイ仮想サーバーを作成するセクションを参照してください。
- NetScaler ADC Standardライセンスのゲートウェイ/VPN仮想サーバーにバインドできるのは、アドレス指定できない認証、承認、および監査仮想サーバーのみです。
- NetScaler ADC標準ライセンスでは、ログインスキーマのカスタマイズは許可されていません。nFactor のサポートは基本で、アプライアンスに付属するデフォルトおよびすでに追加されているログインスキーマのみがあります。管理者は設定で使用できますが、ログインスキーマを追加することはできません。したがって、GUI オプションは無効になります。

使用例

nFactor 認証は、ユーザプロファイルに基づいてダイナミック認証フローを有効にします。場合によっては、フローがユーザーに対してシンプルで直感的になることがあります。それ以外の場合は、Active Directory または他の認証サーバのセキュリティ保護と組み合わせることができます。次に、Gateway に固有の要件をいくつか示します：

1. **動的なユーザー名とパスワードの選択。**従来、Citrix クライアント（ブラウザおよびレシーバを含む）は、最初のパスワードフィールドとしてアクティブディレクトリ（AD）パスワードを使用します。2 番目のパスワードは、ワンタイムパスワード (OTP) 用に予約されています。ただし、AD サーバーを保護するには、まず OTP を検証する必要があります。nFactor は、クライアントの変更を必要とせずにこれを実行できます。
2. **マルチテナント認証エンドポイント。**組織によっては、証明書ユーザーと証明書以外のユーザーに異なる Gateway サーバーを使用します。ユーザーが自分のデバイスを使用してログインする場合、ユーザーのアクセスレベルは使用するデバイスに応じてNetScaler ADCアプライアンスによって異なります。ゲートウェイは、さまざまな認証ニーズに対応できます。
3. **グループメンバーシップに基づく認証。**組織によっては、認証要件を決定するために AD サーバーからユーザープロパティを取得します。認証要件は、ユーザーごとに変更できます。
4. **認証の副要因。**場合によっては、異なる認証ポリシーのペアを使用して、異なるユーザーセットを認証することがあります。ペアポリシーを提供すると、効果的な認証が向上します。従属ポリシーは、1 つのフローから作成できます。このようにして、独立した一連のポリシーは、効率を高め、複雑さを軽減する独自のフローになります。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

認証レスポンスの処理

NetScaler Gateway コールバックレジスタは、認証応答を処理します。AAAD (認証デーモン) 応答と成功/失敗/エラー/ダイアログコードは、コールバックハンドルに送られます。成功/失敗/エラー/ダイアログコードは、Gateway に適切なアクションを実行するように指示します。

クライアントサポート

次の表に、設定の詳細を示します。

CLIENT	NFACTORサポート	認証ポリシーのバインドポイント	EPA
Webブラウザー	はい	認証	はい
Citrix Workspaceアプリ	はい	VPN	はい
ゲートウェイプラグイン	はい	VPN	はい

注：

- Citrix Workspace アプリは、以下のバージョンのサポートされているオペレーティングシステムでnFactor認証をサポートしています。
  - Windows 4.12
  - Linux 13.10
  - Mac 1808
  - iOS 2007
  - Android 1808
  - HTML5: ストアウェブを通じてサポート
  - Chrome: ストアウェブでサポート

コマンドライン設定

Gateway 仮想サーバには、属性として指定された認証仮想サーバが必要です。属性としての仮想サーバ名は、このモデルに必要な唯一の設定です。

```
add authnProfile <name-of-profile> -authnVsName <name-of-auth-vserver>
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

authnVsNameは、認証仮想サーバーの名前です。AuthnvsName 仮想サーバーは、高度な認証ポリシーで構成する必要があり、nFactor 認証に使用されます。

```
add vpn vserver <name> <serviceType> <IP> <PORT> -authnProfile <name-of-profile>

set vpn vserver <name> -authnProfile <name-of-profile>
```

ここで、authnProfile は以前に作成された認証プロファイルです。

相互運用性の課題

レガシー Gateway クライアントのほとんどは、RFWeb クライアントに加えて、Gateway によって送信される応答に基づいてモデル化されています。たとえば、/vpn/index.html に対する 302 応答は、多くのクライアントで想定されています。これらのクライアントは、「`pwcount`」「NSC_CERT」などのさまざまなゲートウェイ Cookie にも依存しています。

エンドポイント分析 (EPA)

nFactorのEPAは、NetScaler ADC 認証、承認、および監査モジュールではサポートされていません。したがって、NetScaler Gateway 仮想サーバーはEPAを実行します。EPA の後、ログイン資格情報は、前述の API を使用して認証仮想サーバーに送信されます。認証が完了すると、Gateway は認証後のプロセスを続行し、ユーザセッションを確立します。

設定ミスに関する考慮事項

Gateway クライアントは、ユーザクレデンシャルを 1 回だけ送信します。Gateway は、ログイン要求でクライアントから 1 つまたは 2 つのクレデンシャルを取得します。レガシーモードでは、最大 2 つの要素があります。取得したパスワードは、これらの要素に使用されます。ただし、nFactor では、設定できるファクタの数は実質的に無制限です。Gateway クライアントから取得したパスワードは、設定されたファクタに対して（設定に従って）再利用されます。ワンタイムパスワード (OTP) を複数回再利用しないように注意する必要があります。同様に、管理者は、ファクタで再使用されるパスワードが実際にそのファクタに適用可能であることを確認する必要があります。

Citrix クライアントの定義

この構成オプションは、NetScaler ADCがブラウザクライアントとReceiverなどのシッククライアントを判別するのに役立ちます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

管理者がすべてのCitrix クライアントのパターンを構成できるように、パターンセット ns_vpn_client_useragent が用意されています。

同様に、「Citrix Receiver」 文字列を上記`patset`にバインドして、ユーザーエージェントに「Citrix Receiver」が含まれるすべてのCitrixクライアントを無視します。

ゲートウェイの nFactor の制限

次の条件が存在する場合、ゲートウェイ認証の nFactor は発生しません。

1. 認証プロファイルがNetScaler Gatewayに設定されていません。
2. 高度な認証ポリシーは認証仮想サーバにバインドされません。同じ認証仮想サーバについては、`authnProfile`を参照してください。
3. HTTP 要求のユーザーエージェント文字列は、 `patset` ns_vpn_client_useragent で構成されたユーザーエージェントと一致します。

これらの条件が満たされない場合は、Gateway にバインドされた従来の認証ポリシーが使用されます。

User-Agent またはその一部が前述の`patset`にバインドされている場合、それらのユーザーエージェントからのリクエストは nFactor フローに参加しません。たとえば、次のコマンドはすべてのブラウザの設定を制限します (すべてのブラウザで user-agent 文字列に「Mozilla」が含まれていると仮定します)。

```
bind patset ns_vpn_client_useragents Mozilla
```

ログインスキーマ

LoginSchema は、ログオンフォームの論理表現です。XML 言語によって定義されています。LoginSchemaの構文は、Citrix の共通形式プロトコル仕様に準拠しています。

LoginSchema はプロダクトの「ビュー」を定義します。管理者は、フォームのカスタマイズした説明、補助テキストなどを提供できます。ログインスキーマには、フォーム自体のラベルが含まれます。お客様は、特定の時点で提示されたフォームを説明する成功または失敗のメッセージを提供できます。

次のコマンドを使用して、ログインスキーマを設定します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
add authentication loginSchema <name> -authenticationSchema <string> [-
userExpression <string>] [-passwdExpression <string>] [-
userCredentialIndex <positive_integer>]

[-passwordCredentialIndex <positive_integer>] [-authenticationStrength
<positive_integer>] [-SSOCredentials ( YES | NO )]
```

パラメータの説明

- name-新しいログインスキーマの名前。これは必須の議論です。最大長：127
- AuthenticationSchema-ログインページ UI に送信される認証スキーマを読み取るためのファイルの名前。このファイルには、ログインフォームをレンダリングするためのCitrix Forms認証プロトコルに基づく要素のxml定義が含まれています。管理者がユーザーに他の資格情報の入力を求めるのではなく、以前に取得した資格情報で続行する場合は、 `noschema` を引数として与えることができます。これは、ユーザー定義ファクターで使用される LoginSchema にのみ適用され、仮想サーバーファクターには適用されません。

これは必須の議論です。最大長：255

- userExpression-ログイン時にユーザー名を抽出するための式。これは、関連する高度なポリシー式であればどれでも使用できます。最大長：127
- PasswdExpression-ログイン時のパスワード抽出の式。これは、関連する高度なポリシー式であればどれでも使用できます。最大長：127
- userCredentialIndex-ユーザーが入力したユーザー名のインデックスがセッションに格納されている必要があります。最小値:1、最大値:16
- PasswordCredentialIndex-ユーザーがパスワードを入力したインデックスは、セッションに格納する必要があります。最小値:1、最大値:16
- 認証強度-現在の認証の重み最小値:0、最大値:65535
- `SSOCredentials` -このオプションは、現在の要素認証情報がデフォルトの SSO (singleSignOn) 資格情報であるかどうかを示します。可能な値:はい、いいえ。デフォルト値:NO

ログインスキーマと nFactor の知識が必要

事前構築されたログインスキーマファイルは、次のCitrix **ADCの場所/nsConfig/loginSchema/にあります**。これらの事前構築された LoginSchema ファイルは、一般的なユースケースに対応しており、必要に応じてわずかなバリエーションに変更できます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

また、カスタマイズがほとんどない単一要素のユースケースのほとんどは、ログインスキーマの設定を必要としません。

管理者は、NetScaler ADCが要因を検出できるようにする他の構成オプションについては、ドキュメントを確認することをお勧めします。ユーザーがクレデンシャルを送信すると、管理者は複数のファクタを設定して、認証ファクタを柔軟に選択して処理できます。

loginSchema を使用せずに二要素認証を構成する

NetScaler ADCは、構成に基づいて二重要素の要件を自動的に決定します。ユーザーがこれらの資格情報を提示すると、管理者は仮想サーバで最初のポリシーセットを構成できます。各ポリシーに対して、「NextFactor」を「パススルー」として構成できます。「パススルー」とは、NetScaler ADCがユーザーにアクセスせずに既存の資格情報セットを使用してログオンを処理する必要があることを意味します。「パススルー」ファクターを使用することで、管理者はプログラムで認証フローを駆動できます。管理者は、nFactor の仕様書または展開ガイドで詳細を読むことをお勧めします。 マルチファクター (nFactor) 認証を参照してください。

ユーザ名とパスワードの表現

ログイン認証情報を処理するには、管理者は LoginSchema を設定する必要があります。LoginSchema のカスタマイズがほとんどないシングルファクタまたはデュアルファクタのユースケースでは、XML 定義を指定する必要はありません。LoginSchema には、ユーザーが提示するユーザー名またはパスワードを変更するために使用できる userExpression や passwdExpression などの他のプロパティがあります。

ログインスキーマは高度なポリシー式であり、ユーザー入力を上書きするためにも使用できます。これは、次の例に示すように、 **-AuthenticationSchema** にパラメータの文字列を追加することで実現できます。

以下は、ユーザー名とパスワードのユーザー入力をそれぞれ変更する例です。

- ユーザ名のユーザ入力を `username@citrix.com` から `username@xyz.com` に変更します。

```
add authentication loginSchema user_schema -authenticationSchema
LoginSchema/DualAuth.xml -userExpression
"AAA.LOGIN.USERNAME.BEFORE_STR("@").APPEND("@xyz.com")"
```

- 構成されたログインスキーマの一部として、ユーザーが第 1 要素にパスワードとパスコードを入力するシナリオを考えてみましょう。 **最初の要素でユーザーによって提供されたパスコード**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

を使用し、2 **番目の要素でパスワードを使用するには**、次のコマンドを使用して既存のログインスキーマを変更できます。

```
add authentication loginSchema user_schema -authenticationSchema
LoginSchema/DualAuth.xml -passwdExpression "AAA.LOGIN.PASSWORD2"
```

```
add authentication loginSchema user_schema_second -authenticationSchema
noschema  -passwdExpression "AAA.LOGIN.PASSWORD"
```

nFactor 構成のハイレベルな手順

次の図は、nFactor の設定に関連する高レベルの手順を示しています。



GUI 構成

このセクションでは、次のトピックについて説明します。

- 仮想サーバーを作成する
- 認証仮想サーバーの作成
- 認証 CERT プロファイルの作成
- 認証ポリシーの作成
- LDAP 認証サーバーを追加する
- LDAP 認証ポリシーを追加する
- RADIUS 認証サーバーを追加する
- RADIUS 認証ポリシーの追加
- 認証ログインスキーマの作成
- ポリシーラベルの作成

仮想サーバーの作成

1. ［**NetScaler Gateway**］**>**［**仮想サーバー**］**に移動します。**
2. ボタンをクリックして、ゲートウェイ仮想サーバーを作成します。
3. 次の情報を入力し、「**OK」**をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

パラメーター名	パラメータの説明
仮想サーバの名前を入力します。	NetScaler Gateway 仮想サーバーの名前。ASCII アルファベット文字またはアンダースコア (_) 文字で始まり、ASCII 英数字、アンダースコア、ハッシュ (#)、ピリオド (.)、スペース、コロン (:)、アットマーク (@)、等号 (=)、およびハイフン (-) のみを含める必要があります。仮想サーバーの作成後に変更できます。次の要件は、NetScaler ADC CLI にのみ適用されます。名前に1つ以上のスペースが含まれる場合は、名前を二重引用符または一重引用符で囲みます（たとえば、「マイサーバー」または「マイサーバー」）。
仮想サーバの IP アドレスタイプを入力します。	ドロップダウンメニューから または オプションを選択します。
仮想サーバの IP アドレスを入力します。	インターネットプロトコルアドレス（IPアドレス）は、通信にインターネットプロトコルを使用するコンピュータネットワークに参加している各機器に割り当てられた数値ラベルです。
仮想サーバーのポート番号を入力します。	ポート番号を入力します。
認証プロファイルを入力します。	仮想サーバ上の認証プロファイルエンティティ。このエンティティは、多要素 (nFactor) 認証のために、認証、承認、および監査仮想サーバーに認証をオフロードするために使用できます。
RDP サーバプロファイルを入力します。	仮想サーバに関連付けられている RDP サーバプロファイルの名前。
を入力します。	この仮想サーバーで許可される同時ユーザーセッションの最大数。この仮想サーバーにログオンできる実際のユーザー数は、ユーザーライセンスの総数によって異なります。
を入力します。	ログオン試行の最大回数。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

パラメーター名	パラメータの説明
ログイン失敗タイムアウトを入力します。	ユーザーが最大許容試行回数を超えた場合に、アカウントがロックされる時間（分）。
Windows EPA プラグインのアップグレードを入力します。	Win のプラグインアップグレード動作を設定するオプション。
Linux EPA プラグインのアップグレードを入力します。	Linux のプラグインアップグレード動作を設定するオプション。
MAC EPA プラグインのアップグレードに入る	Mac のプラグインアップグレード動作を設定するオプション。
一度ログイン	このオプションは、この仮想サーバーのシームレス SSO を有効または無効にします。
ICAのみ	［オン］に設定すると、ユーザーはCitrix Workspaceアプリまたはブラウザーのいずれかを使用してログオンし、 `Wihome` パラメーターで指定されたCitrix Virtual Apps and Desktops環境で構成された公開アプリにアクセスできる基本モードを意味します。ユーザーはNetScaler Gateway プラグインを使用した接続を許可されず、エンドポイントスキャンを構成できません。ログインしてアプリにアクセスできるユーザーの数は、このモードのライセンスによって制限されません。-オフに設定すると、ユーザーがCitrix Workspaceアプリ、ブラウザ、または NetScaler Gateway プラグインのいずれかを使用してログオンできるSmartAccessモードを意味します。管理者は、クライアントシステム上でエンドポイントスキャンを実行するように構成し、その結果を使用して公開アプリへのアクセスを制御できます。このモードでは、クライアントは他のクライアントモード（VPN およびクライアントレス VPN）でゲートウェイに接続できます。ログインしてリソースにアクセスできるユーザーの数は、このモードの CCU ライセンスによって制限されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

パラメーター名	パラメータの説明
認証を有効にする	NetScaler Gateway に接続するユーザーに認証を要求します。
ダブルホップ	NetScaler Gateway アプライアンスをダブルホップ構成で使用します。ダブルホップ展開では、3 つのファイアウォールを使用して DMZ を 2 つのステージに分割することにより、内部ネットワークのセキュリティを強化します。このような展開では、DMZ に 1 つのアプライアンス、セキュアネットワークに 1 つのアプライアンスを配置できます。
ダウンステートフラッシュ	仮想サーバーが DOWN とマークされたら、既存の接続を閉じます。これは、サーバーがタイムアウトした可能性があることを意味します。既存の接続を切断するとリソースが解放され、場合によっては過負荷の負荷分散セットアップの回復が高速化されます。この設定は、接続がダウンしているときに接続を安全に閉じることができるサーバーで有効にします。トランザクションを完了する必要があるサーバーでは、DOWN 状態のフラッシュを有効にしないでください。
DTLS	このオプションは、仮想サーバー上のターンサービスを開始/停止します。
AppFlow ロギング	フローの開始と終了のタイムスタンプ、パケットカウント、バイトカウントなど、標準の NetFlow または IPFIX 情報を含む AppFlow レコードをログに記録します。また、HTTP Web アドレス、HTTP 要求メソッド、応答ステータスコード、サーバー応答時間、待機時間などのアプリケーションレベルの情報を含むレコードも記録します。
ICA プロキシセッションの移行	このオプションは、ユーザーが別のデバイスからログオンしたときに、既存のICAプロキシセッションを転送するかどうかを決定します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

パラメーター名	パラメータの説明
状態	仮想サーバの現在の状態（UP、DOWN、BUSY など）。
デバイス証明書を有効にする	EPA の一部としてのデバイス証明書チェックがオンかオフかを示します。



4. ページの セクションを選択します。
5. **** をクリックしてサーバー証明書を選択します。
6. SSL 証明書を選択し、 ボタンをクリックします。
7. ［**Bind**］ をクリックします。
8. 「 **使用可能な暗号がありません**」という警告が表示された場合は、 **「OK」**をクリックします
9. ボタンをクリックします。
10. セクションで、右上の アイコンをクリックします。

認証仮想サーバーを作成する

1. -> -> に移動します。**
2. ［**追加**］ をクリックします。
3. 次の基本設定を完了して、認証仮想サーバーを作成します。

   注: 設定名の右側にある* 記号は、必須フィールドを示します。

   - 新しい認証仮想サーバの を入力します。
   - **IP アドレスタイプを入力します**。IP アドレスタイプは、アドレス指定不可として設定できます。
   - **IP アドレスを入力します**。IP アドレスはゼロでもよい。
   - **認証仮想サーバのプロトコルタイプを入力します** 。
   - 仮想サーバが接続を受け付ける **TCP ポートを入力します** 。
   - 認証仮想サーバによって設定された認証 Cookie **のドメインを入力します** 。
4. ［**OK**］ をクリックします。
5. をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

6. リストから目的のサーバー証明書を選択します。
7. 目的の SSL 証明書を選択し、 ボタンをクリックします。

   注:認証仮想サーバーには、証明書がバインドされている必要はありません。

   
8. **サーバ証明書バインディングを設定します。**

   - **SNI 処理に使用される 1 つ以上の証明書キーをバインドするには、 ボックスをオンにします。
   - ボタンをクリックします。

認証 CERT プロファイルの作成

1. -> -> -> -> -> に移動します。**
2. タブを選択し、 を選択します。
3. 次のフィールドに入力して、認証 CERT プロファイルを作成します。設定名の右にある*記号は、必須フィールドを示します。

   - **Name** ：クライアント証明書認証サーバプロファイルの名前 (アクション)。
   - **2 要素** — この場合、2 要素認証オプションは NOOP です。
   - **「ユーザー名フィールド」** — ユーザー名の抽出元となる client-cert フィールドを入力します。" Subject "または"Issuer"(両方の二重引用符を含む) のいずれかに設定する必要があります。
   - **グループ名フィールド** -グループが抽出されるクライアント証明書フィールドを入力します。" Subject "または"Issuer"(両方の二重引用符を含む) のいずれかに設定する必要があります。
   - **デフォルト認証グループ** -これは、抽出されたグループに加えて認証が成功した場合に選択されるデフォルトのグループです。
4. ［**Create**］ をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

認証ポリシーを作成する

注：

AAA.loginを使用してポリシールールで第1要素ポリシーを構成する場合、Citrix Workspaceアプリがn Factor展開をサポートするには、次の式をOR条件で構成する必要があります。

```
|| HTTP.REQ.URL.CONTAINS("/cgi/authenticate")
```

1. -> -> -> -> -> **に移動します。
2. ボタンを選択します
3. 認証ポリシーを作成するには、次の情報を入力します。設定名の右にある*記号は、必須フィールドを示します。

   a) — 高度な認証ポリシーの名前を入力します。文字、数字、またはアンダースコア文字 (_) で始まり、文字、数字、およびハイフン (-)、ピリオド (.)、ポンド (#)、スペース ()、アットマーク (@)、等号 (=)、コロン (:)、およびアンダースコア文字のみを含める必要があります。認証ポリシーの作成後は変更できません。

   次の要件は、NetScaler ADC CLIにのみ適用されます。名前に1つ以上のスペースが含まれる場合は、名前を二重引用符または一重引用符で囲みます（たとえば、「認証ポリシー」または「認証ポリシー」）。

   b) **アクションタイプ** -認証アクションのタイプを入力します。

   c) **Action** -ポリシーが一致した場合に実行される認証アクションの名前を入力します。

   d) **ログアクション** -要求がこのポリシーに一致したときに使用するメッセージログアクションの名前を入力します。

   e） **式** -認証サーバーでユーザーを認証するかどうかを決定するためにポリシーが使用するNetScaler ADC名前付きルールの名前またはデフォルトの構文式を入力します。

   f) — このポリシーに関する情報を保持するためのコメントを入力します。
4. ［**作成**］ をクリックします

LDAP 認証サーバーを追加する

1. -> — -> -> -> -> **に移動します。
2. タブを選択し、 ボタンを選択して LDAP **サーバを追加します** 。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

LDAP 認証ポリシーを追加する

1. **セキュリティ > NetScaler ADC AAA-アプリケーショントラフィック > ポリシー > 認証 > 詳細ポリシー > ポリシーに移動します。**
2. をクリックして、認証ポリシーを追加します。
3. 認証ポリシーを作成するには、次の情報を入力します。設定名の右にある*記号は、必須フィールドを示します。

   a) **名前** -高度な認証ポリシーの名前。 文字、数字、またはアンダースコア文字 (_) で始まり、文字、数字、およびハイフン (-)、ピリオド (.)、ポンド (#)、スペース ()、アットマーク (@)、等号 (=)、コロン (:)、およびアンダースコア文字のみを含める必要があります。認証ポリシーの作成後は変更できません。

   次の要件は、NetScaler ADC CLIにのみ適用されます。名前に1つ以上のスペースが含まれる場合は、名前を二重引用符または一重引用符で囲みます（たとえば、「認証ポリシー」または「認証ポリシー」）。

   b) **アクションタイプ** -認証アクションのタイプ。

   c) **Action** ：ポリシーが一致した場合に実行される認証アクションの名前。

   d) **Log Action** ：リクエストがこのポリシーに一致したときに使用するメッセージログアクションの名前。

   e） **式** -認証サーバーでユーザーを認証するかどうかを決定するためにポリシーが使用するNetScaler ADC名前付きルールの名前、またはデフォルトの構文式。

   f) **コメント** -このポリシーに関する情報を保存するためのコメント。
4. **「 作成」をクリックします。**

RADIUS 認証サーバーを追加する

1. > > > > **に移動します。
2. サーバを追加するには、 タブを選択し、 ボタンを選択します。
3. 認証 RADIUS サーバを作成するには、次のように入力します。設定名の右にある*記号は、必須フィールドを示します。

   a. RADIUS **アクションの名前を入力します** 。

   b. RADIUS **サーバに割り当てられているサーバ名またはサーバ****IP** アドレスを入力します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

c. RADIUS **サーバが接続をリッスンするポート番号を入力します** 。

d. の値を数秒で入力します。NetScaler ADCアプライアンスは、構成されたタイムアウト値が期限切れになるまで、RADIUSサーバーからの応答を待ちます。

e. RADIUSサーバーとCitrix **ADCアプライアンス間で共有される秘密キーを入力します** 。秘密キーは、NetScaler ADCアプライアンスがRADIUSサーバーと通信できるようにするために必要です。

f. **秘密キーを確認します**。

4. **「 作成」をクリックします。**

RADIUS 認証ポリシーを追加する

1. **セキュリティ > NetScaler ADC AAA-アプリケーショントラフィック > ポリシー > 認証 > 詳細ポリシー > ポリシーに移動します。**
2. をクリックして、認証ポリシーを作成します。
3. 認証ポリシーを作成するには、次の情報を入力します。設定名の右にある*記号は、必須フィールドを示します。

   a. **Name** ：高度な認証ポリシーの名前。 文字、数字、またはアンダースコア文字 (_) で始まり、文字、数字、およびハイフン (-)、ピリオド (.)、ポンド (#)、スペース ()、アットマーク (@)、等号 (=)、コロン (:)、およびアンダースコア文字のみを含める必要があります。認証ポリシーの作成後は変更できません。

   次の要件は、NetScaler ADC CLIにのみ適用されます。名前に1つ以上のスペースが含まれる場合は、名前を二重引用符または一重引用符で囲みます（たとえば、「認証ポリシー」または「認証ポリシー」）。

   a. **アクションタイプ** -認証アクションのタイプ。

   b. **Action** ：ポリシーが一致した場合に実行される認証アクションの名前。

   c. **ログアクション** -リクエストがこのポリシーに一致する場合に使用するメッセージログアクションの名前。

   d. **式** -認証サーバーでユーザーを認証するかどうかを決定するためにポリシーが使用するNetScaler ADC名前付きルールの名前、またはデフォルトの構文式。

   e. **コメント** -このポリシーに関する情報を保存するための任意のコメント。

4. 「 **OK」をクリックします。**作成した認証ポリシーがポリシーの一覧に表示されます。



© 1997–2026 Citrix Systems, Inc. All rights reserved.

認証ログインスキーマの作成

1. > > に移動します。**
2. タブを選択し、 ボタンをクリックします。
3. 次のフィールドに入力して、認証ログインスキーマを作成します：

   a. 「 **名前を入力** 」— 新しいログインスキーマの名前です。

   b. **認証スキーマの入力** -ログインページ UI に送信される認証スキーマを読み取るファイルの名前。このファイルには、ログインフォームをレンダリングできるようにするには、Citrix Forms認証プロトコルに従って要素のXML定義が含まれている必要があります。管理者がユーザにさらなるクレデンシャルを要求せず、以前に取得したクレデンシャルで続行する場合は、" `noschema` "を引数として与えることができます。これは、ユーザー定義ファクタで使用される loginSchemas にのみ適用され、仮想サーバーファクタには適用されません

   c. **ユーザー式の入力** -ログイン時にユーザー名を抽出するための式

   d. **パスワード式の入力** -ログイン時のパスワード抽出の式

   e. **ユーザー資格情報インデックスの入力** -ユーザーが入力したユーザー名がセッションに格納されるインデックス。

   f. **パスワード認証情報インデックスの入力** -ユーザーが入力したパスワードがセッションに格納される必要があるインデックス。

   g. **認証強度** -現在の認証の重みを入力します。

4. 「 **作成」をクリックします。**作成したログインスキーマプロファイルが、ログインスキーマプロファイルリストに表示されている必要があります。



ポリシーラベルを作成する

ポリシーラベルは、特定のファクタの認証ポリシーを指定します。各ポリシーラベルは 1 つの要素に対応します。ポリシーラベルは、ユーザーに提示する必要があるログインフォームを指定します。ポリシーラベルは、認証ポリシーまたは別の認証ポリシーラベルの次の要素としてバインドする必要があります。通常、ポリシーラベルには、特定の認証メカニズムの認証ポリシーが含まれます。ただし、異なる認証メカニズムの認証ポリシーを持つポリシーラベルを使用することもできます。

1. **セキュリティ > NetScaler ADC AAA-アプリケーショントラフィック > ポリシー > 認証 > 詳細ポリシー > ポリシーラベルに移動します。**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. **［追加］** をクリックします。
3. 次のフィールドに入力して、認証ポリシーラベルを作成します：
   a. 新しい認証ポリシーラベルの を入力します。
   b. **認証ポリシーラベルに関連付けられたログインスキーマを入力します** 。
   c. **［続行］** をクリックします。
4. ドロップダウンメニューから** を選択します。
5. **目的の認証ポリシーを選択し** 、 ボタンをクリックします。
6. 次のフィールドに入力します。
   a. ポリシーバインディングの を入力します。
   b. **Goto 式を入力します** 。この式は、現在のポリシールールが TRUE と評価された場合に評価される次のポリシーの優先度を指定します。



7. 目的の認証ポリシーを選択し、 ボタンをクリックします。
8. ボタンをクリックします。
9. **［完了］** をクリックします。
10. 認証ポリシーラベルを確認します。

nFactor 認証の設定を再キャプチャする

NetScaler ADCリリース12.1ビルド50.x以降、NetScaler Gateway はキャプチャの構成を簡素化する新しいファーストクラスアクション「CaptchaAction」をサポートします。キャプチャはファーストクラスアクションであるため、独自の要素になる可能性があります。キャプチャは nFactor フローのどこにでも挿入できます。

以前は、RfWebUI に変更を加えたカスタム WebAuth ポリシーも作成する必要がありました。CaptchaAction の導入により、JavaScript を変更する必要はありません。

重要

スキーマでユーザー名またはパスワードフィールドと一緒に Captcha が使用されている場合、Captcha が満たされるまで ボタンは無効になります。

キャプチャの設定

キャプチャの設定には 2 つの部分が含まれます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. キャプチャを登録するためのGoogleの設定。
2. ログインフローの一部としてキャプチャを使用するようにNetScaler ADCアプライアンスの構成。

グーグルでのキャプチャの設定

`https://www.google.com/recaptcha/admin#list`でキャプチャのドメインを登録します。

1. このページに移動すると、次の画面が表示されます。



注

`reCAPTCHA` v2 のみを使用します。見えない`reCAPTCHA`はまだプレビュー中です。

2. ドメインが登録されると、「SiteKey」と「secretKey」が表示されます。



注

セキュリティ上の理由から、「SiteKey」と「secretKey」はグレー表示になっています。「SecretKey」は安全に保管する必要があります。

NetScaler ADCアプライアンスのキャプチャ構成

NetScaler ADCアプライアンスのキャプチャ構成は、次の3つの部分に分けることができます。

- キャプチャ画面を表示する
- キャプチャレスポンスを Google サーバーに投稿する
- LDAP 構成はユーザーログオンの 2 番目の要素です (オプション)

キャプチャ画面を表示する

ログインフォームのカスタマイズは、SingleAuthCaptcha.xml ログインスキーマを介して行われます。このカスタマイズは認証仮想サーバーで指定され、ログインフォームをレンダリングするために UI に送信されます。組み込みのログインスキーマ SingleAuthCaptcha.xml は、NetScaler ADC アプライアンスの`/nsconfig/loginSchema/LoginSchema`ディレクトリにあります。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

重要

- ユースケースと異なるスキーマに基づいて、既存のスキーマを変更できます。たとえば、Captcha Factor（ユーザー名やパスワードなし）のみが必要な場合や、Captcha との二重認証が必要な場合などです。
- カスタムの変更を実行したり、ファイルの名前を変更したりする場合は、すべてのログインスキーマを/nsConfig/loginSchema/loginSchemaディレクトリから親ディレクトリ（/nsconfig/loginschema）にコピーすることをお勧めします。

CLI を使用してキャプチャの表示を設定するには

```
-  add authentication loginSchema singleauthcaptcha
-authenticationSchema /nsconfig/loginschema/SingleAuthCaptcha.xml



-  add authentication loginSchemaPolicy singleauthcaptcha -rule true
-action singleauthcaptcha



-  add authentication vserver auth SSL <IP> <Port>



-  add ssl certkey vserver-cert -cert <path-to-cert-file> -key <path-to-
key-file>

-  bind ssl vserver auth -certkey vserver-cert

-  bind authentication vserver auth -policy singleauthcaptcha -priority 5
-gotoPriorityExpression END
```

キャプチャレスポンスを Google サーバーに投稿する

ユーザーに表示する必要がある Captcha を設定した後、管理者は Google サーバーに設定をポストして、ブラウザからの Captcha 応答を確認します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ブラウザから CAPTCHA レスポンスを確認するには

```
-  add authentication captchaAction myrecaptcha -sitekey <sitekey-copied-
from-google> -secretkey <secretkey-from-google>



-  add authentication policy myrecaptcha -rule true -action myrecaptcha

-  bind authentication vserver auth -policy myrecaptcha -priority 1
```

AD 認証が必要かどうかを設定するには、次のコマンドが必要です。それ以外の場合は、この手順は無視してかまいません。

```
-  add authentication ldapAction ldap-new -serverIP x.x.x.x -serverPort
636 -ldapBase "cn=users,dc=aaatm,dc=com" -ldapBindDn adminuser@aaatm.com
-ldapBindDnPassword <password> -encrypted -encryptmethod ENCMTHD_3
-ldapLoginName sAMAccountName -groupAttrName memberof -subAttributeName CN
-secType SSL -passwdChange ENABLED -defaultAuthenticationGroup ldapGroup



-  add authenticationpolicy ldap-new -rule true -action ldap-new
```

LDAP 構成はユーザーログオンの 2 番目の要素です (オプション)

LDAP 認証は Captcha の後に行われ、2 番目の要素に追加します。

```
-  add authentication policylabel second-factor

-  bind authentication policylabel second-factor -policy ldap-new
-priority 10

-  bind authentication vserver auth -policy myrecaptcha -priority 1
-nextFactor second-factor
```

管理者は、負荷分散仮想サーバーまたはNetScaler Gateway アプライアンスがアクセスに使用されているかどうかに応じて、適切な仮想サーバーを追加する必要があります。負荷分散仮想サーバーが必要な場合は、管理者が次のコマンドを構成する必要があります。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
add lb vserver lbtest HTTP <IP> <Port> -authentication ON
-authenticationHost nssp.aaatm.com`
```

nssp.aaatm.com — 認証仮想サーバに解決されます。

キャプチャのユーザー検証

前のセクションで説明したすべての手順を設定したら、前述のユーザインターフェイスの画面キャプチャを参照してください。

1. 認証仮想サーバーがログインページをロードすると、ログオン画面が表示されます。**ログオンは** 、キャプチャが完了するまで無効になります。

2. オプションを選択します。キャプチャウィジェットが表示されます。

3. 完了ページが表示される前に、一連のキャプチャイメージをナビゲートします。
4. AD 資格情報を入力し、 チェックボックスをオンにして、** をクリックします。認証が成功すると、目的のリソースにリダイレクトされます。

   注：

   - AD 認証で Captcha を使用する場合、認証情報の ボタンは、キャプチャが完了するまで無効になります。
   - キャプチャは独自の要素で発生します。したがって、AD のような後続の検証は Captchaの `nextfactor` で行われなければなりません。

NetScaler ADC標準ライセンスでnFactor認証用のゲートウェイ仮想サーバーを作成する

1. ［**NetScaler Gateway**］>［**仮想サーバー**］に移動します。
2. ［**NetScaler Gateway 仮想サーバー** ］ページで、［**追加**］をクリックします。

3. 「**VPN 仮想サーバー** 」ページで次の詳細を入力し、「**OK」**をクリックし、「**続行**」をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 名前：NetScaler Gateway 仮想サーバーの名前
- プロトコル- **SSL**を選択
- IPアドレス-NetScaler Gateway 仮想サーバーのIPアドレス
- ポート-443 と入力します。

4. ページで、 の横にあるプラスアイコンをクリックします。
5. をクリックして、認証プロファイルを設定します。
6. 認証プロファイルの名前を入力し、 をクリックします。
7. 「 **VPN 仮想サーバー** 」ページで次の詳細を入力し、「 **OK」をクリックし、** 「続行」をクリックします。

   - Name：認証、承認、および監査する仮想サーバの名前
   - プロトコル- を選択します。NetScaler ADC Standardライセンスのゲートウェイ/VPN仮想サーバーにバインドできるのは、アドレス指定できない認証、承認、および監査仮想サーバーのみです。

注：

- NetScaler ADC Standardライセンスでは、ポリシーを作成する手順は、サポートされているポリシータイプのプレミアムライセンスと同じです。
- NetScaler ADC Standardライセンスでは、nFactor構成での新しいログインスキーマの追加はサポートされていません。

参照ドキュメント

エンドツーエンド nFactor の設定例については、 nFactor 認証の設定を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Unified Gateway ビジュアライザー

Unified Gateway ビジュアライザは、Unified Gateway ウィザードを使用して構成を視覚的に表現します。Unified Gateway ビジュアライザは、構成の追加と編集、およびバックエンドの問題の診断に使用されます。

Unified Gateway ビジュアライザには、次の情報が表示されます。

構成	構成
事前認証ポリシー	認証ポリシー
CS 仮想サーバ	VPN 仮想サーバー
LB 仮想サーバー	XA/XD アプリ
ウェブアプリ	SaaSアプリ

Unified Gateway 展開により、エンタープライズまたはSaaSアプリケーション、クライアントレスアクセスアプリケーション、Citrix Virtual Apps、およびデスクトップリソースへの単一のURLを介したセキュアなリモートアクセスが可能になります。

Unified Gateway の設定

1. メニューから を選択します。
2. 次の画面で、次の情報があることを確認し、 をクリックします。
    - Unified Gateway のパブリック IP アドレス。
    - オプションのルート CA 証明書を含むサーバー証明書チェーン (.PFX または.PEM)。
    - LDAP/RADIUS/クライアント証明書ベースの認証の詳細。
    - アプリケーションの詳細（SaaS アプリケーションの URL または Citrix Virtual Apps and Desktops サーバーの詳細）。
3. ボタンをクリックします。

Unified Gateway 構成仮想サーバーを作成します。

1. **仮想サーバの設定名を入力します** 。
2. **Unified Gateway展開用のパブリック向けユニUnified Gateway IP アドレスを入力します** 。
3. **ポート番号を入力します** 。ポート番号の範囲は 1 ～ 65535 です。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. ［続行］ をクリックします。

次の情報を入力してサーバー証明書を指定します。

1. または ラジオボタンを選択します。
2. **メニューからサーバー証明書を選択します** 。
3. ボタンをクリックします。

認証を指定するには、次の情報を入力します。

1. メニューから 認証方法を選択します** 。
2. または ** ラジオボタンを選択します。
3. ボタンをクリックします。
4. メニューから を選択します。
5. ［続行］ をクリックします。
6. ［ **Webアプリケーション** ］または［ **Citrix Virtual Apps デスクトップ** ］ラジオボタンを選択します。
7. ［続行］ をクリックします。

アプリケーションを選択

Web アプリケーションを指定するには、次の情報を入力します。

1. ブックマークリンクの を入力します。
2. VPN URL が表すアプリケーションのタイプを選択します。指定できる値は以下のとおりです：
   - イントラネットアプリケーション
   - クライアントレスアクセス
   - SaaS
   - このNetScaler ADCで事前構成されたアプリケーション
3. このチェックボックスをオンにすると、このアプリケーションに Unified Gateway URL からアクセスできるようになります。
4. ブックマークリンクの URL を入力します。
5. アイコン URL から、アイコンファイルを取得するファイルを選択します。最大長 = 255

© 1997–2026 Citrix Systems, Inc. All rights reserved.

6. ボタンをクリックします。
7. ［完了］ をクリックします。
8. ［続行］ をクリックします。
9. ［完了］ をクリックします。

GUI 構成

1. メニューから を選択します。
2. アイコンをクリックして、設定された Gateway インスタンスにアクセスします。

   Unified Gateway ビジュアライザは、次の図に示すようなフロー図のように見えます。

   Unified Gateway ビジュアライザには、PreAuth、 `Auth` 、および セクションがあります。VPN 仮想サーバに事前認証ポリシーが設定されている場合は、 `pre-auth` だけが Unified Gateway ビジュアライザに表示されます。

   Unified Gateway ビジュアライザは、負荷分散および VPN 仮想サーバの状態を示すために色分けスキームを使用します。

色	説明
赤	は、サーバーがダウンしていることを意味します。
灰色	WebApps/Citrix Virtual Appsが構成されていないことを意味します。
緑	仮想サーバーですべてが正常であることを意味します。
オレンジ	は、負荷分散仮想サーバサービスのいずれかを意味します。はダウンしていますが、それでも正常に機能しています。

VPN 仮想サーバーの詳細

VPN 仮想サーバーの詳細を取得するには、 ノードをクリックします**。ポップアップには、C/S ルールやすべてのポリシーなどの詳細が表示されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. （+）アイコンをクリックして、VPN エンティティにポリシーを追加します。



2. 目的のノードをクリックすると、設定済みのポリシーの詳細が表示されます。



VPN 仮想サーバー情報の場合、ポップアップの VPN タイトルは、VPN 仮想サーバーの詳細を説明するスライダーに移動するクリック可能なエンティティです。



VPN サーバーの詳細はここに示されています。



The Pre Auth Block

VPN 仮想サーバに事前認証ポリシーが関連付けられている場合、Unified Gateway Visualizerは `Pre Auth` ブロックを表示します。`Pre Auth` ブロックにはポリシーが表示され、事前認証ポリシーを VPN に追加するオプションが提供されます。

1. をクリックして `preauth` ポリシーを追加します。



事前認証ポリシーが関連付けられていなければ、このブロックはビューから隠されます。

The Auth Block

`Auth` ブロックには、プライマリポリシーとセカンダリポリシーが一覧表示されます。`Auth` ブロックは、ポリシーを追加するオプションを提供します。

1. リストの をクリックしてプライマリ認証バインディングを追加するか、 リストの をクリックしてセカンダリ認証バインディングを追加します。



2. メニューからオプションを選択します。
3. ラジオボタンを選択して、 **既存のサーバまたは新しいサーバを追加するかどうかを指定します** 。
4. メニューからオプションを選択します。
5. メニューから を選択します。
6. ラジオボタンを選択して、**既存のサーバを使用するか 、 新しいサーバを追加するかを指定します** 。
7. **［続行］** をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



StoreFront の追加

1. XA/XD の近くにある をクリックすると、「XA/XD」アプリを追加します。



統合ポイントを選択できます。オプションは、StoreFront、WI、または WionNS です。 **［続行］** をクリックします。

1. StoreFront を構成するには、次のフィールドに入力します。必須の情報を必要とするフィールドは、* で示されます。

フィールド	説明
StoreFront FQDN*	StoreFrontサーバーの完全修飾ドメイン名を入力します。最大長:255 文字。例:// storefront.xendt.net
サイトパス*	StoreFront ですでに構成されているWebサイトのReceiverへのパスを入力します。
`Single Sign-on Domain` *	ユーザー認証のデフォルトドメインを入力します
ストア名*	StoreFront モニターの名前を入力します。

STORENAMEは、StoreFront サーバーの正常性を調べるためにStoreFront サービスストア名を定義する引数です。StoreFront モニターに適用されます。最大長:31\| \|Secure Ticket Authority Server*\|Secure Ticket Authority URLを入力します。通常はDelivery Controllerに存在します。 例:`http://sta` \| \|StoreFrontサーバー*\|StoreFront サーバーのIPアドレスを入力\| \|プロトコル*\|サーバーで使用されるプロトコルを入力します。\| \|ポート*\|サーバーが使用するポートを入力します。\| \|負荷分散\|StoreFront サーバーの負荷分散構成を入力します。\| \|仮想サーバ*\|Unified Gateway 展開用のパブリック向け IP アドレスを入力します。\|

2. をクリックします。**

SaaS を追加する

1. をクリックして SaaS アプリを追加します。 ページに移動します。SaaS を設定するには、次のフィールドに入力します。必須情報を必要とするフィールドには、* が付いています。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

フィールド	説明
名前*	ブックマークリンクの名前を入力します。
アプリケーションの種類	この VPN URL が表すアプリケーションのタイプを入力します。可能な値は次のとおりです。イントラネットアプリケーション/クライアントレスアクセス/SaaS /このNetScaler ADC上の事前構成済みアプリケーション
URL を入力*	イントラネットアプリケーションの URL を入力します。
ファイルを選択	このリソースを表示するためのアイコンファイルを取得する URL を入力します。最大長 = 255

ウェブアプリの追加

1. をクリックして Web アプリを追加します。 ページに移動します。Web アプリケーションを構成するには、次のフィールドに入力します。必須情報を必要とするフィールドには、* が付いています。

フィールド	説明
名前*	ブックマークリンクの名前を入力します。
アプリケーションの種類	この VPN URL が表すアプリケーションのタイプを入力します。可能な値は次のとおりです。イントラネットアプリケーション/クライアントレスアクセス/SaaS /このNetScaler ADC上の事前構成済みアプリケーション
URL を入力*	イントラネットアプリケーションの URL を入力します。
ファイルを選択	このリソースを表示するためのアイコンファイルを取得する URL を入力してください。maxLength = 255

Unified Gateway URL を介してアプリケーションにアクセスできる場合は、アプリケーションをクリックして負荷分散サーバーの詳細にアクセスできます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

（+）をクリックすると新しいポリシーを追加できます。また、ポリシー情報を表示するノードをクリックすると、バインドされたすべてのポリシーを表示できます。

ロードバランサーにバインドされたサービスの数と、全体的な状態情報も表示されます。さらにクリックすると、すべてのサービスが一覧表示されます。新しいサービスをロードバランサーに追加できます。

ロードバランサの詳細については、ポップアップのタイトルがクリック可能で、負荷分散仮想サーバーの詳細ページに表示されます。

モバイル/タブレットデバイスでRADIUSおよびLDAP認証を使用するようにNetScaler Gateway を構成する

このセクションでは、モバイルデバイス/タブレットデバイスでRADIUS認証をプライマリとして使用し、LDAP認証をセカンダリとして使用するようにNetScaler Gateway アプライアンスを構成する方法について説明します。

の項で説明した設定でも、他のすべての接続で LDAP を最初に使用し、次に RADIUS を使用できます。

モバイル/タブレットデバイスで使用するためにCitrix Workspace アプリで2要素認証を構成する場合は、プライマリ認証としてRSA SecureID（RADIUS認証）を追加する必要があります。ただし、Receiverでユーザー名とパスワード、パスコードの入力を求めるプロンプトが表示された場合は、LDAPを最初に設定し、2番目の資格情報としてRADIUSを配置します。管理者の観点から見ると、モバイル以外の構成とは別の構成です。

モバイルデバイス/タブレットデバイスでRADIUS認証をプライマリとして使用し、LDAP認証をセカンダリとして使用するようにNetScaler Gateway アプライアンスを構成するには、次の手順を実行します。

1. 構成ユーティリティから、 **Citrix Gateway > ポリシー > 認証を選択し** 、モバイルデバイスと非モバイルデバイスのLDAPおよびRSAの認証ポリシーを作成します。これは、ユーザがRADIUS 認証をバイパスできる論理条件を回避するために必要です。
2. LDAP の タブの下にある オプションをクリックした後、LDAP **サーバの詳細を入力します** 。
3. 必要な LDAP サーバを選択して、モバイルデバイスの LDAP ポリシーを作成します。

   このポリシーをモバイルデバイスのみにバインドするには、次の式を使用します：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
REQ.HTTP.HEADER User-Agent CONTAINS CitrixReceiver
```

4. をクリックしてポリシーを作成します：

5. モバイルデバイス用の RADIUS ポリシーと RADIUS サーバを作成します。

   - ［ **NetScaler Gateway］>［ポリシー］>［認証］>［RADIUS］**の順に選択します。「サーバー」タブの「 **追加** 」をクリックします。
   - 必要な詳細を追加します。RADIUS 認証のデフォルトポートは 1812 です。

   - このポリシーをモバイルデバイスのみにバインドするには、次の式を使用します：

6. 同じ手順に従って、モバイルデバイス以外の LDAP ポリシーを作成します。このポリシーを非モバイルデバイスのみにバインドするには、次の式を使用します：

```
REQ.HTTP.HEADER User-Agent NOTCONTAINS CitrixReceiver
```

7. モバイルデバイス以外の RADIUS ポリシーを作成します。このポリシーを非モバイルデバイスのみにバインドするには、次の式を使用します：

```
REQ.HTTP.HEADER User-Agent NOTCONTAINS CitrixReceiver
```

8. Citrix Gateway 仮想サーバーの［プロパティ］に移動し、［ **認証** ］タブをクリックします。で、RSA_Mobile ポリシーを最優先として、LDAP_NonMobile ポリシーをセカンダリプライオリティとして追加します：

9. セカンダリ認証ポリシーで、LDAP_Mobile ポリシーを最優先として追加し、次に RSA_NonMobile ポリシーをセカンダリプライオリティとして追加します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

セッションポリシーには、正しいシングルサインオン資格情報インデックスが必要です。つまり、LDAP 資格情報である必要があります。モバイルデバイスの場合、 > の を に設定する必要があります。これは LDAP です。

したがって、モバイルデバイス用と非モバイルデバイス用の 2 つのセッションポリシーが必要です。

- モバイルデバイスの場合、セッションポリシーとセッションプロファイルは、次のスクリーンショットのように表示されます。 セッションポリシーを作成するには、目的の仮想サーバーに移動し、 をクリックし、 セクションに移動して、 記号をクリックします：
- メニューから オプションを選択します。

- 目的のセッションポリシー名を入力し、 をクリックしてプロファイルを作成します。モバイルデバイスの場合、 > の を に設定する必要があります。これは LDAP です。

- モバイルデバイス以外の場合も、同じ手順に従います。 > **の資格情報インデックスは** 、 LDAP である に設定する必要があります。

式を次のように変更する必要があります。

```
REQ.HTTP.HEADER User-Agent NOTCONTAINS CitrixReceiver
```

- モバイル以外のユーザーのプロファイルを作成するには、 をクリックします。

10. 次の図は、必要な仮想サーバの下にあるポリシーとプロファイルを示します。
11. また、StoreFront では、NetScaler Gateway 構成で「ログオンの種類」=「ドメインとセキュリティトークン」を使用するように設定されています。

1つのActive Directory yグループのメンバーに対するNetScaler Gatewayへのアクセスを制限する

NetScaler Gateway は、ログオンアクセスを制限する2つの方法をサポートしています。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- LDAP検索フィルター-LDAP検索フィルター（Active Directory グループメンバーシップなど）に一致するユーザー名のみがNetScaler Gateway にログオンできます。
- NetScaler Gateway セッションポリシーまたはプロファイルでのログオンを許可するグループ-この方法では、複数のActive Directory グループがサポートされます。詳しくは、`<https://support.citrix.com/article/CTX125797>`を参照してください。

この資料では、LDAP 検索フィルタ方式について説明します。

概要

ユーザーがNetScaler Gateway 仮想サーバーのログオンページで資格情報を入力し、Enterキーを押すと、アプライアンスはまずActive Directory（LDAP）でユーザー名を検索します。LDAP 検索フィルタが LDAP ポリシーまたはサーバで定義されていない場合、アプライアンスはすべての Active Directory ユーザ名を検索します。一致が見つかると、アプライアンスはユーザーの完全な識別名（DN）をプルし、ユーザーの DN とパスワードを使用して Active Directory への認証を行います。

LDAP 検索フィルタが定義されている場合は、LDAP 検索フィルタに一致するユーザ名のみが検索され、ユーザ名の一致が検索されます。たとえば、LDAP 検索フィルタが Active Directory グループのメンバーのみを検索するように構成されている場合、ユーザーが入力したユーザー名は、グループのメンバーと一致する必要があります。

前提条件

NetScaler Gateway 仮想サーバーは、LDAP認証用に構成されている必要があります。

1 つの Active Directory グループのメンバーに対して LDAP 検索フィルタを構成する手順

1. アクセス許可を持つ Active Directory グループを特定し、その完全な識別名を取得します。

   グループの完全な識別名を取得する簡単な方法は、Active Directory ユーザーとコンピュータを使用することです。

2. で、 メニューの を有効にします。

3. ツリーでグループオブジェクトを参照し、右クリックして、 をクリックします。 **注:** 「検索」(**Find**) は使用できません。代わりに、ツリー内を移動してオブジェクトを見つける必要があります。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. 右側で、 **属性エディタ (Attribute Editor)** タブに切り替えます。

   このタブは、 **高度な機能が有効になっていて 、 検索機能を使用していない場合にのみ表示されます** 。
5. まで下にスクロールし、ダブルクリックして、クリップボードにコピーします。

   
6. NetScaler Gateway GUIで、［**NetScaler Gateway**］**>**［**仮想サーバー**］に移動します。
7. 既存のNetScaler Gateway 仮想サーバーを選択し、［**編集**］をクリックします。
8. セクションで、 をクリックします。
9. 既存の LDAP ポリシーを右クリックし、 をクリックします。

   
10. セクションの フィールドに **memberOf=** と入力し、等号 (=) の後に Active Directory グループの識別名を貼り付けます。

    検索フィルターの例は次のとおりです。 memberOf=CN=Citrixリモート、OU=Citrix 、DC=Corp、 **DC=ローカル注：** デフォルトでは、NetScalerはActive Directory グループの直接のメンバーであるユーザー名のみを検索します。ネストされたグループを検索する場合は、Microsoft OID:: を LDAP 検索フィルタに追加します。OID は memberOf と = の間に挿入されます。

    例： memberof: 1.2.840.113556.1.4.1941: =CN=Citrix Remote、OU=Citrix、DC=Corp、DC=Local
11. ［**OK**］ をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

高可用性の使用

2つのNetScaler Gateway アプライアンスの高可用性展開は、あらゆるトランザクションで中断のない操作を提供できます。一方のアプライアンスをプライマリノードとして設定し、もう一方のアプライアンスをセカンダリノードとして設定すると、プライマリノードは接続を受け付けてサーバを管理し、セカンダリノードがプライマリを監視します。何らかの理由でプライマリノードが接続を受け付けることができなくなると、セカンダリノードが処理を引き継ぎます。

セカンダリノードは、プライマリノードが接続を受け付けているかどうかを判断するために、定期的なメッセージ（ハートビートメッセージまたはヘルスチェックとも呼ばれます）を送信してプライマリを監視します。ヘルスチェックが失敗した場合、セカンダリノードは指定された期間接続を再試行し、その後、プライマリノードが正常に機能していないと判断します。次に、セカンダリノードがプライマリ（フェールオーバーと呼ばれるプロセス）を引き継ぎます。

フェイルオーバー後、すべてのクライアントは管理対象サーバーへの接続を再確立する必要がありますが、セッション永続性ルールはフェイルオーバー前と同じように維持されます。

Web サーバーのロギングパーシステンスを有効にすると、フェールオーバーによってログデータが失われることはありません。ロギングパーシステンスを有効にするには、ログサーバーの設定でlog.conf ファイルに両方のシステムのエントリが含まれている必要があります。

次の図は、高可用性ペアを使用したネットワーク構成を示しています。

図1：高可用性構成のNetScaler Gateway アプライアンス



高可用性を設定する基本的な手順は次のとおりです：

1. 両方のノードを同じサブネットに配置して、基本設定を作成します。
2. ノードがヘルスチェック情報を通信する間隔をカスタマイズします。
3. ノードが同期を維持するプロセスをカスタマイズします。
4. プライマリからセカンダリへのコマンドの伝播をカスタマイズします。
5. オプションで、フェイルセーフモードを設定して、どちらのノードもプライマリではない状況を回避します。
6. NetScaler Gateway gratuitous ARPメッセージを受け付けないデバイスが環境に含まれている場合は、仮想MACアドレスを構成します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

より複雑な構成の準備ができたら、異なるサブネットに高可用性ノードを構成できます。

高可用性セットアップの信頼性を向上させるために、ルートモニタを設定し、冗長リンクを作成できます。トラブルシューティングやメンテナンスタスクの実行など、状況によっては、ノードを強制的にフェイルオーバーする（プライマリステータスを他のノードに割り当てる）場合や、セカンダリノードを強制的にセカンダリにしたり、プライマリノードをプライマリにしたりしたい場合があります。

高可用性の仕組み

高可用性ペアでNetScaler Gateway を構成すると、セカンダリNetScaler Gateway は、ハートビートメッセージまたはヘルスチェックとも呼ばれる定期的なメッセージを送信して、最初のアプライアンスが接続を受け付けているかどうかを判断することにより、最初のアプライアンスを監視します。ヘルスチェックが失敗した場合、セカンダリNetScaler Gateway は、プライマリアプライアンスが動作していないと判断するまで、指定された時間だけ接続を再試行します。セカンダリアプライアンスがヘルスチェックの失敗を確認すると、セカンダリNetScaler Gateway がプライマリNetScaler Gateway を引き継ぎます。これはフェールオーバーと呼ばれます。

次のポートは、NetScaler Gateway アプライアンス間の高可用性に関する情報を交換するために使用されます。

- UDP ポート 3003 は、間隔のステータスを通信するための hello パケットの交換に使用されます。
- TCP ポート 3010 は、高可用性設定の同期に使用されます。
- TCP ポート 3011 は、構成設定の同期に使用されます。

高可用性の設定に関するガイドライン

高可用性ペアを設定する前に、次の注意事項を確認する必要があります。

- 各NetScaler Gateway アプライアンスは、同じバージョンのNetScaler Gateway ソフトウェアを実行している必要があります。バージョン番号は、構成ユーティリティのページの上部にあります。
- NetScaler Gateway は、2つのアプライアンス間でパスワードを自動的に同期しません。ペア内の他のアプライアンスのユーザー名とパスワードを使用して、各NetScaler Gateway を構成できます。
- プライマリとセカンダリの両方のNetScaler Gateway 上の構成ファイルns.confのエントリは、次の例外を除いて一致する必要があります。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- プライマリおよびセカンダリのNetScaler Gateway アプライアンスは、それぞれ固有のシステムIPアドレスで構成する必要があります。セットアップウィザードを使用して、いずれかのNetScaler Gateway のシステムIPアドレスを構成または変更します。
- 高可用性ペアでは、NetScaler Gateway IDと関連するIPアドレスが他のNetScaler Gatewayを指している必要があります。

  たとえば、AG1とAG2という名前の2つのアプライアンスがある場合は、AG2の一意のNetScaler Gateway IDとIPアドレスを使用してAG1を構成する必要があります。AG1の一意のNetScaler Gateway IDとIPアドレスを使用してAG2を構成する必要があります。

  注：各NetScaler Gateway アプライアンスは、常にノード0として識別されます。各アプライアンスを一意のノード ID で構成します。

- 高可用性ペアの各アプライアンスには、同じライセンスが必要です。ライセンスについて詳しくは、「ライセンス」を参照してください。
- 構成ユーティリティまたはコマンド・ライン・インタフェースを直接使用しない方法 (SSL証明書のインポートや起動スクリプトへの変更など) を使用して、いずれかのノードで構成ファイルを作成する場合は、構成ファイルをもう一方のノードにコピーするか、同じものを作成する必要があります。そのノード上のファイルです。
- 高可用性ペアを設定するときは、プライマリアプライアンスとセカンダリアプライアンスの両方のマッピングされた IP アドレスとデフォルトゲートウェイアドレスが同一であることを確認します。必要に応じて、セットアップウィザードを実行して、マッピングされた IP アドレスをいつでも変更できます。

インストール前のチェックリストを使用して、高可用性展開で構成する必要がある特定の設定の一覧を表示できます。詳細については、 インストール前のチェックリストを参照してください。

高可用性の設定の構成

高可用性構成を設定するには、2つのノードを作成します。各ノードは、もう一方のNetScaler Gateway IPアドレスをリモートノードとして定義します。まず、高可用性を構成する2つのNetScaler ADCアプライアンスのいずれかにログオンし、ノードを追加できます。他のアプライアンスのNetScaler Gateway IPアドレスを新しいノードのアドレスとして指定します。次に、他のアプライアンスにログオンし、最初のアプライアンスのNetScaler Gateway IPアドレスを持つノードを追加します。アルゴリズムは、どのノードがプライマリになり、どのノードがセカンダリになるかを決定します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

アプライアンスを設定する前に、高可用性ノードを追加します。このノードは、高可用性ペアの第1または第2のNetScaler Gateway を表します。高可用性を構成するには、最初にノードを作成し、次に高可用性設定を構成します。

高可用性ノードを追加するには

1. 構成ユーティリティの タブのナビゲーションペインで、 > を展開します。
2. 詳細ペインの タブで、 をクリックします。
3. ［ **HAノードの作成** ］ページの［ **リモートノードのIPアドレス** ］テキストボックスに、リモートノードとして追加するNetScaler ADC NSIPアドレスを入力します。Citrix Gateway IPアドレスがIPv6アドレスの場合は、 **アドレスを入力する前にIPv6チェックボックスを選択してください** 。
4. ローカルノードをリモートノードに自動的に追加する場合は、 を選択します。このオプションを選択しない場合は、リモートノードで表されるアプライアンスにログインし、現在設定しているノードを追加する必要があります。
5. を有効にする時にクリックします**。
6. リモートアプライアンスのユーザー名とパスワードが異なる場合は、 で、 をクリックします。
7. ** に、リモートアプライアンスのユーザー名を入力します。
8. に、リモートアプライアンスのパスワードを入力します。
9. ［**OK**］ をクリックします。

セカンダリノードを有効または無効にするには

セカンダリノードのみを無効または有効にできます。セカンダリノードを無効にすると、プライマリノードへのハートビートメッセージの送信が停止するため、プライマリノードはセカンダリノードのステータスをチェックできなくなります。ノードを有効にすると、そのノードは高可用性構成に参加します。

1. 構成ユーティリティの タブのナビゲーションペインで、 を展開し、 をクリックします。
2. 詳細ペインの タブで、ローカルノードを選択し、 をクリックします。
3. ダイアログボックスの で、 を選択します。
4. ［OK］ をクリックします。ステータスバーに、ノードが正常に構成されたことを示すメッセージが表示されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

高可用性の設定を構成するには

1. 構成ユーティリティの タブのナビゲーションペインで、 > を展開します。
2. 詳細ペインの タブでノードを選択し、 をクリックします。
3. ダイアログボックスの に、ノード識別子の番号を入力します。ID は、他のアプライアンスの一意のノード番号を指定します。
4. にシステムの IP アドレスを入力し、 をクリックします。IP アドレスは、他のアプライアンスの IP アドレスを指定します。

注:高可用性ペアのノードの最大 ID は 64 です。

RPC ノードのパスワードを変更する

他のNetScaler Gateway アプライアンスと通信するには、各アプライアンスには、NetScaler Gateway での認証方法など、他のアプライアンスの知識が必要です。RPCノードは、構成およびセッション情報のシステム間通信に使用される内部システムエンティティです。各NetScaler Gateway には1つのRPCノードが存在し、他のNetScaler Gateway アプライアンスのIPアドレスや認証に使用されるパスワードなどの情報を格納します。別のNetScaler Gateway と接続する NetScaler Gateway は、RPCノード内のパスワードをチェックします。

NetScaler Gateway では、高可用性ペアの両方のアプライアンスでRPCノードのパスワードが必要です。パスワードは両方のアプライアンスで同じである必要があります。プライマリアプライアンスはセカンダリ RPC ノードのパスワードを認識している必要があり、セカンダリアプライアンスはプライマリ RPC ノードのパスワードを認識している必要があります。最初は、各NetScaler Gateway は同じRPCノードパスワードで構成されます。セキュリティを強化するには、デフォルトの RPC ノードパスワードを変更する必要があります。構成ユーティリティを使用して、RPC ノードを構成および変更できます。

RPC ノードは、ノードを追加するとき、またはグローバルサーバー負荷分散 (GSLB) サイトを追加するときに暗黙的に作成されます。RPC ノードを手動で作成または削除することはできません。

重要:

アプライアンス間のネットワーク接続も保護する必要があります。 チェックボックスをオンにして、RPC ノードのパスワードを構成するときに、セキュリティを構成できます。

RPC ノードのパスワードを変更してセキュアな接続を有効にするには

1. > > に移動します。**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. 詳細ペインでノードを選択し、 をクリックします。
3. と に、新しいパスワードを入力します。
4. ［ **ソースIPアドレス**］に、他のNetScaler Gateway アプライアンスのシステムIPアドレスを入力します。
5. 「 **セキュア**」をクリックし、「OK」**をクリックします。

注：

オプションを有効にすると、アプライアンスはノードから他の RPC ノードに送信されるすべての通信を暗号化し、RPC 通信を保護します。

CLIを使用してRPCノードのパスワードを変更するには

コマンドプロンプトで入力します：

```
set ns rpcNode <IPAddress> {-password} [-secure ( YES | NO )]



show ns rpcNode
```

例:

```
> set ns rpcNode 192.0.2.4 -password mypassword -secure YES

 Done

> show rpcNode

.

.

.

 IPAddress:  192.0.2.4 Password:  d336004164d4352ce39e

     SrcIP:  *           Secure:  ON

Done
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
>
```

プライマリアプライアンスとセカンダリアプライアンスの高可用性の設定

RPCノードのパスワードを変更し、セキュアな通信を有効にしたら、構成ユーティリティを使用してプライマリおよびセカンダリNetScaler Gateway 高可用性ノードを構成します。

1. 構成ユーティリティの タブのナビゲーションペインで、 を展開し、 をクリックします。
2. 詳細ペインの タブで、ノードを選択し、 をクリックします。
3. ［高可用性ステータス］で、［有効（HA にアクティブに参加する）］をクリックし、［OK］をクリックします。

通信間隔の設定

NetScaler Gateway を高可用性ペアとして構成すると、セカンダリNetScaler Gateway が特定の間隔（ミリ秒（ミリ秒）でリッスンするように構成できます。これらのインターバルは、hello インターバルおよびデッドインターバルと呼ばれます。

hello 間隔は、ハートビートメッセージがピアノードに送信される間隔です。デッドインターバルは、ハートビートパケットが受信されない場合にピアノードが DOWN とマークされるまでの時間間隔です。ハートビートメッセージは、高可用性ペアの他のノードのポート 3003 に送信される UDP パケットです。

hello 間隔を設定する場合は、200 ～ 1000 の値を使用できます。デフォルト値は 200 です。デッドインターバルの値は 3 ～ 60 です。デフォルト値は3です。

注

デッドインターバルは、hello インターバルの倍数として設定する必要があります。

セカンダリNetScaler Gateway の通信間隔を構成するには

1. 構成ユーティリティの タブのナビゲーションペインで、 を展開し、 をクリックします。
2. 詳細ペインの タブで、ノードを選択し、 をクリックします。
3. で、次のいずれかまたは両方の操作を行います。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 「Hello 間隔 (msec)」に値を入力し、「OK」をクリックします。デフォルトは 200 ミリ秒です。
- 「デッド間隔 (秒)」に値を入力し、「OK」をクリックします。デフォルトの設定は 3 秒です。

NetScaler Gateway アプライアンスの同期

高可用性ペアでのNetScaler Gateway アプライアンスの自動同期は、デフォルトで有効になっています。自動同期を使用すると、1 つのアプライアンスに変更を加え、その変更を 2 番目のアプライアンスに自動的に反映させることができます。同期はポート 3010 を使用します。

同期は、次の場合に開始されます。

- セカンダリノードが再起動します。
- プライマリノードは、フェールオーバー後にセカンダリになります。

同期を無効にできます。これにより、プライマリアプライアンスで変更が発生したときに、セカンダリNetScaler Gateway がその構成をプライマリNetScaler Gateway と同期しないようにできます。同期を強制することもできます。

ペアのセカンダリノードで高可用性同期を有効または無効にします。

高可用性同期を有効または無効にするには

1. 構成ユーティリティの タブのナビゲーションペインで、 を展開し、 をクリックします。
2. 詳細ペインの タブで、ノードを選択し、 をクリックします。
3. ダイアログボックスの で、次のいずれかを実行します。
   - 同期を無効にするには、 チェックボックスをオフにします。
   - 同期を有効にするには、 チェックボックスをオンにします。
4. ［OK］ をクリックします。ステータスバーに、ノード構成が成功したことを示すメッセージが表示されます。

アプライアンス間で同期を強制するには

自動同期に加えて、NetScaler Gateway は、高可用性ペアの2つのノード間の強制同期をサポートします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

プライマリとセカンダリの両方のNetScaler Gateway アプライアンスで同期を強制できます。ただし、同期がすでに進行中の場合、コマンドは失敗し、NetScaler Gateway は警告を表示します。強制同期は、次の状況でも失敗します。

- スタンドアロンシステムで同期を強制します。
- セカンダリノードは無効です。
- セカンダリノードで高可用性同期を無効にします。

1. 構成ユーティリティの タブのナビゲーションペインで、 を展開し、 をクリックします。
2. タブで、 をクリックします。

高可用性セットアップの設定ファイルの同期

高可用性セットアップでは、プライマリノードからセカンダリノードにさまざまな設定ファイルを同期できます。

高可用性セットアップでファイルを同期するためのパラメータ

Mode

実行する同期のタイプ。次の説明では、オプションを指定するコマンドライン引数を、かっこで囲んで説明します。

- **ライセンスとrc.conf (すべて) 以外のすべて** 。システム構成、NetScaler Gateway ブックマーク、SSL証明書、SSL CRLリスト、HTMLインジェクションスクリプト、およびアプリケーションファイアウォールXMLオブジェクトに関連するファイルを同期します。

- **ブックマーク** (bookmarks)。すべてのNetScaler Gateway ブックマークを同期します。

- **SSL 証明書とキー** (`ssl`)。SSL 機能のすべての証明書、キー、および CRL を同期します。

- **ライセンスと rc.conf** (その他)。すべてのライセンスファイルと rc.conf ファイルを同期します。

- **ライセンスと rc.conf (all_plus_misc) を含むすべて** 。システム構成、NetScaler Gateway ブックマーク、SSL証明書、SSL CRLリスト、HTMLインジェクションスクリプト、アプリケーションファイアウォールXMLオブジェクト、ライセンス、およびrc.confファイルに関連するファイルを同期します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注：アプライアンスにNetScaler ADCライセンスをインストールする場合は、さらに多くのオプションを使用できます。

構成ユーティリティを使用して高可用性セットアップのファイルを同期するには

1. ナビゲーションウィンドウで、 を展開し、 をクリックします。
2. 詳細ペインの で、 をクリックします。
3. ［ **ファイル同期の開始** ］ダイアログボックスの［ **モード** ］メニューで、適切な同期の種類（［ライセンスとrc.conf 以外のすべて］など）を選択し、［ **OK］**をクリックします。

コマンド伝播の設定

高可用性セットアップでは、プライマリノードで発行されたコマンドは、プライマリノードでコマンドが実行される前に、セカンダリノードに自動的に伝達され、セカンダリノードで実行されます。コマンドの伝播が失敗した場合、またはセカンダリノードでコマンドの実行が失敗した場合、プライマリノードはコマンドを実行し、エラーをログに記録します。コマンドの伝播では、ポート 3011 が使用されます。

高可用性ペア構成では、プライマリノードとセカンダリノードの両方でコマンドの伝播がデフォルトで有効になっています。高可用性ペアのいずれかのノードで、コマンドの伝播を有効または無効にできます。プライマリノードでコマンドの伝播を無効にすると、コマンドはセカンダリノードに伝播されません。セカンダリノードでコマンドの伝播を無効にすると、プライマリから伝播されたコマンドはセカンダリノードで実行されません。

注:伝播を再度有効にした後は、同期を強制することを忘れないでください。

注：伝播を無効にしているときに同期が発生した場合、伝播の無効化が有効になる前に行った構成関連の変更は、セカンダリノードと同期されます。これは、同期の進行中に伝播が無効になっている場合にも当てはまります。

プライマリノードで伝播を有効または無効にするには

1. 構成ユーティリティの タブのナビゲーションペインで、 を展開し、 をクリックします。
2. 詳細ペインの タブでノードを選択し、 をクリックします。
3. **HA 伝播で**、次のいずれかを実行します：

   - 高可用性伝播を無効にするには、 チェックボックスをオフにします。
   - 高可用性伝播を有効にするには、 チェックボックスをオンにします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. ［**OK**］ をクリックします。

コマンド伝播のトラブルシューティング

次に、コマンドの伝播が失敗する理由と、設定を復元するための解決策を示します。

- ネットワーク接続はアクティブではありません。コマンドの伝達が失敗した場合は、プライマリとセカンダリのNetScaler Gateway アプライアンス間のネットワーク接続を確認します。
- セカンダリNetScaler Gateway にリソースがありません。コマンドの実行がプライマリNetScaler Gateway で成功したが、セカンダリNetScaler Gateway への伝達に失敗した場合は、セカンダリNetScaler Gateway でコマンドを直接実行してエラーメッセージを表示します。このエラーは、コマンドで必要なリソースがプライマリNetScaler Gateway に存在し、セカンダリNetScaler Gateway では使用できないために発生した可能性があります。また、各アプライアンスのライセンスファイルが一致していることを確認します。

  たとえば、すべてのセキュアソケットレイヤー（SSL）証明書が各NetScaler Gateway に存在することを確認します。初期化スクリプトのカスタマイズが両方のNetScaler Gateway アプライアンスに存在することを確認します。
- 認証エラー。認証失敗のエラーメッセージが表示された場合は、各アプライアンスの RPC ノード設定を確認します。

フェイルセーフモードを構成する

高可用性構成では、フェイルセーフモードでは、両方のノードがヘルスチェックに失敗したときに、1 つのノードが常にプライマリになります。フェイルセーフモードでは、ノードが部分的にしか使用できない場合に、バックアップメソッドがアクティブになり、トラフィックを処理できます。

高可用性フェイルセーフモードは、各ノードで個別に構成します。

次の表に、フェイルセーフのケースをいくつか示します。NOT_UP 状態は、ノードがヘルスチェックに失敗したが、ノードが部分的に利用可能であることを意味します。UP 状態は、ノードがヘルスチェックに合格したことを意味します。

表1. フェールセーフモードの場合

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ノード A (プライマリ) のヘルス状態	ノード B（セカンダリ）のヘルス状態	デフォルトの高可用性動作	フェイルセーフ対応の高可用性動作	説明
NOT_UP (最後に失敗した)	NOT_UP (最初に失敗した)	A (二次)、B (二次)	A (プライマリ)、B (セカンダリ)	両方のノードが次々に障害が発生した場合、最後のプライマリノードであったノードはプライマリのままです。
NOT_UP (最初に失敗した)	NOT_UP (最後に失敗した)	A (二次)、B (二次)	A (セカンダリ)、B (プライマリ)	両方のノードが次々に障害が発生した場合、最後のプライマリノードであったノードはプライマリのままです。
上へ	上へ	A (プライマリ)、B (セカンダリ)	A (プライマリ)、B (セカンダリ)	両方のノードがヘルスチェックに合格した場合、フェイルセーフを有効にした場合の動作は変更されません。
上へ	NOT_UP	A (プライマリ)、B (セカンダリ)	A (プライマリ)、B (セカンダリ)	セカンダリノードだけに障害が発生した場合、フェイルセーフを有効にした場合の動作は変更されません。
NOT_UP	上へ	A (セカンダリ)、B (プライマリ)	A (セカンダリ)、B (プライマリ)	プライマリだけに障害が発生した場合、フェイルセーフを有効

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ノード A (プライマリ) のヘルス状態	ノード B（セカンダリ）のヘルス状態	デフォルトの高可用性動作	フェイルセーフ対応の高可用性動作	説明
				にした場合の動作は変更されません。
NOT_UP	UP (STAYSECONDARY)	A (二次)、B (二次)	A (プライマリ)、B (セカンダリ)	セカンダリがSTAYSECONDARYとして設定されている場合、プライマリは障害が発生してもプライマリのままです。

フェールセーフモードを構成するには

1. 構成ユーティリティの タブのナビゲーションペインで、 を展開し、 をクリックします。
2. 詳細ペインの タブで、ノードを選択し、 をクリックします。
3. ［ノードの構成］ダイアログボックスの［フェールセーフモード］で、［両方のノードが正常でない場合でもプライマリノードを1つ維持する］を選択し、［OK］をクリックします。

仮想 MAC アドレスの設定

仮想MACアドレスは、高可用性セットアップのプライマリおよびセカンダリNetScaler Gatewayアプライアンスで共有されます。

高可用性セットアップでは、プライマリNetScaler Gateway は、マッピングされたIPアドレスや仮想IPアドレスなど、すべてのフローティングIPアドレスを所有します。このプロトコルは、これらの IP アドレスに対するアドレス解決プロトコル（ARP）要求に対して、独自の MAC アドレスで応答します。その結果、外部デバイス（ルーターなど）のARPテーブルは、フローティングIPアドレスとプライマリNetScaler Gateway MACアドレスで更新されます。フェイルオーバーが発生すると、セカンダリNetScaler Gateway が新しいプライマリNetScaler Gateway として引き継ぎます。次に、gratuitous Address Resolution Protocol（GARP; 無償アドレス解決プロトコル）を使用して、プライマリアプライアンスから取得したフローティング IP アドレスをアドバタイズします。新しいプライマリアプライアンスがアドバタイズする MAC アドレスは、自身のインターフェイスの MAC アドレスです。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

一部のデバイスは、NetScaler Gateway によって生成されたGARPメッセージを受け入れません。その結果、一部の外部デバイスは、古いプライマリNetScaler Gateway によってアドバタイズされた古いIPからMACへのマッピングを保持します。この状況では、サイトが利用できなくなる可能性があります。この問題を解決するには、高可用性ペアの両方のNetScaler Gateway アプライアンスで仮想MACアドレスを構成します。この構成は、両方のNetScaler Gateway アプライアンスが同じMACアドレスを持つことを意味します。その結果、フェイルオーバーが発生しても、セカンダリNetScaler Gateway のMACアドレスは変更されず、外部デバイスのARPテーブルを更新する必要はありません。

仮想 MAC アドレスを作成するには、仮想ルータ ID（ID）を作成し、インターフェイスにバインドします。高可用性セットアップでは、ユーザは両方のアプライアンスのインターフェイスに ID をバインドする必要があります。

仮想ルータ ID がインターフェイスにバインドされると、システムは仮想ルータ ID を最後のオクテットとする仮想 MAC アドレスを生成します。汎用仮想 MAC アドレスの例は、00:00:5 e: 00:01:\ <VRID\ > です。たとえば、値 60 の仮想ルータ ID を作成し、それをインターフェイスにバインドした場合、結果の仮想 MAC アドレスは 00:00:5 e: 00:01:3 c になります。ここで、3c は仮想ルータ ID の 16 進数表現です。1 ～ 254 の範囲の 255 個の仮想ルータ ID を作成できます。

IPv4 および IPv6 の仮想 MAC アドレスを設定できます。

IPv4 仮想 MAC アドレスの設定

IPv4 仮想 MAC アドレスを作成してインターフェイスにバインドすると、インターフェイスから送信される IPv4 パケットはすべて、インターフェイスにバインドされた仮想 MAC アドレスを使用します。インターフェイスにバインドされた IPv4 仮想 MAC アドレスがない場合、インターフェイスの物理 MAC アドレスが使用されます。

汎用仮想 MAC アドレスは 00:00:5 e: 00:01:\ <VRID\ > の形式になります。たとえば、値が 60 の VRID を作成し、それをインターフェイスにバインドすると、生成される仮想 MAC アドレスは 00:00:5 e: 00:01:3 c になります。ここで、3c は VRID の 16 進数表現です。1 ～ 255 の値で 255 個の VRIDs を作成できます。

IPv4 仮想 MAC アドレスの作成または変更

IPv4 仮想 MAC アドレスを作成するには、仮想ルータ ID を割り当てます。その後、仮想 MAC アドレスをインターフェイスにバインドできます。複数の仮想ルータ ID を同じインターフェイスにバインドすることはできません。仮想 MAC アドレスの設定を確認するには、仮想 MAC アドレスと、仮想 MAC アドレスにバインドされたインターフェイスを表示して調べる必要があります。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

仮想 MAC アドレスを設定するためのパラメータ

VID

> 仮想 MAC アドレスを識別する仮想ルータ ID。可能な値:1 ～ 255

ifnum

> 仮想 MAC アドレスにバインドされるインターフェイス番号（スロット/ポート表記）。

仮想 MAC アドレスを設定するには

1. > に移動し、 をクリックします。
2. 詳細ペインの タブで、 をクリックします。
3. ダイアログボックスの に値を入力します。
4. の でネットワークインターフェイスを選択し、、、 の順にクリックします。

仮想 MAC アドレスを作成すると、その仮想 MAC アドレスが構成ユーティリティに表示されます。ネットワークインターフェイスを選択した場合、仮想ルータ ID はそのインターフェイスにバインドされます。

仮想 MAC アドレスを削除するには

仮想 MAC アドレスを削除するには、対応する仮想ルータ ID を削除する必要があります。

1. > に移動し、** をクリックします。
2. 詳細ペインで項目を選択し、 をクリックします。

仮想 MAC アドレスをバインドおよびバインド解除するには

仮想ルーターIDを作成したら、NetScaler Gateway でネットワークインターフェイスを選択し、仮想ルーターIDをネットワークインターフェイスにバインドしました。また、ネットワークインターフェイスから仮想MACアドレスをバインド解除できますが、NetScaler Gateway でMACアドレスは構成したままにしておきます。

1. > に移動し、 をクリックします。
2. 詳細ウィンドウで、アイテムを選択し、 をクリックします。
3. でネットワークインターフェイスを選択し、、、 の順にクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

IPv6 仮想 MAC アドレスの設定

NetScaler Gateway は、IPv6パケットの仮想MACアドレスをサポートしています。IPv4 仮想 MAC アドレスがインターフェイスにバインドされている場合でも、任意のインターフェイスを IPv6 用の仮想 MAC アドレスにバインドできます。インターフェイスから送信される IPv6 パケットは、そのインターフェイスにバインドされた仮想 MAC アドレスを使用します。インターフェイスにバインドされた仮想 MAC アドレスがない場合、IPv6 パケットは物理 MAC を使用します。

IPv6 用の仮想 MAC アドレスの作成または変更

IPv6 仮想 MAC アドレスに IPv6 仮想ルータ ID を割り当てて、IPv6 仮想 MAC アドレスを作成します。次に、仮想 MAC アドレスをインターフェイスにバインドします。複数の IPv6 仮想ルータ ID を 1 つのインターフェイスにバインドすることはできません。仮想 MAC アドレスの設定を確認するには、仮想 MAC アドレスおよび仮想 MAC アドレスにバインドされたインターフェイスを表示および確認します。

IPv6 用の仮想 MAC アドレスを設定するためのパラメータ

- `Virtual Router ID`

  仮想 MAC アドレスを識別する仮想ルータ ID。可能な値:1 ～ 255

- `ifnum`

  仮想 MAC アドレスにバインドされるインターフェイス番号（スロット/ポート表記）。

IPv6 の仮想 MAC アドレスを構成するには

1. 構成ユーティリティの タブで、 > を展開し、 をクリックします。
2. 詳細ペインの タブで、次のいずれかの操作を行います。
   - 新しい仮想 MAC アドレスを作成するには、 をクリックします。
   - 既存の仮想 MAC アドレスを変更するには、 をクリックします。
3. または ダイアログボックスの に、vrID6などの値を入力します。
4. インターフェイスの関連付けで、 > > をクリックします。ステータスバーに、仮想 MAC アドレスが設定されていることを示すメッセージが表示されます。

IPv6 の仮想 MAC アドレスを削除するには

1. 構成ユーティリティの タブで、 > を展開し、 をクリックします。
2. 詳細ペインの タブで、削除する仮想ルーター ID を選択し、 をクリックします。ステータスバーに、仮想 MAC アドレスが削除されたことを示すメッセージが表示されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

異なるサブネットでの高可用性ペアの設定

一般的な高可用性展開は、高可用性ペアの両方のアプライアンスが同じサブネット上にある場合です。高可用性展開は、各アプライアンスが異なるネットワークにある2つのNetScaler Gatewayアプライアンスで構成することもできます。このトピックでは、後者の設定について説明し、設定例と、1 つのネットワーク内およびネットワーク間での高可用性設定の違いの一覧を示します。

リンク冗長性とルートモニタを設定することもできます。これらのNetScaler Gateway 機能は、クロスネットワークの高可用性構成で役立ちます。これらの機能は、パートナーアプライアンスがアクティブであることを確認するために、各NetScaler Gateway で使用されるヘルスチェックプロセスもカバーします。

独立したネットワーク構成の仕組み

NetScaler Gateway アプライアンスは、2つの異なるネットワーク上のR3およびR4と呼ばれる異なるルーターに接続されています。アプライアンスは、これらのルータを介してハートビートパケットを交換します。ハートビートパケットは、接続がアクティブであることを確認する一定の間隔で発生する信号です。この構成を拡張して、任意の数のインターフェイスを含む展開に対応できます。

注:ネットワークでスタティックルーティングを使用する場合は、ハートビートパケットが正常に送受信されるように、すべてのシステム間にスタティックルートを追加する必要があります。（システムでダイナミックルーティングを使用する場合、スタティックルートは不要です）。

高可用性ペアのアプライアンスが2つの異なるネットワークに存在する場合、セカンダリNetScaler Gateway には独立したネットワーク構成が必要です。つまり、異なるネットワーク上のNetScaler Gateway アプライアンスは、マッピングされたIPアドレス、仮想LAN、またはネットワークルートを共有できません。高可用性ペアのNetScaler Gateway アプライアンスが異なる構成可能なパラメーターを持つこのタイプの構成は、独立ネットワーク構成または対称ネットワーク構成と呼ばれます。

次の表に、独立したネットワーク構成の構成可能なパラメーターをまとめ、各NetScaler Gatewayでパラメーターを設定する方法を示します。

設定可能なパラメータ	動作
IP アドレス	NetScaler Gateway 固有。そのアプライアンスでのみアクティブです。
仮想 IP アドレス	フローティング。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

設定可能なパラメータ	動作
仮想 LAN	NetScaler Gateway 固有。そのアプライアンスでのみアクティブです。
ルート	NetScaler Gateway 固有。そのアプライアンスでのみアクティブです。リンク負荷分散（LLB）ルートはフローティングです。
アクセスコントロールリスト (ACL)	フローティング (共通)。両方のアプライアンスでアクティブです。
動的ルーティング	NetScaler Gateway 固有。そのアプライアンスでのみアクティブです。セカンダリNetScaler Gateway もルーティングプロトコルを実行し、アップストリームルーターとピアリングする必要があります。
L2モード	フローティング (共通)。両方のアプライアンスでアクティブです。
L3モード	フローティング (共通)。両方のアプライアンスでアクティブです。
リバースネットワークアドレス変換 (NAT)	NetScaler Gateway 固有。NAT IP アドレスがフローティングであるため、仮想 IP アドレスを持つリバース NAT。

注:

INC モードの IPSET は、パブリック IP アドレスでサポートされます。詳細については、「Azure ロードバランサーを使用したNetScaler ADC 高可用性フロントエンド IP 検証済みリファレンスデザイン」を参照してください。

リモートノードの追加

高可用性ペアの 2 つのノードが異なるサブネットに存在する場合、各ノードのネットワーク構成は異なる必要があります。したがって、2 つの独立したシステムを高可用性ペアとして機能するように設定するには、設定プロセス中に独立したネットワークコンピューティングモードを指定する必要があります。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

高可用性ノードを追加するときは、接続されていない、またはトラフィックに使用されていない各インターフェイスの高可用性モニタを無効にする必要があります。

独立ネットワークコンピューティングモード用のリモートノードを追加するには

1. 構成ユーティリティの タブのナビゲーションペインで、 > を展開します。
2. 詳細ウィンドウで、 タブをクリックし、 をクリックします。
3. ［高可用性セットアップ］ダイアログボックスの［ **リモートノードのIPアドレス** ］テキストボックスに、リモートノードであるアプライアンスのNetScaler Gateway IPアドレスを入力します。

   IPv6 アドレスを使用するには、IP アドレスを入力する前に チェックボックスをクリックします。
4. ローカルノードをリモートノードに自動的に追加する場合は、 を選択します。このオプションを選択しない場合は、リモートノードで表されるアプライアンスにログオンし、現在構成しているノードを追加する必要があります。
5. クリックすると、ダウンしているインターフェイスまたはチャネルの HA モニタのクリアが有効になります。
6. セルフモードで INC (独立ネットワーク構成) モードをオンにする場合にクリックします。
7. **［OK］** をクリックします。 ページには、高可用性構成のローカルノードとリモートノードが表示されます。

リモートノードを削除するには

1. 構成ユーティリティの タブのナビゲーションペインで、 > を展開します。
2. 詳細ペインで、 タブをクリックします。
3. 削除するノードを選択し、、 の順にクリックします。

ルートモニタの設定

ルートモニタを使用すると、テーブルにダイナミックに学習されたルートまたはスタティックルートが含まれているかどうかにかかわらず、高可用性ステートを内部ルーティングテーブルに依存させることができます。高可用性構成では、各ノードのルートモニタが内部ルーティングテーブルをチェックして、特定のネットワークに到達するためのルートエントリが常に存在することを確認します。ルートエントリが存在しない場合、ルートモニタの状態は DOWN に変わります。

NetScaler Gateway アプライアンスにネットワークに到達するための静的ルートのみがあり、ネットワークのルートモニターを作成する場合は、静的ルートの監視対象静的ルートを有効にする必

© 1997–2026 Citrix Systems, Inc. All rights reserved.

要があります。モニタ対象のスタティックルートは、到達不能なスタティックルートを内部ルーティングテーブルから削除します。スタティックルートでモニタ対象スタティックルートを無効にすると、到達不能なスタティックルートが内部ルーティングテーブルに残り、ルートモニタの目的が失われます。

ルートモニタは、 設定を有効または無効にした場合にサポートされます。次の表に、高可用性セットアップのルートモニタと、独立ネットワーク構成を有効または無効にした場合の動作を示します。

無効になっている独立ネットワーク構成モードで高可用性のルートモニタ	有効な独立ネットワーク構成モードで高可用性のルートモニタ
ルートモニタはノードによって伝達され、同期中に交換されます。	ルートモニタは、ノードによって伝播されず、同期中に交換されることもありません。
ルートモニタは、現在のプライマリノードでのみアクティブです。	ルートモニタは、プライマリノードとセカンダリノードの両方でアクティブです。
NetScaler Gateway アプライアンスは、ルートエントリが内部ルーティングテーブルに存在するかどうかにかかわらず、ルートモニターの状態を常にUPとして表示します。	対応するルートエントリが内部ルーティングテーブルに存在しない場合、NetScaler Gateway アプライアンスは、ルートモニターの状態をダウンとして表示します。
ルートモニターは、次の場合にルートの監視を開始し、NetScaler Gateway が動的ルートを学習できるようにします。これには最大180秒かかる場合があります：再起動、フェイルオーバー、v6ルートのroute6コマンドの設定、`msr` v4ルートのルート有効/無効コマンド、新しいルートモニターの追加	該当なし。

ルートモニタは、独立ネットワーク構成モードを無効にし、プライマリノードからのゲートウェイを高可用性フェールオーバーの条件の 1 つとして到達不能にする場合に便利です。

たとえば、次の図に示すように、NetScaler Gateway アプライアンスNS1とNS2が同じサブネットにあり、ルーターR1とスイッチSW1、SW2、およびSW3を持つツーアームトポロジの高可用性セットアップで、独立したネットワーク構成を無効にします。このセットアップでは R1 が唯一のルータであるため、現在のプライマリノードから R1 に到達できないときはいつでも、高可用性セットアップをフェールオーバーします。各ノードにルートモニタ（それぞれ RM1 と RM2）を設定して、そのノードからの R1 の到達可能性を監視できます。



© 1997–2026 Citrix Systems, Inc. All rights reserved.

NS1 を現在のプライマリノードとして使用すると、ネットワークフローは次のようになります：

1. NS1 上のルートモニタ RM1 は、NS1 の内部ルーティングテーブルを監視し、ルータ R1 のルートエントリの存在を確認します。NS1 と NS2 は、スイッチ SW1 または SW3 を介して定期的にハートビートメッセージを交換します。
2. スイッチ SW1 に障害が発生すると、NS1 のルーティングプロトコルは R1 に到達できないことを検出し、内部ルーティングテーブルから R1 のルートエントリを削除します。NS1 と NS2 は、スイッチ SW3 を介してハートビートメッセージを定期的に交換します。
3. R1 のルートエントリが内部ルーティングテーブルに存在しないことを検出すると、RM1 はフェールオーバーを開始します。R1 へのルートが NS1 と NS2 の両方からダウンしている場合、アプライアンスの 1 つが R1 に到達して接続を復元できるようになるまで、180 秒ごとにフェイルオーバーが実行されます。

ルートモニタの追加または削除

高可用性ペアのアプライアンスが異なるネットワーク上にある場合、NetScaler Gateway の高可用性の状態は、アプライアンスに到達できるかどうかによって異なります。クロスネットワーク高可用性構成では、各NetScaler Gateway のルートモニターが内部ルーティングテーブルをスキャンして、他のNetScaler Gateway のエントリが常に存在することを確認します。

ルートモニタを追加するには

1. 構成ユーティリティの タブのナビゲーションペインで、 を展開し、 をクリックします。
2. ダイアログボックスの タブで、、 の順にクリックします。
3. ［ルートモニターの指定］の［ネットワーク］に、他のNetScaler Gateway アプライアンスのネットワークのIPアドレスを入力します。

   IPv6 アドレスを構成するには、 をクリックし、IP アドレスを入力します。
4. に、他のネットワークのサブネットマスクを入力し、、 の順にクリックします。

この手順が完了すると、ルートモニターはNetScaler Gateway にバインドされます。

注：ルートモニターがNetScaler Gateway にバインドされていない場合、いずれかのアプライアンスの高可用性の状態は、インターフェイスの状態によって決まります。

ルートモニタを削除するには

1. 構成ユーティリティの タブのナビゲーションペインで、 を展開し、 をクリックします。
2. タブで、、 の順にクリックします。
3. ［構成済みルートモニタ］でモニタを選択し、［削除］、［OK］の順にクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

リンク冗長性の設定

リンク冗長性は、ネットワークインターフェイスをグループ化して、他の機能しているインターフェイスを持つNetScaler Gateway の1つのネットワークインターフェイスの障害によるフェールオーバーを防ぎます。プライマリNetScaler Gateway の最初のインターフェイスで障害が発生すると、フェイルオーバーがトリガーされますが、最初のインターフェイスは2番目のリンクを使用してユーザー要求を処理できます。リンクの冗長性を構成すると、2つのインターフェイスをフェールオーバーインターフェイスセットにグループ化して、プライマリNetScaler Gateway のすべてのインターフェイスが機能しない限り、単一のリンクの障害によってセカンダリNetScaler Gateway へのフェールオーバーが発生するのを防ぐことができます。

フェールオーバーインターフェイスセット内の各インターフェイスは、独立したブリッジエントリを保持します。障害が発生したインターフェイスセットにバインドされていないNetScaler Gateway で有効で高可用性の監視インターフェイスは、クリティカルインターフェイスと呼ばれます。これらのインターフェイスのいずれかに障害が発生すると、フェールオーバーがトリガーされるためです。

リンク冗長性を設定するには

1. 構成ユーティリティの タブのナビゲーションペインで、 を展開し、 をクリックします。
2. タブで、 をクリックします。
3. に、セットの名前を入力します。
4. で、 をクリックします。
5. で、インターフェイスを選択し、矢印をクリックしてインターフェイスを に移動します。
6. 2 番目のインターフェイスについてステップ 4 と 5 を繰り返し、 をクリックします。

インターフェイス間のフェールオーバーに必要な数だけインターフェイスを追加できます。

フェールオーバーインターフェイスセットからインターフェイスを削除するには

1. 構成ユーティリティの タブのナビゲーションペインで、 を展開し、 をクリックします。
2. タブで、セットを選択し、 をクリックします。

フェールオーバーインターフェイスセットを削除するには

フェイルオーバーインターフェイスセットが不要になった場合は、NetScaler Gateway から削除できます。

1. 構成ユーティリティの タブのナビゲーションペインで、 を展開し、 をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. タブで、セットを選択し、 をクリックします。

フェイルオーバーの原因を理解する

次のイベントは、高可用性構成でフェールオーバーを引き起こす可能性があります。

1. セカンダリノードが、セカンダリノードで設定されたデッドインターバルを超える期間、プライマリノードからハートビートパケットを受信しない場合。デッドインターバルの設定の詳細については、「通信インターバルの設定」を参照してください。ノードがピアノードからハートビートパケットを受信しない原因としては、次のようなものがあります。
   - ネットワーク構成に問題があると、ハートビートが高可用性ノード間のネットワークを通過できなくなります。
   - ピアノードでハードウェアまたはソフトウェア障害が発生し、その原因でフリーズする（ハング）、リブートしたり、ハートビートパケットの処理や転送を停止したりします。
2. プライマリノードで SSL カードのハードウェア障害が発生します。
3. プライマリノードは、ネットワークインターフェイス上で 3 秒間ハートビートパケットを受信しません。
4. プライマリノードで、フェールオーバーインターフェイスセット (FIS) またはリンクアグリゲーション (LA) チャネルの一部ではなく、高可用性モニタ (HAMON) が有効になっているネットワークインターフェイスは失敗します。インターフェイスは有効になっていますが、DOWN 状態になります。
5. プライマリノードでは、FIS 内のすべてのインターフェイスで障害が発生します。インターフェイスは有効になっていますが、DOWN 状態になります。
6. プライマリノードで、HAMON が有効になっている LA チャネルで障害が発生します。インターフェイスは有効になっていますが、DOWN 状態になります。
7. プライマリノードでは、すべてのインターフェイスで障害が発生します。この場合、フェールオーバーは HAMON の設定に関係なく発生します。
8. プライマリノードでは、すべてのインターフェイスが手動で無効になります。この場合、フェールオーバーは HAMON の設定に関係なく発生します。
9. いずれかのノードで force failover コマンドを発行して、フェールオーバーを強制します。
10. プライマリノードにバインドされているルートモニタがダウンします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ノードからのフェイルオーバーの強制

たとえば、プライマリノードを交換またはアップグレードする必要がある場合は、フェールオーバーを強制的に実行できます。プライマリノードまたはセカンダリノードのいずれかから強制的にフェールオーバーできます。強制フェールオーバーは継承されたり、同期されたりしません。強制フェイルオーバー後の同期ステータスを表示するには、ノードのステータスを表示できます。

次の状況では、強制フェールオーバーを実行できません。

- スタンドアロンシステムにフェールオーバーを強制する。
- セカンダリノードは無効です。
- セカンダリノードはセカンダリのままになるように設定されます。

NetScaler Gateway アプライアンスは、強制フェイルオーバーコマンドの実行時に潜在的な問題を検出すると、警告メッセージを表示します。メッセージには、警告をトリガーした情報が含まれ、続行する前に確認を要求します。

プライマリノードまたはセカンダリノードでフェールオーバーを強制する

プライマリノードでフェールオーバーを強制すると、プライマリがセカンダリになり、セカンダリがプライマリになります。強制フェールオーバーは、プライマリノードがセカンダリノードが稼働中であると判断できる場合にのみ可能です。

セカンダリノードがダウンしている場合、force failover コマンドは次のエラーメッセージを返します。「ピアの状態が無効なため、操作できません。修正して再試行してください。」

セカンダリシステムが要求状態または非アクティブの場合、コマンドは次のエラーメッセージを返します。 `"Operation not possible now. Please wait for system to stabilize before retrying."`

セカンダリノードから force failover コマンドを実行すると、セカンダリノードはプライマリノードになり、プライマリノードはセカンダリノードになります。強制フェールオーバーは、セカンダリノードのヘルス状態が良好で、ノードがセカンダリを維持するように構成されていない場合にのみ発生します。

セカンダリノードがプライマリノードになれない場合、またはセカンダリノードがセカンダリのままになるように設定されている場合（STAYSECONDARYオプションを使用）、ノードは次のエラーメッセージを表示します。「自分の状態が無効であるため、操作はできません。詳細については、ノードを参照してください。」

© 1997–2026 Citrix Systems, Inc. All rights reserved.

プライマリノードまたはセカンダリノードでフェールオーバーを強制するには

1. 構成ユーティリティの タブのナビゲーションペインで、 を展開し、 をクリックします。
2. 詳細ウィンドウの タブで、プライマリノードを選択し、 で をクリックします。
3. ダイアログボックスで、 をクリックします。

プライマリノードを強制的にプライマリのままにする

高可用性構成では、アプライアンスのフェイルオーバー後もプライマリNetScaler Gateway を強制的にプライマリのままにすることができます。この設定は、スタンドアロンのNetScaler Gateway アプライアンスと、高可用性ペアのプライマリアプライアンスであるNetScaler Gateway でのみ構成できます。

プライマリノードを強制的にプライマリに保つには

1. 構成ユーティリティの タブのナビゲーションペインで、 を展開し、 をクリックします。
2. 詳細ペインの タブで、ノードを選択し、 をクリックします。
3. で、 をクリックし、 をクリックします。

この設定は、次のコマンドを使用することによってのみクリアできます。

```
clear configuration full
```

次のコマンドは、NetScaler Gateway の高可用性構成を変更しません。

```
clear configuration basic
```

```
clear configuration extended
```

セカンダリノードを強制的にセカンダリに維持する

高可用性セットアップでは、プライマリNetScaler Gateway の状態に関係なく、セカンダリNetScaler Gateway を強制的にセカンダリのままにすることができます。NetScaler Gateway をセカンダリのままにするように構成すると、プライマリNetScaler Gateway に障害が発生してもセカンダリのままになります。

たとえば、既存の高可用性セットアップで、プライマリNetScaler Gateway をアップグレードする必要があり、このプロセスに指定された時間がかかるとします。アップグレード中、プライマリNetScaler Gateway が使用できなくなる場合がありますが、セカンダリNetScaler Gateway が引き継ぐことは望ましくありません。プライマリNetScaler Gateway で障害が検出された場合でも、セカンダリNetScaler Gateway のままにします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

高可用性ペアのNetScaler Gateway のステータスがセカンダリになるように構成されている場合、高可用性ステートマシンの移行には参加しません。NetScaler Gateway のステータスは、構成ユーティリティの［ **ノード** ］タブで確認できます。

この設定は、スタンドアロンとセカンダリNetScaler Gateway の両方で機能します。

高可用性ノードを設定すると、そのノードは伝播または同期されず、設定が構成されている NetScaler Gateway のみに影響します。

セカンダリノードを強制的にセカンダリに保つには

1. 構成ユーティリティの タブのナビゲーションペインで、 を展開し、 をクリックします。
2. 詳細ペインの タブでノードを選択し、 をクリックします。
3. で、 をクリックし、 をクリックします。

NetScaler Gateway をアクティブな高可用性アプライアンスとしてサービスに戻すには

1. 構成ユーティリティの タブのナビゲーションペインで、 を展開し、 をクリックします。
2. 詳細ペインの タブで、プライマリノードとして維持するアプライアンスを選択し、 をクリックします。
3. で、 をクリックし、 をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

クラスタリングの使用

NetScaler Gateway をクラスタ構成に展開して、VPNクライアントトラフィックに高スループット、高可用性、およびスケーラビリティを提供できます。クラスターでは、NetScaler Gateway アプライアンスまたは仮想マシンのグループが単一のシステムイメージとして動作し、ユーザーセッションを調整し、ネットワークリソースへのトラフィックを管理します。NetScaler Gateway クラスターは、クラスターノードとして構成された最小2台および最大32台のNetScaler Gateway アプライアンスまたは仮想マシンを使用して構築できます。

NetScaler Gateway クラスターの構成を開始する前に、NetScaler ADCクラスタリングのドキュメントをお読みください 。このドキュメントの次のトピックに特に注意してください。

- 使用する予定のシステムが要件を満たしていることを確認するには、ハードウェアおよびソフトウェアの要件を参照してください 。
- クラスタリングの概念については、クラスタリングの仕組みを参照してください 。
- 展開を計画し、環境に関連する可能性のある警告を特定するには、 ノード間通信の設定を参照してください 。

NetScaler Gateway クラスターは、スポッティングされたVIP構成タイプのNetScaler ADCクラスターとして動作します。

重要：

XenApp およびXenDesktopウィザードはクラスタリングに対応していないため 、［GUI］>［ナビゲーションペイン］>［Citrix製品との統合］セクションにXXenApp および XenDesktopウィザードが表示されません** 。

クラスタリングの構成

NetScaler Gateway クラスタリングをセットアップする際の主なタスクは次のとおりです：

1. 構成コーディネーターとなるNetScaler Gateway アプライアンスまたは仮想マシンを決定し、そのシステムにクラスターインスタンスを作成します（クラスターインスタンスがまだ存在しない場合）。
2. NetScaler Gateway システムをノードとしてクラスターに参加させます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. STICKY オプションを設定して、クラスタインスタンスにノードグループを作成します。
4. 1 つのクラスタノードをクラスタノードグループにバインドします。
5. 構成コーディネーターでNetScaler Gateway 仮想サーバーを構成し、クラスターノードグループにバインドします。

NetScaler ADCクラスターを構成するには、複数の方法があります。次の一連のタスクでは、構成ユーティリティで使用できる最も直接的な方法を使用します。

構成ユーティリティを使用してNetScaler Gateway クラスターインスタンスを作成するには

展開の詳細を整理したら、構成コーディネーターであるNetScaler Gateway で構成を開始します。

注意:クラスターインスタンスを作成すると、設定がクリアされます。参照用に既存のシステム設定を保存する必要がある場合は、クラスタ構成を続行する前にコピーをアーカイブします。クラスタで使用される既存の設定は、クラスタの確立後に構成コーディネータに再適用できます。

1. NSIPアドレスでNetScaler ADC構成ユーティリティにログオンします。
2. ノード、 サブノードの順に展開します。
3. 詳細ウィンドウで、 をクリックします。
4. ダイアログボックスで、クラスタの作成に必要なパラメータを設定します。
    a. クラスターインスタンス ID を入力します。クラスターインスタンス ID は、クラスターインスタンスの数値識別子です。デフォルト値は 1 ですが、1 ～ 16 の任意の数値に設定できます。
    b. クラスタ IP アドレスを入力します。クラスタ IP アドレスは、クラスタの構成コーディネータの IP アドレスで、クラスタの管理 IP アドレスです。
    c. 優先するバックプレーンインターフェイスを選択します。これは、クラスタノード間の通信に使用するこのNetScaler Gateway インターフェイスです。
5. ［Create］ をクリックします。
6. システムの再起動を確認するプロンプトが表示されたら、 をクリックします。
7. ノードが起動し、同期が成功したら、クラスタ IP アドレスから、ノードとクラスタ IP アドレスの両方の RPC 認証情報を変更します。RPC ノードのパスワードの変更の詳細については、「RPC ノードのパスワードを変更する」を参照してください。
8. システムが再起動するのを待ちます。使用可能になったら、手順 4 (2) で設定したクラスタ IP アドレスで構成ユーティリティにログオンします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注： 詳細ペインで** 、NSIP アドレスのローカルノードが構成コーディネーターとして報告されます。これにより、ベースクラスターインスタンスが動作中であることを確認します。

構成コーディネーターのローカルノードは、自動的にクラスタに追加されます。次のタスクでは、さらにノードを追加できます。

NetScaler Gateway クラスターへのノードの追加

クラスターインスタンスが確立されたら、他のNetScaler Gateway ノードをクラスターに追加できます。

NetScaler Gateway システムをクラスターに追加するには、構成ユーティリティを使用して、クラスターノードの作成およびクラスターへの参加の設定をリモートで発行します。

注：クラスターへのノードの追加は、NetScaler Gateway セットアップを構成する前に完了する必要があります。この方法では、クラスター構成に何か問題があり、クラスターを削除してやり直す必要がある場合に、NetScaler Gateway 構成を繰り返す必要はありません。

1. クラスターIPアドレスでNetScaler ADC構成ユーティリティにログオンします。
2. 「 **システム** 」ノードを展開し、次に「クラスタ」サブノードを展開します。
3. 詳細ウィンドウで、 をクリックします。
4. 詳細ペインで、 をクリックします。
5. ペインで、このノードの一意のノード ID を入力します。
6. クラスタノードとして追加するシステムのNetScaler ADC IPアドレスを入力します。
7. ［ **クラスターノードの資格情報** ］ペインで、リモートNetScaler Gateway システムの NetScaler Gateway ユーザー名とパスワードを入力します。
8. ウィンドウで、ローカルの承認済みユーザーのパスワードを入力します。
9. **［Create］** をクリックします。
10. メッセージが表示されたら、 をクリックしてシステム構成を保存し、リモートのCitrix Gatewayのウォームリブートを実行します。
11. ノードが起動し、同期が成功したら、クラスタ IP アドレスから、ノードとクラスタ IP アドレスの両方の RPC 認証情報を変更します。RPC ノードのパスワードの変更の詳細については、「 RPC ノードのパスワードを変更する」を参照してください。

クラスターノードとして構成する追加のリモートNetScaler Gateway システムごとに、手順4から11を繰り返します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

クラスタノードが 詳細ペインの に含まれていることを確認します。欠落しているノードがある場合は、必要なすべてのノードがリストされるまで、手順 4 〜 10 を繰り返します。

クラスタノードグループの作成

クラスタノードを追加したら、クラスタノードグループを作成できます。

1. クラスターIPアドレスでNetScaler ADC構成ユーティリティにログオンします。
2. 「 **システム** 」ノードを展開し、次に「クラスタ」サブノードを展開します。
3. をクリックします。
4. 詳細ペインで、 をクリックします。
5. クラスタノードグループの名前を入力します。
6. NetScaler Gateway 仮想サーバーの種類をサポートするには、［ **スティッキー** ］オプションを選択します。
7. ［**続行**］ をクリックします。

これで、クラスタノードグループが確立されました。構成ユーティリティのこの領域を離れる前に、ローカルNetScaler Gateway ノードを新しいクラスターノードグループにバインドできます。これは、クラスタグループにバインドされている唯一のノードです。

ローカルクラスタノードをクラスタノードグループにバインドします

NetScaler Gateway クラスター構成はスポットタイプであるため、ノードグループにバインドできるノードは1つのみです。次の手順は、構成コーディネーター上のローカルノードをノードグループにバインドしますが、クラスター内の任意のノードをこのバインドに使用できます。

1. ペインで、 を展開します。
2. 中央の ペインで、 を選択します。
3. 画面で、 をクリックします。
4. このNetScaler Gateway システムのNSIPアドレスで表されるローカルノードを選択します。
5. をクリックします。
6. ［OK］ をクリックします。
7. ［完了］ をクリックします。

これで、クラスターにデータが入力され、次のタスクで構成されたとおりにNetScaler Gateway 仮想サーバーを共有する準備が整いました。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler Gateway 仮想サーバーをクラスターノードグループにバインドする

クラスターが確立されたら、クラスター展開が機能するNetScaler Gateway 構成の構築に進むことができます。構成をクラスターに関連付けるには、NetScaler Gateway 仮想サーバーを作成し、スティッキータイプに設定されているクラスターノードグループにバインドする必要があります。仮想サーバーがクラスターノードグループにバインドされたら、NetScaler Gateway の構成を続行できます。

複数のNetScaler Gateway 仮想サーバーが構成されている場合は、それらもクラスターノードグループにバインドする必要があります。

注： NetScaler Gateway 仮想サーバーがまだ構成されていない場合は、最初に［**システム**］>［**設定**］>［**基本機能の構成**］で**NetScaler Gateway および認証、承認、および監査機能を有効にする必要があります。**

1. クラスターIPアドレスでNetScaler ADC構成ユーティリティにログオンします。
2. 「**システム**」ノードを展開し、次に「クラスタ」サブノードを展開します。
3. をクリックします。
4. ペインで、目的のノードグループ名を選択し、 をクリックします。
5. 右側の ペインで、 オプションを展開し、 アイコンをクリックして仮想サーバーを追加します。
6. VPN 仮想サーバーの種類を選択し、 をクリックします。
7. ［**Bind**］ をクリックします。
8. 必要な仮想サーバーが表示されている場合は、それを選択し、「**挿入**」、 **「OK」**の順にクリックします。
9. 新しい仮想サーバーを作成する必要がある場合は、 をクリックします。NetScaler ADC仮想サーバーの構成に進みます。最低限必要なのは、仮想サーバーを作成してクラスターノードグループにバインドできるようにすることだけです。
10. ［NetScaler Gateway 仮想サーバー］ボックスの一覧で仮想サーバーが使用可能になったら、それを選択し、［**挿入**］をクリックします。
11. ［**OK**］ をクリックします。
12. ［**完了**］ をクリックします。

注：複数のNetScaler Gateway 仮想サーバーが構成されている場合は、これと同じ方法でそれらもクラスターノードグループにバインドする必要があります。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Unified Gateway

Unified Gateway を備えたNetScaler ADC：1つのURL

Unified Gateway を搭載したNetScaler ADCにより、デスクトップユーザーおよびモバイルユーザー向けに、単一のURLを介したあらゆるアプリケーションへの簡素化された安全なアクセスが可能になります。この単一の URL の背後には、アプリケーションへのリモートアクセスの構成、セキュリティ、および制御を一元的に管理できます。また、リモートユーザーは、必要なすべてのアプリケーションへのシームレスなシングルサインオンと、ログイン/ログアウトの操作性が向上しました。

これを実現するために、Citrix ADC with Gatewayは、Citrix ADCのコンテンツスイッチング機能および広範な認証インフラストラクチャとともに、この単一のURLを通じて組織のサイトやアプリケーションへのアクセスを提供します。また、リモートユーザーは、iOSまたはAndroidのモバイルデバイスと、NetScaler Gateway クライアントプラグインを備えたLinux、PC、またはMacシステムを使用して、どこにいてもUnified Gateway URLに均一にアクセスできます。

Unified Gateway 展開では、次のカテゴリのアプリケーションへの単一の URL アクセスを許可します。

- イントラネットアプリケーション。
- クライアントレスアプリケーション
- サービスとしてのソフトウェアアプリケーション
- NetScaler ADCによって提供される事前構成されたアプリケーション
- Citrix Virtual Apps and Desktops 公開アプリケーション

イントラネットアプリケーションは 、セキュアなエンタープライズネットワーク内に存在する任意の Web ベースのアプリケーションです。これらは、組織のイントラネットサイト、バグ追跡アプリケーション、Wiki などの内部リソースです。

通常、 **セキュアなエンタープライズネットワーク内に存在するクライアントレスアプリケーションの** Unified Gateway は、Outlook Web Access と SharePoint への単一の URL アクセスを提供します。これらのアプリケーションは、リモートユーザーが使用する必要がある専用のクライアントソフトウェアを使用せずに、Exchange 電子メールおよびチームリソースへのアクセスを提供します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SaaS アプリケーションは、一般にクラウドアプリケーションとも呼ばれ、組織が依存している ShareFile、Salesforce、NetSuite などの外部クラウドベースのアプリケーションです。SAML ベースのシングルサインオンは、それを提供する SaaS アプリケーションでサポートされています。

一部の組織では、**NetScaler ADC負荷分散構成で展開されたNetScaler ADCサーバーアプリケーションを事前に構成している場合があります**。多くの場合、これは「リバースプロキシ」アプリケーションとも呼ばれます。Unified Gateway は、展開用の仮想サーバーが同じNetScaler ADC Unified Gatewayインスタンスまたはアプライアンスに存在する場合、これらのアプリケーションをサポートします。これらのアプリケーションは、Unified Gateway 構成とは独立した独自の認証構成を持つ場合があります。

公開された **Citrix Virtual Apps and Desktops の公開アプリケーションは**、Unified Gateway URL を通じて利用可能にすることができます。SmartAccess および SmartControl ポリシーは、オプションで、これらのリソースに対する詳細なポリシーとアクセス制御に適用できます。

Unified Gateway 構成ウィザード

Unified Gateway 展開でNetScaler ADCを構成するための推奨される方法は、Unified Gateway 構成ウィザードを使用することです。ウィザードでは、構成を順を追って実行し、必要なすべての仮想サーバー、ポリシー、および式を作成し、提供された詳細に基づいて設定を適用します。初期セットアップ後、ウィザードを使用して展開を管理し、その動作を監視できます。

注：

Unified Gateway 構成ウィザードでは、システムの初期設定は実行されません。NetScaler Gateway アプライアンスまたはVPXインスタンスは、Unified Gateway を構成する前に基本インストールを完了している必要があります。基本構成を完了するには、「初回セットアップウィザードを使用したNetScaler Gatewayの構成」のインストール手順を参照してください。

ウィザードによって設定される Unified Gateway 要素は次のとおりです。

- Unified Gateway プライマリ仮想サーバ
- Unified Gateway 仮想サーバの SSL サーバ証明書
- プライマリ認証およびオプションのセカンダリ認証設定
- ポータル・テーマの選択とオプションのカスタマイズ
- Unified Gateway ポータルを介してアクセスされるユーザアプリケーション

© 1997–2026 Citrix Systems, Inc. All rights reserved.

これらの各要素について、構成情報を提供する必要があります。基本的な Unified Gateway 展開では、次の情報が必要です。

- プライマリ Unified Gateway 仮想サーバの場合、展開のパブリック IP アドレスと IP ポート番号。これは、DNS でUnified Gateway URL のホスト名に解決される IP アドレスです。たとえば、Unified Gateway 展開の URL が `https://mycompany.com/` の場合、IP アドレスは mycompany.com に解決される必要があります。
- 展開用の署名付き SSL サーバ証明書。NetScaler Gateway は、PEMまたはPFX形式の証明書をサポートしています。
- プライマリ認証サーバ情報。この認証構成でサポートされている認証システムは、LDAP/Active Directory、RADIUS、および証明書ベースです。セカンダリ LDAP または RADIUS 認証設定も作成される場合があります。認証サーバの IP アドレスは、関連する管理者クレデンシャルまたはディレクトリ属性とともに指定する必要があります。証明書認証の場合、デバイス証明書属性と CA 証明書を指定する必要があります。
- ポータル・テーマが選択されている場合があります。カスタマイズまたはブランド化されたポータル設計が必要な場合は、ウィザードを使用してカスタムグラフィックをシステムにアップロードできます。
- Web ベースのユーザアプリケーションでは、個々のアプリケーションの URL を指定する必要があります。SAML シングルサインオン認証を使用する Web アプリケーションの場合、ユーティリティは、他のオプションの SAML パラメータとともにアサーションコンシューマサービス URL を収集します。SAML 認証システムを使用するアプリケーションの構成の詳細を事前に収集します。
- Citrix Virtual Apps and Desktops の公開リソースをUnified Gateway展開環境で使用できるようにするには、統合ポイント（StoreFront、Web Interface、またはNetScaler ADC上のWeb Interface）を指定する必要があります。このユーティリティには、統合ポイントの完全修飾ドメイン名、サイトパス、シングルサインオンドメイン、Secure Ticket Authority (STA) サーバーの URL、および統合ポイントのタイプに応じてその他が必要です。

追加の構成管理

代替SSL設定やセッションポリシーなど、Unified Gateway構成ユーティリティでは利用できないサイト固有の設定については、NetScaler Gateway 構成ユーティリティで必要な設定を管理できます。これらの設定は、Unified Gateway 構成ユーティリティによって作成されたコンテンツスイッチングまたは VPN 仮想サーバで変更できます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

コンテンツスイッチング仮想サーバー

これは、展開のメインIPアドレスとURLの背後にあるNetScaler ADC構成エンティティです。SSLサーバ証明書とパラメータは、この仮想サーバで管理されます。この仮想サーバーは展開の応答ネットワークホストであるため、必要に応じて ICMP サーバーの応答と RHI の状態をこの仮想サーバーで変更できます。コンテンツスイッチ仮想サーバーは、 > > の タブにあります。

重要：

Unified Gateway 環境をリリース 13.0 ビルド 58.x 以降にアップグレードすると、ゲートウェイまたは VPN 仮想サーバーの前に構成されているコンテンツスイッチング仮想サーバーで DTLS ノブが無効になります。アップグレード後、コンテンツスイッチング仮想サーバーで DTLS ノブを手動で有効にします。設定にウィザードを使用している場合は、DTLS ノブを有効にしないでください。

VPN 仮想サーバー

Unified Gateway 構成のその他すべての VPN パラメータ、プロファイル、およびポリシーバインディングは、メイン認証構成を含め、この仮想サーバで管理されます。このエンティティは、**Citrix Gateway** > **仮想サーバーの** ［**構成**］タブで管理されます。関連する VPN 仮想サーバーの名前には、Unified Gateway の初期構成時にコンテンツスイッチング仮想サーバーに付けられた名前が含まれます。

注：

Unified Gateway 展開用に作成された VPN 仮想サーバはアドレス指定できず、0.0.0.0 IP アドレスが割り当てられます。

Unified Gateway に関するよくある質問

Unified Gateway とは何ですか

Unified Gatewayは、NetScaler ADC 11.0リリースの新機能であり、単一の仮想サーバー（Unified Gateway 仮想サーバーと呼ばれる）でトラフィックを受信し、必要に応じてそのトラフィックをUnified Gateway仮想サーバーにバインドされている仮想サーバーに内部的に転送する機能を提供します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Unified Gateway 機能を使用すると、エンドユーザは（Unified Gateway 仮想サーバに関連付けられた）単一の IP アドレスまたは URL を使用して複数のサービスにアクセスできます。管理者は、IPアドレスを解放し、NetScaler Gateway 展開の構成を簡素化できます。

各Unified Gateway 仮想サーバーは、フォーメーションの一部として、ゼロ個以上の負荷分散仮想サーバーとともに、1つのNetScaler Gateway 仮想サーバーをフロントエンドにすることができます。Unified Gateway は、NetScaler ADCアプライアンスのコンテンツスイッチング機能を使用して機能します。

Unified Gateway の展開の例をいくつか示します：

- Unified Gateway 仮想サーバー->
- Unified Gateway 仮想サーバー->
- Unified Gateway 仮想サーバー->
- Unified Gateway 仮想サーバー->

各負荷分散仮想サーバーは、Microsoft ExchangeやCitrix ShareFileなどのバックエンドサービスをホストする標準負荷分散サーバーであればどれでもかまいません。

Unified Gateway を使用する理由

Unified Gateway 機能を使用すると、エンドユーザは（Unified Gateway 仮想サーバに関連付けられた）単一の IP アドレスまたは URL を使用して複数のサービスにアクセスできます。管理者にとっての利点は、IPアドレスを解放し、NetScaler Gateway 展開の構成を簡素化できることです。

複数の Unified Gateway 仮想サーバを使用できますか

はい。Unified Gateway 仮想サーバは必要な数だけ存在できます。

Unified Gateway でコンテンツスイッチングが必要なのはなぜですか

コンテンツスイッチング仮想サーバーは、トラフィックを受信し、内部的に適切な仮想サーバーに誘導する仮想サーバーであるため、コンテンツスイッチング機能が必要です。コンテンツスイッチング仮想サーバーは、Unified Gateway 機能のプライマリコンポーネントです。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

11.0 より前のリリースでは、コンテンツスイッチングを使用して複数の仮想サーバのトラフィックを受信できます。その使用方法は Unified Gateway とも呼ばれますか

複数の仮想サーバーのトラフィックを受信するためのコンテンツスイッチ仮想サーバーの使用は、11.0 より前のリリースでサポートされています。ただし、コンテンツスイッチングでは、NetScaler Gateway 仮想サーバーにトラフィックを転送することはできません。

11.0の拡張により、コンテンツスイッチング仮想サーバーは、NetScaler Gateway 仮想サーバーを含む任意の仮想サーバーにトラフィックを転送できます。

Unified Gateway のコンテンツスイッチングポリシーで何が変わったのですか

1. コンテンツスイッチングアクション用の新しいコマンドラインパラメータ「-targetVServer」が追加されました。新しいパラメーターは、ターゲットのNetScaler Gateway 仮想サーバーを指定するために使用されます。例：

   add cs action UG_CSACT_MyUG -targetVserver UG_VPN_MyUG

   NetScaler Gateway 構成ユーティリティでは、コンテンツスイッチングアクションに新しいオプション「ターゲット仮想サーバー」が追加されました。このオプションは、NetScaler Gateway 仮想サーバーを参照できます。
2. 新しい高度なポリシー式is_vpn_urlを使用して、NetScaler Gateway および認証固有のリクエストを照合できます。

Unified Gatewayで現在サポートされていないNetScaler Gatewayの機能は何ですか?

Unified Gateway では、すべての機能がサポートされています。ただし、VPN プラグインを介したネイティブログオンでは、軽微な問題（問題 ID 544325）が報告されています。この場合、シームレスシングルサインオン (SSO) は機能しません。

Unified Gateway では、EPA スキャンの動作はどのようなものですか

Unified Gateway では、エンドポイント分析はNetScaler Gateway アクセス方法に対してのみトリガーされ、NetScaler ADC AAA TMアクセスではトリガーされません。NetScaler Gateway 仮想サーバーで認証が行われているにもかかわらず、ユーザーがNetScaler ADC AAA TM仮想サーバーにアクセスしようとすると、EPAスキャンはトリガーされません。ただし、ユーザがクライアントレス VPN/フル VPN アクセスを取得しようとすると、設定された EPA スキャンがトリガーされます。その場合は、認証またはシームレス SSO のいずれかが行われます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Unified Gateway のライセンス要件は何ですか

Unified Gateway は、アドバンスドライセンスおよびプレミアムライセンスでのみサポートされます。NetScaler Gateway のみのライセンスエディションまたはスタンダードライセンスエディションでは使用できません。

Unified Gatewayで使用されるNetScaler Gateway 仮想サーバーには、IP/ポート/SSL構成が必要ですか?

Unified Gateway仮想サーバーで使用されるNetScaler Gateway 仮想サーバーの場合、NetScaler Gateway 仮想サーバーでIP/ポート/SSL構成は必要ありません。ただし、RDPプロキシ機能の場合、同じSSL/TLSサーバー証明書をNetScaler Gateway 仮想サーバーにバインドできます。

NetScaler Gateway 仮想サーバー上にあるSSL/TLS証明書を、Unified Gateway 仮想サーバーで使用するために再プロビジョニングする必要がありますか

NetScaler Gateway 仮想サーバーに現在バインドされている証明書を再プロビジョニングする必要はありません。既存の SSL 証明書を自由に再利用し、それらを Unified Gateway 仮想サーバーにバインドできます。

単一の URL とマルチホスト展開の違いは何ですか? どちらが必要ですか

単一の URL は、Unified Gateway 仮想サーバが 1 つの完全修飾ドメイン名 (FQDN) のトラフィックを処理する能力を指します。この制限は、証明書のサブジェクトに FQDN が入力された SSL/TLS サーバ証明書を Unified Gateway が使用する場合に存在します。例:ug.citrix.com

Unified Gateway がワイルドカードサーバ証明書を使用している場合、複数のサブドメインのトラフィックを処理できます。例:*.citrix.com

もう 1 つのオプションは、複数の SSL/TLS サーバー証明書のバインドを可能にするサーバー名インジケータ (SNI) 機能を備えた SSL/TLS 構成です。例：auth.citrix.com、auth.citrix.de、auth.citrix.co.uk、auth.citrix.co.jp

単一ホストと複数ホストは、Web サーバー (Apache HTTP サーバーや Microsoft インターネットインフォメーションサービス (IIS) など) で Web サイトが一般的にホストされる方法に似ています。単一のホストがある場合は、Apache でエイリアスまたは「仮想ディレクトリ」を使用する場合と同じ方法で、サイトパスを使用してトラフィックを切り替えることができます。複数のホストがある場合は、Apache で仮想ホストを使用する場合と同様に、ホストヘッダーを使用してトラフィックを切り替えます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Unified Gateway ではどのような認証メカニズムを使用できますか

NetScaler Gateway と互換性のある既存の認証メカニズムはすべて、Unified Gateway とも互換性があります。

これには、LDAP、RADIUS、SAML、Kerberos、証明書ベースの認証などが含まれます。

アップグレード前にNetScaler Gateway 仮想サーバーで構成されている認証メカニズムは、NetScaler Gateway 仮想サーバーがUnified Gateway 仮想サーバーの背後に配置されたときに自動的に使用されます。アドレス指定不可能なIPアドレス（0.0.0.0）をNetScaler Gateway 仮想サーバーに割り当てる以外に、追加の構成手順は必要ありません。

「selfAuth」認証とは何ですか

selfAuth は、それ自体では認証タイプではありません。selfAuth は、URL の作成方法を記述します。VPN URL設定には 、新しいコマンドラインパラメータ`ssotype`を使用できます。例：

```
> add vpn url RGB RGB "http://blue.citrix.lab/" -vServerName Blue -ssotype selfauth
```

selfAuth は、 `ssotype` パラメータの値の 1 つです。このタイプの URL は、Unified Gateway 仮想サーバと同じドメインにないリソースにアクセスするために使用できます。この設定は、ブックマークを構成するときに構成ユーティリティで確認できます。

「StepUp」認証」って何ですか

NetScaler ADC AAA TMリソースにアクセスするために、より安全なレベルの認証が必要な場合は、StepUp認証を使用できます。コマンドラインで、authnProfile コマンドを使用して authenticationLevel パラメーターを設定します。例：

```
add authentication authnProfile AuthProfile -authnVsName AAATMVserver
-AuthenticationHost auth.citrix.lab -AuthenticationDomain citrix.lab **-
**AuthenticationLevel 100
```

この認証プロファイルは、負荷分散仮想サーバーにバインドされます。

ステップアップ認証はNetScaler ADC AAA TM仮想サーバーでサポートされていますか

はい、サポートされています。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

`login once/logout once`って何ですか

`Login Once`：VPNユーザーは、NetScaler ADC AAA TMまたはNetScaler Gateway仮想サーバーのいずれかに一度ログインします。それ以降、VPN ユーザーはすべてのエンタープライズ/クラウド/Web アプリケーションにシームレスにアクセスできます。ユーザは再認証される必要はありません。ただし、再認証は、NetScaler ADC AAA TM StepUp などの特殊なケースに対して行われます。

`Logout Once`：最初のNetScaler ADC AAA TMまたはNetScaler Gatewayセッションが作成された後、そのユーザーの後続のNetScaler ADC AAA TMまたはNetScaler Gatewayセッションを作成するために使用されます。これらのセッションのいずれかがログアウトすると、NetScaler ADCアプライアンスはユーザーの他のアプリケーションまたはセッションもログアウトします。

負荷分散仮想サーバーレベルでNetScaler ADC AAA TM負荷分散仮想サーバー固有の認証バインドを使用して、共通の認証ポリシーをUnified Gatewayレベルで指定できますか? このユースケースをサポートするための構成手順を教えてください

Unified Gateway の背後にあるNetScaler ADC AAA TM仮想サーバーに個別の認証ポリシーを指定する必要がある場合は、個別のアドレス指定可能な認証仮想サーバーが必要です（通常のNetScaler ADC AAA TM構成と同様）。負荷分散仮想サーバーの認証ホスト設定は、この認証仮想サーバーを指し示す必要があります。

バインドされたNetScaler ADC AAA TM仮想サーバーが独自の認証ポリシーを持つように、Unified Gatewayをどのように構成しますか

このシナリオでは、負荷分散サーバーで、NetScaler ADC AAA TM仮想サーバーを指すように認証FQDNオプションを設定する必要があります。NetScaler ADC AAA TM仮想サーバーは、独立したIPアドレスを持っており、NetScaler ADCおよびクライアントから到達可能である必要があります。

NetScaler ADC AAA TM認証仮想サーバーは、Unified Gateway 仮想サーバーを介して来るユーザーを認証するために必要ですか?

なしNetScaler Gateway 仮想サーバーは、NetScaler ADC AAA TM ユーザーも認証します。

NetScaler Gateway 認証ポリシーは、Unified Gateway 仮想サーバーまたはNetScaler Gateway 仮想サーバーでどこで指定しますか

認証ポリシーは、NetScaler Gateway 仮想サーバーにバインドされます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Unified Gateway コンテンツスイッチング仮想サーバーの背後にあるNetScaler ADC AAA TM仮想サーバーで認証を有効にするにはどうすればよいですか

NetScaler ADC AAA TM で認証を有効にし、認証ホストをUnified Gateway コンテンツスイッチング FQDN にポイントします。

コンテンツスイッチの後ろに TM 仮想サーバーを追加する方法 (単一の URL とマルチホスト)

単一のURLに対してNetScaler ADC AAA TM仮想サーバーを追加することと、複数のホストに追加することには違いはありません。いずれの場合も、仮想サーバーはコンテンツスイッチングアクションのターゲットとして追加されます。単一の URL とマルチホストの違いは、コンテンツスイッチングポリシールールによって実装されます。

仮想サーバーがUnified Gateway 仮想サーバーの背後に移動された場合、NetScaler ADC AAA TM負荷分散仮想サーバーにバインドされた認証ポリシーはどうなりますか?

認証ポリシーは認証仮想サーバーにバインドされ、認証仮想サーバーは負荷分散仮想サーバーにバインドされます。Unified Gateway仮想サーバーの場合、NetScaler Gateway 仮想サーバーを単一の認証ポイントとして使用することをお勧めします。これにより、認証仮想サーバーで認証を実行する必要がなくなります（または特定の認証仮想サーバーの必要性さえあります）。認証ホストをUnified Gateway仮想サーバーのFQDNを指すようにすることで、NetScaler Gateway 仮想サーバーによって認証が行われることが保証されます。認証ホストに Unified Gateway のコンテンツスイッチングをポイントし、まだ認証仮想サーバがバインドされている場合、認証仮想サーバにバインドされた認証ポリシーは無視されます。ただし、認証ホストを独立したアドレス指定可能な認証仮想サーバーを指す場合、バインドされた認証ポリシーが有効になります。

NetScaler ADC AAA TMセッションのセッションポリシーをどのように構成しますか?

Unified Gateway で、NetScaler ADC AAA TM仮想サーバーに認証仮想サーバーが指定されていない場合、NetScaler ADC AAA TMセッションはNetScaler Gatewayセッションポリシーを継承します。認証仮想サーバーが指定されている場合、その仮想サーバーにバインドされたNetScaler ADC AAA TMセッションポリシーが適用されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler ADC 11.0のNetScaler Gatewayポータルの変更点は何ですか?

11.0より前のNetScaler ADCリリースでは、グローバルレベルで単一のポータルのカスタマイズを設定できます。特定のNetScaler ADCアプライアンス内のすべてのゲートウェイ仮想サーバーは、グローバルポータルのカスタマイズを使用します。

NetScaler ADC 11.0では、ポータル・テーマ機能を使用して、複数のポータル・テーマを設定できます。テーマはグローバルにバインドすることも、特定の仮想サーバーにバインドすることもできます。

NetScaler ADC 11.0はNetScaler Gatewayポータルのカスタマイズをサポートしていますか

構成ユーティリティーを使用して、新しいポータル・テーマ機能を使用して、ポータル・テーマを完全にカスタマイズおよび作成できます。さまざまな画像をアップロードしたり、配色を設定したり、テキストラベルを変更したりすることができます。

カスタマイズ可能なポータルページは次のとおりです。

- ログインページ
- エンドポイント分析ページ
- エンドポイント分析エラーページ
- ポストエンドポイント分析ページ
- VPN 接続ページ
- ポータルのホームページ

このリリースでは、独自のポータル設計でNetScaler Gateway 仮想サーバーをカスタマイズできます。

ポータル・テーマは、NetScaler ADCの高可用性またはクラスター展開でサポートされていますか?

はい。ポータルのテーマは、NetScaler ADCの高可用性およびクラスター展開でサポートされています。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

カスタマイズは、NetScaler ADC 11.0アップグレードプロセスの一環として移行されますか?

なしrc.conf/rc.netscalerファイルの変更または10.1/10.5のカスタムテーマ機能を使用して呼び出されたNetScaler Gateway ポータルページに対する既存のカスタマイズは、NetScaler ADC 11.0へのアップグレード時に自動的に移行されません。

NetScaler ADC 11.0のポータルテーマの準備をするために従うべきアップグレード前の手順はありますか

既存のカスタマイズは、rc.conf ファイルまたは rc.netscaler ファイルから削除する必要があります。

もう 1 つのオプションは、カスタムテーマを使用する場合は、 設定を割り当てる必要があることです：

1. ［ **構成］>［NetScaler Gateway］>［グローバル設定］**に移動します
2. をクリックします。
3. をクリックし、 リストから を選択します。

rc.confまたはrc.netscalerによって呼び出されるNetScaler ADCインスタンスに保存されているカスタマイズがあります。ポータル・テーマに移動するにはどうすればよいですか

Citrix ナレッジセンターの記事CTX126206には 、10.0ビルド73.5001.eまでのNetScaler ADC 9.3および10.0リリースのこのような構成について詳しく説明しています。NetScaler ADC 10.0ビルド10.0 73.5002.e（10.1および10.5を含む）以降、UITHEME CUSTOMパラメータを使用して、再起動後もカスタマイズを保持できるようになりました。カスタマイズがNetScaler ADCハードドライブに保存されており、これらのカスタマイズを引き続き使用する場合は、11.0 GUIファイルをバックアップし、既存のカスタムテーマファイルに挿入します。 **ポータルのテーマに移動する場合は、まず の または で UITHEME パラメーターの設定を解除する必要があります。**または、DEFAULT または GREENBUBBBLE に設定することもできます。その後、ポータル・テーマの作成とバインドを開始できます。

NetScaler ADC 11.0にアップグレードする前に、現在のカスタマイズをエクスポートして保存するにはどうすればよいですか? エクスポートしたファイルを別のNetScaler ADCアプライアンスに移動できますか?

ns_gui_custom フォルダにアップロードされたカスタマイズファイルは、ディスク上に保存され、アップグレード後も保持されます。ただし、これらのファイルは、新しいNetScaler ADC 11.0カーネルおよびカーネルの一部である他のGUIファイルと完全に互換性があるとは限りません。し

© 1997–2026 Citrix Systems, Inc. All rights reserved.

たがって、11.0のGUIファイルをバックアップし、バックアップをカスタマイズすることをお勧めします。

さらに、構成ユーティリティには、 **ns_custom_guiフォルダーを別のCitrix** ADCアプライアンスにエクスポートするユーティリティはありません。SSHまたはWinSCPなどのファイル転送ユーティリティを使用して、NetScaler ADCインスタンスからファイルを削除します。

ポータル・テーマは、NetScaler ADC AAA TM 仮想サーバーでサポートされていますか

はい。ポータル・テーマは、NetScaler ADC AAA TM 仮想サーバーでサポートされています。

NetScaler Gateway 11.0のRDPプロキシ機能の変更点は何ですか?

NetScaler ADC 10.5.e拡張リリース以降、RDPプロキシに多くの機能強化が加えられました。NetScaler ADC 11.0では、この機能は最初にリリースされたビルドから利用できます。

ライセンスの変更

NetScaler ADC 11.0のRDPプロキシ機能は、プレミアムエディションとアドバンスドエディションでのみ使用できます。Citrix 同時ユーザー（CCU）ライセンスは、ユーザーごとに取得する必要があります。

コマンドを有効にする

NetScaler ADC 10.5.eでは、RDPプロキシを有効にするコマンドはありませんでした。NetScaler ADC 11.0では、有効コマンドが追加されました：

```
enable feature rdpproxy
```

このコマンドを実行するには、機能のライセンスが必要です。

RDP プロキシのその他の変更

サーバプロファイルの事前共有キー（PSK）属性が必須になりました。

RDPプロキシ用の既存のNetScaler ADC 10.5.e構成をNetScaler ADC 11.0に移行するには、次の詳細を理解し、対処する必要があります。

管理者が既存の RDP プロキシ構成を選択した Unified Gateway 展開に追加する場合は、次の手順を実行します：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- NetScaler Gateway 仮想サーバーのIPアドレスを編集し、アドレス指定できないIPアドレス（0.0.0.0）に設定する必要があります。
- SSL/TLSサーバー証明書、認証ポリシーは、選択したUnified Gatewayフォーメーションの一部であるNetScaler Gateway 仮想サーバーにバインドする必要があります。

NetScaler ADC 10.5.eに基づくリモートデスクトッププロトコル（RDP）プロキシ構成をNetScaler ADC 11.0にどのように移行しますか

オプション1：プレミアムライセンスまたはアドバンスドライセンスを使用して、RDPプロキシ構成の既存のNetScaler Gateway 仮想サーバーをそのまま維持します。

オプション2：RDPプロキシ構成で既存のNetScaler Gateway 仮想サーバーを移動し、Unified Gateway 仮想サーバーの背後に配置します。

オプション3：RDPプロキシ構成を持つスタンドアロンのNetScaler Gateway 仮想サーバーを既存のStandard Editionアプライアンスに追加します。

NetScaler ADC 11.0リリースを使用して、RDPプロキシ構成用にNetScaler Gateway をどのようにセットアップしますか

NS 11.0 リリースを使用して RDP プロキシを展開するには、次の 2 つのオプションがあります：

1. 外部に面したNetScaler Gateway 仮想サーバーを使用する。これには、NetScaler Gateway 仮想サーバーに対して外部から見えるIPアドレス/FQDNが1つ必要です。このオプションは、NetScaler ADC 10.5.eで利用可能なものです。
2. Unified Gateway 仮想サーバーを使用して、NetScaler Gateway 仮想サーバーをフロントエンドにします。

オプション2では、NetScaler Gateway 仮想サーバーはアドレス指定不可能なIPアドレス（0.0.0.0）を使用するため、独自のIPアドレス/FQDNを必要としません。

HDX Insight はUnified Gateway と互換性がありますか

NetScaler GatewayをUnified Gateway で展開する場合は、次の条件を満たす必要があります。

- NetScaler Gateway 仮想サーバーには、有効なSSL証明書がバインドされている必要があります。
- HDX Insightのレポートを作成するために、NetScaler ADM でAppFlowレコードを生成するには、NetScaler Gateway仮想サーバーが稼働状態になっている必要があります。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

既存のHDX Insight構成を移行するにはどうすればよいですか

移行は必要ありません。NetScaler Gateway 仮想サーバーがUnified Gateway ゲートウェイ仮想サーバーの背後に配置されている場合、NetScaler Gateway 仮想サーバーにバインドされたAppFlowポリシーが引き継がれます。

NetScaler Gateway仮想サーバーのNetScaler ADM 上の既存のデータについては、次の2つの可能性があります：

- NetScaler Gateway 仮想サーバーのIPアドレスがUnified Gatewayへの移行の一環としてUnified Gateway 仮想サーバーに割り当てられている場合、データはCitrix Unified Gateway ateway 仮想サーバーにリンクされたままになります
- Unified Gateway 仮想サーバーに別のIPアドレスが割り当てられている場合、NetScaler Gateway 仮想サーバーからのAppFlowデータはその新しいIPアドレスにリンクされます。したがって、既存のデータは新しいデータの一部ではありません。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler Gateway アプライアンスでのVPN構成

重要:

このセクションのスクリーンキャプチャは、次の理由によりグレースケールスキームで維持されます。

- 視覚障害のある読者、特に色覚障害や色覚障害のある読者を支援します。
- グレースケールイメージの使用は、ユーザーのブラウザやオペレーティングシステムで行われた可能性のあるカラーコーディングのカスタマイズの影響を示さない一般的な形式でイメージを表します。

ユーザーは、次の方法を使用して、NetScaler Gateway を介して組織のネットワークリソースに接続できます。

- ユーザーデバイスにインストールされているすべてのCitrixプラグインを含むCitrix Workspaceアプリ。
- Webブラウザーを使用してアプリケーション、デスクトップ、およびShareFileにユーザーが接続できるようにするWeb向けCitrix Workspace アプリ。
- Secure Hub: ユーザーがiOSおよびAndroidデバイスからSecure Mail、WorxWeb、およびモバイルアプリケーションにアクセスできるようにします。
- Windows、macOS X、またはLinux用のNetScaler Gatewayプラグイン。
- iOSおよびAndroid向けのNetScaler Gatewayアプリ。
- Java向けNetScaler Gateway プラグイン。
- クライアントレスアクセス。ユーザソフトウェアをインストールしなくても、ユーザに必要なアクセス権をユーザに提供します。
- Citrix SD-WAN プラグインとの相互運用性。

ユーザーがNetScaler Gatewayプラグインをインストールしてから、Windows Server 2008用のCitrix Virtual Apps 6.5（機能パックおよび機能パック2を含む）、Citrix 仮想デスクトップ7.0以降からCitrix Workspaceアプリをインストールすると、Citrix Workspace アプリは自動的にNetScaler

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Gatewayプラグインを追加します。ユーザーは、WebブラウザーまたはCitrix WorkspaceアプリからNetScaler Gateway プラグインに接続できます。

SmartAccess は、エンドポイント分析スキャンの結果に基づいて、ユーザーデバイスに許可されるアクセス方法を自動的に決定します。スマートアクセスの詳細については、「SmartAccess 構成」を参照してください。

NetScaler Gateway は、iOSおよびAndroidモバイルデバイス向けのCitrix Endpoint Management業務用モバイルアプリをサポートしています。NetScaler Gateway には、マイクロVPNトンネルを確立するiOSモバイルデバイスからNetScaler Gateway に接続できるSecure Browse が含まれています。Secure Hubに接続するAndroidデバイスは、マイクロVPNトンネルを自動的に確立し、内部ネットワークのリソースへのWebおよびモバイルアプリケーションレベルの安全なアクセスを提供します。 ユーザーが業務用モバイルアプリを搭載したAndroidデバイスから接続する場合は、NetScaler Gateway でDNS設定を構成する必要があります。詳細については、「Android デバイスの DNS サフィックスを使用した DNS クエリのサポート」を参照してください。

ユーザーがNetScaler Gateway プラグインを使用して接続する方法

NetScaler Gateway は以下のように動作する：

- ユーザーがVPNトンネルを介してネットワークリソースにアクセスしようとすると、NetScaler Gateway プラグインは組織の内部ネットワーク宛てのすべてのネットワークトラフィックを暗号化し、パケットをNetScaler Gateway に転送します。
- NetScaler Gateway は、SSLトンネルを終了し、プライベートネットワーク宛ての着信トラフィックを受け入れ、そのトラフィックをプライベートネットワークに転送します。NetScaler Gateway は、セキュリティで保護されたトンネルを介してリモートコンピューターにトラフィックを戻します。

ユーザーが Web アドレスを入力すると、ログオンページが表示され、そこで資格情報を入力してログオンします。資格情報が正しい場合、NetScaler Gateway はユーザーデバイスとのハンドシェイクを終了します。

ユーザーとAccess Gatewayの間にプロキシサーバーがある場合は、プロキシサーバーと認証のための資格情報を指定できます。詳細については、「ユーザー接続のプロキシサポートの有効化」を参照してください。

NetScaler Gateway プラグインがユーザーデバイスにインストールされます。最初の接続後、ユーザーが Windows ベースのコンピューターを使用してログオンした場合、通知領域のアイコンを使用して接続を確立できます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

セキュアトンネルの確立

ユーザーがNetScaler Gateway プラグイン、Secure Hub、またはCitrix Workspace アプリで接続すると、クライアントソフトウェアはポート443（またはNetScaler Gateway の構成済みポート）を介して安全なトンネルを確立し、認証情報を送信します。トンネルが確立されると、NetScaler Gateway は、NetScaler Gateway プラグイン、Secure Hub、またはCitrix Workspace アプリに構成情報を送信します。アドレスプールを有効にすると、セキュリティで保護されるネットワークを記述し、IPアドレスを含みます。

セキュアな接続を介してプライベートネットワークトラフィックをトンネルする

NetScaler Gateway プラグインが起動し、ユーザーが認証されると、指定されたプライベートネットワークを宛先とするすべてのネットワークトラフィックがキャプチャされ、安全なトンネルを介してNetScaler Gateway にリダイレクトされます。Citrix Workspace アプリは、NetScaler Gateway プラグインをサポートして、ユーザーのログオン時に安全なトンネルを介して接続を確立する必要があります。

Secure Hub、Secure Mail、WorxWebは、マイクロVPNを使用して、iOSおよびAndroidモバイルデバイス用のセキュアなトンネルを確立します。

NetScaler Gatewayは、ユーザーデバイスが確立するすべてのネットワーク接続をインターセプトし、SSL（Secure Sockets Layer）を介してNetScaler Gatewaysに多重化します。NetScaler Gatewayでは、トラフィックが逆多重化され、接続が正しいホストとポートの組み合わせに転送されます。

接続は、単一のアプリケーション、アプリケーションのサブセット、またはイントラネット全体に適用される管理セキュリティポリシーの対象となります。リモートユーザが VPN 接続を介してアクセスできるリソース（IP アドレス/サブネットペアの範囲）を指定します。

NetScaler Gateway プラグインは、定義されたイントラネットアプリケーションの次のプロトコルをインターセプトしてトンネリングします。

- TCP (すべてのポート)
- UDP (すべてのポート)
- ICMP（タイプ 8 および 0-エコー要求/応答）

ユーザーデバイス上のローカルアプリケーションからの接続は、NetScaler Gateway に安全にトンネリングされ、NetScaler Gateway はターゲットサーバーへの接続を再確立します。ターゲットサーバーは、プライベートネットワーク上のローカルNetScaler Gateway からの接続として認識し、ユーザーデバイスを隠します。これは、リバースネットワークアドレス変換 (NAT) とも呼ばれます。IP アドレスを非表示にすると、送信元の場所にセキュリティが追加されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ローカルでは、ユーザーデバイス上で、SYN-ACK、PUSH、ACK、FINパケットなどの接続関連トラフィックはすべて、NetScaler Gateway プラグインによって再作成され、プライベートサーバーから表示されます。

ファイアウォールとプロキシ経由で接続する

NetScaler Gateway プラグインのユーザーは、次の図に示すように、別の組織のファイアウォール内に配置されることがあります：



NATファイアウォールは、NetScaler Gateway からユーザーデバイスに安全なパケットをルーティングできるようにするテーブルを保持します。回線指向接続の場合、NetScaler Gateway はポートマップされたリバースNAT変換テーブルを保持します。リバースNAT変換テーブルを使用すると、NetScaler Gateway は接続を照合し、正しいポート番号を持つユーザーデバイスにパケットをトンネル経由で送信し、パケットが正しいアプリケーションに返されるようにします。

NetScaler Gateway プラグインのアップグレードを制御する

システム管理者は、NetScaler ADCプラグインのバージョンがNetScaler Gateway リビジョンと一致しない場合のNetScaler ADCプラグインの実行方法を制御します。新しいオプションは、Mac、Windows、またはオペレーティングシステムのプラグインのアップグレード動作を制御します。

VPNプラグインの場合、NetScaler ADCアプライアンスのユーザーインターフェイスの2つの場所でアップグレードオプションを設定できます。

- グローバル設定で
- セッションプロファイルレベル

要件

- Windows EPA および VPN プラグインのバージョンは 11.0.0.0 より大きくなければなりません
- Mac EPA プラグインのバージョンは 3.0.0.31 より大きくなければなりません
- Mac VPN プラグインのバージョンは 3.1.4 (357) より大きくなければなりません

注：

NetScaler ADCアプライアンスを11.0リリースにアップグレードすると、アップグレード制御構成に関係なく、以前のすべてのVPN（およびEPA）プラグインが最新バージョンにアップグレードされます。以降のアップグレードでは、以前のアップグレード制御設定が尊重されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

プラグインビヘイビア

NetScaler Gateway では、クライアントの種類ごとに、次の3つのオプションを使用してプラグインのアップグレード動作を制御できます：

- **いつも**

エンドユーザーのプラグインのバージョンがNetScaler ADCアプライアンスに同梱されているプラグインと一致しない場合、プラグインは常にアップグレードされます。これはデフォルトの動作です。エンタープライズで複数のプラグインバージョンを実行したくない場合は、このオプションを選択します。

- **必須** (およびセキュリティ)

プラグインは、必要であると判断された場合にのみアップグレードされます。アップグレードは、次の 2 つの状況で必要であるとみなされます。

- インストールされているプラグインは、現在のNetScaler ADCアプライアンスのバージョンと互換性がありません。
- インストールされているプラグインは、必要なセキュリティ修正のために更新する必要があります。

プラグインのアップグレード回数を最小限にしたいが、プラグインのセキュリティアップデートを見逃したくない場合は、このオプションを選択します。

- **決して**

プラグインはアップグレードされません。

VPN プラグインのアップグレードを制御するための CLI パラメータ

NetScaler Gateway は、WindowsおよびMacオペレーティングシステム用の2種類のプラグイン（EPAおよびVPN）をサポートしています。セッションレベルでVPNプラグインのアップグレード制御をサポートするために、NetScaler Gateway はwindowsInPluginUpgradeとmacPluginUpgradeという名前の2つのセッションプロファイルパラメーターをサポートしています。

これらのパラメータは、グローバル、仮想サーバ、グループ、およびユーザレベルで使用できます。各パラメータには、、、または の値を指定できます。これらのパラメータの詳細については、「 プラグインビヘイビア」を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

EPA プラグインのアップグレードを制御するための CLI パラメータ

NetScaler Gateway は、WindowsおよびMacオペレーティングシステム用のEPAプラグインをサポートしています。仮想サーバーレベルでEPAプラグインのアップグレード制御をサポートするために、NetScaler Gateway は windowsEpaPluginUpgrade および macePAPluginUpgrade という名前の2つの仮想サーバーパラメーターをサポートしています。

パラメータは、仮想サーバレベルで使用できます。各パラメータには、、、または の値を指定できます。これらのパラメータの詳細については、「 プラグインビヘイビア」を参照してください

VPN 構成

Windows、Linux、および Mac プラグインの **VPN 構成については** 、以下の手順に従ってください。

1. > > に移動します。**
2. 目的のセッションポリシーを選択し、 をクリックします。
3. タブを選択します。
4. これらのダイアログボックスのオプションは、アップグレードの動作に影響します。

   - いつも
   - エッセンシャル
   - 決して

   デフォルトは です。
5. 各オプションの右側にあるチェックボックスをオンにします。アップグレード動作を適用する頻度を選択します。

EPA 構成

Windows、Linux、および Apple プラグインの EPA 構成については、以下の手順に従ってください。

1. **［NetScaler Gateway］>［仮想サーバー］**に移動します。
2. サーバを選択し、 ボタンをクリックします。
3. **鉛筆アイコンをクリックします** 。
4. をクリックします

© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. 表示されるダイアログボックスは、アップグレードの動作に影響します。以下の種類から選択できます。

   - いつも
   - エッセンシャル
   - 決して

NetScaler Gatewayでの完全VPNのセットアップ

このセクションでは、NetScaler Gateway アプライアンスで完全VPNセットアップを構成する方法について説明します。ネットワークに関する考慮事項と、ネットワーキングの観点から問題を解決するための理想的なアプローチが含まれています。

前提条件

- SSL 証明書をインストールし、VPN 仮想サーバーにバインドします。
  - CTX109260- NetScalerアプライアンスでパブリックSSL証明書を生成してインストールする方法
  - CTX122521- NetScalerアプライアンスのデフォルト証明書を、アプライアンスのホスト名と一致する信頼できるCA証明書に置き換える方法
  - Citrix ドキュメント- SSLベースの仮想サーバーへの証明書とキーのペアのバインド
- NetScaler Gateway の認証プロファイルを作成します。
  - 詳しくは、Citrix のドキュメント- 外部ユーザー認証の構成を参照してください。
  - 詳細については、「チェックリスト: AD FS を使用してシングルサインオンを実装および管理する」を参照してください。
- Citrix VPN クライアントをダウンロードします。
- 完全な VPN 接続を許可するセッションポリシーを作成します。

ユーザーがNetScaler Gateway プラグイン、Secure Hub、またはCitrix Workspace アプリで接続すると、クライアントソフトウェアはポート443（またはNetScaler Gateway の構成済みポート）を介して安全なトンネルを確立し、認証情報を送信します。トンネルが確立されると、NetScaler Gateway は、NetScaler Gateway プラグイン、Citrix Secure Hub、またはCitrix Workspace アプリに、セキュリティで保護されるネットワークを記述する構成情報を送信します。イントラネット IP を有効にすると、この情報には IP アドレスも含まれます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ユーザーデバイス接続を構成するには、内部ネットワークでユーザーがアクセスできるリソースを定義します。ユーザーデバイス接続の設定には、次の作業が含まれます。

- 分割トンネリング
- アドレスプール (イントラネット IP) を含むユーザーの IP アドレス
- プロキシサーバーを介した接続
- ユーザーがアクセスを許可されるドメインの定義
- タイムアウト設定
- シングルサインオン
- NetScaler Gateway を介して接続するユーザーソフトウェア
- モバイルデバイスへのアクセス

ほとんどのユーザーデバイス接続は、セッションポリシーの一部であるプロファイルを使用して構成します。また、認証ごとのポリシー、トラフィックポリシー、および認可ポリシーを使用して、ユーザーデバイスの接続設定を定義することもできます。また、イントラネットアプリケーションを使用して構成することもできます。

NetScaler Gateway アプライアンスで完全VPNセットアップを構成する

NetScaler Gateway アプライアンスでVPNセットアップを構成するには、次の手順を実行します。

1. > に移動します。
2. 次のスクリーンショットに示すように、 ノードを選択します。DNS ネームサーバーが一覧表示されていることを確認します。使用できない場合は、DNS ネームサーバーを追加します。

3. **NetScaler Gateway >［ポリシー］**を展開
4. ノードを選択します。
5. ［NetScaler Gateway セッションポリシーとプロファイル］ページで、［ **プロファイル** ］タブをクリックし、［ **追加**］をクリックします。 ［NetScaler Gateway セッションプロファイルの構成］ダイアログボックスで構成する各コンポーネントについて、それぞれのコンポーネントの［ **グローバルを上書き** ］オプションを選択します。
6. タブをクリックします。
7. ユーザが VPN にログインするときに任意の URL を表示する場合は、 フィールドにイントラネットポータルの URL を入力します。ホームページパラメータが「nohomepage.html」に設定されている場合、ホームページは表示されません。プラグインが起動すると、ブラウザインスタンスが起動し、自動的に強制終了されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

8. リストから目的の設定を選択します。
9. FullVPN を使用する場合は、 リストから を選択します。
10. リストから が選択されていることを確認します。
11. 必要に応じて、「 **Web アプリケーションへのシングルサインオン** 」オプションを選択します。
12. 次のスクリーンショットに示すように、必要に応じて オプションが選択されていることを確認します。

13. **［セキュリティ］** タブをクリックします。
14. **「**デフォルト認証アクション」リストから「許可」**が選択されていることを確認します。**

15. **［Published Applications］** タブをクリックします。
16. ［ **公開アプリケーション** ］オプションの［ **ICAプロキシ** ］リストで［ **OFF** ］が選択されていることを確認します。

17. **［Create］** をクリックします。
18. **［閉じる］** をクリックします。
19. **仮想サーバーの［NetScaler Gateway セッションポリシーとプロファイル］ページの［ポリシー］タブをクリックするか、必要に応じてグループ/ユーザーレベルでセッションポリシーを有効にします。**
20. 次のスクリーンショットに示すように、必須の式または true を使用してセッションポリシーを作成します。

21. セッションポリシーを VPN 仮想サーバーにバインドします。詳細については、「 バインドセッションポリシー」を参照してください。

    分割トンネルが ON に設定されている場合は、VPN に接続したときにユーザがアクセスするイントラネットアプリケーションを設定する必要があります。イントラネットアプリケーションについて詳しくは、「 Citrix Secure Accessクライアントのイントラネットアプリケーションの構成」を参照してください。

    a. **［NetScaler Gateway］>［リソース］>［イントラネットアプリケーション］** に移動します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

b. イントラネットアプリケーションを作成します。Windows クライアントを使用した FullVPN の場合は、 を選択します。許可するプロトコル (TCP、UDP、または ANY)、宛先タイプ (IP アドレスとマスク、IP アドレス範囲、またはホスト名) を選択します。



c. 必要に応じて、次の式を使用して iOS と Android の VPN の新しいポリシーを設定します。

```
HTTP.REQ.HEADER("User-Agent").CONTAINS("CitrixVPN")&&HTTP.REQ.HEADER("User-Agent").CONTAINS("NSGiOSplugin")&&HTTP.REQ.HEADER("User-Agent").CONTAINS("Android")
```

d. 必要に応じて、ユーザー/グループ/VSERVER レベルで作成されたイントラネットアプリケーションをバインドします。

その他のパラメーター

以下に、設定可能なパラメータの一部と、それぞれの簡単な説明を示します。



分割トンネルオフ

分割トンネルがオフに設定されている場合、NetScaler Gateway プラグインはユーザーデバイスから発信されるすべてのネットワークトラフィックをキャプチャし、VPNトンネルを介して NetScaler Gateway にトラフィックを送信します。つまり、VPNクライアントは、クライアントPCからNetScaler Gateway VIPを指すデフォルトルートを確立します。つまり、宛先に到達するには、すべてのトラフィックをトンネル経由で送信する必要があります。すべてのトラフィックがトンネルを介して送信されるため、許可ポリシーは、トラフィックが内部ネットワークリソースへの通過を許可されるか、拒否されるかを決定する必要があります。

「オフ」に設定すると、Web サイトへの標準 Web トラフィックを含むすべてのトラフィックがトンネルを通過します。このWebトラフィックを監視および制御することが目的の場合は、NetScaler ADCアプライアンスを使用してこれらの要求を外部プロキシに転送する必要があります。ユーザーデバイスは、プロキシサーバーを介して接続し、内部ネットワークにアクセスすることもできます。

NetScaler Gateway は、HTTP、SSL、FTP、およびSOCKSプロトコルをサポートしています。ユーザー接続のプロキシサポートを有効にするには、NetScaler Gateway でこれらの設定を指定する必要があります。NetScaler Gateway 上のプロキシサーバーで使用されるIPアドレスとポートを指定できます。プロキシサーバーは、内部ネットワークへのその後のすべての接続のフォワードプロキシとして使用されます。

詳細については、「 ユーザー接続のプロキシサポートの有効化」を参照してください

© 1997–2026 Citrix Systems, Inc. All rights reserved.

分割トンネル ON

分割トンネリングを有効にして、NetScaler Gateway プラグインがNetScaler Gateway に不要なネットワークトラフィックを送信しないようにすることができます。分割トンネルが有効な場合、NetScaler Gateway プラグインは、NetScaler Gateway によって保護されたネットワーク（イントラネットアプリケーション）宛てのトラフィックのみをVPNトンネル経由で送信します。NetScaler Gateway プラグインは、保護されていないネットワークを宛先とするネットワークトラフィックをNetScaler Gateway に送信しません。NetScaler Gateway プラグインが起動すると、NetScaler Gateway からイントラネットアプリケーションの一覧を取得し、クライアントPCのイントラネットアプリケーションタブで定義されている各サブネットのルートを確立します。NetScaler Gateway プラグインは、ユーザーデバイスから送信されるすべてのパケットを調べ、パケット内のアドレスをイントラネットアプリケーションのリスト（VPN接続の開始時に作成されたルーティングテーブル）と比較します。パケット内の宛先アドレスがイントラネットアプリケーションの1つ内にある場合、NetScaler Gateway プラグインはVPNトンネルを介してNetScaler Gateway にパケットを送信します。宛先アドレスが定義済みのイントラネットアプリケーションにない場合、パケットは暗号化されず、ユーザーデバイスはクライアント PC で最初に定義された既定のルーティングを使用してパケットを適切にルーティングします。分割トンネリングを有効にすると、イントラネットアプリケーションは、インターセプトされ、トンネルを介して送信されるネットワークトラフィックを定義します。

リバース分割トンネル

NetScaler Gateway は、NetScaler Gateway が傍受しないネットワークトラフィックを定義するリバース分割トンネリングもサポートしています。分割トンネリングをリバースに設定すると、イントラネットアプリケーションは、NetScaler Gateway が傍受しないネットワークトラフィックを定義します。リバース分割トンネリングを有効にすると、内部IPアドレスに向けられたすべてのネットワークトラフィックはVPNトンネルをバイパスし、他のトラフィックはNetScaler Gatewayを経由します。リバース分割トンネリングを使用して、すべての非ローカル LAN トラフィックをログに記録できます。たとえば、ユーザーがホームワイヤレスネットワークを持ち、NetScaler Gateway プラグインを使用してログオンしている場合、NetScaler Gateway は、ワイヤレスネットワーク内のプリンターまたは別のデバイス宛てのネットワークトラフィックを傍受しません。

分割トンネリングの設定

1. ［**構成**］>［**Citrix Gateway**］>［**ポリシー**］>［**セッション**］に移動します。
2. 詳細ペインの タブで、プロファイルを選択し、 をクリックします。
3. ［**クライアントエクスペリエンス**］タブで、［**分割トンネル**］の横にある［**グローバルオーバーライド**］を選択し、オプションを選択して［**OK］**をクリックします。

   分割トンネリングおよび認可の設定

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler Gateway の展開を計画するときは、分割トンネリングと、デフォルトの承認アクションと承認ポリシーを考慮することが重要です。

たとえば、ネットワークリソースへのアクセスを許可する認可ポリシーがあるとします。分割トンネリングがオンに設定されており、NetScaler Gateway 経由でネットワークトラフィックを送信するようにイントラネットアプリケーションを構成していない。NetScaler Gateway にこの種類の構成がある場合、リソースへのアクセスは許可されますが、ユーザーはリソースにアクセスできません。



承認ポリシーがネットワークリソースへのアクセスを拒否した場合、NetScaler Gateway プラグインはトラフィックをNetScaler Gateway に送信しますが、次の条件でリソースへのアクセスは拒否されます。

- 分割トンネリングが ON に設定されている。
- イントラネットアプリケーションは、ネットワークトラフィックをNetScaler Gateway 経由でルーティングするように構成されている

承認ポリシーの詳細については、以下を参照してください：

- 認可の設定
- 承認ポリシーの構成
- デフォルトのグローバル認証の設定

内部ネットワークリソースへのネットワークアクセスを構成するには

1. **構成** > **NetScaler Gateway > リソース > イントラネットアプリケーション**の順に移動します。
2. 詳細ペインで、 をクリックします。
3. ネットワークアクセスを許可するためのパラメータを入力し、、 の順にクリックします。

VPNユーザーのイントラネットIPを設定しない場合、ユーザーはトラフィックをNetScaler Gateway VIPに送信し、そこからNetScaler ADCアプライアンスは内部LAN上のイントラネットアプリケーションリソースに新しいパケットを作成します。この新しいパケットは、SNIP からイントラネットアプリケーションに向けて発信されます。ここから、イントラネットアプリケーションはパケットを取得して処理し、そのパケットの送信元（この場合は SNIP）への応答を試みます。SNIP はパケットを取得し、要求を行ったクライアントに応答を送信します。

イントラネットIPアドレスが使用されると、ユーザーはトラフィックをNetScaler Gateway VIPに送信し、そこからNetScaler ADCアプライアンスはクライアントIPをプールの構成されたイントラ

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ネットIPの1つにマップします。NetScaler ADCアプライアンスはイントラネットIPプールを所有することになるため、これらの範囲を内部ネットワークで使用しないでください。NetScaler ADCアプライアンスは、DHCPサーバーが行うように、着信VPN接続にイントラネットIPを割り当てます。NetScaler ADCアプライアンスは、ユーザーがアクセスするLAN上のイントラネットアプリケーションへの新しいパケットを構築します。この新しいパケットは、イントラネット IP の 1 つからイントラネットアプリケーションに向けて発信されます。ここから、イントラネットアプリケーションはパケットを取得して処理し、そのパケットの送信元（イントラネット IP）への応答を試みます。この場合、応答パケットは、イントラネットIPが配置されているNetScaler ADCアプライアンスにルーティングする必要があります（NetScaler ADCアプライアンスはイントラネットIPサブネットを所有しています）。このタスクを実行するには、ネットワーク管理者が SNIP のいずれかを指すイントラネット IP へのルートを持っている必要があります。非対称トラフィックを回避するために、パケットがNetScaler ADCアプライアンスを最初に送信するルートを保持するSNIPにトラフィックをポイントバックすることをお勧めします。

分割トンネリングオプション

次に、さまざまな分割トンネリングオプションを示します。



分割トンネルオフ

分割トンネルがオフに設定されている場合、Citrix Secure Accessクライアントはユーザーデバイスから送信されるすべてのネットワークトラフィックをキャプチャし、そのトラフィックをVPNトンネルを介してNetScaler Gatewayに送信します。つまり、VPNクライアントは、クライアントPCからNetScaler Gateway VIPを指すデフォルトルートを確立します。つまり、宛先に到達するには、すべてのトラフィックをトンネル経由で送信する必要があります。すべてのトラフィックがトンネルを介して送信されるため、許可ポリシーは、トラフィックが内部ネットワークリソースへの通過を許可されるか、拒否されるかを決定する必要があります。

「オフ」に設定すると、Web サイトへの標準 Web トラフィックを含むすべてのトラフィックがトンネルを通過します。このWebトラフィックを監視および制御することが目的の場合は、NetScaler Gateway アプライアンスを使用してこれらの要求を外部プロキシに転送する必要があります。ユーザーデバイスは、プロキシサーバーを介して接続し、内部ネットワークにアクセスすることもできます。

NetScaler Gateway は、HTTP、SSL、FTP、およびSOCKSプロトコルをサポートしています。ユーザー接続のプロキシサポートを有効にするには、NetScaler Gateway でこれらの設定を指定する必要があります。NetScaler Gateway 上のプロキシサーバーで使用されるIPアドレスとポート

© 1997–2026 Citrix Systems, Inc. All rights reserved.

を指定できます。プロキシサーバーは、内部ネットワークへのその後のすべての接続のフォワードプロキシとして使用されます。

詳細については、次のリンクを参照してください。

- ユーザー接続のプロキシサポートの有効化

分割トンネル ON

分割トンネリングを有効にして、Citrix Secure AccessクライアントがNetScaler Gateway に不要なネットワークトラフィックを送信しないようにすることができます。分割トンネルが有効になっている場合、Citrix Secure Accessクライアントは、NetScaler Gatewayによって保護されているネットワーク（イントラネットアプリケーション）宛てのトラフィックのみをVPNトンネル経由で送信します。Citrix Secure Accessクライアントは、保護されていないネットワーク宛てのネットワークトラフィックをNetScaler Gatewayに送信しません。Citrix Secure Accessクライアントが起動すると、NetScaler Gateway からイントラネットアプリケーションのリストを取得し、クライアントPCのイントラネットアプリケーションタブで定義された各サブネットのルートを確立します。Citrix Secure Accessクライアントは、ユーザーデバイスから送信されたすべてのパケットを調べ、パケット内のアドレスをイントラネットアプリケーションのリスト（VPN接続の開始時に作成されたルーティングテーブル）と比較します。パケットの宛先アドレスがイントラネットアプリケーションの1つ内にある場合、Citrix Secure AccessクライアントはVPNトンネルを介してNetScaler Gatewayにパケットを送信します。宛先アドレスが定義済みのイントラネットアプリケーションにない場合、パケットは暗号化されず、ユーザーデバイスはクライアント PC で最初に定義された既定のルーティングを使用してパケットを適切にルーティングします。分割トンネリングを有効にすると、イントラネットアプリケーションは、インターセプトされ、トンネルを介して送信されるネットワークトラフィックを定義します。

リバース分割トンネル

NetScaler Gateway は、NetScaler Gateway が傍受しないネットワークトラフィックを定義するリバース分割トンネリングもサポートしています。分割トンネリングをリバースに設定すると、イントラネットアプリケーションは、NetScaler Gateway が傍受しないネットワークトラフィックを定義します。リバース分割トンネリングを有効にすると、内部IPアドレスに向けられたすべてのネットワークトラフィックはVPNトンネルをバイパスし、他のトラフィックはNetScaler Gatewayを経由します。リバース分割トンネリングを使用して、すべての非ローカル LAN トラフィックをログに記録できます。たとえば、ユーザーが自宅のワイヤレスネットワークを使用してCitrix Secure Accessクライアントでログオンしている場合、NetScaler Gateway はワイヤレスネットワーク内のプリンターまたは別のデバイス宛のネットワークトラフィックを傍受しません。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注：

Windows向けCitrix Secure Accessクライアントは、Citrix Secure Accessバージョン22.6.1.5以降のFQDNベースのリバース分割トンネルもサポートしています。

注意事項

IP ベースのリバース分割トンネリング:

- IP アドレスベースのルールの数は 1024 に制限されています。
- DNE ドライバーと WFP ドライバーの両方でサポートされています。

ホスト名ベースのリバース分割トンネリング:

- VPN セッション中にアクセスできるホスト名の数は、FQDN スプーフィング範囲で指定された使用可能な IP アドレスの数によって制限されます。これは、すべてのホスト名が FQDN スプーフィング範囲から 1 つの IP アドレスを占めるためです。IP 範囲がなくなると、最後に割り当てられた IP アドレスが次の新しいホスト名に再利用されます。
- DNS サフィックスを設定する必要があります。

注：

Windows クライアントの場合、ホスト名ベースのリバース分割トンネリングは WFP ドライバーでのみサポートされます。WFP ドライバモードを有効にし、レジストリ値として「EnableWFP」を設定します。詳しくは、「Windows フィルタリングプラットフォームを使用する Windows Citrix Secure Access クライアント」を参照してください。

IPベースおよびホスト名ベースのリバース分割トンネリング:

- WFP ドライバーでのみサポートされます。IP ベースのリバース分割トンネリングとホスト名ベースのリバース分割トンネリングに記載されているその他のガイドラインはすべて適用されます。

ネームサービス解決を構成する

NetScaler Gateway のインストール中に、NetScaler Gateway ウィザードを使用して、ネームサービスプロバイダーなどのその他の設定を構成できます。ネームサービスプロバイダーは、完全修飾ドメイン名 (FQDN) を IP アドレスに変換します。NetScaler Gateway ウィザードでは、次の操作も実行できます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- DNS サーバーまたは WINS サーバーを構成する
- DNS ルックアップの優先度を設定する
- サーバーへの接続を再試行する回数を設定します。

NetScaler Gateway ウィザードを実行すると、DNSサーバーを追加できます。セッションプロファイルを使用して、別のDNSサーバーとWINSサーバーをNetScaler Gateway に追加できます。その後、ウィザードで最初に構成した名前解決サーバーとは異なる名前解決サーバーに接続するようにユーザーおよびグループに指示できます。

NetScaler Gateway で別のDNSサーバーを構成する前に、名前解決用のDNSサーバーとして機能する仮想サーバーを作成します。

セッションプロファイル内に DNS サーバーまたは WINS サーバーを追加するには

1. 構成ユーティリティで、［構成］タブ >［ **NetScaler Gateway**］ > ［**ポリシー**］ > ［**セッション**］
2. 詳細ペインの タブで、プロファイルを選択し、 をクリックします。
3. タブで、次のいずれかの操作を行います。
   - DNSサーバーを構成するには、「 DNS**仮想**サーバー」の横にある「 **グローバル上書き**」をクリックし、サーバーを選択して、「 **OK**」をクリックします。
   - WINS サーバーを構成するには、「 WINS **Server IP**」の横にある「 **グローバル上書き**」をクリックし、IP アドレスを入力して「 **OK**」をクリックします。

参照ドキュメント

- 分割トンネリング
- ユーザーがCitrix Secure Access Agentに接続する方法
- NetScaler Gatewayについて
- ユーザーのアクセス方法を選択します

ユーザーのアクセス方法を選択します

次のシナリオでユーザー接続を提供するようにNetScaler Gateway を構成できます：

- Citrix Workspace アプリを使用したユーザー接続。Citrix Workspace アプリは、サーバーファーム内の公開アプリケーションまたは仮想デスクトップへのアクセスをユーザーに提供する、StoreFront またはWeb Interfaceと互換性があります。Citrix Workspace アプリは、ICA ネットワークプロトコルを使用してユーザー接続を確立するソフトウェアです。ユーザーは、

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ユーザーデバイスにCitrix Workspace アプリをインストールします。ユーザーがWindowsベースまたはMacベースのコンピューターにCitrix Workspace アプリをインストールすると、Citrix Workspace アプリは、ユーザー接続用のNetScaler Gateway プラグインを含むすべてのプラグインを使用します。NetScaler Gateway は、Android向けCitrix Workspace アプリおよびiOS向けCitrix Workspace アプリからの接続もサポートしていますユーザーは、Citrix Endpoint Management、StoreFront、またはWeb Interfaceを介して、仮想デスクトップおよびWindowsベース、ウェブ、モバイル、およびSaaSアプリケーションに接続できます。

- Secure Hubとのユーザー接続。ユーザーは、Endpoint Managementで構成されたモバイル、ウェブ、およびSaaSアプリケーションに接続できます。ユーザーは、モバイルデバイス（AndroidまたはiOS）にSecure Hubをインストールします。ユーザーがSecure Hubにログオンすると、WorxMailとWorxWeb、およびEndpoint Managementにインストールした他のモバイルアプリをインストールできます。Secure Hub、Secure Mail、およびWorxWebは、マイクロVPNテクノロジを使用して、NetScaler Gateway を介して接続を確立します。
- NetScaler Gateway プラグインをスタンドアロンアプリケーションとして使用することによるユーザー接続。NetScaler Gateway プラグインは、ユーザーがユーザーデバイスにダウンロードしてインストールできるソフトウェアです。ユーザーがプラグインを使用してログオンすると、ユーザーはオフィスにいるかのようにセキュリティで保護されたネットワーク内のリソースにアクセスできます。リソースには、電子メールサーバー、ファイル共有、イントラネットWeb サイトが含まれます。
- クライアントレスアクセスを使用したユーザ接続。クライアントレスアクセスにより、NetScaler GatewayプラグインやCitrix Workspaceアプリなどのソフトウェアをユーザーデバイスにインストールしなくても、ユーザーが必要とするアクセスが可能になります。クライアントレスアクセスでは、Outlook Web AccessやSharePoint、Citrix Virtual Appsで公開されているアプリケーション、Citrix Virtual Apps and Desktopsからの仮想デスクトップ、およびAccess Interfaceを介したセキュリティで保護されたネットワーク内のファイル共有などの限定されたWebリソースセットへの接続が可能になります。ユーザーは、WebブラウザーにNetScaler Gateway Webアドレスを入力して接続し、選択肢ページでクライアントレスアクセスを選択します。
- 事前認証または認証後スキャンが失敗した場合のユーザー接続。このシナリオは、アクセスシナリオフォールバックと呼ばれます。アクセスシナリオフォールバックを使用すると、ユーザーデバイスが最初のエンドポイント分析スキャンに合格しない場合、Citrix Workspaceアプリを使用して、NetScaler Gateway プラグインからStoreFront またはWeb Interfaceにフォールバックできます。

  ユーザーがCitrix Workspaceアプリを介してNetScaler Gateway にログオンすると、事前認証スキャンは機能しません。認証後スキャンは、NetScaler Gateway がVPNトンネルを確立するときに機能します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ユーザーは、次の方法を使用して、NetScaler Gateway プラグインをダウンロードしてインストールできます。

- Webブラウザーを使用してNetScaler Gateway に接続する。
- NetScaler Gateway 接続を受け入れるように構成されているStoreFront に接続しています。
- グループポリシーオブジェクト (GPO) を使用してプラグインをインストールする。
- NetScaler ADCプラグインをマーチャンダイジングサーバーにアップロードする。

ユーザーアクセス用にNetScaler Gateway プラグインを展開する

NetScaler Gateway には、ユーザーアクセス用の次のプラグインが付属しています：

- Windows向けNetScaler Gatewayプラグイン
- Mac版NetScaler Gateway プラグイン
- Java向けNetScaler Gateway プラグイン

ユーザーが初めてNetScaler Gateway にログオンすると、WebページからNetScaler Gateway プラグインをダウンロードしてインストールします。ユーザーは、Windowsベースのコンピューターの通知領域にあるNetScaler Gateway アイコンをクリックしてログオンします。macOS X コンピュータでは、ユーザは **Dock または** メニューからログオンできます。NetScaler Gateway を新しいソフトウェアバージョンにアップグレードすると、NetScaler Gateway プラグインはユーザーデバイス上で自動的に更新されます。

Java向けNetScaler Gateway プラグインは、Javaをサポートするすべてのユーザーデバイスで使用できます。Java向けNetScaler Gateway プラグインは、ほとんどのTCPベースのアプリケーションをサポートしますが、Windows向けNetScaler Gateway プラグインまたはmacOS X用のNetScaler Gatewayプラグインの一部の機能のみを提供します。Java向けNetScaler Gateway プラグインは、定義したネットワークリソースへの制限付きアクセスを提供します。Javaプラグインの詳細については、「Java向けNetScaler Gateway プラグイン」を参照してください。

MSIインストーラーパッケージを使用してNetScaler Gateway プラグインを展開する

NetScaler Gateway プラグインは、Microsoft Active Directory インフラストラクチャまたはWindows Server アップデートサービスなどの標準のサードパーティMSI展開ツールを使用して展開できます。Windows インストーラーパッケージをサポートするツールを使用する場合は、MSIファイルをサポートする任意のツールを使用してパッケージを展開できます。次に、展開ツールを使用して、適切なユーザーデバイスにソフトウェアを展開してインストールします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

一元化された展開ツールを使用する利点

- セキュリティ要件に準拠する能力。たとえば、管理者以外のユーザーのソフトウェアインストール権限を有効にせずに、ユーザーソフトウェアをインストールできます。
- ソフトウェアのバージョンを管理します。ソフトウェアの更新バージョンをすべてのユーザーに同時に展開できます。
- スケーラビリティ。一元化された展開戦略は、より多くのユーザーをサポートするように簡単に拡張できます。
- ポジティブなユーザーエクスペリエンス。このプロセスにユーザを関与させることなく、インストール関連の問題の展開、テスト、およびトラブルシューティングを行うことができます。

ユーザーソフトウェアのインストールに対する管理制御が優先され、ユーザーデバイスへのアクセスがすぐに利用できる場合は、このオプションをお勧めします。

詳細については、「Active Directory yからNetScaler Gateway プラグインを展開する」を参照してください。

展開するソフトウェアプラグインを決定する

NetScaler Gateway 展開環境がユーザーデバイスにソフトウェアプラグインを必要としない場合、展開はクライアントレスアクセスを提供すると見なされます。このシナリオでは、ユーザーはネットワークリソースにアクセスするのに Web ブラウザだけを必要とします。ただし、一部の機能では、ユーザーのデバイスにプラグインソフトウェアが必要です。

ユーザー用のNetScaler Gateway プラグインを選択する

NetScaler Gateway を構成するときに、ユーザーのログオン方法を選択できます。ユーザーは、次のいずれかのプラグインを使用してログオンできます。

- Windows向けNetScaler Gatewayプラグイン
- macOS 向けNetScaler Gateway プラグイン
- Java向けNetScaler Gateway プラグイン

セッションポリシーを作成し、そのポリシーをユーザー、グループ、または仮想サーバーにバインドして、構成を完了します。グローバル設定を構成して、プラグインを有効にすることもできます。グローバルプロファイルまたはセッションプロファイル内で、プラグインタイプとして Windows/macOS X または Java のいずれかを選択します。ユーザーがログオンすると、グローバルに、またはセッションプロファイルとポリシーで定義されているプラグインを受け取ります。プラグインタイプ用に個別のプロファイルを作成します。セッションプロファイルでは、 **Windows/**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

macOS X または Java のいずれかしか選択できません。Java用のNetScaler Gateway プラグインを構成するには、「Java向けNetScaler Gateway プラグインを使用した接続」を参照してください。

プラグインをグローバルに構成する

1. ナビゲーションペインにある、［Configuration］タブの構成ユーティリティで、［NetScaler Gateway］を展開し、［Global Settings］をクリックします。
2. 詳細ペインの で、 をクリックします。
3. ［クライアントエクスペリエンス］タブで、［プラグインの種類］の横にある［Windows/macOS X］を選択し、［OK］をクリックします。

セッションプロファイルで Windows または macOS のプラグインタイプを構成する

1. 構成ユーティリティの［構成］タブのナビゲーションペインで、［**Citrix Gateway**］>［**ポリシー** ］を展開し、［**セッション**］をクリックします。
2. 次のいずれかを行います：
   - 新しいセッションポリシーを作成する場合は、詳細ペインで をクリックします。
   - 既存のポリシーを変更する場合は、ポリシーを選択し、 をクリックします。
3. プロファイルを作成するか、既存のプロファイルを変更します。これを行うには、次のいずれかを実行します：
   - 「**リクエストプロファイル**」の横にある「**新規**」をクリックします。
   - 「**リクエストプロファイル**」の横にある「**変更**」をクリックします。
4. タブで、 の横にある をクリックし、 を選択します。
5. 次のいずれかを行います：
   - 新しいプロファイルを作成する場合は、 をクリックし、ポリシーダイアログボックスで式を設定し、、 の順にクリックします。
   - 既存のプロファイルを変更する場合は、選択後、「OK」 を 2 回クリックします。

Windows向けNetScaler Gatewayプラグイン

ユーザーがNetScaler Gateway にログオンすると、ユーザーデバイスにNetScaler Gateway プラグインをダウンロードしてインストールします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

プラグインをインストールするには、ユーザーがローカル管理者または Administrators グループのメンバーである必要があります。この制限は、初回のインストールにのみ適用されます。プラグインのアップグレードには、管理者レベルのアクセス権は必要ありません。

ユーザーがNetScaler Gateway に接続して使用できるようにするには、次の情報を提供する必要があります：

- NetScaler Gateway Webアドレス（例： `<https://NetScalerGatewayFQDN/>`
- エンドポイントのリソースとポリシーを構成した場合、NetScaler Gateway プラグインを実行するためのシステム要件

ユーザーデバイスの構成によっては、次の情報も提供する必要があります：

- ユーザーが自分のコンピュータでファイアウォールを実行している場合、アクセスを許可したリソースに対応する IP アドレスとのトラフィックをファイアウォールがブロックしないように、ファイアウォールの設定を変更する必要がある場合があります。NetScaler Gateway プラグインは、Windows XPではインターネット接続ファイアウォールを、Windows XP Service Pack 2、Windows Vista、Windows 7、Windows 8、Windows 8.1ではWindowsファイアウォールを自動的に処理する。
- NetScaler Gateway 接続を介してFTPにトラフィックを送信するユーザーは、パッシブ転送を実行するようにFTPアプリケーションを設定する必要があります。パッシブ転送とは、FTP サーバーからリモートコンピューターへのデータ接続が確立されるのではなく、リモートコンピューターが FTP サーバーへのデータ接続を確立することを意味します。
- 接続を介して X クライアントアプリケーションを実行したいユーザーは、コンピュータ上で X サーバ (など `XManager`) を実行する必要があります。
- Receiver for WindowsまたはReceiver for Macをインストールするユーザーは、Receiverから、またはWebブラウザーを使用してNetScaler Gatewayプラグインを起動できます。ReceiverまたはWebブラウザーを使用してNetScaler Gateway プラグインを使用してログオンする方法について、ユーザーに指示します。

ユーザーは、ファイルやアプリケーションを、組織のネットワークに対してローカルであるかのように操作するため、ユーザーを再トレーニングしたり、アプリケーションを構成したりする必要はありません。

セキュリティで保護された接続を初めて確立するには、Webログオンページを使用してNetScaler Gateway にログオンします。Web アドレスの一般的な形式は`<https://companyname.com>`です。ユーザーがログオンすると、NetScaler Gateway プラグインをコンピューターにダウンロードしてインストールできます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Windows版NetScaler Gateway プラグインをインストールする

1. Webブラウザーで、NetScaler Gateway のWebアドレスを入力します。
2. ユーザー名とパスワードを入力し、 をクリックします。
3. を選択し、 をクリックします。
4. 指示に従ってプラグインをインストールします。

ダウンロードが完了すると、NetScaler Gateway プラグインが接続され、Windowsベースのコンピューターの通知領域にメッセージが表示されます。

ユーザーがWebブラウザーを使用せずにCitrix Gateway プラグインに接続できるようにする場合は、 **ユーザーがWindowsベースのコンピューターの通知領域にあるCitrix Gateway** アイコンを右クリックするか、［スタート］メニューからプラグインを起動したときにログオンダイアログボックスを表示するようにプラグインを構成できます。

Windows版NetScaler Gateway プラグインのログオンダイアログボックスを構成する

ログオンダイアログボックスを使用するようにNetScaler Gateway プラグインを構成するには、ユーザーがログオンしてこの手順を完了する必要があります。

1. Windowsベースのコンピューターでは、通知領域でNetScaler Gateway アイコンを右クリックし、［NetScaler Gateway の構成］をクリックします。
2. タブをクリックし、 をクリックします。
3. ［オプション］タブで、［ログオンにNetScaler Gateway プラグインを使用する］をクリックします。 注：Receiver内から［NetScaler Gateway の構成］ダイアログボックスを開いた場合、［ オプション］タブは使用できません。

Windows版NetScaler Gateway プラグインのインターセプトモードを設定する

Windows用のNetScaler Gateway プラグインを構成する場合は、傍受モードを構成して透過に設定する必要もあります。

1. 構成ユーティリティで、［構成］タブをクリックし、［ **NetScaler Gateway**］**>**［**リソース**］**の順に展開し、** ［ **イントラネットアプリケーション**］をクリックします。
2. 詳細ペインで、 をクリックします。
3. ** に、ポリシーの名前を入力します。
4. をクリックします。
5. 「 **プロトコル**」で「 **任意**」を選択します。
6. で、 と を選択します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

7. に IP アドレスを入力します。
8. にサブネットマスクを入力し、、** の順にクリックします。

ADC 構成に基づいてエンドユーザーにローカル LAN アクセスを強制する

Citrix ADCリリース13.0、ビルド85.15以降、管理者はエンドユーザーがクライアントマシンでローカルLANアクセスオプションを無効にすることを制限できます。既存のローカル LAN アクセスパラメータ値に、FORCED という新しいオプションが追加されました。ローカル LAN アクセス値が FORCED に設定されている場合、クライアントマシンのエンドユーザーはローカル LAN アクセスが常に有効になります。エンドユーザーは、Citrix Secure AccessクライアントUIでローカルLAN設定を無効にすることはできません。管理者がエンドユーザーにローカルLANアクセスを有効または無効にするオプションを提供したい場合は、ローカルLANアクセスパラメーターをONに再構成する必要があります。

GUI を使用して オプションを有効にするには:

1. ［**Citrix Gateway**］>［**グローバル設定**］>［**グローバル設定の変更**］に移動します。
2. タブをクリックし、 をクリックします。
3. で を選択します

CLI を使用して Forced オプションを有効にするには、次のコマンドを実行します。

```
set vpn parameter -localLanAccess FORCED
```

Java向けNetScaler Gateway プラグイン

Java向けNetScaler Gateway プラグインは、Javaをサポートするすべてのユーザーデバイスで使用できます。

注:

次のオペレーティングシステムおよび Web ブラウザでは、Java ランタイム環境 (JRE) バージョン 1.4.2 から JRE の最新バージョンまでが必要です。

- macOS X
- Linux
- Windows XP（全バージョン）、Windows Vista、Windows 7、Windows 8
- Internet Explorer

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Firefox
- Safari 1.2 ウェブブラウザの最新バージョンまで

Java向けNetScaler Gateway プラグインは、ほとんどのTCPベースのアプリケーションをサポートしますが、Windows用のNetScaler Gatewayプラグインまたは macOS X用のNetScaler Gatewayプラグインの一部の機能のみを提供します。

ユーザーは、Java向けNetScaler Gateway プラグインを使用するために、ユーザーデバイスの管理者権限を必要としません。セキュリティ上の理由から、使用するユーザーデバイスに関係なく、特定の仮想サーバー、グループ、またはユーザーに対してこのプラグインバージョンを使用することを要求する場合があります。

ユーザーデバイスにJava向けNetScaler Gateway プラグインをインストールするようにNetScaler Gateway を構成するには、セッションポリシーを構成し、仮想サーバー、グループ、またはユーザーにバインドします。

ユーザーが Windows 7 を実行しているコンピューターからログオンする場合、プロキシサーバー情報は Internet Explorer で自動的に設定されません。ユーザーは、Windows 7 を実行しているコンピューターでプロキシサーバーを手動で構成する必要があります。

Java 用NetScaler Gatewayプラグインの設定

1. **NetScaler Gateway > ポリシー**に移動し 、「 **セッション**」をクリックします。
2. 詳細ペインで、「 **プロファイル** 」タブをクリックします。
3. セッションプロファイルを選択して をクリックします。
4. 「クライアントエクスペリエンス」タブの「プラグインタイプ」の横にある「 **グローバル上書き**」をクリックし、「 **Java**」を選択して「 **OK**」をクリックします。

インターセプトモードを設定するには

セッションポリシーを作成したら、イントラネットアプリケーションを作成し、Java向けNetScaler Gateway プラグインを使用してログオンするユーザーの傍受モードを定義します。

1. **NetScaler Gateway >「リソース** 」に移動し、「イントラネットアプリケーション」をクリック**します**。
2. 詳細ペインで、 をクリックします。
3. に、名前を入力します。
4. 「 プロ**キシ**」をクリックします。
5. に IP アドレスを入力します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

6. に、ポート番号を入力します。
7. に IP アドレスを入力します。
8. にポート番号を入力し、 をクリックし、 **をクリック**し**ます。

ソースIPアドレスとポート番号を指定しない場合、NetScaler Gateway はIPアドレスに127.0.0.1、ポートに0を自動的に使用します。

Windows ベースのコンピューターで HOSTS ファイルを更新します

Windows Vista、Windows 7、またはWindows 8を実行しているコンピューターで、ユーザーがJava向けNetScaler Gateway プラグインを使用してログオンすると、TCPイントラネットアプリケーションのネットワークトラフィックはトンネリングされません。Vista および Windows 7 を実行しているコンピュータでは、HOSTS ファイルは自動的に更新されません。イントラネットアプリケーションを HOSTS ファイルに手動で追加します。

Windows ベースのコンピュータでは、メモ帳または別のテキストエディタで HOSTS ファイルを編集できます。メモ帳で HOSTS ファイルを編集する場合は、管理者としてメモ帳を実行する必要があります。Java向けNetScaler Gateway プラグインのイントラネットアプリケーションのマッピングエントリを追加し、ファイルを保存します。

NetScaler Gateway プラグインをActive Directory から展開する

ユーザーデバイスにNetScaler Gateway プラグインをインストールするための管理者権限がユーザーにない場合は、Active Directory からユーザー用のプラグインを展開できます。この方法を使用してNetScaler Gateway プラグインを展開すると、インストールプログラムを展開し、グループポリシーを使用してプログラムを展開できます。このタイプの展開の一般的な手順は次のとおりです。

- MSI パッケージを抽出します。
- グループポリシーを使用してプラグインを配布する。
- 配布ポイントを作成する。
- グループポリシーオブジェクトを使用してNetScaler Gateway プラグインパッケージを割り当てる。

  注： Active Directory からのNetScaler Gateway プラグインの配布は、Windows 7、Windows 8、およびWindows 10でのみサポートされています。

MSIパッケージは、構成ユーティリティまたはCitrix Webサイトからダウンロードできます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

構成ユーティリティからNetScaler Gateway プラグインのMSIパッケージをダウンロードするには

1. 構成ユーティリティで、 をクリックします。
2. ［NetScaler Gateway プラグイン］で［ **Windows用NetScaler Gatewayプラグインのダウンロード** ］をクリックし、 **nsvpnc_setup.exe** ファイルをWindowsサーバーに保存します。

   注：

   - 64 ビットコンピュータでは、Agee_setup.exe ファイルを Windows サーバに保存する必要があります。
   - ［ **ファイルのダウンロード** ］ダイアログボックスが表示されない場合は、Ctrl キーを押して［ **Windows用NetScaler Gateway プラグインをダウンロード**］リンクをクリックします。

3. コマンドプロンプトで、 **nsvpnc_setup.exe** を保存したフォルダに移動し、次のように入力します。

   ```
   nsvpnc_setup /c
   ```

   これにより、ファイル agee.msi が抽出されます。

   注: 64 ビットコンピュータでは、 **Agee_setup.exe** を保存したフォルダに移動して、次のように入力します。

   ```
   Agee_setup.exe /c
   ```

   これにより、ファイル agee64.msi が抽出されます。
4. 解凍したファイルを Windows サーバ上のフォルダに保存します。

ファイルを展開したら、Windows Server のグループポリシーを使用してファイルを配布します。

配布を開始する前に、グループポリシー管理コンソールを Windows Server 2003、Windows Server 2008、または Windows Server 2012 にインストールします。詳細については、Windows オンラインヘルプを参照してください。

注： グループポリシーを使用してNetScaler Gateway プラグインを公開する場合は、パッケージをユーザーデバイスに割り当てることをお勧めします。MSI パッケージはデバイスごとにインストールされます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ソフトウェアを配布する前に、Microsoft インターネットセキュリティおよびアクセラレーション (ISA) サーバーなどの公開サーバー上のネットワーク共有に配布ポイントを作成します。

配布ポイントを作成するには

1. 管理者として公開サーバーにログオンします。
2. フォルダを作成し、配布パッケージにアクセスする必要があるすべてのアカウントの読み取り権限でネットワーク上で共有します。
3. コマンドプロンプトで、解凍したファイルを保存するフォルダに移動し、「msiexec-a agee.msi」と入力します。
4. ［ **ネットワークの場所** ］画面で ［ **変更** ］ をクリックし、NetScaler Gateway プラグインの管理用インストールを作成する共有フォルダーに移動します。
5. 「 **OK**」 をクリックし、「 **インストール**」をクリックします。

抽出したパッケージをネットワーク共有に配置したら、Windows のグループポリシーオブジェクトにパッケージを割り当てます。

NetScaler Gateway プラグインを管理対象ソフトウェアパッケージとして正常に構成すると、ユーザーデバイスの次回起動時にプラグインが自動的にインストールされます。

注:
インストールパッケージがコンピュータに割り当てられたら、ユーザーはコンピュータを再起動する必要があります。

インストールが開始されると、NetScaler Gateway プラグインがインストール中であるというメッセージが表示されます。

Active Directory を使用してNetScaler Gateway プラグインを管理する

NetScaler Gateway プラグインの各リリースは、パッチとしてではなく、製品のフルインストールとしてパッケージ化されています。ユーザーがログオンし、NetScaler Gateway プラグインがプラグインの新しいバージョンを検出すると、プラグインは自動的にアップグレードされます。また、Active Directory yを使用して、NetScaler Gateway プラグインを展開してアップグレードすることもできます。

これを行うには、NetScaler Gateway プラグインの配布ポイントを作成します。グループポリシーオブジェクトを作成し、新しいバージョンのプラグインをそのオブジェクトに割り当てます。次に、新しいパッケージと既存のパッケージの間にリンクを作成します。リンクを作成すると、NetScaler Gateway プラグインが更新されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ユーザーデバイスからNetScaler Gateway プラグインを削除する

NetScaler Gateway プラグインをユーザーデバイスから削除するには、グループポリシーオブジェクトエディターから割り当てられたパッケージを削除します。

プラグインがユーザーデバイスから削除されると、プラグインがアンインストール中であることを示すメッセージがユーザーに表示されます。

Active Directory yを使用してNetScaler Gateway プラグインのインストールをトラブルシューティングする

ユーザーデバイスの起動時に割り当てられたパッケージのインストールに失敗すると、アプリケーションイベントログに次の警告が表示されることがあります：

ソフトウェアインストール設定の変更を適用できませんでした。管理者がグループポリシーのログオンの最適化を有効にしているため、ソフトウェアインストールポリシーのアプリケーションが次のログオンまで遅延しました。エラーは次のとおりです。グループポリシーフレームワークは、同期フォアグラウンドポリシーの更新で拡張機能を呼び出す必要があります。

このエラーは、Windows XP の高速ログオンの最適化が原因で、オペレーティングシステムがグループポリシーオブジェクトの処理を含むすべてのネットワークコンポーネントを初期化する前にユーザーがログオンできることが原因です。ポリシーによっては、有効にするために複数の再起動が必要な場合があります。この問題を解決するには、Active Directory で高速ログオン最適化を無効にします。

管理対象ソフトウェアのインストールに関するその他の問題のトラブルシューティングを行うには、グループポリシーを使用してWindowsインストーラーログを有効にすることをお勧めします。

NetScaler Gateway プラグインとCitrix Workspace アプリを統合する

NetScaler Gateway はCitrix Workspace アプリをサポートしています。オーケストレーションシステムは、次のコンポーネントで構成されています。

- Windows 3.4 以降向けのCitrix Workspace アプリ
- Mac向けCitrix Workspaceアプリ
- Android向けCitrix Workspaceアプリ
- iOS向けCitrix Workspaceアプリ
- StoreFront 2.1 またはそれ以降

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Endpoint Management 2.8以降またはCitrix Endpoint Management 10
- Citrix Webサイトでホストされ ているCitrix更新サービス

NetScaler Gateway とCitrix 製品との互換性について詳しくは、「Citrix 製品との互換性」を参照してください。

ユーザーがアプライアンスにログオンすると、NetScaler Gateway プラグインによってWebブラウザーが開き、Citrix Workspaceアプリのホームページへのシングルサインオンを許可するようにNetScaler Gateway を構成できます。ユーザーは、ホームページからCitrix Workspace アプリをダウンロードできます。

ユーザーがCitrix Workspace アプリでログオンすると、ユーザー接続は次の方法でNetScaler Gateway 経由でルーティングできます。

- Endpoint Management に直接アクセスする
- StoreFront に直接アクセスする
- Endpoint ManagementでMDXモバイルアプリを構成しない場合は、StoreFront、Endpoint Managementの順に指定します。
- Endpoint ManagementでMDXモバイルアプリを構成する場合は、Endpoint ManagementとStoreFront の順に指定します

注：

Endpoint Management に直接ルーティングされる接続は、Endpoint Management 2.0、Endpoint Management 2.5、Endpoint Management 2.6、Endpoint Management 2.8、およびEndpoint Management 2.9でのみサポートされます。ネットワークにEndpoint Management 1.1を展開している場合、ユーザー接続はStoreFront 経由でルーティングする必要があります。

ユーザーがCitrix Workspace アプリに接続する方法

ユーザーは、Citrix Workspace アプリから次のアプリケーション、デスクトップ、およびデータに接続できます。

- StoreFront およびWeb Interfaceで公開されているWindowsベースのアプリケーションと仮想デスクトップ
- Citrix Endpoint Management を介してアクセスされるShareFileデータ

ユーザーは、次のCitrix Workspace アプリのいずれかを使用してログオンできます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Citrix Workspaceアプリ（Web）
- Windows向けCitrix Workspaceアプリ
- Mac向けCitrix Workspaceアプリ
- iOS向けCitrix Workspaceアプリ
- Android向けCitrix Workspaceアプリ

ユーザーは、Webブラウザーまたはユーザーデバイスの Citrix Workspace アプリのアイコンを使用して、Web向けCitrix Workspace アプリでログオンできます。

ユーザーが任意のバージョンの Citrix Workspace アプリでログオンすると、アプリケーション、ShareFileデータ、およびデスクトップがブラウザーまたはCitrix Workspace アプリウィンドウに表示されます。

Citrix Workspace アプリのアイコンを切り離す

Citrix Workspaceアプリと統合されたNetScaler Gateway プラグインを使用してCitrix Virtual Apps and Desktopsの展開を構成すると、VPNに接続しているユーザーにはプラグインのアイコンが表示されません。 **NetScaler Gateway プラグインアイコンは** 、通常、WindowsのシステムトレイまたはmacOS X Finderのメニューバーにあります。このアイコンは、プラグインの設定とコントロールへのインタフェースです。Windowsユーザーの場合、Citrix WorkspaceアプリとNetScaler Gatewayプラグインが統合されている場合、Citrix Workspaceアプリの［ **バージョン情報** ］ダイアログボックスにNetScaler Gateway プラグインのコントロールが表示されます。macOS Xユーザーの場合、統合後に使用できるNetScaler Gateway プラグインのコントロールはありません。

一部の統合展開では、基盤となる機能の統合を維持しながら、プラグインコントロールを公開する必要がある場合があります。これを行うには、次のCLIコマンドまたはNetScaler ADC構成ユーティリティタスクを使用して、VPNクライアントのアイコン統合を切り替えます。

CLI を使用したアイコン統合の設定

コマンドプロンプトで次を入力します：

```
set vpn parameter [-iconWithReceiver (ON/OFF)]
```

GUI を使用したアイコン統合の設定

1. ［構成］タブで、［ **NetScaler Gateway］>［グローバル設定］**に移動します。
2. をクリックし、 タブを選択します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. をクリックします。**
4. Citrix Workspaceアプリで［ **VPNプラグインアイコンを表示する** ］を選択します。

ICA 接続用の IPv6 を構成する

NetScaler Gateway は、ICA接続のIPv6アドレスをサポートしています。IPv6を使用したWeb InterfaceまたはStoreFront への接続は、IPv4接続と同様に機能します。ユーザーがNetScaler Gateway Webアドレスを使用して接続すると、NetScaler Gateway はWeb Interfaceまたは StoreFront への接続をプロキシします。

1つのDMZに展開されたNetScaler Gateway またはダブルホップDMZに展開されたNetScaler Gateway のIPv6を構成できます。

NetScaler Gateway でIPv6を有効にするには、コマンドラインを使用します。次のガイドラインを使用できます。

- アプライアンスで IPv6 を有効にします。
- サブネット IP アドレスを設定します。
- DNS 解決順序を設定します。
- Web InterfaceまたはStoreFront のWebアドレスを設定します。
- Secure Ticket Authority（STA）をNetScaler Gateway にバインドします。

デフォルトでは、マッピング IP アドレスは IPv6 アドレスをサポートしていません。ユーザー通信を内部ネットワークにルーティングするには、サブネットIPアドレスを作成し、サブネットIPアドレスを使用するようにNetScaler Gateway を構成する必要があります。

ネットワークに複数のIPv6サブネットを展開する場合は、NetScaler Gateway で、ネットワーク内のサブネットごとに複数のIPv6サブネットIPアドレスを作成します。ネットワークルーティングは、サブネット IP アドレスを使用して IPv6 パケットをそれぞれのサブネットに送信します。

CLI を使用して ICA プロキシの IPv6 を構成するには

1. PuTTYなどのセキュアシェル（SSH）接続を使用して、NetScaler Gateway にログオンします。コマンドプロンプトで次を入力します：

```
enable ns feature IPv6PT. This enables IPv6.



enable ns mode USNIP.
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
set dns parameter –resolutionOrder AAAAThenAQuery AThenAAAAQuery
OnlyAAAAQuery OnlyAQuery



set vpn parameter -wihome `http://XD_domain/Citrix/StoreWeb`
```

各項目の意味は次のとおりです <xd_domain> StoreFront のドメイン名またはIPアドレスのいずれかです。

例:

```
set vpn parameter -wihome `http://storefront.domain.com/Citrix/StoreWeb`.
```

または

```
set vpn parameter -wihome `http://[1000:2000::3000]/Citrix/StoreWeb`
```

注:

IPv6 アドレスを使用してこのパラメータを設定する場合は、IP アドレスを括弧で囲む必要があります。

NetScaler Gateway でCitrix Workspaceアプリのホームページを構成する

Citrix Workspace アプリのホームページは、グローバルに構成することも、セッションプロファイルの一部として構成することもできます。NetScaler Gateway を介してStoreFront を認識しない Citrix Workspace アプリをWebおよびそれ以前のバージョンのCitrix Workspaceアプリ用に構成する場合は、2つの別々のセッションプロファイルを作成する必要があります。ユーザーが正常にログオンできるように、Citrix Workspace アプリのホームページのフィールドには、各プロファイルの正しいWebアドレスが必要です。

NetScaler Gateway を介してStoreFront を認識するCitrix Workspaceアプリの場合、Web向けCitrix Workspace アプリとCitrix Workspace アプリでプロファイルを共有できます。ただし、Web向け

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix Workspaceアプリのセッションプロファイルと、他のすべてのCitrix WorkCitrix Workspaceアプリ用に個別のセッションプロファイルを構成することをお勧めします。

Citrix Workspace アプリのホームページをグローバルに構成するには

Citrix Workspace アプリのホームページをグローバルに構成するには：

1. ナビゲーションペインにある、［Configuration］タブの構成ユーティリティで、［NetScaler Gateway］を展開し、［Global Settings］をクリックします。
2. 詳細ペインの で、 をクリックします。
3. ［グローバルNetScaler Gateway 設定］ダイアログボックスで、［公開アプリケーション］タブをクリックします。
4. Citrix Workspace アプリのホームページで、Citrix Workspace アプリまたはWeb向けCitrix Workspace アプリのホームページのWebアドレスを入力し、［OK］をクリックします。

セッションプロファイルでCitrix Workspace アプリのホームページを構成するには

セッションプロファイルでCitrix Workspace アプリのホームページを構成するには：

1. 構成ユーティリティの［構成］タブのナビゲーションペインで、［ **Citrix Gateway**］>［**ポリシー** ］を展開し、［ **セッション**］をクリックします。
2. 詳細ペインの タブで、 をクリックします。
3. ［ **NetScaler Gateway セッションプロファイルの作成** ］ダイアログボックスの［ **公開アプリケーション** ］タブで、［ **Citrix Receiverホームページ** ］の横にある［ **グローバル上書き**］をクリックします。
4. Citrix Workspace アプリのホームページで、Citrix Workspace アプリまたはWeb向けCitrix Workspaceアプリのホームページのアドレスを入力し、［ **作成**］をクリックします。

Citrix Workspace アプリのテーマをNetScaler Gateway のログオンページに適用する

GUIを使用して、Citrix Workspace アプリテーマをNetScaler Gateway のログオンページに適用できます。Citrix Workspace アプリのテーマ、デフォルトのテーマ、または作成したカスタムテーマを切り替えることができます。

1. ナビゲーションペインにある、［Configuration］タブの構成ユーティリティで、［NetScaler Gateway］を展開し、［Global Settings］をクリックします。
2. 詳細ペインの で、 をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. ［グローバルNetScaler Gateway 設定］ダイアログボックスで、［クライアントエクスペリエンス］タブをクリックします。
4. 「UI テーマ」の横にある「緑色のバブル」をクリックし、「OK」をクリックします。

   このコマンドは、元のログオンページをReceiverテーマで上書きします。注:別のテーマを適用した後、キャッシュされたページが表示されないようにブラウザのキャッシュをクリアするようにユーザーにアドバイスします。

NetScaler Gateway ログオンページのカスタムテーマを作成する

GUIを使用して、NetScaler Gateway のログオンページのカスタムテーマを作成できます。デフォルトのテーマのままにすることも、Citrix Workspace アプリのテーマを使用することもできます。ログオンページにカスタムテーマを適用する場合は、NetScaler Gateway コマンドラインを使用してテーマを作成して展開します。次に、GUI を使用してカスタムテーマページを設定します。

カスタムテーマページは、NetScaler Gateway グローバル設定を使用して構成します。

この機能は、次のバージョンのNetScaler Gateway で使用できます。

- NetScaler Gateway 10.1
- アクセスゲートウェイ 10、ビルド 73.5002.e（Endpoint Managementバージョン2.5、2.6、または2.8でこの機能を使用するには、ビルド71.6104.eの後にこのビルドをインストールする必要があります）
- アクセスゲートウェイ 10、ビルド 71.6104.e

CLI を使用したカスタムテーマの作成と展開

コマンドラインを使用してカスタムテーマを作成して展開するには:

1. NetScaler Gateway コマンドラインにログオンします。
2. コマンドプロンプトで、shell と入力します。
3. コマンドプロンプトで「`mkdir /var/ns_gui_custom; cd /netscaler; tar -cvzf /var/ns_gui_custom/customtheme.tar.gz ns_gui/*`」と入力します。
4. 構成ユーティリティを使用してカスタムテーマに切り替え、/var/ns_gui_custom/ns_gui/VPN でカスタマイズを変更します。次の操作を実行できます：

   - css/ctx.authentication.css ファイルを編集します。
   - カスタムロゴを /var/ns_gui_custom/ns_gui/VPN/media フォルダにコピーします。**注:** WinSCP を使用してファイルを転送できます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. 複数のNetScaler Gateway アプライアンスがある場合は、すべてのアプライアンスについて手順3と4を繰り返します。

NetScaler Gateway Windows VPN クライアントレジストリキー

VPN クライアントのレジストリキーは、 **HKEY_LOCAL_MACHINE\ SOFTWARE\ Citrix\ Secure Access Client**の下にあります。次の表に、NetScaler Gateway VPNクライアントのレジストリキー、値、および各値の簡単な説明を示します。

レジストリキー	レジストリタイプ	値と説明
AlwaysOnService	REG_DWORD	1 => マシンレベルのトンネルを確立するが、ユーザーレベルのトンネルは確立しない。2 => マシンレベルのトンネルとユーザーレベルのトンネルを確立する。
AlwaysOnURL	REG_SZ	ユーザーが接続するNetScaler Gateway 仮想サーバーのURL。例: `https://xyz.companyDomain.com`
AlwaysOn	REG_DWORD	1 => VPN障害時にネットワークアクセスを許可する。2=> VPN障害時にネットワークアクセスをブロックする。
locationDetection	REG_DWORD	1 => 位置検出を有効にする。0 => 位置検出を無効にする。
suffixList	REG_SZ	セミコロンで区切られたイントラネットドメインのリスト。位置検出が有効な場合に使用されます。
AlwaysOnWhitelist	REG_SZ	Always On 厳密モードでドライバーによってホワイトリストに登録される IP アドレス

© 1997–2026 Citrix Systems, Inc. All rights reserved.

レジストリキー	レジストリタイプ	値と説明
		または FQDN のセミコロン区切りのリスト。
ProductVersion	REG_SZ	NetScaler Gateway プラグインがインストールされている現在のバージョン。
InstallDir	REG_SZ	NetScaler Gateway プラグインがインストールされている場所。
userCertCAList	REG_SZ	常時接続サービスのコンテキストで使用され、カスタマーはクライアント証明書の選択元となる CA のリストを指定できます。
addedRoutes/modifiedRoutes	REG_SZ	内部プラグイン通信用に作成されます。ユーザーはこのキーを変更してはなりません。
ProductCode	REG_SZ	このキーは内部で使用されます。ユーザーはこのキーを変更してはならない
EnableAutoUpdate	REG_DWORD	クライアント側からプラグインアップデート機能を制御するために使用されます。0 に設定すると、自動更新機能が無効になります。1 に設定すると、ADC 構成が考慮されます。
Connected	REG_DWORD	接続に成功すると、このキーは 1 に設定され、それ以外の場合は 0 に設定されます。このキーは内部で使用されます。ユーザーはこのキーを変更してはなりません。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

レジストリキー	レジストリタイプ	値と説明
EnableVA	REG_DWORD	IIPが存在する場合にCitrix 仮想アダプタを有効にする必要がある場合。このキーは内部で使用されます。ユーザーはこのキーを変更してはなりません。
DisableGA	REG_DWORD	1 に設定すると、Google Analyticsが無効になります。
DisableCredProv	REG_DWORD	[ユーザーログオン前に常時接続] が有効になっている場合、Windows VPN プラグインは、ログオン画面にトンネルの状態を表示するための資格情報プロバイダーを追加します。この追加機能が必要ない場合は、このレジストリを作成し、1 に設定します。
ClientControl	REG_DWORD	1 => ユーザーがログアウトしたり、他のゲートウェイに接続したりすることを許可します。0 => ユーザーがログアウトしたり、他のゲートウェイに接続したりすることをブロックします。
ForcedLogging	REG_DWORD	デバッグロギングを有効にするには、このキーを 1 に設定します。
NoDHCPRoute	REG_DWORD	1 に設定すると、DHCP サーバールートは追加されません。
DisableIntuneDeviceEnrollment	REG_DWORD	1 に設定すると、Intune デバイスの登録は実行されません。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

レジストリキー	レジストリタイプ	値と説明
HttpTimeout	REG_DWORD	HTTP タイムアウトは秒単位で設定されます。タイムアウトが設定されていない場合、デフォルトのタイムアウトが使用されます。デフォルトのタイムアウト値は 100 秒で、Windows 標準に基づいています。
DisableIconHide	REG_DWORD	1 => Citrix Workspace アプリとゲートウェイプラグインがタスクバーに表示されます。0 => ゲートウェイプラグインアイコンは、Windows向け Citrix Workspace アプリと統合されています。完全な VPN セッションを実行している場合、ゲートウェイプラグインはタスクバーに表示されません。
EnableWFP	REG_DWORD	デフォルト値 0 => デフォルトではDNEは有効になっています。1 => VPNプラグインはWFPを使用します。0 => VPNプラグインはDNEを使用します。
SecureAccessLogInScript	REG_SZ	Citrix Secure Accessサービスは、Citrix Secure Private Accessサービスに接続するときに、このレジストリキーを使用してログインスクリプト構成にアクセスします。詳細については、「ログインとログアウトのスクリプト設定レジストリ」を参照してください。
SecureAccessLogOutScript	REG_SZ	Citrix Secure Accessサービスは、Citrix Secure Private

© 1997–2026 Citrix Systems, Inc. All rights reserved.

レジストリキー	レジストリタイプ	値と説明
		Accessサービスに接続するときに、このレジストリキーを使用してログアウトスクリプト構成にアクセスします。詳細については、「ログインとログアウトのスクリプト設定レジストリ」を参照してください。

重要:

レジストリキーは、展開に基づいて適用できます。たとえば、AlwaysOn Service レジストリは AlwaysOn サービスにのみ適用されますが、ClientControl レジストリは常にオンサービスには適用されません。詳細については、個々の展開ドキュメントを参照してください。

認証Cookieに HttpOnly フラグを強制する

NetScaler Gatewayリリース13.0-89.x以降では、VPNシナリオの認証クッキー、つまりNSC_AAACクッキーとNSC_TMASクッキーでHTTPOnlyフラグを使用できます。NSC_TMAS 認証Cookie は nFactor 認証時に使用され、NSC_AAAC Cookie は認証セッションに使用されます。Cookie の HttpOnly フラグは、JavaScript ドキュメントCookie オプションを使用してCookie アクセスを制限します。これにより、クロスサイトスクリプティングによる Cookie の盗難を防ぐことができます。

対応シナリオ

HttpOnly フラグは nFactor 認証でサポートされています。

NetScaler ADC AAA パラメータの HTTPOnlyCookie ノブを tmsession の HTTPOnlyCookie ノブとともに使用したときの動作：

- 認証、承認、および監査パラメータの HTTPOnlyCookie ノブが有効になっていて nFactor 認証が使用されている場合、認証、承認、および監査パラメータの HTTPOnlyCookie ノブは TM セッションの HTTPOnlyCookie ノブよりも優先されます。また、NSC_TMAS と NSC_AAAC はどちらも、セッションタイプ（VPN セッション、TM セッション、または nFactor 認証中）に関係なく、HTTPOnly とマークされます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- HTTPOnlyCookie ノブを無効にすると、VPN セッションに HTTPOnly フラグは設定されません。認証、承認、および監査シナリオでは、HttpOnly フラグは TM セッションノブの値に基づいて設定されます。

CLI を使用して HTTPOnly 機能を設定します

- HTTPOnly フラグを有効にする

```
set aaa parameter -httpOnlyCookie ENABLED
```

- HttpOnly 機能のステータスを確認してください

```
show aaa parameter
```

制限事項

- HttpOnly機能を有効にすると、Citrix Secure Accessクライアントの［ホームページ］ボタンが機能しません。
- HttpOnly フラグは従来の認証では設定されていません。

VPN ユーザー用のユーザーポータルをカスタマイズする

VPNユーザーにポータルを提供するNetScaler Gateway インストールには、ポータルテーマを選択して、ポータルページのカスタマイズされたルックアンドフィールを作成するオプションが含まれています。提供されているテーマのセットから選択することも、テーマをテンプレートとして使用して、カスタマイズまたはブランド設定されたポータルを構築することもできます。構成ユーティリティーを使用して、新しいロゴ、背景画像、カスタム入力ボックスラベル、および CSS ベースのポータル・デザインのその他のさまざまな属性を追加して、テーマを変更できます。組み込みのポータルテーマには、英語、フランス語、スペイン語、ドイツ語、日本語の 5 つの言語のコンテンツが含まれています。Web ブラウザーによって報告されるロケールに応じて、異なるユーザーが異なる言語で表示されます。

VPN ユーザーがサインインを許可される前に VPN ユーザーに提示されるカスタム EULA を作成できます。EULA 機能は、ロケール固有のバージョンの EULA をサポートします。これは、Web ブラウザーで報告されたロケールに基づいてユーザーに提示されます。

ポータル・テーマと EULA 構成はどちらも、VPN 仮想サーバーと VPN グローバル・レベルで個別にバインドできます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

重要：

Citrix は、コードの変更が必要なカスタマイズをサポートしていません。また、デフォルトのテーマに戻す以外の問題を解決するためのサポートも提供していません。

ポータル・テーマの適用

リリース 13.0 ビルド 67.43 以降、VPN ポータルはデフォルトで RfWebUI テーマを使用するように設定されます。以前は、 `Caxton theme` がデフォルトのテーマでした。緑の吹き出しと X1 のテーマを適用することもできます。

キャクストンのテーマ

グリーンバブルのテーマ

X1のテーマ

提供されているテーマは、VPN 仮想サーバーに直接適用することも、グローバル VPN バインディングとして適用することもできます。

ポータル・テーマを VPN 仮想サーバーにバインドする

ポータル・テーマは、既存の仮想サーバー上にバインドすることも、新しい仮想サーバーを作成する場合にもバインドできます。

CLI を使用してポータル・テーマを VPN 仮想サーバーにバインドする

コマンドプロンプトで次を入力します：

```
bind vpn vserver <name> - portaltheme <name>
```

GUI を使用してポータル・テーマを VPN 仮想サーバーにバインドする

1. ［**構成**］タブで、［**NetScaler Gateway**］に移動し、［**仮想サーバー**］をクリックします。
2. 仮想サーバーを選択し、 をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. ポータル・テーマがまだ仮想サーバーにバインドされていない場合は、詳細ウィンドウの の下にある をクリックします。それ以外の場合、 オプションは詳細ウィンドウですでに展開されています。
4. 詳細ウィンドウの で、 をクリックして ウィンドウを展開します。
5. `Click` **クリックして選択します。**
6. ウィンドウで、テーマ名をクリックし、 をクリックします。
7. **［Bind］** をクリックします。
8. **［完了］** をクリックします。

VPN 仮想サーバーを作成する場合は、 **編集ペインで手順** 3 から始まる前の手順の手順に従って、ポータル・テーマをバインドできます。

ポータル・テーマを VPN グローバルにバインドする

CLI を使用してポータルテーマを VPN グローバルにバインドする

コマンドプロンプトで、「;」と入力します：

```
bind vpn global portaltheme <name>
```

GUI を使用してポータルテーマを VPN グローバルにバインドする

1. **［ 構成 ］** タブで、 **［ NetScaler Gateway］に移動します。**
2. メインの詳細ペインで、 **［ NetScaler Gateway ポリシーマネージャー］** をクリックします。
3. **「+」** アイコンをクリックします。
4. **「 バインドポイント 」** リストで、 **「 リソース」** を選択します。
5. リストで、 を選択します。**
6. **［続行］** をクリックします。
7. **「 バインドポイント」** 画面で、 **「 バインドを追加」** をクリックします。
8. をクリックします。
9. ウィンドウで、テーマ名をクリックし、 をクリックします。
10. **［Bind］** をクリックします。
11. **［閉じる］** をクリックします。
12. **「 完了」をクリックします。**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ヒント：

変更を行った後、コマンドラインで 'save ns config'コマンドを使用するか、構成ユーティリティの保存アイコンをクリックして、変更がNetScaler ADC構成ファイルに保存されていることを確認します。

ポータル・テーマの作成

カスタム・ポータル・デザインを作成するには、提供されているポータル・テーマの 1 つをテンプレートとして使用します。選択したテンプレートテーマのコピーが、指定した名前で作成されます。

ストックポータル・テーマをカスタム・ポータル・テーマのテンプレートとして使用する

ポータル・テーマを作成するには、構成ユーティリティまたはコマンドラインを使用してテーマ・エンティティを作成します。ただし、詳細なカスタマイズコントロールは、構成ユーティリティ内でのみ使用できます。

CLI を使用したポータル・テーマの作成

コマンドプロンプトで、「;」と入力します：

```
add portaltheme <name> basetheme <name>
```

GUI を使用したポータル・テーマの作成

1. ［ **構成** ］タブで、［ **NetScaler Gateway**］ に移動し、［ **ポータルのテーマ**］をクリックします。
2. メインの詳細ペインで、 をクリックします。
3. テーマの名前を入力し、テンプレートリストからテンプレートを選択して、 **「OK」**をクリックします。
4. この時点で、ポータル・テーマの編集ウィンドウが初めて表示されます。 **［OK］** をクリックして終了します。

初回表示で新しいポータル・テーマのカスタマイズに進むことができます。

新しいテーマを作成したら、それを VPN 仮想サーバーまたは VPN グローバルにバインドできます。新しいテーマは、作成直後またはカスタマイズの完了後にバインドできます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ポータル・テーマのカスタマイズ

ポータル・テーマをカスタマイズするには、構成ユーティリティーの Portal Theme インターフェースを使用します。最良の結果を得るには、このインターフェイスのさまざまな要素を理解してから使用する必要があります。

ポータル・テーマ・インターフェースについて

Citrix Gateway **構成ユーティリティでポータルテーマインターフェイスを開くには** 、［ **構成** ］タブで［ **Citrix Gateway** ］に移動し、［ **ポータルテーマ**］をクリックします。「 *ポータル・テーマの作成」の説明に従ってテーマを作成すること* も 、メインの詳細ペインで既存のテーマを選択して「 **編集**」をクリックすることもできます。

ポータル・テーマのカスタマイズ・ページには、ポータル・デザインを変更するための 4 つの主要コンポーネント・ペイン（「 **ポータル・テーマ** 」ペイン、「ルック・アンド・フィール」ペイン、「 **詳細設定** 」ペイン、「 **言語** 」ペイン）があります。



ページ上部の ペインには、編集用にロードされているテーマと、そのベースになっているテンプレートテーマが表示されます。この表示オプションを使用すると、ユーザ接続で VPN にアクセスしなくても、カスタマイズ内容を表示できます。表示オプションを使用するには、テーマを VPN 仮想サーバーにバインドする必要があり、バインディングは表示ウィンドウを閉じた後も有効です。

ページの中央にある ペインを使用して、ヘッダー、背景色とイメージ、フォントプロパティ、ロゴなど、テーマの一般的なプロパティを構成します。このウィンドウが編集モードの場合、属性の凡例を使用して、ポータルページでのルックアンドフィール属性の使用場所に関するガイダンスとして使用できます。

ペインには、個々のポータルページの画面上のコンテンツコントロールが含まれています。ページのコンテンツを編集用に読み込むには、一覧表示されたページの 1 つをクリックします。ページコントロールは、他の中央ペインの下に開きます。ページが変更されていない限り、ポータル・テーマの編集全体にわたって ペインでページが折りたたまれたままになります。

ペインでは、 ペインで編集対象としてページを選択したときにロードされる言語を選択できます。デフォルトでは、英語のページが読み込まれます。

カスタマイズ可能なページ属性のタイプ

ポータル・テーマをカスタマイズする場合、ポータル・テーマ・インターフェースで属性の範囲を変更できます。編集可能なテキストとサポートされている言語に加えて、ポータルのレイアウト

© 1997–2026 Citrix Systems, Inc. All rights reserved.

のグラフィカル要素をニーズに合わせて調整できます。各ページ要素タイプには、変更する前に考慮すべきパラメータまたは推奨事項があります。

ポータルのデザインは、ページの背景、ハイライト、タイトルと本文コンテンツのテキスト、ボタンコントロール、ホバー応答などの属性の色を指定します。カラー属性をカスタマイズするには、選択したアイテムのカラー値を直接入力するか、付属のカラーピッカーを使用してカラー値を生成します。このインターフェイスでは、有効な HTML カラー値を RGBA フォーマット、HTML 16 進トリプレットフォーマット、および X11 カラー名で入力できます。カラーピッカーは、属性の入力フィールドの横にあるカラーボックスをクリックすると、適用可能な任意のカラー属性でアクセスできます。

Fonts

フォントの色に加えて、一部のページ属性のフォントサイズを変更できます。これらの各属性について、ポータルの設計によって決定されるように、各属性で使用できるサイズがメニューに表示されます。

イメージ

画像の場合、各コントロールで使用できるポップアップの説明に、推奨サイズおよびその他の要件が示されます。説明は、ページ上の属性の位置とその機能によって異なります。PNG または JPEG のイメージファイル形式を使用できます。アップロードするイメージを選択するには、アイテムのファイル名の下にあるチェックボックスをオンにし、ローカルコンピュータのドライブ上のイメージの場所を参照します。

ラベル

セクションでは、変更する特定のポータルページのテキストを選択できます。ページのデフォルトの英語テキストを変更しても、他の言語のテキストは再翻訳されません。代替言語のページコンテンツは便宜上提供されていますが、カスタマイズを行う場合は手動で更新する必要があります。ページの別の言語バージョンを編集するには、開いているポータルページの アイコンをクリックして、ウィンドウが開いている場合は、まずウィンドウを折りたたみます。次に、［言語］ペインで言語を選択し**、［**OK］**をクリックします。 ウィンドウから開いたすべてのポータルページは、別の言語を選択するまでその言語で表示されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

重要

高可用性展開またはクラスター展開では、ポータルテーマがプライマリまたは構成コーディネーターのNetScaler ADCエンティティでそれぞれ作成された場合にのみ、共有構成全体にポータルテーマが分散されます。

古いポータルのカスタマイズ

リリース11.0より前のNetScaler Gateway またはAccess Gateway で作成されたカスタムポータル設計を手動で変更してインストールする場合は、カスタマイズインターフェイスで新しいポータルテーマから開始することを強くお勧めします。それができない場合は、カスタマイズを手動で適用できますが、そのための直接的なサポートは提供されません。

手動でカスタマイズしたポータルを使用する場合は、カスタマイズしたポータルをグローバルポータル構成として設定する必要があります。ただし、そうすると、適用されたグローバルポータル構成を VPN *仮想サーバー・レベルのポータル・テーマ・バインディングで上書きすることはできません* 。この場合、構成ユーティリティまたはコマンドラインを使用して VPN 仮想サーバーバインディングを作成しようとすると、エラーが返されます。

また、高可用性およびクラスタ構成の場合、NetScaler ADCファイルシステム上の基礎となるファイルは自動共有構成で配布されないため、展開内のすべてのノードで手動カスタマイズを実行する必要があります。

カスタムポータル構成を手動で作成する

NetScaler Gateway 11.0へのアップグレード後に古いカスタマイズされたポータル構成を手動で適用するには、既存のポータルページのコピーを変更し、カスタマイズされたポータルファイルをNetScaler ADCファイルシステムに配置し、 **UITHEMEパラメーターとしてCUSTOMを選択する必要があります** 。

WinSCPまたはその他のセキュアコピープログラムを使用して、NetScaler ADCファイルシステムにファイルを転送できます。

1. NetScaler Gateway コマンドラインにログオンします。
2. コマンドプロンプトで**shell**と入力します。
3. コマンドプロンプトで、 *mkdir /var/ns_gui_custom; cd /netscaler; tar-cvzf /var/ns_gui_custom/customtheme.tar.gz ns_gui/ と入力します。**
4. コマンドプロンプトで、 **cd /var/netscaler/ログオン/テーマ/**と入力します

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 緑の泡のテーマをカスタマイズする場合は、**cp-r `Greenbubble` Custom** と入力して、緑の泡のテーマのコピーを作成します。
- 既定のテーマ (`Caxton`) をカスタマイズする場合は、 **cp-r 既定のカスタムと入力します。**
- X1 テーマをカスタマイズするには、**cp-r X1 カスタムと入力します。**

5. **/var/NetScaler/Logon/themes/Customにコピーしたファイルに必要な変更を加え** 、テーマを手動でカスタマイズします。
   - **css/base.css**に必要な編集を行います。
   - カスタムイメージを **/var/ns_gui_custom/ns_gui/vpn/media** ディレクトリにコピーします。
   - **resources/** ディレクトリにあるファイルのラベルを変更します。これらのファイルは、ポータルでサポートされるロケールに対応しています。
   - HTML ページまたは JavaScript ファイルへの変更も必要な場合は、 **/var/ns_gui_custom/ns_gui/**内のファイルに関連するものを作成できます。
6. すべてのカスタマイズの変更が完了したら、プロンプトで次のように入力します。 **tar —cvzf /var/ns_gui_custom/customtheme.tar.gz /var/ns_gui_custom/ns_gui/***

重要

前の手順でテーマディレクトリをコピーする場合、NetScaler ADCシェルインターフェイスではディレクトリ名の大文字と小文字が区別されるため、コピーしたフォルダー名は「カスタム」と正確に入力する必要があります。ディレクトリ名を正確に入力しないと、**UITHEME** 設定が **CUSTOM**に設定されているときにフォルダは認識されません。

カスタマイズしたテーマを VPN グローバルパラメータとして選択します

手動でカスタマイズされたポータル構成が完了し、NetScaler ADCファイルシステムにコピーされたら、NetScaler Gateway 構成に適用する必要があります。これは、UITHEME パラメーターを CUSTOM に設定することで実行され、コマンドラインまたは構成ユーティリティで完了できます。

コマンドラインを使用するには、次のコマンドを入力して **UIPHEME** パラメーターを設定します。

```
set vpn parameter UITHEME CUSTOM
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

構成ユーティリティを使用して UITHEME パラメーターを設定するには、以下の手順に従います。

1. 「 **構成** 」タブで、「 **Citrix Gateway」>「グローバル設定」**に移動します。
2. をクリックします。
3. タブをクリックします。
4. 画面の下部までスクロールし、 リストメニューから を選択します。
5. ［**OK**］ をクリックします。

手動でカスタマイズしたポータルが、VPN ユーザーに提示されるポータル設計になりました。

EULA を作成する

VPN ポータルシステムには、ポータル構成に EULA を適用するオプションが用意されています。EULAがVPNグローバルスコープまたは関連するVPN仮想サーバーのいずれかでNetScaler Gateway構成にバインドされると、VPNユーザーはVPNへの認証を許可される前に、利用規約としてのEULAに同意する必要があります。

ポータルのテーマと同様に、ユーザーには、Web ブラウザーによって報告されるロケールに基づいて、言語固有の EULA が提供されます。ロケールがサポートされている言語のいずれとも一致しない場合、提供されるデフォルトの言語は英語です。EULA ごとに、サポートされている各言語でカスタムメッセージを入力できます。翻訳済みのコンテンツは、ポータル・テーマのような EULA 構成には提供されません。ユーザーの報告されたロケールが、EULA コンテンツが入力されていない言語と一致する場合、ユーザーは VPN ログインページの リンクをクリックすると、空白のページが返されます。

EULAを作成するには、構成ユーティリティの［ **構成** ］タブの［NetScaler Gateway］ **>［グローバル設定］>［EULA］または［NetScaler Gateway］****［リソース］>［EULA］**のいずれかのコントロールを使用できます。 ペインのコントロールは、VPN グローバル EULA バインディングの管理に使用され、 > ノードのコントロールは、EULA 設定に関する一般的な操作に使用されます。VPN仮想サーバーのEULAバインディングを管理するには、 **［NetScaler Gateway］>［仮想サーバー］でVPN仮想サーバーを編集します。**一部のコマンドは、EULA エンティティを管理するためのコマンドラインでも使用できます。ただし、完全な EULA 管理コントロールは、構成ユーティリティでのみ使用できます。

CLI を使用して EULA エンティティを作成する

コマンドプロンプトで次を入力します：

```
add vpn eula <name>
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

GUI を使用して EULA エンティティを作成する

1. ［**NetScaler Gateway** > ［リソース］ > ［**EULA**］に移動します。
2. をクリックして、エンティティを作成します。
3. エンティティの名前を入力します。
4. 各言語について、関連するタブの下にコンテンツを貼り付けます。プレーンテキストまたは HTML タグを使用して、 改行を追加する`<br>`タグを含め、コンテンツの書式を設定することができます。
5. ［**Create**］ をクリックします。

EULA エンティティが作成されると、VPN 設定にグローバルにバインドすることも、VPN 仮想サーバーにバインドすることもできます。

CLI を使用して EULA を VPN グローバルにバインドする

コマンドプロンプトで、「;」と入力します：

```
bind vpn global eula <name>
```

GUI を使用して EULA を VPN グローバルにバインドする

1. 「 **構成** 」タブで、「 **Citrix Gateway」>「グローバル設定」**に移動します。
2. メインの詳細ウィンドウで、 をクリックします。
3. ［**Add Binding**］ をクリックします。
4. をクリックします。
5. EULA エンティティを選択し、 をクリックします。
6. ［**Bind**］ をクリックします。
7. ［**閉じる**］ をクリックします。

CLI を使用して EULA を VPN 仮想サーバーにバインドする

コマンドプロンプトで、「;」と入力します：

```
bind vpn vserver <name> eula <name>
```

GUI を使用して EULA を VPN 仮想サーバーにバインドする

1. ［ **構成** ］タブで、［ **NetScaler Gateway**］ > ［**仮想サーバー**］ **の順に選択します。**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. メインの詳細ペインで、VPN 仮想サーバーを選択し、 をクリックします。
3. ページの右側にある ペインで、 をクリックします。
4. 新しく追加された EULA ペインで、 をクリックします。
5. `Click` **クリックして選択します。**
6. EULA エンティティを選択し、 をクリックします。
7. **［Bind］** をクリックします。
8. **［完了］** をクリックします。

カスタムページを作成して、古いブラウザまたはサポートされていないブラウザをアップグレードするようにユーザに促す

クライアントがSSLv3などの安全でない暗号を使用してNetScaler VIPアドレスに接続すると、クライアントはカスタムページにリダイレクトされ、Internet Explorer、Firefox、Chrome、またはSafariの最新バージョンにアップグレードするように求められます。

注: インターネット技術タスクフォース (ITEF) の RFC6176 によると、TLS サーバーは SSLv2 をサポートしてはなりません。したがって、NetScalerアプライアンスはリリース12.1以降のSSLv2をサポートしていません。

SSLに基づいてサポートされていない古いブラウザをアップグレードするようにユーザーに促すカスタムページを作成する方法

- ルール`client.ssl.version.eq()`を使用してNetScalerレスポンダーポリシーを作成します。バージョンは SSL プロトコルのバージョンを返します。
  - トランザクションが SSL ベースでない場合は 0 を返します。
  - トランザクションが SSLv2 の場合は 0x002 を返します。
  - トランザクションが SSLv3 の場合は 0x300 を返します。
  - トランザクションが TLSv1 の場合は 0x301 を返します。
- レスポンダーポリシーをトリガーするには、SSLv3（またはその他の以前のバージョン）を有効にする必要があります。

  たとえば、NetScalerアプライアンスでSSLv3が無効になっていて、SSLv3を使用する古いブラウザーを使用しているクライアントが接続を試みると、アクセスは拒否されます。
- 導入環境で SSLv3 またはそれ以前のバージョンを指定期間（1 か月または 2 か月）に必要とする場合は、次の設定を行います：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- SSLv3 プロトコルを有効にします。
- カスタムページを更新して、指定した期間が過ぎると、ブラウザがアプライアンスに接続できないという情報を含めます。

NetScaler Gateway でクライアントレスVPNアクセスを構成する

クライアントレスアクセスにより、ユーザーは、NetScaler Gateway プラグインやReceiverなどのユーザーソフトウェアをインストールしなくても、必要なアクセスが可能になります。ユーザーは Web ブラウザを使用して、Outlook Web Access などの Web アプリケーションに接続できます。

クライアントレスアクセスを設定するには、次の手順を実行します。

- グローバルに、またはユーザー、グループ、または仮想サーバーにバインドされたセッションポリシーを使用して、クライアントレスアクセスを有効にします。
- Web アドレスのエンコード方式の選択。

特定の仮想サーバに対してのみクライアントレスアクセスを有効にするには、クライアントレスアクセスをグローバルに無効にしてから、それを有効にするセッションポリシーを作成します。

NetScaler Gateway ウィザードを使用してアプライアンスを構成する場合は、ウィザード内でクライアントレスアクセスを構成するかどうかを選択できます。ウィザードの設定はグローバルに適用されます。NetScaler Gateway ウィザードでは、次のクライアント接続方法を構成できます。

- NetScaler Gateway プラグイン。ユーザーは、NetScaler Gateway プラグインを使用してのみログオンできます。
- NetScaler Gateway プラグインを使用し、アクセスシナリオのフォールバックを許可します。ユーザーは、NetScaler Gateway プラグインを使用してNetScaler Gateway にログオンします。ユーザデバイスがエンドポイント分析スキャンに失敗した場合、ユーザはクライアントレスアクセスを使用してログオンすることが許可されます。これが発生すると、ユーザーはネットワークリソースへのアクセスが制限されます。
- ユーザが Web ブラウザとクライアントレスアクセスを使用してログオンできるようにします。ユーザはクライアントレスアクセスを使用してのみログオンでき、ネットワークリソースへのアクセスは制限されます。

クライアントレス VPN アクセスポリシーの仕組み

Web アプリケーションへのクライアントレスアクセスを設定するには、ポリシーを作成します。クライアントレスアクセスポリシーの設定は、構成ユーティリティで構成できます。クライアント

© 1997–2026 Citrix Systems, Inc. All rights reserved.

レスアクセスポリシーは、ルールとプロファイルで構成されます。NetScaler Gateway に付属する事前構成済みのクライアントレスアクセスポリシーを使用できます。また、独自のカスタムクライアントレスアクセスポリシーを作成することもできます。

NetScaler Gateway には、次の事前構成されたポリシーが用意されています。

- Outlook Web Access と Outlook Web アプリケーション
- SharePoint 2007
- その他すべての Web アプリケーション

注:

OWA 2016 および SharePoint 2016 は、高度なクライアントレスアクセスを使用する場合にのみサポートされます。

事前設定されたクライアントレスアクセスポリシーの次の特性に留意してください。

- これらは自動的に設定され、変更できません。
- 各ポリシーはグローバルレベルでバインドされます。
- クライアントレスアクセスをグローバルに有効にするか、セッションポリシーを作成しない限り、各ポリシーは適用されません。
- クライアントレスアクセスを有効にしない場合でも、グローバルバインディングを削除または変更することはできません。

他のWebアプリケーションのサポートは、NetScaler Gateway で構成する書き換えポリシーによって異なります。作成したカスタムポリシーをテストして、アプリケーションのすべてのコンポーネントが正常に書き換えられるようにすることをお勧めします。

Receiver for Android、Receiver for iOS、またはCitrix Secure Hubからの接続を許可する場合は、クライアントレスアクセスを有効にする必要があります。iOSデバイス上で動作するCitrix Secure Hubの場合は、セッションプロファイル内でSecure Browse も有効にする必要があります。Secure Browse クライアントレスアクセスが連携して、iOS デバイスからの接続を許可します。ユーザーが iOS デバイスに接続しない場合は、Secure Browse を有効にする必要はありません。

クイック設定ウィザードは、モバイルデバイスの正しいクライアントレスアクセスポリシーと設定を構成します。クイック構成ウィザードを実行して、StoreFront およびCitrix Endpoint Managementへの接続に関する正しいポリシーを構成することをお勧めします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

カスタムクライアントレスアクセスポリシーは、グローバルにバインドすることも、仮想サーバにバインドすることもできます。クライアントレスアクセスポリシーを仮想サーバにバインドする場合は、カスタムポリシーを作成してバインドする必要があります。クライアントレスアクセスに対してグローバルまたは仮想サーバに対して異なるポリシーを適用するには、カスタムポリシーのプライオリティ番号を変更して、カスタムポリシーのプライオリティ番号を事前設定されたポリシーよりも小さくします。これにより、カスタムポリシーのプライオリティが高くなります。仮想サーバに他のクライアントレスアクセスポリシーがバインドされていない場合は、事前設定されたグローバルポリシーが優先されます。

注:

事前設定されたクライアントレスアクセスポリシーのプライオリティ番号は変更できません。

クライアントレス VPN アクセスを有効にする

グローバルレベルでクライアントレスアクセスを有効にすると、すべてのユーザがクライアントレスアクセスの設定を受け取ります。NetScaler Gateway ウィザード、グローバルポリシー、またはセッションポリシーを使用して、クライアントレスアクセスを有効にすることができます。

グローバル設定またはセッションプロファイルでは、クライアントレスアクセスには次の設定があります。

- **オン**。クライアントレスアクセスを有効にします。クライアントの選択を無効にし、StoreFront を構成または無効にしない場合、ユーザーはクライアントレスアクセスを使用してログオンします。
- **オフ**。クライアントレスアクセスは、デフォルトでは有効になっていません。クライアントレスアクセスは、ユーザーがNetScaler Gateway プラグインでログオンした後に有効になります。クライアントの選択を無効にし、StoreFront を構成または無効にしない場合、ユーザーは NetScaler Gateway プラグインを使用してログオンします。ユーザがログオンしたときにエンドポイント分析が失敗した場合、ユーザにはクライアントレスアクセスが可能な選択肢ページが表示されます。
- **無効**。クライアントレスアクセスは無効です。 を選択すると、ユーザはクライアントレスアクセスを使用してログオンできず、クライアントレスアクセスのアイコンは選択ページに表示されません。

NetScaler Gateway ウィザードを使用してクライアントレスアクセスを有効にしない場合は、グローバルに、または構成ユーティリティを使用してセッションポリシーで有効にすることができます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

クライアントレスアクセスをグローバルに有効にするには

1. 構成ユーティリティの［構成］タブのナビゲーションペインで、［Citrix Gateway］を展開し、［ **グローバル設定**］をクリックします。
2. 詳細ペインの で、 をクリックします。
3. ［ **クライアントエクスペリエンス** ］タブで、［ **クライアントレスアクセス**］の横にある［ **オン**］**を選択し、** ［ **OK**］**をクリックします。

セッションポリシーを使用してクライアントレスアクセスを有効にするには

選択したユーザ、グループ、または仮想サーバのグループだけにクライアントレスアクセスを使用する場合は、クライアントレスアクセスをグローバルに無効またはクリアします。次に、セッションポリシーを使用して、クライアントレスアクセスを有効にし、ユーザー、グループ、または仮想サーバーにバインドします。

1. 構成ユーティリティの［構成］タブのナビゲーションペインで、［ **NetScaler Gateway**］**> ［ポリシー］>［セッション］の順に展開します。**
2. 詳細ペインの タブで、 をクリックします。
3. ** に、ポリシーの名前を入力します。
4. 「 **リクエストプロファイル**」の横にある「 **新規**」をクリックします。
5. ** に、プロファイルの名前を入力します。
6. タブの **の横にある をクリックし、 を選択**して ** をクリックします。
7. ダイアログボックスで、 の横にある を選択し、 を選択し、 をクリックして をクリックし、** をクリックします。
8. をクリックし、** をクリックします。

クライアントレスアクセスを有効にするセッションポリシーを作成したら、ユーザー、グループ、または仮想サーバーにバインドします。

Web アドレスをエンコードする

クライアントレスアクセスを有効にすると、内部 Web アプリケーションのアドレスをエンコードするか、アドレスをクリアテキストのままにしておくかを選択できます。設定は次のとおりです。

- あいまい。これは、標準のエンコーディングメカニズムを使用して、リソースのドメインとプロトコル部分を隠します。
- 。Web アドレスはエンコードされず、ユーザーに表示されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 暗号化。ドメインとプロトコルは、セッションキーを使用して暗号化されます。Web アドレスが暗号化されている場合、同じ Web リソースのユーザセッションごとに URL が異なります。ユーザがエンコードされた Web アドレスをブックマークし、Web ブラウザに保存してからログオフすると、ユーザがログオンし、ブックマークを使用して再度 Web アドレスに接続しようとすると、Web アドレスに接続できなくなります。 注:ユーザーがセッション中に暗号化されたブックマークをAccess Interfaceに保存すると、ユーザーがログオンするたびにブックマークが機能します。

この設定は、グローバルに構成することも、セッションポリシーの一部として構成することもできます。セッションポリシーの一部としてエンコーディングを構成する場合は、ユーザー、グループ、または仮想サーバーにバインドできます。

Web アドレスエンコーディングをグローバルに構成する

1. ナビゲーションペインにある、［Configuration］タブの構成ユーティリティで、［NetScaler Gateway］を展開し、［Global Settings］をクリックします。
2. 詳細ペインの で、 をクリックします。
3. ［クライアントエクスペリエンス］タブで、［クライアントレスアクセス URL エンコーディング］の横にあるエンコーディングレベルを選択し、［OK］をクリックします。

セッションポリシーを作成して Web アドレスエンコーディングを構成する

1. 構成ユーティリティの［構成］タブのナビゲーションペインで、［ **NetScaler Gateway**］> **［ポリシー** ］を展開し、［セッション］をクリックします。
2. 詳細ペインの タブで、 をクリックします。
3. に、ポリシーの名前を入力します。
4. 「リクエストプロファイル」の横にある「 新規」をクリックします。
5. に、プロファイルの名前を入力します。
6. 「 クライアントエクスペリエンス 」タブで、「 クライアントレスアクセス URL エンコーディング」の横にある「 グローバルオーバーライド」をクリックし、エンコードレベルを選択して「 OK」をクリックします。
7. ダイアログボックスで、 の横にある を選択し、 を選択し、 をクリックして をクリックし、 をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

クライアントレスアクセスポリシーの作成

デフォルトのクライアントレスアクセスポリシーと同じ設定を使用したいが、ポリシーを仮想サーバにバインドする場合は、デフォルトのポリシーをコピーして、ポリシーの新しい名前を指定できます。構成ユーティリティを使用して、デフォルトポリシーをコピーできます。

新しいポリシーを仮想サーバーにバインドした後、ユーザーがログオンしたときに最初に実行されるように、ポリシーの優先順位を設定できます。

デフォルト設定を使用してクライアントレスアクセスポリシーを作成する

1. 構成ユーティリティのナビゲーションペインで、［**Citrix Gateway**］ **>** ［**ポリシー** ］を展開し、［クライアントレスアクセス］をクリックします。
2. 詳細ウィンドウの タブで、既定のポリシーをクリックし、 をクリックします。
3. にポリシーの新しい名前を入力し、、 の順にクリックします。

クライアントレスアクセスポリシーを仮想サーバにバインドする

ポリシーを作成したら、そのポリシーを仮想サーバーにバインドします。

1. 構成ユーティリティの［構成］タブのナビゲーションペインで、［ NetScaler Gateway ］を展開し、［ 仮想サーバー］をクリックします。
2. 詳細ペインで仮想サーバーを選択し、 をクリックします。
3. ［NetScaler Gateway 仮想サーバーの構成］ダイアログボックスで、［ポリシー］タブをクリックし、［クライアントレス］をクリックします。
4. 「ポリシーの挿入」をクリックし、リストからポリシーを選択して、「OK」をクリックします。

クライアントレスアクセスポリシー式の作成と評価

クライアントレスアクセス用のポリシーを作成する場合、ポリシーの独自の式を作成できます。エクスプレッションの作成が完了したら、エクスプレッションの精度を評価できます。

1. 構成ユーティリティのナビゲーションペインで、［**Citrix Gateway**］ **>** ［**ポリシー** ］を展開し、［クライアントレスアクセス］をクリックします。
2. 詳細ウィンドウの タブで、既定のポリシーをクリックし、 をクリックします。
3. に、ポリシーの名前を入力します。
4. の横にある をクリックします。
5. に、プロファイルの名前を入力します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

6. 書き換え設定を構成し、 をクリックします。
7. ダイアログボックスの で、 をクリックします。
8. 「式の追加」ダイアログ・ボックスで、式を作成し、「OK」をクリックします。
9. ダイアログボックスで、 をクリックし、式が正しいとテストされたら、 をクリックします。

NetScaler Gateway を使用した高度なクライアントレス VPN アクセス

クライアントレスVPNは、クライアントマシンにVPNクライアントアプリケーションを使用せずに、NetScaler Gateway を介して企業のイントラネットリソースへのリモートアクセスを提供する方法を認識します。クライアントレス VPN は、クライアント側の Web ブラウザを使用して、エンタープライズ Web アプリケーション、ポータル、およびその他のリソースへのリモートアクセスを提供します。 高度なクライアントレス VPN ソリューションにより、クライアントレス VPN に関する次の制限が排除されます。

- 相対 URL は時々識別できません。
- 動的に生成された相対 URL は識別できません。

高度なクライアントレス VPN は、絶対 URL とホスト名を識別し、HTTP-Respones/Web ページに存在する相対 URL を書き換えるのではなく、新しいユニークな方法でそれらを書き換えます。SharePoint では、URL の書き換えに既定のフォルダーを使用する必要がなくなり、カスタム SharePoint アクセスがサポートされます。

前提条件

次に、高度なクライアントレス VPN を設定するための前提条件を示します。

- **ワイルドカードサーバー証明書** -高度なクライアントレス VPN は独自の方法で URL を書き換えます。この一意性は、ユーザーごとのすべての URL で維持されます。たとえば、Web アプリケーションが `https://webapp.customer.com` でホストされ 、VPN 仮想サーバが `https://vpn.customer.com` でホストされている場合 、高度なクライアントレス VPN はそれを `https://cvpneqwerty.vpn.customer.com` として書き換えます。つまり、すべての URL は VPN 仮想サーバーのサブドメインとして書き換えられます。この新しい URL では、`cvpneqwerty` を `https://webapp.customer.com` に復号化できます。文字列 `cvpneqwerty` は動的であるため、SSL の場合は、ワイルドカード証明書を使用して VPN 仮想サーバをバインドする必要があります。

  サーバがでホストされている場合 `https://vpn.customer.com`、サーバ証明書には、証明書 CN または SAN（CN=共通名、SAN= サブジェクト代替名）の一部として（vpn.customer.com および.vpn.customer.com）のエントリが必要です。この証明書をバインドするプロセスは、NetScaler Gateway でも同じです。 **注:** ワイルドカード証明書は、1 レベル (つまり、

© 1997–2026 Citrix Systems, Inc. All rights reserved.

..customer.com は許可されていません)。すでにワイルドカード証明書（*.customer.com 用）を使用して`https://vpn.customer.com`をホスティングしている場合、これは高度なクライアントレス VPN では機能しません。`*.vpn.customer.com`で新しい証明書を取得する必要があります。

- **ワイルドカード DNS エントリ** -クライアント（Web ブラウザ）は、高度なクライアントレス VPN アプリケーションの FQDN を解決する必要があります。NetScaler Gateway サーバーをセットアップするときに、vpn.customer.comを解決するためにDNSエントリを構成しておく必要があります。これにより、ブラウザは vpn.customer.com を VPN 仮想サーバーの IP アドレスに解決できます。`https://cvpnqwerty.vpn.customer.com`のようなURLを同じ IP (VPN) 仮想サーバーの IP アドレスに解決するには、`vpn.customer.com`のメインの新しいレコードを追加する必要があります。DNS サーバーでドメイン設定を見つけ、以前と同じ IP アドレスを持つ「*」の新しいホストレコードを追加します。ホストレコードを追加したら、`https://cpvnanything.vpn.customer.com`の正常な ping 応答を確認する必要があります。

高度なクライアントレス VPN アクセスの設定

コマンドラインインターフェイスを使用して高度なクライアントレス VPN アクセスを設定するには、コマンドプロンプトで次のように入力します。

```
set vpn parameter -clientlessVpnMode ON

set vpn parameter -advancedClientlessVpnMode ENABLED
```

セッションアクションが仮想サーバにバインドされている場合は、そのセッションアクションに対して高度なクライアントレス VPN モードオプションも有効にする必要があります。

例:

```
set vpn sessionaction SessionActionName -advancedclientlessvpn ENABLED
```

NetScaler ADC GUIを使用して高度なクライアントレスVPNアクセスを構成するには：

1. NetScaler GUIで、［**構成**］>［**Citrix NetScaler**］>［**グローバル設定**］の順に移動します。
2. 「**グローバル設定**」ページで、「**グローバル設定の変更**」をクリックし、「クライアントエクスペリエンス」タブを選択します。
3. タブの リストで、 をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. タブの リストで、 をクリックします。 **高度なクライアントレスVPNモードのリストから STRICTを選択すると** 、Citrix ADCアプライアンスは従来のクライアントレスVPN形式の StoreFront URLにのみ応答し、他のすべての従来のクライアントレスVPN要求をブロックします。このオプションは、内部 Web リソースを配信するための、アプライアンスのより安全な設定を提供します。

注：

- セッションアクションが仮想サーバーにバインドされている場合は、［**NetScaler Gateway セッションプロファイルの構成**］ページの［**クライアントエクスペリエンス**］**タブから、そのセッションアクションの［高度なクライアントレスVPNモード**］オプションを有効にする必要があります。
- オプションを選択すると、グローバル設定をオーバーライドできます。
- 高度なクライアントレス VPN 機能は、セッションレベルでも設定できます。

注意事項

高度なクライアントレス VPN は、エンタープライズ Web アプリケーションへのアクセスを提供することを目的としています。このようなアプリには、必要なすべての種類のリソース（JavaScript、CSS、画像など）に対して FQDN が 1 つしかありません。内部アプリケーションの完全な FQDN をシングルオクテット（クライアントレス VPN）にエンコードするため、サブドメインの関係が失われます。その結果、エンタープライズ WebApp を CORS で設定すると、高度なクライアントレス VPN 経由でアクセスする際に問題が発生することがあります。

ユーザーのドメインアクセスを構成する

ユーザがクライアントレスアクセスを使用して接続する場合、ユーザがアクセスを許可するネットワークリソース、ドメイン、および Web サイトを制限できます。NetScaler Gateway ウィザードまたはグローバル設定を使用して、ドメインへのアクセスを含めるか除外するリストを作成できます。

すべてのネットワークリソース、ドメイン、および Web サイトへのアクセスを許可してから、除外リストを作成できます。除外リストは、ユーザーがアクセスを許可されていない特定のリソースセットを引用しています。ユーザーは、除外リストに含まれるドメインにはアクセスできません。

また、すべてのネットワークリソース、ドメイン、および Web サイトへのアクセスを拒否し、特定の包含リストを作成することもできます。包含リストには、ユーザーがアクセスできるリソースを挙げています。ユーザーは、リストに表示されていないドメインにはアクセスできません。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注：Citrix Endpoint ManagementまたはStoreFront のクライアントレスアクセスポリシーを構成し、ユーザーがReceiver for Webに接続する場合は、Receiver for Webがアクセスできるドメインを許可する必要があります。これは、NetScaler Gateway がStoreFront およびEndpoint Managementのネットワークトラフィックを書き換えるために必要です。

NetScaler Gateway ウィザードを使用してドメインアクセスを構成するには

1. 構成ユーティリティで、［構成］タブをクリックし、ナビゲーションペインで［ NetScaler Gateway］をクリックします。
2. 詳細ペインの［はじめに］で、［ NetScaler Gateway ウィザード］をクリックします。
3. をクリックし、 ページが表示されるまで、ウィザードの指示に従います。
4. をクリックし、次のいずれかを実行します。
   - 除外するドメインのリストを作成するには、 をクリックします。
   - 含まれるドメインのリストを作成するには、 をクリックします。
5. にドメイン名を入力し、 をクリックします。
6. リストに追加するドメインごとにステップ 5 を繰り返し、完了したら OK をクリックします。
7. NetScaler Gateway ウィザードを使用して、アプライアンスの構成を続行します。

構成ユーティリティを使用してドメイン設定を構成するには

構成ユーティリティのグローバル設定を使用して、ドメインリストを作成または変更することもできます。

1. ナビゲーションペインにある、［Configuration］タブの構成ユーティリティで、［NetScaler Gateway］を展開し、［Global Settings］をクリックします。
2. 詳細ペインの で、 をクリックします。
3. 次のいずれかを行います：
   - 除外するドメインのリストを作成するには、 をクリックします。
   - 含まれるドメインのリストを作成するには、 をクリックします。
4. にドメイン名を入力し、 をクリックします。
5. リストに追加するドメインごとにステップ 4 を繰り返し、完了したら OK をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SharePoint 2003、SharePoint 2007、およびSharePoint 2013のクライアントレス VPN アクセス

NetScaler Gateway は、1つ以上のSharePoint 2003、SharePoint 2007、またはSharePoint 2013サイトのコンテンツを書き直して、NetScaler Gatewayプラグインを必要とせずにユーザーがコンテンツを利用できるようにします。書き換えプロセスを正常に完了するには、ネットワーク内の各SharePointサーバーのホスト名を使用してNetScaler Gateway を構成する必要があります。

NetScaler Gateway ウィザードまたは構成ユーティリティを使用して、SharePointサイトのホスト名を構成できます。

NetScaler Gateway ウィザードで、ウィザード内を移動して設定を構成します。 ページが表示されたら、SharePoint サイトの Web アドレスを入力し、 をクリックします。

NetScaler Gateway ウィザードの実行後に初めてWebサイトを追加したり、SharePointを構成したりするには、構成ユーティリティを使用します。

重要：

クラシッククライアントレスアクセスは、SharePoint 2013 と OWA 2013 までのバージョンをサポートしています。アドバンストクライアントレスアクセスは、SharePoint 2016 と OWA 2016、およびそれ以降のバージョンをサポートします。

NetScaler ADC GUIを使用してSharePointのクライアントレスアクセスを構成する

1. **NetScaler Gateway** > **グローバル設定**に 移動します。
2. 詳細ウィンドウの で、 をクリックします。
3. の に、SharePoint サイトのホスト名を入力し、 をクリックします。
4. リストに追加する SharePoint サイトごとに手順 3 を繰り返し、完了したら **「OK」** をクリックします。

SharePoint サイトをホームページとして設定する

SharePoint サイトをユーザーのホームページとして設定する場合は、セッションプロファイルを構成し、SharePoint サイトのホスト名を入力します。

SharePoint サイトをホームページとして構成するには

1. ［**NetScaler Gateway**］>［**ポリシー**］に移動し、 ［**セッション**］をクリックします。
2. 詳細ペインで、 をクリックします。
3. ** に、ポリシーの名前を入力します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. 「**リクエストプロファイル**」の横にある「**新規**」をクリックします。
5. に、プロファイルの名前を入力します。
6. タブの の横にある をクリックし、** SharePoint サイトの名前を入力します。
7. の横にある をクリックし、 を選択して、** をクリックします。
8. ダイアログボックスで、 の横にある を選択し、 を選択し、 をクリックして をクリックし、 をクリックします。

セッションポリシーを完了したら、ユーザー、グループ、仮想サーバーに、またはグローバルにバインドします。ユーザーがログオンすると、SharePoint Web サイトがホームページとして表示されます。

SharePoint 2007 サーバーの名前解決を有効にする

SharePoint 2007 サーバーは、構成されたサーバー名をホスト名としてさまざまな URL 内の応答の一部として送信します。構成されたSharePointサーバー名が完全修飾ドメイン名（FQDN）でない場合、NetScaler Gateway はSharePointサーバー名を使用してIPアドレスを解決できず、一部のユーザー関数はエラーメッセージ「HTTP: 1.1 Gateway Timeout」でタイムアウトします。これらの機能には、ファイルのチェックインとチェックアウト、ワークスペースの表示、およびユーザーがクライアントレスアクセスを使用してログオンしているときの複数のファイルのアップロードが含まれます。

この問題を解決するには、次のいずれかを試してください。

- 名前解決の前にSharePointホスト名がFQDNに変換されるように、NetScaler Gateway でDNSサフィックスを構成します。
- すべてのSharePointサーバー名に対して、NetScaler Gateway のローカルDNSエントリを構成します。
- すべての SharePoint サーバー名を変更して、完全修飾ドメイン名を使用します。たとえば、SharePoint の代わりに SharePoint.intranetDomain のように、

DNS サフィックスを構成する

1. 構成ユーティリティの タブのナビゲーションペインで、 を展開し、 をクリックします。
2. 詳細ペインで、 をクリックします。
3. に、サフィックスとしてイントラネットドメイン名を入力し、、 の順にクリックします。

追加するドメインごとにステップ 3 を繰り返すことができます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler Gateway 上のすべてのSharePointサーバー名のローカルDNSレコードを構成するには

1. 構成ユーティリティのナビゲーションウィンドウで、 > を展開し、 をクリックします。
2. 詳細ペインで、 をクリックします。
3. ****に、DNS アドレスレコードの SharePoint ホスト名を入力します。
4. に、SharePoint サーバーの IP アドレスを入力し、、、 の順にクリックします。

A レコードを追加するホスト名には、CNAME レコードがあってはなりません。また、アプライアンスに重複した A レコードが存在することはできません。

クライアントレス VPN アクセスパーシステント Cookie を有効にする

永続的なクッキーは、SharePoint サーバーでホストされている Microsoft Word、Excel、および PowerPoint ドキュメントを開いて編集するなど、SharePoint の特定の機能にアクセスするために必要です。

永続的な Cookie はユーザーデバイス上に残り、HTTP 要求ごとに送信されます。NetScaler Gateway は、永続Cookieをユーザーデバイス上のプラグインに送信する前に暗号化し、セッションが存在する限り、Cookieを定期的に更新します。セッションが終了すると、Cookie は古くなります。

NetScaler Gateway ウィザードでは、管理者は永続クッキーをグローバルに有効にすることができます。セッションポリシーを作成して、ユーザー、グループ、または仮想サーバーごとに永続的な Cookie を有効にすることもできます。

パーシステント Cookie では、次のオプションを使用できます。

- はパーシステント Cookie を有効にし、ユーザーは SharePoint に保存されている Microsoft ドキュメントを開いて編集できます。
- は永続的な Cookie を無効にし、ユーザーは SharePoint に保存されている Microsoft ドキュメントを開いたり編集したりできなくなります。
- は、セッション中に永続的な Cookie を許可または拒否するようにユーザーに求めます。

ユーザーが SharePoint に接続しない場合、クライアントレスアクセスには永続的な Cookie は必要ありません。

SharePoint のクライアントレス VPN アクセス用の永続クッキーを構成する

SharePoint のクライアントレスアクセス用の永続的な Cookie は、グローバルに、またはセッションポリシーの一部として構成できます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

パーシステント Cookie をグローバルに設定するには

1. ナビゲーションペインにある、［Configuration］タブの構成ユーティリティで、［NetScaler Gateway］を展開し、［Global Settings］をクリックします。
2. 詳細ペインの で、 をクリックします。
3. ［クライアントエクスペリエンス］タブで、［クライアントレスアクセス永続的 Cookie］の横にあるオプションを選択し、［OK］をクリックします。

セッションポリシーの一部としてパーシステント Cookie を設定するには

1. 構成ユーティリティの［構成］タブのナビゲーションペインで、［ **NetScaler Gateway**］> **［ポリシー** ］を展開し、［セッション］をクリックします。
2. 詳細ペインの タブで、 をクリックします。
3. に、ポリシーの名前を入力します。
4. 「リクエストプロファイル」の横にある「 新規」をクリックします。
5. に、プロファイルの名前を入力します。
6. タブで、 の横にある をクリックし、オプションを選択して、 をクリックします。
7. ダイアログボックスで、 の横にある 、、、、 の順にクリックします。

Web Interface を介したクライアントレスアクセスのユーザ設定の保存

ユーザーがクライアントレスアクセスを使用してWeb Interfaceにログオンしてログオフすると、ユーザーが複数回ログオンしたときにCookieが永続的であっても、NetScaler Gateway は前のセッションで設定されたクライアント消費Cookieを転送しません。GUI または CLI を使用して、Cookie をクライアント Cookie のパターンセットにバインドし、セッション間の Web Interface 設定を保持できます。

構成ユーティリティを使用して Web インターフェイス永続性の Cookie をバインドするには

1. 構成ユーティリティの［構成］タブで、［ **NetScaler Gateway**］> **［ポリシー** ］の順に展開し、［ **クライアントレスアクセス**］をクリックします。
2. 右側のペインの タブで、 をクリックします。
3. ダイアログボックスの に、ポリシーの名前を入力します。
4. の横にある をクリックします。
5. に、プロファイルの名前を入力します。
6. タブの で、 を選択し、 をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

7. ダイアログボックスの 領域の に、次のパラメータを入力します：
   - `WIUser` 次に、 をクリックします。
   - `WINGDevice` 次に、 をクリックします。
   - `WINGSession` 次に、 をクリックします。
8. 「**OK**」 をクリックし、「**作成**」をクリックします。
9. ダイアログボックスの に「true」と入力し、、 の順にクリックします。

コマンドラインを使用して Web インターフェイスの永続性のために Cookie をバインドするには

1. PuTTYなどのセキュアシェル（SSH）接続を使用して、NetScaler Gateway コマンドラインにログオンします。
2. コマンドプロンプトで、shell と入力します。
3. コマンドプロンプトで、次のコマンドを入力します。

```
bind policy patset ns_cvpn_default_client_cookies WIUser

bind policy patset ns_cvpn_default_client_cookies WINGDevice

bind policy patset ns_cvpn_default_client_cookies WINGSession
```

4. **Enter**キーを押します。

モバイルデバイス用のCitrix SSO VPNクライアント

Citrix SSOは、モバイルデバイス（macOS、iOS、iOS）用のVPNクライアントです。Citrix SSOは、macOS、iOS、およびAndroidで完全なモバイルデバイス管理（MDM）サポートを提供します。MDM サーバーを使用すると、管理者はデバイスレベルの VPN プロファイルとアプリごとの VPN プロファイルをリモートで構成および管理できます。 Citrix SSOは、一般的に使用される機能のほとんどもサポートしています。

参照ドキュメント

- NetScaler Gatewayクライアント
- NetScaler Gateway VPNクライアントとサポートされる機能

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ページの設定

NetScaler Gateway を構成して、ユーザーに複数のログオンオプションを提供できます。クライアント選択ページを構成すると、ユーザーは 1 つの場所から次の選択肢を使用してログオンできます。

- Windows向けNetScaler Gatewayプラグイン
- macOS X向けNetScaler Gatewayプラグイン
- Java向けNetScaler Gateway プラグイン
- StoreFront
- Web Interface
- クライアントレスアクセス

ユーザーは、NetScaler Gateway または仮想サーバーにバインドされた証明書のWebアドレスを使用してNetScaler Gateway にログオンします。セッションポリシーとプロファイルを作成すると、ユーザーが受け取るログオンの選択肢を決定できます。NetScaler Gateway の構成方法に応じて、［クライアントの選択］ページには、次のログオンの選択肢を表す最大3つのアイコンが表示されます。

- ネットワークアクセス。ユーザーがWebブラウザーを使用してNetScaler Gateway に初めてログオンし、［ネットワークアクセス］を選択すると、ダウンロードページが表示されます。ユーザーが をクリックすると、プラグインがダウンロードされ、ユーザーデバイスにインストールされます。ダウンロードとインストールが完了すると、Access Interfaceが表示されます。新しいをインストールするか、古いバージョンのNetScaler Gateway に戻すと、Windows向けNetScaler Gateway プラグインは、アプライアンスのバージョンにサイレントにアップグレードまたはダウングレードします。ユーザーがMac向けNetScaler Gateway プラグインを使用して接続する場合、ユーザーのログオン時に新しいアプライアンスのバージョンが検出されると、プラグインはサイレントにアップグレードします。このバージョンのプラグインは、サイレントにダウングレードしません。
- Web InterfaceまたはStoreFront。ユーザーがログオンする Web インターフェイスを選択すると、 ページが表示されます。ユーザーは、公開アプリケーションまたは仮想デスクトップにアクセスできます。ユーザーがStoreFront を選択してログオンすると、Receiverが開き、ユーザーはアプリケーションとデスクトップにアクセスできます。 注：StoreFront をクライアントの選択肢として構成した場合、アプリケーションとデスクトップはAccess Interfaceの左ペインに表示されません。
- クライアントレスアクセス。ユーザがクライアントレスアクセスを選択してログオンすると、Access Interfaceまたはカスタマイズされたホームページが表示されます。Access Interfaceで

© 1997–2026 Citrix Systems, Inc. All rights reserved.

は、ユーザーはファイル共有、Web サイトに移動したり、Outlook Web Access を使用したりできます。

ユーザーがJava向けCitrix Gateway プラグインを選択すると 、プラグインが起動し、ユーザーはログオンします。選択肢ページは表示されません。

Secure Browse を使用すると、ユーザーはiOSデバイスからNetScaler Gateway 経由で接続できます。Secure Browse を有効にすると、ユーザーがSecure Hubを使用してログオンすると、Secure Browseによってクライアント選択ページが無効になります。

ログオン時に ページを表示する

クライアント選択オプションを有効にすると、NetScaler Gateway への認証が成功した後、ユーザーはNetScaler Gateway プラグイン、Web Interface、Receiver、またはクライアントレスアクセスを使用して1つのWebページからログオンできます。ログオンが成功すると、Web ページにアイコンが表示され、ユーザーは接続を確立する方法を選択できます。また、Java向けNetScaler Gateway プラグインが選択肢ページに表示されるように構成することもできます。

エンドポイント分析を使用したり、アクセスシナリオのフォールバックを実装したりすることなく、クライアントの選択を有効にできます。クライアントセキュリティ式を定義しない場合、ユーザーはNetScaler Gateway で構成された設定の接続オプションを受け取ります。ユーザーセッションに Client Security 式が存在し、ユーザーデバイスがエンドポイント分析スキャンに失敗した場合、Web Interface が構成されている場合、選択肢ページには Web Interface を使用するオプションのみが表示されます。それ以外の場合、ユーザはクライアントレスアクセスを使用してログオンできます。

クライアントの選択肢は、グローバルに設定するか、セッションプロファイルとポリシーを使用して設定します。

重要：

クライアントの選択肢を構成するときは、検疫グループを構成しないでください。エンドポイント分析スキャンに失敗し、検疫され、エンドポイントスキャンに合格したユーザーデバイスと同じように扱われるユーザーデバイス。

クライアントの選択肢オプションをグローバルに有効にする

1. GUIの［構成］タブのナビゲーションペインで［ **NetScaler Gateway** ］を展開し、［ **グローバル設定**］をクリックします。
2. 詳細ペインの で、 をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. 「クライアントエクスペリエンス」タブで、「**詳細設定**」をクリックします。
4. タブで、 をクリックし、** をクリックします。

セッションポリシーの一部としてクライアントの選択肢を有効にする

また、セッションポリシーの一部としてクライアントの選択肢を構成し、それをユーザー、グループ、および仮想サーバーにバインドすることもできます。

1. GUIの［構成］タブのナビゲーションペインで、［**NetScaler Gateway**］>［**ポリシー**］**の順に展開し、**［**セッション**］をクリックします。
2. 詳細ペインの タブで、 をクリックします。
3. に、ポリシーの名前を入力します。
4. 「リクエストプロファイル」の横にある「**新規**」をクリックします。
5. に、プロファイルの名前を入力します。
6. 「クライアントエクスペリエンス」タブで、「**詳細設定**」をクリックします。
7. ［全般］タブの［クライアントの選択］の横にある［**グローバル上書き**］、［**クライアントの選択**］、［**OK**］、［**作成**］の順にクリックします。
8. ダイアログボックスで、 の横にある を選択し、 を選択し、 をクリックして をクリックし、 をクリックします。

クライアント選択オプションの設定

セッションプロファイルとポリシーを使用してクライアントの選択を有効にすることに加えて、ユーザーソフトウェアの設定を構成する必要があります。たとえば、ユーザーがNetScaler Gateway プラグイン、StoreFront またはWeb Interface、またはクライアントレスアクセスのいずれかを使用してログオンできるようにする場合です。3 つのオプションとクライアントの選択肢をすべて有効にする 1 つのセッションプロファイルを作成します。次に、プロファイルをアタッチした式を True 値に設定したセッションポリシーを作成します。次に、セッションポリシーを仮想サーバーにバインドします。

セッションポリシーとプロファイルを作成する前に、ユーザーの認可グループを作成する必要があります。

承認グループを作成する

1. 構成ユーティリティの［構成］タブのナビゲーションペインで［**NetScaler Gateway**］>［**ユーザー管理**］の順に選択し、［**AAAグループ**］をクリックします。
2. 詳細ペインで、 をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. に、グループの名前を入力します。
4. タブでユーザーを選択し、それぞれの をクリックし、 をクリックして をクリックします。

次の手順は、NetScaler Gateway プラグイン、StoreFront、およびクライアントレスアクセスを持つクライアント選択のセッションプロファイルの例です。

クライアント選択用のセッションプロファイルを作成する

1. 構成ユーティリティの［構成］タブのナビゲーションペインで、［**NetScaler Gateway**］**>［ポリシー］>［セッション］の順に展開します。**
2. 詳細ペインで、 タブをクリックし、 をクリックします。
3. ** に、プロファイルの名前を入力します。
4. タブで、次の操作を行います。
   a. 「ホームページ」の横にある「**グローバル上書き**」をクリックし、「**ホームページを表示**」をオフにします。これにより、Access Interfaceが無効になります。
   b. の横にある をクリックし、 を選択します。
   c. の横にある をクリックし、 を選択します。
   d. をクリックし、 の横にある をクリックし、 をクリックします。
5. 「**セキュリティ**」タブの「**デフォルト承認アクション**」の横にある「**グローバル上書き**」をクリックし、「**許可**」を選択します。
6. タブの をクリックします。
7. で をクリックし、 をクリックしてグループを選択します。
8. タブで、次の操作を行います：
   a. の横にある をクリックし、 を選択します。
   b. ［**Web Interfaceアドレス**］の横にある［**グローバル上書き**］をクリックし、StoreFrontのWebアドレス（など）を入力します `<http://ipAddress/Citrix/>`。
   c. の横にある をクリックし、 を選択します。
   d. **「シングル・サインオン・ドメイン」の横にある「グローバル上書き」をクリックし、ドメインの名前を入力します。**
9. をクリックし、 をクリックします。

Citrix Gateway Plug-in for Javaをクライアントオプションとして使用する場合は、［**クライアントエクスペリエンス**］タブの［プラグインの種類］で［**Java**］を選択します。この選択肢を選択

© 1997–2026 Citrix Systems, Inc. All rights reserved.

する場合は、イントラネットアプリケーションを構成し、傍受モードを に設定する必要があります。

セッションプロファイルを作成したら、セッションポリシーを作成します。ポリシー内で、プロファイルを選択し、式を True 値に設定します。

StoreFront をクライアントの選択肢として使用するには、NetScaler Gateway でSecure Ticket Authority（STA）も構成する必要があります。STA は仮想サーバにバインドされています。

注：

StoreFront を実行しているサーバーが使用できない場合、Citrix Virtual Apps 選択肢は選択肢ページに表示されません。

STA サーバをグローバルに設定する

1. 構成ユーティリティの［構成］タブのナビゲーションペインで［ **NetScaler Gateway］**を展開し、［ **グローバル設定**］をクリックします。
2. 詳細ペインの で、Secure Ticket Authority が使用する **STA サーバーのバインド/**バインド解除をクリックします 。
3. ダイアログボックスで、 をクリックします。
4. ダイアログボックスの に STA サーバーの Web アドレスを入力し、 をクリックします。
5. 手順3と4を繰り返してSTAサーバーをさらに追加し、「 **OK」**をクリックします。

STA を仮想サーバにバインドする

1. 構成ユーティリティの［構成］タブのナビゲーションペインで、［ **NetScaler Gateway** ］を展開し、［ **仮想サーバー**］をクリックします。
2. 詳細ペインで仮想サーバーを選択して、 **［Open］** をクリックします。
3. ［ **公開アプリケーション** ］タブの［ **Secure Ticket Authority**］の下の［ **アクティブ**］で、STAサーバーを選択し、［ **OK］**をクリックします。

STA サーバーは、 タブでも追加できます。

アクセスシナリオのフォールバックの設定

SmartAccessを使用すると、NetScaler Gateway は、エンドポイント分析スキャンの結果に基づいて、ユーザーデバイスに許可されるアクセス方法を自動的に判断できます。アクセスシナリオフォールバックは、ユーザーデバイスが最初のエンドポイント分析スキャンに合格しない場合

© 1997–2026 Citrix Systems, Inc. All rights reserved.

に、Citrix Workspaceアプリを使用してユーザーデバイスをNetScaler Gateway プラグインからWeb InterfaceまたはStoreFront にフォールバックできるようにすることで、この機能をさらに拡張します。

アクセスシナリオのフォールバックを有効にするには、NetScaler Gateway へのログオン時にユーザーが別のアクセス方法を受け取るかどうかを決定する認証後ポリシーを構成します。この認証後ポリシーは、グローバルに、またはセッションプロファイルの一部として設定するクライアントセキュリティ式として定義されます。セッションプロファイルを構成すると、プロファイルはセッションポリシーに関連付けられ、ユーザー、グループ、または仮想サーバーにバインドされます。アクセスシナリオのフォールバックを有効にすると、NetScaler Gateway はユーザー認証後にエンドポイント分析スキャンを開始します。フォールバック認証後スキャンの要件を満たさないユーザーデバイスの結果は次のとおりです：

- クライアントの選択が有効になっている場合、ユーザーはCitrix Workspace アプリのみを使用してWeb InterfaceまたはStoreFront にログオンできます。
- クライアントレスアクセスとクライアント選択が無効になっている場合、ユーザーはWeb InterfaceまたはStoreFront にのみアクセスできるグループに隔離されます。
- NetScaler Gateway でクライアントレスアクセスとWeb InterfaceまたはStoreFront が有効になっていて、ICAプロキシが無効になっている場合、ユーザーはクライアントレスアクセスにフォールバックします。
- Web InterfaceまたはStoreFront が構成されておらず、クライアントレスアクセスが許可に設定されている場合、ユーザーはクライアントレスアクセスにフォールバックします。

クライアントレスアクセスが無効になっている場合は、アクセスシナリオフォールバック用に次の設定の組み合わせを設定する必要があります。

- フォールバック認証後スキャンのクライアントセキュリティパラメータを定義します。
- Web インターフェイスのホームページを定義します。
- クライアントの選択肢を無効にします。
- ユーザーデバイスがクライアントセキュリティチェックに失敗すると、ユーザーは、Web InterfaceまたはStoreFront および公開アプリケーションへのアクセスのみを許可する検疫グループに配置されます。

アクセスシナリオフォールバックのポリシーの作成

アクセスシナリオのフォールバック用にNetScaler Gateway を構成するには、次の方法でポリシーとグループを作成する必要があります：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- エンドポイント分析スキャンが失敗した場合にユーザーが配置される検疫グループを作成します。
- エンドポイント分析スキャンが失敗した場合に使用されるグローバルWeb InterfaceまたはStoreFront 設定を作成します。
- グローバル設定を上書きするセッションポリシーを作成し、そのセッションポリシーをグループにバインドします。
- エンドポイント分析が失敗した場合に適用されるグローバルクライアントセキュリティポリシーを作成します。

アクセスシナリオフォールバックを設定する場合は、次の注意事項に従ってください。

- クライアント選択またはアクセスシナリオフォールバックを使用するには、すべてのユーザーに Endpoint Analysis プラグインが必要です。エンドポイント分析を実行できない場合、またはスキャン中にスキャンをスキップを選択した場合、ユーザーはアクセスを拒否されます。注：スキャンをスキップするオプションは、NetScaler Gateway 10.1、ビルド120.1316.eで削除されました
- クライアント選択を有効にすると、ユーザーデバイスがエンドポイント分析スキャンに失敗すると、ユーザーは検疫グループに配置されます。ユーザーは、NetScaler GatewayプラグインまたはCitrix Workspaceアプリのいずれかを使用して、Web InterfaceまたはStoreFront に引き続きログオンできます。 注：クライアントの選択を有効にする場合は、検疫グループを作成しないことをお勧めします。エンドポイント分析スキャンに失敗したユーザーデバイスは、エンドポイントスキャンに合格したユーザーデバイスと同様に隔離されます。
- エンドポイント分析スキャンが失敗し、ユーザーが検疫グループに配置された場合、検疫グループにバインドされたポリシーは、検疫グループにバインドされたポリシーと同等またはそれ以下の優先度番号を持つユーザーに直接バインドされたポリシーがない場合にのみ有効です。
- Access Interfaceと、Web InterfaceまたはStoreFront に異なるWebアドレスを使用できます。ホームページを構成すると、NetScaler Gateway プラグインではAccess Interfaceのホームページが優先され、Web Interfaceユーザーの場合はWeb Interfaceホームページが優先されます。StoreFront では、Citrix Workspace アプリのホームページが優先されます。

検疫グループを作成する

1. 構成ユーティリティの［構成］タブのナビゲーションペインで、［**Citrix Gateway**］>［**ユーザー管理**］を展開し、［**AAAグループ**］をクリックします。
2. 詳細ペインで、 をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. にグループの名前を入力し**、 をクリックし、** をクリックします。 **重要**:検疫グループの名前は、ユーザーが所属する可能性のあるドメイングループの名前と一致してはなりません。検疫グループが Active Directory グループ名と一致する場合、ユーザーデバイスがエンドポイント分析セキュリティスキャンに合格しても、ユーザーは隔離されます。

グループを作成した後、ユーザーデバイスがエンドポイント分析スキャンに失敗した場合にWeb InterfaceにフォールバックするようにNetScaler Gateway を構成します。

ユーザー接続を検疫するための設定を構成する

1. 構成ユーティリティの［構成］タブのナビゲーションペインで、［Citrix Gateway］を展開し、［ **グローバル設定**］をクリックします。
2. 詳細ペインの で、 をクリックします。
3. ［ **グローバルNetScaler Gateway 設定** ］ダイアログボックスの［ **公開アプリケーション** ］タブで、［ **ICAプロキシ**］の横にある［ **オフ**］を選択します。
4. ［ **Web Interfaceアドレス**］の横に、StoreFront またはWeb InterfaceのWebアドレスを入力します。
5. ［ **シングルサインオンドメイン**］の横に、Active Directory ドメインの名前を入力し、［ **OK］**をクリックします。

グローバル設定を構成したら、グローバルICAプロキシ設定を上書きするセッションポリシーを作成し、セッションポリシーを検疫グループにバインドします。

アクセスシナリオフォールバックのセッションポリシーを作成する

1. 構成ユーティリティの［構成］タブのナビゲーションペインで、［ **Citrix Gateway］ > ［ポリシー** ］を展開し、［ **セッション**］をクリックします。
2. 詳細ペインで、 をクリックします。
3. ** に、ポリシーの名前を入力します。
4. 「 **リクエストプロファイル**」の横にある「 **新規**」をクリックします。
5. タブで、 の横にある をクリックし、 を選択して、** をクリックします。
6. ダイアログボックスで、 の横にある を選択し、 を選択し、 をクリックして をクリックし、** をクリックします。

セッションポリシーを作成したら、ポリシーを検疫グループにバインドします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

セッションポリシーを検疫グループにバインドします

1. 構成ユーティリティの［構成］タブのナビゲーションペインで、［**Citrix Gateway**］>［**ユーザー管理**］を展開し、［**AAAグループ**］をクリックします。
2. 詳細ウィンドウで、グループを選択し、 をクリックします。
3. をクリックします。
4. タブで、 を選択し、 をクリックします。
5. 「**ポリシー名**」でポリシーを選択し、 **「OK」**をクリックします。

NetScaler Gateway でWeb InterfaceまたはStoreFront を有効にするセッションポリシーとプロファイルを作成したら、グローバルクライアントセキュリティポリシーを作成します。

グローバルクライアントセキュリティポリシーを作成する

1. 構成ユーティリティの［構成］タブのナビゲーションペインで、［Citrix Gateway］を展開し、［**グローバル設定**］をクリックします。
2. 詳細ペインの で、 をクリックします。
3. タブの をクリックします。
4. に式を入力します。システム式の構成の詳細については、「システム式の設定」および「[複合クライアントセキュリティ式の構成](/en-us/netscaler-gateway/13/install/ng-policies-profiles-wrapper-con/ng-config-system-expressions-con)」を参照してください
5. 「**検疫グループ**」で、グループ手順で設定したグループを選択し、 **「OK」**をクリックします。

NetScaler Gateway プラグインの接続を構成する

ユーザーデバイス接続を構成するには、内部ネットワークでユーザーがアクセスできるリソースを定義します。ユーザーデバイス接続の設定には、次のものが含まれます。

- ユーザーがアクセスを許可されるドメインを定義する。
- アドレスプール (イントラネット IP) を含む、ユーザーの IP アドレスを構成します。
- タイムアウト設定を構成する。
- シングルサインオンの設定。
- クライアント代行受信の設定。
- 分割トンネリングの設定。
- プロキシサーバーを介した接続の設定。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- NetScaler Gateway を介して接続するためのユーザーソフトウェアの構成。
- モバイルデバイスのアクセスを設定する。

ほとんどのユーザーデバイス接続は、セッションポリシーの一部であるプロファイルを使用して構成します。また、イントラネットアプリケーション、事前認証、およびトラフィックポリシーを使用して、ユーザーデバイスの接続設定を定義することもできます。

注:

Windows VPN プラグインと EPA プラグインは、さまざまな操作のテレメトリデータを収集します。この機能を無効にするには、クライアントマシンで次の操作を行います。

REG_DWORD タイプのレジストリ「HKLM\ ソフトウェア\ Citrix\ Secure Access Client\ DisableGA」を 1 に設定します。

ユーザセッション数の設定

特定の時点でNetScaler Gateway に接続できるユーザーの最大数を、グローバルレベルまたは仮想サーバーレベルごとに構成できます。アプライアンスに接続するユーザーの数が構成した値を超えると、NetScaler Gateway でセッションは作成されません。ユーザー数が許可した数を超えると、ユーザーはエラーメッセージを受け取ります。

グローバルユーザー制限を設定するには

ユーザー制限をグローバルに設定すると、この制限は、システム上の異なる仮想サーバーとのセッションを確立するすべてのユーザーに適用されます。ユーザーセッション数が設定した値に達すると、NetScaler Gateway に存在する仮想サーバーで新しいセッションを確立できなくなります。

NetScaler Gateway のデフォルトの認証タイプを設定するときに、グローバルレベルで最大ユーザー数を設定します。

1. ナビゲーションペインにある、［Configuration］タブの構成ユーティリティで、［NetScaler Gateway］を展開し、［Global Settings］をクリックします。
2. 詳細ウィンドウの で、 をクリックします。
3. ［グローバル認証設定］ダイアログボックスの［最大ユーザー数］にユーザー数を入力し、［OK］をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

仮想サーバーあたりのユーザー制限を設定するには

また、システム上の各仮想サーバにユーザ制限を適用することもできます。仮想サーバーごとのユーザー制限を構成すると、制限は特定の仮想サーバーとのセッションを確立するユーザーにのみ適用されます。他の仮想サーバーとのセッションを確立するユーザーは、この制限の影響を受けません。

1. 構成ユーティリティの［構成］タブのナビゲーションペインで、［ NetScaler Gateway ］を展開し、［ 仮想サーバー］をクリックします。
2. 詳細ペインで仮想サーバーをクリックし、 をクリックします。
3. 「最大ユーザー」にユーザー数を入力し、「OK」をクリックします。

タイムアウト設定を構成する

指定した分数の間接続にアクティビティがない場合、強制的に切断するようにNetScaler Gatewayを構成できます。セッションがタイムアウト (切断) する 1 分前に、ユーザーはセッションの終了を示すアラートを受信します。セッションが終了すると、ユーザーは再度ログオンする必要があります。

次のタイムアウトオプションを使用できます。

- **強制タイムアウト。**この設定を有効にすると、ユーザーの操作に関係なく、タイムアウト間隔が経過するとNetScaler Gateway によってセッションが切断されます。タイムアウト間隔が過ぎても接続が切断されないようにするためにユーザーが実行できるアクションはありません。この設定は、NetScaler Gatewayプラグイン、Citrix Workspaceアプリ、Secure Hub、またはWebブラウザーを介して接続するユーザーに適用されます。最小値は 1 で、最大値は 65535 です。
- **セッションタイムアウト。**この設定を有効にすると、指定した間隔でネットワークアクティビティが検出されないと、NetScaler Gateway によってセッションが切断されます。この設定は、NetScaler Gateway プラグイン、Citrix Workspaceアプリ、Citrix Secure Hub、またはWebブラウザーを介して接続するユーザーに適用されます。デフォルトのタイムアウト設定は 30 分です。最小値は 1 で、最大値は 65535 です。
- **アイドルセッションのタイムアウト。**指定した間隔でマウス、キーボード、タッチなどのユーザー操作がない場合、NetScaler Gateway プラグインがアイドルセッションを終了するまでの時間。この設定は、NetScaler Gateway プラグインで接続するユーザーにのみ適用されます。最小値は 1 で、最大値は 9999 です。

1 ～ 65536 の値を入力して、タイムアウト間隔の分を指定することで、任意のタイムアウト設定を有効にできます。これらの設定を複数有効にすると、最初のタイムアウト間隔が経過すると、ユーザーデバイス接続は閉じられます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

タイムアウト設定は、グローバル設定を構成するか、セッションプロファイルを使用して構成します。プロファイルをセッションポリシーに追加すると、ポリシーはユーザー、グループ、または仮想サーバーにバインドされます。タイムアウト設定をグローバルに構成すると、その設定はすべてのユーザセッションに適用されます。

注：

- Always On（サービスモードまたはユーザモード）では、VPN クライアントはすべてのタイムアウトを無視します。強制タイムアウトとセッションタイムアウトの決定はNetScaler ADCアプライアンスで行われるため、これらのタイムアウトは意図したとおりに機能します。このようなタイムアウトが発生すると、VPN プラグインは自動認証を実行しようとします。

  Always On では、ユーザデバイスは常にVPNトンネルを介して接続する必要があるため、強制タイムアウトまたはクライアントアイドルタイムアウトを設定しないでください。ただし、セッションタイムアウトを設定して、古いセッションを取り除くことができます。
- Microsoft Outlook などの一部のアプリケーションは、ユーザーの介入なしにネットワークトラフィックプローブを電子メールサーバーに自動的に送信します。アイドルセッションタイムアウトとセッションタイムアウトを構成して、ユーザーデバイス上で無人状態のセッションが妥当な時間内にタイムアウトするようにすることをお勧めします。

強制タイムアウトを構成する

強制タイムアウトは、指定した時間が経過するとNetScaler Gateway プラグインを自動的に切断します。強制タイムアウトは、グローバルに、またはセッションポリシーの一部として設定できます。

グローバル強制タイムアウトを構成する

1. 構成ユーティリティの［ **構成** ］タブのナビゲーションペインで、［Citrix Gateway］を展開し、［ **グローバル設定**］をクリックします。
2. 詳細ペインの で、 をクリックします。
3. タブで、 をクリックします。
4. に、ユーザーが接続を維持できる分数を入力します。
5. ［強制タイムアウト警告 (分)］に、接続が切断される予定であることをユーザーに警告するまでの分数を入力し、［ **OK］**をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

セッションポリシー内で強制タイムアウトを構成する

強制タイムアウトを受信するユーザーをさらに制御するには、セッションポリシーを作成し、そのポリシーをユーザーまたはグループに適用します。

1. 構成ユーティリティの［**構成**］タブのナビゲーションペインで、［**Citrix Gateway**］>［**ポリシー**］を展開し、［**セッション**］をクリックします。
2. 詳細ペインで、 をクリックします。
3. に、ポリシーの名前を入力します。
4. 「リクエストプロファイル」の横にある「**新規**」をクリックします。
5. に、プロファイルの名前を入力します。
6. タブで、 をクリックします。
7. の をクリックし、 にユーザーが接続を維持できる分数を入力します。
8. の横にある をクリックし、接続が切断されることをユーザーに警告する時間を分単位で入力します。［**OK**］ を2回クリックします。
9. ダイアログボックスで、 の横にある を選択し、 を選択し、 をクリックして をクリックし、** をクリックします。

セッションタイムアウトまたはアイドルタイムアウトの設定

NetScaler ADC GUIを使用して、セッションおよびクライアントのタイムアウト設定をグローバルに構成したり、セッションポリシーを作成したりできます。セッションポリシーとプロファイルを作成するときは、式を True に設定します。

注:

グローバル設定を明示的に上書きせず、 > でセッションタイムアウトを設定すると、再ログインを必要とする認証ループが発生する可能性があります。これは、デフォルトのセッションタイムアウトが 30 分であっても発生します。

GUI を使用してセッションまたはクライアントのアイドルタイムアウトをグローバルに設定するには

1. ［構成］タブの**ナビゲーションペイン**で、［**NetScaler Gateway**］ を展開し、［**グローバル設定**］をクリックします。
2. 詳細ペインの で、 をクリックします。
3. タブで、次のいずれかまたは両方の操作を行います。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- に、分数を入力します。
- ［ **クライアントアイドルタイムアウト (分)**］に分数を入力し、［ **OK］**をクリックします。

GUI を使用してセッションポリシーを使用してセッションまたはクライアントのアイドルタイムアウト設定を構成するには

1. ［ **構成** ］タブのナビゲーションペインで［ **NetScaler Gateway** ］>［ **ポリシー** ］の順に展開し、［ **セッション**］をクリックします。
2. **［NetScaler Gateway セッションポリシーとプロファイル** ］ページで、［ **セッションプロファイル**］、［ **追加**］の順にクリックします。
3. に、プロファイルの名前を入力します。
4. タブで、次のいずれかまたは両方の操作を行います。
   - の横にある をクリックし、分数を入力して をクリックします。
   - の横にある をクリックし、分数を入力して をクリックします。
5. a. **［NetScaler Gateway セッションポリシーとプロファイル** ］ページで、［ **セッションポリシー**］、［ **追加**］の順にクリックします。
6. **［NetScaler Gateway セッションの作成］ポリシーで、**
   - に、ポリシーの名前を入力します。
   - で、規則の条件が満たされた場合に新しいセッションポリシーによって適用されるアクションを指定するプロファイルを選択します。
   - を選択します。
   - フィールドに、ポリシーに一致するトラフィックを指定して、式または名前付き式の名前を追加します。
   - をクリックし、 をクリックします。

内部ネットワークリソースに接続する

NetScaler Gateway を構成して、ユーザーが内部ネットワークのリソースにアクセスできるようにすることができます。分割トンネリングを無効にすると、ユーザーデバイスからのすべてのネットワークトラフィックがNetScaler Gateway に送信され、承認ポリシーによって、トラフィックが内部ネットワークリソースへの通過を許可されるかどうかが決定されます。分割トンネリングを有効にすると、内部ネットワーク宛のトラフィックのみがユーザーデバイスによって傍受され、

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler Gateway に送信されます。イントラネットアプリケーションを使用して、NetScaler Gateway がインターセプトするIPアドレスを構成します。

Windows版NetScaler Gateway プラグインを使用している場合は、インターセプトモードをトランスペアレントに設定します。Java向けNetScaler Gateway プラグインを使用している場合は、インターセプトモードをプロキシに設定します。代行受信モードをトランスペアレントに設定すると、以下を使用してネットワークリソースへのアクセスを許可できます。

- 単一の IP アドレスとサブネットマスク
- IP アドレスの範囲

代行受信モードをプロキシに設定すると、宛先 IP アドレス、送信元 IP アドレス、およびポート番号を設定できます。

内部ネットワークリソースへのネットワークアクセスを構成する

1. 構成ユーティリティの［ **構成** ］タブのナビゲーションペインで、［NetScaler Gateway］、［リソース］、［ **イントラネットアプリケーション］の順に展開します。**
2. 詳細ペインで、 をクリックします。**
3. ネットワークアクセスを許可するためのパラメータを入力し、、 の順にクリックします。**

分割トンネリングの設定

分割トンネリングを有効にして、NetScaler Gateway プラグインがNetScaler Gateway に不要なネットワークトラフィックを送信しないようにすることができます。

分割トンネリングを有効にしない場合、NetScaler Gateway プラグインはユーザーデバイスから発信されるすべてのネットワークトラフィックをキャプチャし、VPNトンネルを介してNetScaler Gateway にトラフィックを送信します。

分割トンネリングを有効にすると、NetScaler Gateway プラグインは、NetScaler Gateway によって保護されているネットワーク宛てのトラフィックのみをVPNトンネル経由で送信します。NetScaler Gateway プラグインは、保護されていないネットワークを宛先とするネットワークトラフィックをNetScaler Gateway に送信しません。

NetScaler Gateway プラグインが起動すると、NetScaler Gateway からイントラネットアプリケーションのリストを取得します。NetScaler Gateway プラグインは、ユーザーデバイスからネットワーク上で送信されるすべてのパケットを調べ、パケット内のアドレスをイントラネットアプリケーションのリストと比較します。パケット内の宛先アドレスがイントラネットアプリケーションの1つ内にある場合、NetScaler Gateway プラグインはVPNトンネルを介してNetScaler Gateway にパケットを送信します。宛先アドレスが定義済みのイントラネットアプリケーション

© 1997–2026 Citrix Systems, Inc. All rights reserved.

にない場合、パケットは暗号化されず、ユーザーデバイスはパケットを適切にルーティングします。分割トンネリングを有効にすると、イントラネットアプリケーションによって傍受されるネットワークトラフィックが定義されます。

注：

ユーザーがCitrix Workspace アプリを使用してサーバーファーム内の公開アプリケーションに接続する場合は、分割トンネリングを構成する必要はありません。

NetScaler Gateway は、NetScaler Gateway が傍受しないネットワークトラフィックを定義するリバース分割トンネリングもサポートしています。分割トンネリングをリバースに設定すると、イントラネットアプリケーションは、NetScaler Gateway が傍受しないネットワークトラフィックを定義します。リバース分割トンネリングを有効にすると、内部IPアドレスに向けられたすべてのネットワークトラフィックはVPNトンネルをバイパスし、他のトラフィックはNetScaler Gatewayを経由します。リバース分割トンネリングを使用して、すべての非ローカル LAN トラフィックをログに記録できます。たとえば、ユーザーがホームワイヤレスネットワークを持ち、NetScaler Gateway プラグインを使用してログオンしている場合、NetScaler Gateway は、ワイヤレスネットワーク内のプリンターまたは別のデバイス宛てのネットワークトラフィックを傍受しません。

イントラネットアプリケーションの詳細については、「クライアント代行受信の構成」を参照してください。

分割トンネリングは、セッションポリシーの一部として設定します。

分割トンネリングを設定するには

1. 構成ユーティリティの［構成］タブのナビゲーションペインで、［**Citrix Gateway ポリシー**］を展開し、［**セッション**］**をクリックします。**
2. 詳細ペインの タブで、プロファイルを選択し、 をクリックします。**
3. ［**クライアントエクスペリエンス**］タブで、［**分割トンネル**］の横にある［**グローバルオーバーライド**］を選択し、オプションを選択して［**OK**］ を 2 回クリックします。

分割トンネリングおよび認可の設定

NetScaler Gateway の展開を計画するときは、分割トンネリングと、デフォルトの承認アクションと承認ポリシーを考慮することが重要です。

たとえば、ネットワークリソースへのアクセスを許可する認可ポリシーがあるとします。分割トンネリングがオンに設定されており、NetScaler Gateway 経由でネットワークトラフィックを送信するようにイントラネットアプリケーションを構成していない。NetScaler Gateway にこの種類の構

© 1997–2026 Citrix Systems, Inc. All rights reserved.

成がある場合、リソースへのアクセスは許可されますが、ユーザーはリソースにアクセスできません。

承認ポリシーがネットワークリソースへのアクセスを拒否し、分割トンネリングがオンに設定されており、イントラネットアプリケーションがネットワークトラフィックをNetScaler Gateway 経由でルーティングするように構成されている場合、NetScaler Gateway プラグインはトラフィックをNetScaler Gateway に送信しますが、リソースへのアクセスは拒否されます。

分割トンネリングの詳細については、「分割トンネリングの設定」を参照してください。

クライアント傍受を構成する

NetScaler Gateway のユーザー接続の傍受ルールは、イントラネットアプリケーションを使用して構成します。デフォルトでは、アプライアンス上でシステム IP アドレス、マッピング IP アドレス、またはサブネット IP アドレスを設定すると、これらの IP アドレスに基づいてサブネットルートが作成されます。イントラネットアプリケーションは、これらのルートに基づいて自動的に作成され、仮想サーバーにバインドできます。分割トンネリングを有効にする場合は、クライアント傍受が発生するイントラネットアプリケーションを定義する必要があります。

構成ユーティリティを使用して、イントラネットアプリケーションを構成できます。イントラネットアプリケーションは、ユーザー、グループ、または仮想サーバーにバインドできます。

分割トンネリングを有効にし、ユーザーがWorxWebまたはWorxMailを使用して接続する場合、クライアント傍受を構成するときに、Citrix Endpoint ManagementとExchangeサーバーのIPアドレスを追加する必要があります。分割トンネリングを有効にしない場合、イントラネットアプリケーションでEndpoint ManagementおよびExchange IPアドレスを構成する必要はありません。

分割トンネリング設定の詳細については、「分割トンネリングの設定」を参照してください。

NetScaler Gateway プラグイン用のイントラネットアプリケーションを構成する

リソースへのユーザーアクセス用のイントラネットアプリケーションを作成するには、以下を定義します：

- 1 つの IP アドレス
- IP アドレスの範囲
- ホスト名

NetScaler Gateway でイントラネットアプリケーションを定義すると、Windows向けCitrix Secure Accessエージェントは、リソース宛てのユーザートラフィックを傍受し、そのトラフィックを NetScaler Gateway 経由で送信します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

イントラネットアプリケーションを構成するときは、次の点を考慮してください：

- 分割トンネルがオンの場合、
  - イントラネットアプリケーションを構成します。
  - イントラネットアプリケーションをすべての認証、承認、および監査グループに割り当てます。
- 分割トンネルがオフの場合、
  - すべてのトラフィックは VPN トンネルを傍受します。
  - イントラネットアプリケーションを構成する必要はありません。
- 分割トンネルが逆の場合、
  - イントラネットアプリケーションを構成します。イントラネットアプリケーションで指定されていないトラフィックは、VPN トンネルを通過します。
  - VPN から除外するイントラネットアプリケーションをすべての認証、承認、および監査グループに割り当てます。

重要:

分割トンネルの設定に関係なく、インターセプションは **TRANSPARENT** に設定する必要があります。

注：

- イントラネットアプリケーションを構成するときは、接続に使用するプラグインソフトウェアのタイプに対応するインターセプトモードを選択する必要があります。
- イントラネットアプリケーションをプロキシインターセプトとトランスペアレントインターセプトの両方に設定することはできません。

1 つの IP アドレス用のイントラネットアプリケーションを作成するには

1. ［構成］タブのナビゲーションペインで、［**Citrix Gateway リソース**］を展開し、［**イントラネットアプリケーション**］をクリックします。
2. 詳細ペインで、 をクリックします。**
3. ** に、プロファイルの名前を入力します。
4. **「イントラネットアプリケーションの作成」ダイアログボックスで、「TRANSPARENT」を選択します。**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. で、 と を選択します**。**
6. 「 **プロトコル**」で、ネットワークリソースに適用するプロトコルを選択します。
7. に IP アドレスを入力します。
8. に「サブネットマスク」と入力し、、 の順にクリックします。**

IP アドレス範囲を設定するには

Web、電子メール、ファイル共有など、ネットワークに複数のサーバがある場合は、ネットワークリソースの IP 範囲を含むネットワークリソースを設定できます。この設定により、ユーザーは IP アドレス範囲に含まれるネットワークリソースにアクセスできます。

1. ［構成 ］タブの**ナビゲーションペイン**で、［ **NetScaler Gateway リソース**］ を展開し、［イントラネットアプリケーション］をクリックします**。**
2. 詳細ペインで、 をクリックします。**
3. ** に、プロファイルの名前を入力します。
4. 「 **プロトコル**」で、ネットワークリソースに適用するプロトコルを選択します。
5. 「イントラネットアプリケーションの**作成** 」ダイアログボックスで、「**TRANSPARENT**」を選択します。
6. で、 を選択します。**
7. に開始**IP アドレスを入力し、 に終了 IP アドレスを入力し、、 の順にクリックします。**

ホスト名のイントラネットアプリケーションを作成するには

1. ［構成］タブのナビゲーションペインで、［ **Citrix Gateway リソース**］ を展開し、［ **イントラネットアプリケーション**］をクリックします。
2. 詳細ペインで、 をクリックします。**
3. に、プロファイルの名前を入力します。
4. **「イントラネットアプリケーションの作成」ダイアログボックスで、「TRANSPARENT」を選択します。**
5. で、 を選択します。
6. で を選択し、、 **の順にクリックします。**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

重要：

- リリース 13.0 ビルド 36.27 以降では、Windows VPN プラグインは、分割トンネリングのホスト名（FQDN）ベースのルールをサポートします。NetScaler ADCアプライアンスとWindows VPNプラグインの両方をリリース13.0ビルド36.27以降にアップグレードする必要があります。
- ワイルドカードホスト名もサポートされています。たとえば、ホスト名が「*.example.com」のイントラネットアプリケーションが構成されている場合、`a1.example.com`、`b2.example.com`などがトンネリングされます。
- ホスト名ベースのイントラネットアプリケーションは、分割トンネリングが ON または REVERSE に設定されている場合にのみ機能します。
- ホスト名ベースのルールは、リバース分割トンネリングではサポートされていません。

Java向けNetScaler Gateway プラグインのイントラネットアプリケーションを構成する

ユーザーがJava向けNetScaler Gateway プラグインを使用して接続する場合は、イントラネットアプリケーションを構成し、傍受モードをプロキシに設定する必要があります。Java向けNetScaler Gateway プラグインは、プロファイルで指定されたユーザーデバイスのループバックIPアドレスとポート番号を使用してトラフィックを傍受します。

ユーザーがWindowsベースのデバイスから接続している場合、NetScaler Gateway Plug-in for Java は、プロファイルで指定されたループバックIPアドレスとポートにアクセスするようにアプリケーションホスト名を設定して、ホストファイルの変更を試みます。ユーザーは、HOST ファイルを変更するためのユーザーデバイスに対する管理者権限を持っている必要があります。

ユーザーが Windows 以外のデバイスから接続している場合は、イントラネットアプリケーションプロファイルで指定された送信元 IP アドレスとポート値を使用して、アプリケーションを手動で構成する必要があります。

Java向けNetScaler Gateway プラグインのイントラネットアプリケーションを構成するには

1. ［構成］タブの**ナビゲーションペイン**で、［**NetScaler Gateway リソース**］ を展開し、［イントラネットアプリケーション］をクリックします**。**
2. 詳細ペインで、 をクリックします。**
3. ** に、プロファイルの名前を入力します。
4. **「 プロキシ」をクリックします。**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. と に、宛先 IP アドレスとポートを入力します。
6. と に、送信元 IP アドレスとポートを入力します。

> **注:**
>
> 送信元 IP アドレスを 127.0.0.1 のループバック IP アドレスに設定して下さい。IP アドレスを指定しない場合、ループバック IP アドレスが使用されます。ポート値を入力しない場合、宛先ポートの値が使用されます。

ネームサービス解決を構成する

NetScaler Gateway のインストール中に、NetScaler Gateway ウィザードを使用して、ネームサービスプロバイダーなどのその他の設定を構成できます。ネームサービスプロバイダーは、完全修飾ドメイン名 (FQDN) を IP アドレスに変換します。NetScaler Gateway ウィザードでは、DNSサーバーまたはWINSサーバーの構成、DNSルックアップの優先順位、およびサーバーへの接続を再試行する回数を設定できます。

NetScaler Gateway ウィザードを実行すると、DNSサーバーを追加できます。セッションプロファイルを使用して、NetScaler Gateway にさらにDNSサーバーとWINSサーバーを追加できます。その後、ウィザードで最初に構成した名前解決サーバーとは異なる名前解決サーバーに接続するようにユーザーおよびグループに指示できます。

NetScaler Gateway で追加のDNSサーバーを構成する前に、名前解決用のDNSサーバーとして機能する仮想サーバーを作成します。

セッションプロファイル内に DNS サーバーまたは WINS サーバーを追加する

1. 構成ユーティリティの［構成］タブの**ナビゲーションペイン**で、［**NetScaler Gateway** ポリシー］を展開し、［**セッション**］**をクリックします。**
2. 詳細ペインの タブで、プロファイルを選択し、 をクリックします。
3. タブで、次のいずれかの操作を行います。

   - DNSサーバーを構成するには、「DNS仮想サーバー」の横にある「**グローバル上書き**」をクリックし、サーバーを選択して、「**OK**」**をクリックします。**
   - WINS サーバーを構成するには、「WINS Server IP」の横にある「**グローバル上書き**」をクリックし、IP アドレスを入力して「**OK」**をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

重要：

VPN セッションプロファイルにアタッチされたアドレス指定不能 DNS 仮想サーバーでは、レスポンダーポリシーが評価されません。

ユーザー接続のプロキシサポートを有効にする

ユーザーデバイスは、内部ネットワークにアクセスするためにプロキシサーバーを介して接続できます。NetScaler Gateway は、HTTP、SSL、FTP、およびSOCKSプロトコルをサポートしています。ユーザー接続のプロキシサポートを有効にするには、NetScaler Gateway の設定を指定します。NetScaler Gateway 上のプロキシサーバーで使用されるIPアドレスとポートを指定できます。プロキシサーバーは、内部ネットワークへのその後のすべての接続のフォワードプロキシとして使用されます。

プロキシ設定

プロキシ設定は、ブラウザーまたはNetScaler ADCアプライアンスで構成できます。ブラウザーまたはアプライアンスでプロキシ設定を構成するには、［**グローバルNetScaler Gateway 設定**］>［**クライアントエクスペリエンス**］**タブ** >［**詳細設定**］>［**プロキシ**］の順に移動し、必要に応じて［ **ブラウザ** ］または［ **NS** ］を選択します。

- **ブラウザ:ブラウザでプロキシ設定を構成する場合**、自動プロキシ設定ファイルへのリンクを提供することで、自動設定オプションを使用できます。自動構成は、手動設定を上書きする場合があります。

  また、「 **ブラウザ**」を選択すると、プロキシ例外オプションを選択して、以前に構成したプロキシをバイパスできます。

  注: ブラウザプロキシの設定に関する機能は 、クライアントの種類によって異なります。詳しくは、「 NetScaler Gateway VPNクライアントとサポートされる機能」を参照してください。
- **NS**：NetScaler ADCアプライアンスでプロキシ設定を構成する場合、自動構成オプションは使用できません。アプライアンスでプロキシ設定を構成する場合、以前に構成したプロキシをバイパスすることはできません。
- **オフ**:このオプションを選択すると、NetScaler GatewayはVPNプラグインのプロキシ設定を無効にします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ユーザー接続のプロキシサポートを構成するには

1. ナビゲーションペインで［**Citrix Gateway**］を展開し、［**グローバル設定**］**をクリックします。**
2. 詳細ペインの で、 をクリックします。
3. 「クライアントエクスペリエンス」タブで、「**詳細設定**」をクリックします。
4. **タブの で、 を選択します。**
5. プロトコルの場合は、IP アドレスとポート番号を入力し、［**OK**］**をクリックします。**

注：

- を選択した場合は、セキュリティで保護された HTTP 接続と保護されていない HTTP 接続のみをサポートするプロキシサーバーを構成できます。
- NetScaler Gateway でプロキシサポートを有効にしたら、プロトコルに対応するプロキシサーバーのユーザーデバイスの構成の詳細を指定します。

  プロキシサポートを有効にすると、NetScaler Gateway はプロキシサーバーの詳細をクライアントのWebブラウザーに送信し、ブラウザーのプロキシ構成を変更します。

  - When the user device connects to Citrix Gateway, the user device can communicate with the proxy server directly for connection to the user's network.
  - When the user device disconnects from Citrix Gateway, the proxy settings are restored to the previous default settings, that was present before connecting to the VPN plug-in.

NetScaler Gateway のすべてのプロトコルを使用するように1つのプロキシサーバーを構成するには

1つのプロキシサーバーを構成して、NetScaler Gateway が使用するすべてのプロトコルをサポートできます。この設定では、すべてのプロトコルに対して 1 つの IP アドレスとポートの組み合わせが提供されます。

1. ナビゲーションペインで［**Citrix Gateway**］を展開し、［**グローバル設定**］をクリックします。
2. 詳細ペインの で、 をクリックします。
3. 「**クライアントエクスペリエンス**」タブで、「**詳細設定**」**をクリックします。**
4. タブの で、 を選択します。**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. プロトコルの場合は、IP アドレスとポート番号を入力します。
6. ［すべてのプロトコルに同じプロキシサーバーを使用する］をクリックし、［**OK**］**をクリックします。**

分割トンネリングを無効にし、すべてのプロキシ設定を［オン］に設定すると、プロキシ設定がユーザーデバイスに伝播されます。プロキシ設定が Appliance に設定されている場合、設定はユーザーデバイスには反映されません。

NetScaler Gateway は、ユーザーデバイスの代わりにプロキシサーバーに接続します。プロキシ設定はユーザーのブラウザに伝達されないため、ユーザーデバイスとプロキシサーバー間の直接通信はできません。

NetScaler Gateway をプロキシサーバーとして構成するには

NetScaler Gateway をプロキシサーバーとして構成する場合、セキュリティで保護されていないセキュアなHTTPのみがサポートされるプロトコルです。

1. ナビゲーションペインで［**Citrix Gateway**］ を展開し、［**グローバル設定**］**をクリックします。**
2. 詳細ペインの で、 をクリックします。
3. 「**クライアントエクスペリエンス**」タブで、「**詳細設定」をクリックします。**
4. タブの で、 を選択します。
5. プロトコルの場合は、IP アドレスとポート番号を入力し、［**OK**］**をクリックします。**

アドレスプールの設定

状況によっては、NetScaler Gateway プラグインを使用して接続するユーザーに、NetScaler Gateway の一意のIPアドレスが必要になる場合があります。たとえば、Samba 環境では、マップされたネットワークドライブに接続する各ユーザーは、異なる IP アドレスから発信されているように見える必要があります。グループのアドレスプール（IPプーリングとも呼ばれる）を有効にすると、NetScaler Gateway は各ユーザーに一意のIPアドレスエイリアスを割り当てることができます。

アドレスプールは、イントラネット IP アドレスを使用して構成します。次のタイプのアプリケーションでは、IP プールから取得された一意の IP アドレスを使用する必要がある場合があります。

- ボイスオーバー IP
- アクティブFTP
- インスタントメッセージング

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- セキュアシェル (SSH)
- コンピュータのデスクトップに接続するための仮想ネットワークコンピューティング (VNC)
- クライアントデスクトップに接続するためのリモートデスクトップ (RDP)

NetScaler Gateway に接続するユーザーに内部IPアドレスを割り当てるように、NetScaler Gateway を構成できます。固定 IP アドレスをユーザーに割り当てることも、IP アドレスの範囲をグループ、仮想サーバー、またはシステムにグローバルに割り当てることもできます。

NetScaler Gateway では、内部ネットワークのIPアドレスをリモートユーザーに割り当てることができます。内部ネットワークの IP アドレスは、リモートユーザをアドレス指定することができます。IP アドレスの範囲を使用することを選択した場合、システムはオンデマンドでその範囲の IP アドレスをリモートユーザに動的に割り当てます。

アドレスプールを設定するときは、次の点に注意してください。

- 割り当てられた IP アドレスは正しくルーティングされる必要があります。正しいルーティングを確実に行うには、次の点を考慮してください。
  - 分割トンネリングを有効にしない場合は、IP アドレスが Network Address Translation（NAT; ネットワークアドレス変換）デバイスを介してルーティングできることを確認してください。
  - イントラネット IP アドレスを持つユーザー接続によってアクセスされるサーバーには、それらのネットワークに到達するための適切なゲートウェイが構成されている必要があります。
  - ユーザーソフトウェアからのネットワークトラフィックが内部ネットワークにルーティングされるように、NetScaler Gateway でゲートウェイまたは静的ルートを構成します。
- IP アドレス範囲を割り当てるときは、連続したサブネットマスクだけを使用できます。範囲のサブセットは、下位レベルのエンティティに割り当てることができます。たとえば、IP アドレス範囲が仮想サーバーにバインドされている場合は、範囲のサブセットをグループにバインドします。
- IP アドレス範囲は、バインドレベル内の複数のエンティティにバインドできません。たとえば、グループにバインドされているアドレス範囲のサブセットを 2 番目のグループにバインドすることはできません。
- NetScaler Gateway では、ユーザーセッションでアクティブに使用されているIPアドレスを削除またはバインド解除することはできません。
- 内部ネットワーク IP アドレスは、次の階層を使用してユーザーに割り当てられます。
  - ユーザーの直接バインディング

© 1997–2026 Citrix Systems, Inc. All rights reserved.

    - グループ割り当てアドレスプール
    - 仮想サーバ割り当てアドレスプール
    - グローバルアドレス範囲

- アドレス範囲の割り当てに使用できるのは、連続したサブネットマスクだけです。ただし、割り当てられた範囲のサブセットは、下位レベルのエンティティにさらに割り当てられる場合があります。 バインドされたグローバルアドレス範囲には、次の範囲をバインドできます。
    - 仮想サーバー
    - グループ
    - ユーザー
- バインドされた仮想サーバーのアドレス範囲には、次のサブセットをバインドできます。
    - グループ
    - ユーザー

バインドされたグループアドレス範囲は、ユーザーにバインドされたサブセットを持つことができます。

IP アドレスがユーザーに割り当てられると、アドレスプールの範囲がなくなるまで、そのアドレスはユーザーの次回のログオン用に予約されます。アドレスが使い果たされると、NetScaler Gateway は、NetScaler Gateway から最も長くログオフしたユーザーのIPアドレスを再利用します。

アドレスを再利用できず、すべてのアドレスがアクティブに使用されている場合、NetScaler Gateway はユーザーのログオンを許可しません。この状況を回避するには、他のすべてのIPアドレスが使用できない場合に、NetScaler Gateway でマップされたIPアドレスをイントラネットIPアドレスとして使用できるようにします。

イントラネット IP DNS 登録

イントラネット IP がクライアントマシンに割り当てられ、VIP トンネルの確立後に、VPN プラグインは、そのクライアントマシンがドメインに参加しているかどうかをチェックします。クライアントマシンがドメインに参加しているマシンである場合、VPN プラグインは DNS 登録プロセスを開始し、マシンのホスト名イントラネットと割り当てられたイントラネット IP アドレスを結び付けます。この登録は、トンネルの確立解除前に元に戻されます。

DNS 登録を正常に行うには、次の`nsapimgr`ノブが設定されていることを確認してください。また、権限のある DNS サーバーが「非セキュア」DNS 更新を許可するように設定されていることを確認します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **`nsapimgr` -ys enable_vpn_dns_override=1**: このフラグは、他の構成パラメータとともにNetScaler Gateway VPNクライアントに送信されます。このフラグが設定されていない状態でVPNクライアントがDNS/WINS要求をインターセプトすると、対応する「GET/DNS」HTTP要求をトンネル経由でNetScaler Gateway仮想サーバーに送信し、解決されたIPアドレスを取得します。ただし、「enable_vpn_dnstruncate_fix」フラグが設定されている場合、VPNクライアントはDNS/WINS要求をNetScaler Gateway仮想サーバーに透過的に転送します。この場合、DNSパケットはVPNトンネルを介してそのままNetScaler Gateway仮想サーバーに送信されます。これは、NetScaler Gateway で構成されたネームサーバーから返されるDNSレコードが大きく、UPD応答パケットに収まらない場合に役立ちます。この場合、クライアントがTCP-DNSを使用するようフォールバックすると、このTCP-DNSパケットはそのままNetScaler Gatewayサーバーに到達するため、NetScaler GatewayサーバーはDNSサーバーにTCP-DNSクエリを行います。
- **nsapimgr-ys enable_vpn_dnstruncate_fix=1**: このフラグは NetScaler Gateway サーバー自体によって使用されます。このフラグが設定されている場合、NetScaler Gatewayは、NetScaler Gatewayで構成されたDNSサーバーへの「DNSポートでのTCP接続」の宛先をオーバーライドします（受信TCP-DNSパケットに元々存在していたDNSサーバーIPに送信しようとするのではなく）。UDP DNS 要求の場合、デフォルトでは、DNS 解決用に設定された DNS サーバが使用されます。Windows用NetScaler Gateway プラグインは、セキュアなDNSアップデートと非セキュアなDNS 21.7.1.1 以降のビルドでは、セキュア DNS 更新サポートがデフォルトで存在します。

  Windows プラグインのセキュア DNS アップデートは、デフォルトでは無効になっています。有効にするには、`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access` に REG_DWORD 型の値を作成して 1 に設定します。

  - 値を 1 に設定すると、VPN プラグインはセキュリティで保護されていない DNS アップデートを最初に試みます。セキュリティで保護されていない DNS の更新が失敗した場合、VPN プラグインは安全な DNS の更新を試みます。
  - セキュリティで保護された DNS アップデートのみを試すには、値を 2 に設定します。

これらのノブの設定の詳細については、「`<https://support.citrix.com/article/CTX200243>`」を参照してください。

ユーザー、グループ、または仮想サーバーのアドレスプールを構成する

1. 構成ユーティリティのナビゲーションペインで、［**NetScaler Gateway］**を展開し、次のいずれかの操作を行います：
   - 「NetScaler Gateway ユーザー管理」を展開し、「**AAA ユーザー**」をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 「**Citrix Gateway**」>「**ユーザー管理**」を展開し、「**AAAグループ**」をクリックします。
- **NetScaler Gateway** を展開し、「**仮想サーバー**」をクリックします。

2. 詳細ウィンドウで、ユーザー、グループ、または仮想サーバーをクリックし、 をクリックします。
3. タブの に IP アドレスとサブネットマスクを入力し、 をクリックします。
4. プールに追加するIPアドレスごとに手順3を繰り返し、［**OK**］をクリックします。

アドレスプールをグローバルに設定

1. 構成ユーティリティの［**構成**］タブのナビゲーションペインで、［**Citrix Gateway**］を展開し、［**グローバル設定**］をクリックします。
2. 詳細ペインの［**イントラネットIP**］で、［すべてのクライアントNetScaler Gateway セッションで使用する一意の静的IPアドレスまたはIPアドレスのプールを割り当てるには、イントラネットIPを構成します］をクリックします。
3. ダイアログボックスで、、** の順にクリックします。
4. に IP アドレスとサブネットマスクを入力し、 をクリックします。
5. プールに追加するIPアドレスごとに手順3と4を繰り返し、［**OK**］をクリックします。

アドレスプールオプションの定義

セッションポリシーまたはグローバルNetScaler Gateway 設定を使用して、ユーザーセッション中にイントラネットIPアドレスを割り当てるかどうかを制御できます。アドレスプールオプションを定義すると、イントラネットIPアドレスをNetScaler Gateway に割り当てる一方で、特定のユーザーグループのイントラネットIPアドレスの使用を無効にすることができます。

アドレスプールは、次の 3 つの方法のいずれかでセッションポリシーを使用して設定できます：

- `Nospillover` -イントラネット IP アドレスのアドレスプールを構成すると、プールから使用可能な IP を持つセッションが取得されます。使用可能なイントラネット IP アドレスをすべて使用したユーザーには、 ページが表示されます。
- **スピルオーバー** -アドレスプールを構成し、マッピング IP をイントラネット IP アドレスとして使用する場合、マップされた IP アドレスは、使用可能なすべてのイントラネット IP アドレスを使用したユーザーに使用されます。
- **Off** -アドレスプールは設定されていません。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注:

マッピング IP アドレスが設定されていない場合、SNIP が使用されます。

アドレスプールを定義するには

1. 構成ユーティリティの［ **構成** ］タブのナビゲーションペインで、［ **Citrix Gateway**］**>**［**ポリシー**］**を展開し、**［ **セッション**］をクリックします。
2. 詳細ペインの タブで、 をクリックします。
3. ** に、ポリシーの名前を入力します。
4. 「 **リクエストプロファイル**」の横にある「 **新規**」をクリックします。
5. に、プロファイルの名前を入力します。
6. タブで、 をクリックします。
7. の横にある をクリックし、オプションを選択します。
8. 手順9で を選択した場合は、 の横にある をクリックし、アプライアンスのホスト名を選択して をクリックし、** をクリックします。
9. ダイアログボックスで、式を作成し、、 の順にクリックします。

転送ログオンページの設定

ユーザーがイントラネットIPアドレスを使用できず、NetScaler Gateway との別のセッションを確立しようとすると、［ログオンの転送］ページが表示されます。［ログオンの転送］ページでは、ユーザーは既存のNetScaler Gateway セッションを新しいセッションに置き換えることができます。

ログオンの転送ページは、ログオフ要求が失われた場合や、ユーザーがクリーンログオフを実行しなかった場合にも使用できます。例：

- ユーザーには静的イントラネットIPアドレスが割り当てられ、既存のNetScaler Gateway セッションがあります。ユーザーが別のデバイスから 2 つ目のセッションを確立しようとすると、「ログオンの転送」ページが表示され、ユーザーはセッションを新しいデバイスに転送できます。
- ユーザーには5つのイントラネットIPアドレスが割り当てられ、NetScaler Gateway を介して5つのセッションがあります。ユーザーが 6 回目のセッションを確立しようとすると、「ログオンの転送」ページが表示され、ユーザーは既存のセッションを新しいセッションに置き換えることを選択できます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

メモ：

- ユーザーに IP アドレスが割り当てられていないため、新しいセッションを確立できない場合、エラーメッセージが表示されます。
- Citrix Secure Access for Android 23.12.1以降のバージョンでは、常時接続VPNモードでのNetScaler Gatewayの転送ログオン機能がサポートされています。

Transfer Logon ページは、アドレスプールを設定してスピルオーバーを無効にした場合にのみ表示されます。

DNS サフィックスを構成する

ユーザーがNetScaler Gateway にログオンし、IPアドレスが割り当てられると、ユーザー名とIPアドレスの組み合わせのDNSレコードがNetScaler Gateway DNSキャッシュに追加されます。DNS レコードがキャッシュに追加されたときにユーザー名に追加するように DNS サフィックスを構成できます。これにより、ユーザは DNS 名で参照され、IP アドレスよりも覚えやすくなります。ユーザーがNetScaler Gateway からログオフすると、レコードはDNSキャッシュから削除されます。

DNS サフィックスを構成するには

1. 構成ユーティリティの［ **構成** ］タブのナビゲーションペインで、［ **Citrix Gateway**］ **>** ［**ポリシー**］**を展開し、** ［ **セッション**］をクリックします。
2. 詳細ペインの タブで、セッションポリシーを選択し、 をクリックします。
3. 「リクエストプロファイル」の横にある「 **変更**」をクリックします。
4. タブで、 をクリックします。
5. **「イントラネット IP DNS サフィックス」の横にある「グローバルを上書き」をクリックし、DNS サフィックスを入力して「OK」を 3 回クリックします。**

VoIP 電話のサポート

Citrix Gatewayをスタンドアロンアプライアンスとしてインストールし、ユーザーがCitrix Secure Accessクライアントに接続すると、Citrix GatewayはボイスオーバーIP（VoIP）ソフトフォンとの双方向通信をサポートします。

Citrix Secure AccessがサポートするVoIPソフトフォンの一部は次のとおりです：

- Cisco Softphone

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Avaya IP Softphone

セキュアトンネリングは、IP PBX と、ユーザデバイス上で実行されているソフトフォンソフトウェアとの間でサポートされています。VoIPトラフィックが安全なトンネルを通過できるようにするには、Citrix Secure Accessクライアントとサポートされているソフトフォンのいずれかを同じユーザーデバイスにインストールする必要があります。

VoIPトラフィックが安全なトンネルを介して送信される場合、Citrix Secure Accessは次のソフトフォン機能をサポートします：

- IP ソフトフォンから発信された発信コール
- IP ソフトフォンに発信される着信コール
- 双方向音声トラフィック
- VoIP アプリケーションによる TCP および UDP 制御フロー

注：

DNE を使用する UDP 制御フローでは、非アクティブ時間が 30 秒以上続くと VoIP アプリケーションが切断されます。そのため、VoIPアプリケーションがUDP制御メッセージングをサポートしていて問題が発生した場合は、Citrix Secure AccessをWFPモードで使用することをお勧めします。

VoIP ソフトフォンのサポートは、イントラネット IP アドレスを使用して設定します。各ユーザーのイントラネット IP アドレスを構成する必要があります。Cisco Softphone Communication を使用している場合は、イントラネット IP アドレスを設定してユーザにバインドした後、追加の設定は必要ありません。イントラネット IP アドレスの構成の詳細については、「アドレスプールの構成」を参照してください。

分割トンネリングを有効にする場合は、イントラネットアプリケーションを作成し、Avaya Softphone アプリケーションを指定します。さらに、透過的な代行受信を有効にする必要があります。

Access Interfaceの設定

NetScaler Gateway には、ユーザーがログオンした後に表示されるデフォルトのホームページが含まれています。デフォルトのホームページはAccess Interfaceと呼ばれます。Access Interface をホームページとして使用するか、Web Interface をホームページまたはカスタムホームページとして設定します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Access Interfaceには 3 つのパネルがあります。展開環境にWeb Interfaceがある場合、ユーザーはAccess Interfaceの左側のパネルでReceiverにログオンできます。展開環境にStoreFront がある場合、ユーザーは左側のパネルからReceiverにログオンできません。

Access Interfaceは、内部および外部のWebサイトへのリンク、および内部ネットワークのファイル共有へのリンクを提供するために使用されます。Access Interfaceは、次の方法でカスタマイズできます。

- Access Interfaceの変更。
- Access Interfaceリンクの作成。

ユーザーは、Web サイトやファイル共有への独自のリンクを追加して、Access Interfaceをカスタマイズすることもできます。ユーザーは、ホームページを使用して、内部ネットワークからデバイスにファイルを転送することもできます。

注:

ユーザーがログオンし、Access Interface からファイル共有を開こうとすると、ファイル共有は開かず、「サーバーへの TCP 接続に失敗しました」というエラーメッセージが表示されます。この問題を解決するには、NetScaler Gateway システムのIPアドレスからTCPポート445および139のファイルサーバーIPアドレスへのトラフィックを許可するようにファイアウォールを構成します。

Access Interfaceの変更

Access Interface に依存するのではなく、カスタマイズされたホームページにユーザーを誘導したい場合があります。これを行うには、NetScaler Gateway にホームページをインストールし、新しいホームページを使用するようにセッションポリシーを構成します。

カスタマイズしたホームページをインストールするには

1. 構成ユーティリティで、［**構成**］タブをクリックし、ナビゲーションペインで［**Citrix Gateway**］**をクリックします。**
2. 詳細ペインの で、 をクリックします 。
3. ネットワーク上のコンピュータ上のファイルからホームページをインストールするには、 でをクリックし、ファイルに移動して、 をクリックします。**
4. NetScaler Gateway にインストールされているホームページを使用するには、［リモートパス］で［**参照**］をクリックし、ファイルを選択して［**選択**］**をクリックします。**
5. をクリックし、 をクリックします**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Access Interfaceをカスタムホームページに置き換える

グローバル設定またはセッションポリシーおよびプロファイルのいずれかを使用して、カスタムホームページを構成して、デフォルトのホームページであるAccess Interfaceを置き換えることができます。ポリシーを構成したら、ポリシーをユーザー、グループ、仮想サーバー、またはグローバルにバインドできます。カスタムホームページを構成すると、ユーザーのログオン時にAccess Interfaceは表示されません。

カスタムホームページをグローバルに構成する

1. 構成ユーティリティの［ **構成** ］タブのナビゲーションペインで、［ **Citrix Gateway** ］を展開し、［ **グローバル設定］をクリックします。**
2. 詳細ペインの で、 をクリックします。
3. タブの で、 をクリックし、** カスタムホームページの Web アドレスを入力します。
4. 「 **OK」をクリックし、「**閉じる」をクリックします。**

セッションプロファイルでのカスタムホームページの設定

1. 構成ユーティリティの［ 構成 ］タブの**ナビゲーションペイン**で、［ **NetScaler Gateway** ポリシー ］を展開し、［ **セッション］をクリックします。**
2. 詳細ペインの タブで、 をクリックします。**
3. に、ポリシーの名前を入力します。
4. 「 **リクエストプロファイル**」の横にある「 **新規」をクリックします。**
5. ** に、プロファイルの名前を入力します。
6. タブの の横にある をクリックし **、 をクリックして、ホームページの Web アドレスを入力します。
7. ダイアログボックスで、 の横にある を選択し、 を選択し、 をクリックして をクリックし、**をクリックします。**

Web リンクの作成と適用

Access Interfaceは、ユーザが使用できる内部リソースへのリンクのセットを表示するように設定できます。これらのリンクを作成するには、最初にリンクをリソースとして定義する必要があります。次に、それらをユーザー、グループ、仮想サーバー、またはグローバルにバインドして、Access Interfaceでアクティブにします。作成したリンクは、 の下の ウィンドウに表示されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

重要：

NetScaler ADCリリース13.0ビルド64.xx以降では、NetScaler Gateway を介したファイル共有はサポートされていません。

エンタープライズブックマークの作成

セッションポリシーでAccess Interfaceリンクを作成するには

1. 構成ユーティリティの［ **構成** ］タブのナビゲーションペインで、［ **NetScaler Gateway**］> ［**リソース** ］の順に展開し、［ **ポータルブックマーク**］**をクリックします。**
2. 詳細ペインで、 をクリックします。**



3. に、ブックマークの名前を入力します。
4. ** に、リンクの説明を入力します。**説明はAccess Interfaceに表示されます。**
5. に、アプリケーションの Web アドレスを入力します。
6. に、関連する負荷分散/コンテンツスイッチング仮想サーバーの名前を入力します。この情報は入力しなくても構いません。
7. **Icon URLでは、**アップロードされたアイコンは、デフォルトテーマを除くすべてのテーマでサポートされています。推奨最大サイズは 70 x 70 ピクセルです。透明な画像を使用することをおすすめします。この情報は入力しなくても構いません。
8. で、URL が表すアプリケーションのタイプ（VPN、クライアントレス VPN、または SaaS）を選択します。この情報は入力しなくても構いません。
9. で、ブックマークに設定する SSO タイプを選択します。SSO を設定すると、ユーザーはその後のログオン時に資格情報を入力しなくてもアプリケーションにアクセスできます。次の SSO タイプがサポートされています。

    - Unified Gateway: この SSO 設定により、単一の URL からアプリケーションの複数のリソースへの安全なリモートアクセスが可能になります。
    - 自己認証：このSSO構成では、NetScaler Gateway ユーザーはアプリケーションにアクセスするためのログイン資格情報を入力するよう求められます。
    - SAMLベースの認証：このSSO構成では、NetScaler Gateway はIdPを使用してユーザーの詳細を検証し、SAMLアサーションを生成してSPに送信します。検証に合格すると、SSOは成功します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注：

クライアントレスアクセスを有効にすると、Webサイトへの要求がNetScaler Gateway を経由するようにできます。たとえば、 Googleのブックマークを追加したとします。「 **NetScaler Gateway をリバースプロキシとして使用する** 」チェックボックスを選択します。このチェックボックスをオンにすると、Webサイト要求はユーザーデバイスから NetScaler Gateway に送信され、次にWebサイトに送信されます。チェックボックスをオフにすると、要求はユーザーデバイスから Web サイトに送信されます。このチェックボックスは、クライアントレスアクセスを有効にした場合にのみ使用できます。

10. をクリックし、 をクリックします**。**

Access Interfaceリンクをバインドするには

Access Interfaceリンクは、次の場所にバインドできます。

- ユーザー
- グループ
- 仮想サーバー

構成を保存すると、 タブの でユーザーがリンクを使用できるようになります。このタブは、ユーザーが正常にログオンした後に最初に表示されるページです。

1. 構成ユーティリティのナビゲーションペインで、次のいずれかの操作を行います：
   - 「 **Citrix Gateway ユーザー管理** 」を展開し、「 **AAA ユーザー**」をクリックします。
   - ［**NetScaler Gateway ユーザー管理** ］を展開し、［ **AAAグループ］をクリックします。**
   - **Citrix Gateway** を展開し、「 **仮想サーバー」をクリックします。**
2. 詳細ウィンドウで、次のいずれかの操作を行います：
   - ユーザーを選択し、 をクリックします。
   - グループを選択し、 をクリックします。
   - 仮想サーバーを選択し、 をクリックします。
3. ダイアログボックスで、 タブをクリックします。
4. ［ **使用可能なブックマーク**］で、1つまたは複数のブックマークを選択し、右矢印をクリックしてブックマークを［構成済みのブックマーク］の下に移動してから、 **［OK］をクリックします。**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

GUI を使用してブックマークをグローバルにバインドするには

1. ［**構成**］タブのナビゲーションペインで、［**Citrix Gateway**］を展開し、［**グローバル設定**］**をクリックします。**
2. 詳細ペインの［**ブックマーク**］で、 **NetScaler Gateway ポータルページでアクセス可能にするHTTPおよびWindowsファイル共有アプリケーションへのリンクの作成をクリックします。**

   
3. ダイアログボックスで、 をクリックします。**
4. で、1 つ以上のブックマークを選択し、右矢印をクリックしてブックマークを に移動し、次にの下に移動します。

CLI を使用してエンタープライズブックマークを追加するには

コマンドプロンプトで入力します：

```
add vpn url <urlName> <linkName> <actualURL>  [-ssotype <ssotype>]
```

例:

Web ブックマーク

```
add vpn url google google "https://www.google.com"
```

CLI を使用してエンタープライズブックマークをバインドするには

Enterprise ブックマークは、ユーザー、グループ、仮想サーバー、およびグローバルレベルにバインドできます。

```
bind aaa user <userName> -urlName <string>

bind aaa group <groupName> -urlName <string>

bind vpn vserver <vserverName> -urlName <string>

bind vpn global –urlName <string>
```

例:

```
bind vpn global -urlName google
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

個人用ブックマークの作成

個人用 Web サイトは、VPN 仮想サーバーからのみ作成できます。個人用ブックマークを追加するためのNetScaler Gateway 管理GUIはありません。

1. VPN 仮想サーバーにログオンします。
2. または をクリックして、ブックマークを追加します。
3. **［追加］** をクリックします。



4. Web サイト名、住所、説明などのブックマークの詳細を入力します。



5. **［追加］** をクリックします。

追加した Web サイトは、それぞれのタブの下に表示されます。



ブックマークでユーザー名トークンを構成する

特別なトーク ン %`username`% を使用して、ブックマークとファイル共有 URL を構成できます。ユーザーがログオンすると、トークンは各ユーザーのログオン名に置き換えられます。たとえば、\\\ EmployeeServer\\%`username`%\ というフォルダに、Jack という名前の従業員用のブックマークを作成するとします。ジャックがログオンすると、ファイル共有 URL は\\\ EmployeeServer\ Jack\ にマップされます。ブックマークでユーザー名トークンを構成するときは、次の状況に留意してください。

- 1 つの認証タイプを使用している場合は、トークン%`username`% がユーザー名に置き換えられます。
- 2 要素認証を使用している場合は、プライマリ認証タイプのユーザー名が%`username`% トークンを置き換えるために使用されます。
- クライアント証明書認証を使用している場合は、クライアント証明書認証プロファイルのユーザー名フィールドを使用して、 %`username`% トークンを置き換えます。

トラフィックポリシー

トラフィックポリシーを使用すると、ユーザー接続の次の設定を構成できます：

- 信頼できないネットワークからアクセスされる機密性の高いアプリケーションのタイムアウトを短縮します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 一部のアプリケーションで TCP を使用するようにネットワークトラフィックを切り替えます。 を選択した場合は、特定のアプリケーションのシングルサインオンを有効または無効にする必要があります。
- NetScaler Gateway プラグインのトラフィックに他のHTTP機能を使用する状況を特定する。
- ファイルタイプの関連付けで使用されるファイル名拡張子の定義。

トラフィックポリシーを作成する

トラフィックポリシーを設定するには、プロファイルを作成し、次のパラメータを設定します：

- プロトコル (HTTP または TCP)
- アプリケーションのタイムアウト
- Web アプリケーションへのシングルサインオン
- フォームシングルサインオン
- ファイルタイプの関連付け
- リピータプラグイン
- Kerberos 制約付き委任 (KCD) アカウント

トラフィックポリシーを作成したら、ポリシーを仮想サーバ、ユーザ、グループ、またはグローバルにバインドできます。

たとえば、Web アプリケーション PeopleSoft Human Resources が内部ネットワークのサーバーにインストールされているとします。このアプリケーションのトラフィックポリシーを作成して、宛先 IP アドレス、宛先ポートを定義し、ユーザーがアプリケーションにログオンしたままにできる時間（15 分など）を設定できます。

アプリケーションに対する HTTP 圧縮などの他の機能を設定する場合は、トラフィックポリシーを使用して設定を構成できます。ポリシーを作成するときは、アクションに HTTP パラメータを使用します。式で、アプリケーションを実行しているサーバーの宛先アドレスを作成します。

トラフィックポリシー表現の例

トラフィックポリシーの表現例を次に示します。

- `add vpn trafficPolicy trafPol1 "HTTP.REQ.URL.CONTAINS(\"/Citrix/\") || HTTP.REQ.URL.CONTAINS(\"10.102.\")")" trafAct1`
- `add vpn trafficPolicy trafPol2 "HTTP.REQ.HOSTNAME.CONTAINS(\"portal-srv\") || HTTP.REQ.URL.CONTAINS(\"homePage\"))" trafAct2`
- `add vpn trafficPolicy trafPol3 true trafAct3`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

GUI を使用したトラフィックポリシーの設定

1. ［**NetScaler Gateway**］ **>** ［**ポリシー** ］の順に展開し、［ **トラ**
2. 詳細ペインの タブで、 をクリックします。
3. ダイアログボックスの に、ポリシーの名前を入力します。
4. 「 **リクエストプロファイル**」の横にある「 **新規**」をクリックします。
5. ** に、プロファイルの名前を入力します。
6. で、 または を選択します。

   注： プロトコルとして を選択した場合、シングルサインオンを構成できず、この設定はプロファイルダイアログボックスで無効になります。
7. に、分数を入力します。この設定では、ユーザーが Web アプリケーションにログオンしたままにできる時間を制限します。
8. Web アプリケーションへのシングルサインオンを有効にするには、 で を選択します。

   注:フォームベースのシングルサインオンを使用する場合は、トラフィックプロファイル内で設定を構成できます。詳細については、「 フォームベースのシングルサインオンの設定」を参照してください。
9. ファイルの種類の関連付けを指定するには、 で を選択します。
10. リピータプラグインを使用してネットワークトラフィックを最適化するには、Citrix SD-WAN で［ **オン**］を選択し、［ **作成**］、［ **閉じる**］の順にクリックします。
11. アプライアンスで KCD を設定する場合は、 でアカウントを選択します。

    アプライアンスでのKCDの構成について詳しくは、「 NetScalerアプライアンスでのKerberos制約付き委任の構成」を参照してください。
12. ダイアログボックスで、式を作成または追加し、 をクリックし、** をクリックします。

フォームベースのシングルサインオンの設定

フォームベースのシングルサインオンを使用すると、ユーザーはネットワーク内のすべての保護されたアプリケーションに 1 回ログオンできます。NetScaler Gateway でフォームベースのシングルサインオンを構成すると、ユーザーはパスワードをもう一度入力しなくても、HTMLフォームベースのログオンを必要とするWebアプリケーションにアクセスできます。シングルサインオンを使用しない場合、ユーザーは各アプリケーションにアクセスするために個別にログオンする必要があります。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

フォームシングルサインオンプロファイルを作成したら、フォームシングルサインオンプロファイルを含むトラフィックプロファイルとポリシーを作成します。詳細については、 トラフィックポリシーの作成を参照してください。

フォームベースのシングルサインオンの設定

1. 「 **Citrix Gateway**」>「**ポリシー**」を展開し、 「 **トラフィック**」をクリックします。
2. 詳細ペインで、 タブをクリックし、 をクリックします。
3. ** に、プロファイルの名前を入力します。
4. に、完了したフォームの送信先の URL を入力します。

   注: URL はルート相対 URL です。
5. に、ユーザー名フィールドの属性の名前を入力します。
6. に、パスワードフィールドの属性の名前を入力します。
7. **SSO 成功ルールで**、ポリシーによって呼び出されたときにこのプロファイルが実行するアクションを説明する式を作成します。このフィールドの下にある 、、および ボタンを使用して、エクスプレッションを作成することもできます。

   このルールは、シングルサインオンが成功したかどうかをチェックします。
8. に、ユーザー名フィールドの値、アンパサンド (&)、パスワードフィールドの値を入力します。

   値の名前は、名前1=値1&名前2=値2 のようにアンパサンド (&) で区切ります。
9. に、完全なレスポンスサイズに許容するバイト数を入力します。フォームを抽出するために解析する応答のバイト数を入力します。
10. 「 **抽出**」で、名前/値のペアが静的か動的かを選択します。既定の設定は です。
11. で、ログオン資格情報をログオンサーバーに送信するためにシングルサインオンフォームで使用される HTTP メソッドを選択します。デフォルトは Get です。
12. をクリックし、** をクリックします。

SAML シングルサインオンの設定

シングルサインオン (SSO) 用の SAML 1.1 または SAML 2.0 プロファイルを作成できます。ユーザーは、シングルサインオン用の SAML プロトコルをサポートする Web アプリケーションに接続できます。NetScaler Gateway は、SAML Webアプリケーションのアイデンティティプロバイダー（IdP）シングルサインオンをサポートしています。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SAML シングルサインオンの設定

1. 構成ユーティリティの［構成］タブのナビゲーションペインで、［**NetScaler Gateway**］>［**ポリシー** ］の順に展開し、［トラフィック］をクリックします。
2. 詳細ペインで、 タブをクリックします。
3. 詳細ペインで、［Add］ をクリックします。
4. に、プロファイルの名前を入力します。
5. に、X.509 証明書の名前を入力します。
6. に、ID プロバイダーまたはサービスプロバイダーのアサーションコンシューマサービスを入力します。アサーションコンシューマサービスURL（ACS URL）は、ユーザに SSO 機能を提供します。
7. で、 と からポリシーの式を作成します。「演算子」(Operator) リストから選択して、式の評価方法を定義します。式をテストするには、 をクリックします。
8. で、 または を選択
9. に、SAML アプリケーションの ID を入力します。
10. ［Create］ をクリックしてから、［Close］ をクリックします。

トラフィックポリシーをバインドする

トラフィックポリシーは、仮想サーバー、グループ、ユーザー、およびNetScaler Gateway Global にバインドできます。構成ユーティリティを使用して、トラフィックポリシーをバインドできます。

GUI を使用してトラフィックポリシーをグローバルにバインドする

1. 構成ユーティリティの［構成］タブのナビゲーションペインで、［**Citrix Gateway**］>［**ポリシー**］ を展開し、［トラフィック］をクリックします。
2. 詳細ペインでポリシーを選択し、 で をクリックします。
3. ダイアログボックスの で、 をクリックします。
4. ［ポリシー名］でポリシーを選択し、［ OK］をクリックします。

トラフィックポリシーの削除

いずれかの構成ユーティリティを使用して、NetScaler Gateway からトラフィックポリシーを削除できます。構成ユーティリティを使用してトラフィックポリシーを削除し、ポリシーがユーザー、グループ、または仮想サーバレベルにバインドされている場合は、まずポリシーをバインド解除する必要があります。その後、ポリシーを削除できます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

GUI を使用してトラフィックポリシーをバインド解除する

1. ［**NetScaler Gateway**］を展開し、 ［ **仮想サーバー**］をクリックします。
   - 「**NetScaler Gateway**」>「**ユーザー管理**」を展開し 、「 **AAAグループ**」をクリックします。
   - 「 **Citrix Gateway**」>「**ユーザー管理** 」を展開し、「 **AAAユーザー**」をクリックします。
2. 詳細ペインで、仮想サーバー、グループ、またはユーザーを選択し、 をクリックします。
3. ［**NetScaler Gateway 仮想サーバーの構成**］、［**AAAグループの構成**］、または［ **AAAユーザーの構成** ］ダイアログボックスで、 ［ **ポリシー** ］タブをクリックします。
4. をクリックし、ポリシーを選択して、 をクリックします。
5. 「 **OK**」をクリックし、 「 **閉じる**」をクリックします。

トラフィックポリシーのバインドが解除されたら、ポリシーを削除できます。

GUI を使用してトラフィックポリシーを削除する

1. 「 **NetScaler Gateway**」>「**ポリシー**」を展開し、「 **トラフィック**」をクリックします。
2. 詳細ペインの タブで、トラフィックポリシーを選択し、 をクリックします。

セッションポリシー

セッションポリシーは、ユーザー、グループ、仮想サーバー、およびグローバルに適用される式と設定の集合です。

セッションポリシーを使用して、ユーザー接続の設定を構成します。ソフトウェアユーザーのログオンに使用する設定を定義できます。たとえば、Windows用のNetScaler GatewayプラグインやMac用のNetScaler Gatewayプラグインなどです。また、ユーザーにCitrix Workspace アプリまたはSecure Hubでのログオンを要求する設定を構成することもできます。ユーザーが認証されると、セッションポリシーが評価され、適用されます。

セッションポリシーは、次の規則に従って適用されます：

- セッションポリシーは、常に設定内のグローバル設定よりも優先されます。
- セッションポリシーを使用して設定されていない属性またはパラメータは、仮想サーバ用に確立されたポリシーに設定されます。
- グローバル構成は、セッションポリシーまたは仮想サーバーによって設定されていない他の属性を設定します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

重要:

次の手順は、セッションポリシーを作成するための一般的なガイドラインです。クライアントレスアクセスや公開アプリケーションへのアクセスなど、さまざまな構成のセッションポリシーを構成するための具体的な手順があります。手順には、特定の設定を構成するための指示が含まれている場合があります。ただし、この設定は、セッションプロファイルとポリシーに含まれる多くの設定の 1 つになる場合があります。

Citrix Endpoint ManagementまたはStoreFront をネットワークに展開する場合は、クイック構成ウィザードを使用してセッションポリシーとプロファイルを構成することをお勧めします。ウィザードの実行時に、展開の設定を定義します。NetScaler Gateway は、必要な認証、セッション、およびクライアントレスアクセスポリシーを作成します。

セッションポリシーを作成する

1. 構成ユーティリティの［構成］タブのナビゲーションペインで、［**NetScaler Gateway**］>［**ポリシー** ］を展開し、［セッション］をクリックします。
2. 詳細ペインの タブで、 をクリックします。
3. に、ポリシーの名前を入力します。
4. 「リクエストプロファイル」の横にある「 新規」をクリックします。
5. に、プロファイルの名前を入力します。
6. セッションプロファイルの設定を完了し、 をクリックします。
7. ダイアログボックスで、ポリシーの式を追加し、 をクリックし、 をクリックします。 注:式で を選択すると、ポリシーがバインドされているレベルに常に適用されます。

セッションポリシー表現の例

セッションポリシーの表現例は次のとおりです。

- `add vpn sessionPolicy sessPol1 "HTTP.REQ.HEADER(\"User-Agent\").CONTAINS(\"CitrixReceiver\") || HTTP.REQ.HEADER(\"User-Agent\").CONTAINS(\"CitrixWorkspace\")" sessAct1`
- `add vpn sessionPolicy sessPol2 "HTTP.REQ.HEADER(\"User-Agent\").CONTAINS(\"CitrixReceiver\").NOT" sessAct2`
- `add vpn sessionPolicy sessPol3 true sessAct3`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

セッションポリシーのバインド

セッションポリシーを作成したら、ユーザー、グループ、仮想サーバー、またはグローバルにバインドします。セッションポリシーは、次の順序で階層として適用されます。

- ユーザー
- グループ
- 仮想サーバー
- グローバルに

GUI を使用してセッションポリシーを仮想サーバーにバインドする

1. ［**NetScaler Gateway**］>［**仮想サーバー**］に移動します。
2. 仮想サーバを選択し、 をクリックします。新しい仮想サーバーを作成することもできます。
3. セクションまで下にスクロールし、 アイコンをクリックします。
4. ** で を選択します。
5. **「タイプの選択」**で、「**要求**」を選択し、「**続行**」をクリックします。
6. ** で、この仮想サーバーにバインドするポリシーを選択します。
7. に、ポリシーのプライオリティ番号を入力します。
8. ［**Bind**］ をクリックします。

GUI を使用して、セッションポリシーを認証、承認、および監査グループにバインドする

1. **NetScaler Gateway > ユーザー管理 > AAA グループに移動します。**
2. 既存の認証、承認、および監査グループを選択し、 をクリックします。認証、承認、および監査グループを作成することもできます。
3. で、 をクリックし、** アイコンをクリックします。
4. ** で を選択し、 をクリックします。
5. で、この認証、承認、および監査グループにバインドするポリシーを選択します。
6. に、ポリシーのプライオリティ番号を入力します。
7. ［**Bind**］ をクリックします。

GUI を使用して、セッションポリシーを認証、承認、および監査中のユーザーにバインドする

1. **NetScaler Gateway > ユーザー管理 > AAAユーザーに移動します。**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. 既存のNetScaler ADCユーザーを選択し、［**編集**］をクリックします。認証、承認、および監査ユーザーを作成することもできます。
3. で、 をクリックし、** アイコンをクリックします。
4. ** で を選択し、 をクリックします。
5. で、この認証、承認、および監査ユーザーにバインドするポリシーを選択します。
6. に、ポリシーのプライオリティ番号を入力します。
7. ［**Bind**］ をクリックします。

注:優先度の詳細については、`<https://support.citrix.com/article/CTX214588>`を参照してください。

セッションプロファイルを作成する

セッションプロファイルには、ユーザー接続の設定が含まれています。

セッションプロファイルは、ユーザーデバイスがポリシー表現条件を満たしたときにユーザーセッションに適用されるアクションを指定します。プロファイルは、セッションポリシーで使用されます。構成ユーティリティを使用して、セッションポリシーとは別にセッションプロファイルを作成し、そのプロファイルを複数のポリシーに使用できます。1 つのポリシーで使用できるプロファイルは 1 つだけです。

セッションプロファイルでユーザー接続のネットワーク設定を構成する

セッションプロファイルの タブを使用して、ユーザー接続の次のネットワーク設定を構成できます：

- DNS サーバー
- WINS サーバの IP アドレス
- イントラネット IP アドレスとして使用できるマップされた IP アドレス
- アドレスプール (イントラネット IP アドレス) のスピルオーバー設定
- イントラネット IP DNS サフィックス
- HTTP ポート
- 強制タイムアウト設定

セッションプロファイルで接続設定を構成する

セッションプロファイルの「 **クライアントエクスペリエンス** 」タブを使用して、次の接続設定を構成できます：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Access Interfaceまたはカスタマイズされたホームページ
- Web ベースの電子メールの Web アドレス (Outlook Web Access など)
- プラグインの種類（Windowsの場合はNetScaler Gatewayプラグイン、macOS Xの場合はNetScaler Gatewayプラグイン、Javaの場合はNetScaler Gatewayプラグイン）
- 分割トンネリング
- セッションおよびアイドルタイムアウトの設定
- クライアントレスアクセス
- クライアントレスアクセス URL エンコーディング
- プラグインの種類 (Windows、Mac、または Java)
- Web アプリケーションへのシングルサインオン
- 認証用のクレデンシャルインデックス
- Windows でのシングルサインオン
- クライアントのクリーンアップ動作
- ログオンスクリプト
- クライアントデバッグ設定
- 分割DNS
- プライベートネットワーク IP アドレスとローカル LAN アクセスへのアクセス
- クライアントの選択肢
- プロキシ設定

ユーザー接続の設定の構成について詳しくは、「NetScaler Gateway プラグインの接続の構成」を参照してください。

セッションプロファイルでセキュリティ設定を構成する

セッションプロファイルの タブを使用して、次のセキュリティ設定を構成できます：

- デフォルトの承認アクション (許可または拒否)
- iOS デバイスからの接続のSecure Browse
- 検疫グループ
- オーソリゼーショングループ

NetScaler Gateway での承認の構成について詳しくは、「承認の構成」を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

セッションプロファイルでのCitrix Virtual Apps and Desktops の設定の構成

セッションプロファイルの［**公開アプリケーション**］タブを使用して、Citrix Virtual Apps and Desktopsを実行しているサーバーへの接続に関する次の設定を構成できます：

- ICAプロキシ：Citrix Workspace アプリを使用したクライアント接続
- Web インターフェイスアドレス
- Web インターフェイスポータルモード
- サーバーファームドメインへのシングルサインオン
- Citrix Workspace アプリのホームページ
- アカウントサービスアドレス

  詳細については、「Web Interfaceを介した公開アプリケーションおよび仮想デスクトップへのアクセスの提供」を参照してください。

セッションプロファイルは、セッションポリシーとは別に作成できます。ポリシーを作成するときに、ポリシーにアタッチするプロファイルを選択できます。

GUI を使用してセッションプロファイルを作成するには

1. 構成ユーティリティの［構成］タブのナビゲーションペインで、［**NetScaler Gateway**］>［**ポリシー**］**を展開し、**［**セッション**］をクリックします。
2. 詳細ウィンドウで、 タブをクリックし、 をクリックします。
3. プロファイルの設定を行います。
4. をクリックし、 をクリックします。

プロファイルを作成したら、そのプロファイルをセッションポリシーに含めることができます。

GUI を使用してセッションポリシーにプロファイルを追加するには

1. 構成ユーティリティのナビゲーションペインで、「**Access Gateway**」>「**ポリシー** 」を展開し、「**セッション**」をクリックします。
2. 「**ポリシー** 」タブで、次のいずれかを実行します。
   - をクリックしてセッションポリシーを作成します。
   - ポリシーを選択し、 をクリックします。
3. 「**リクエスト・プロファイル**」で、リストからプロファイルを選択します。
4. セッションポリシーの構成を完了し、次のいずれかを実行します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

a. をクリックし、** をクリックしてポリシーを作成します。

b. ［**OK**］**をクリックし、** ［**閉じる** ］をクリックしてポリシーを変更します。

StoreFront のNetScaler Gateway セッションポリシーを構成する

この記事では、Citrix WorkspaceアプリまたはWebブラウザーを使用しているユーザーのために、StoreFront でNetScaler Gateway ドメインのみの認証を構成する方法について説明します。

最小要件

- Citrix StoreFront 2.xまたは3.0
- NetScaler ADC 10.5以上
- Windows向けCitrix Workspaceアプリ4.x
- Mac向けCitrix Workspaceアプリ11.8
- Webブラウザー（Web向けCitrix Workspaceアプリ）
- CTX108876-NetScaler ADCアプライアンスでLDAP認証を構成する方法で説明されているように、NetScaler ADCアプライアンスで構成された認証
- StoreFront サーバーおよびNetScaler Gateway 用に構成されたSSL証明書。次のトピックについて詳しくは、 StoreFront のドキュメントを参照してください。

  - StoreFront 2.6のインストールとセットアップ

    - Windows Server 2012証明書
    - SSL バインドをサイトに追加するには
    - NetScaler ADCアプライアンス10.5の証明書のインストールと管理

StoreFront でNetScaler Gateway を構成する

Webブラウザーベースのアクセス用のセッションポリシーを作成する

1. ［**NetScaler Gateway**］**>**［**ポリシー**］**>**［**セッション**］ に移動します。
2. ［**セッションポリシー**］ タブで ［**追加**］ をクリックします。
3. ［**名前**］ に、セッションポリシーの名前を入力します。たとえば、Web_Browser_Policy のようにします。
4. ［**プロファイル**］ で、 ［**追加**］ をクリックします。 ［**NetScaler Gateway セッションポリシーの作成** ］ページが表示されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. 必須フィールドを更新し、「**作成**」をクリックします。



6. **NetScaler Gateway のセッションポリシーとプロファイルページで** 、セッションポリシーを選択します。
7. **セッションプロファイルを追加するには、「プロファイル」フィールドに移動し、「追加」をクリックします。** ［**NetScaler Gateway セッションプロファイルの作成**］ページが表示されます。

   セッションプロファイルに名前を割り当てます。すべてのタブの**［グローバルオーバーライド**]チェックボックスをオンにすると、NetScaler Gateway グローバルパラメーターから継承された値を上書きできます。 次の設定例では、必須パラメータについて説明しています：
8. タブで、次の設定を行います：

   - **接続**の強制終了：ユーザーがNetScaler Gateway にログオンする前に存在していた接続をNetScaler Gatewayで切断し、ユーザーが接続していて分割トンネリングが無効になっている場合に受信接続を禁止するかどうかを指定します。



9. 「**クライアントエクスペリエンス**」タブで、次の設定を行います：

   - **分割トンネル**：NetScaler Gateway で定義されているイントラネットアプリケーションのトラフィックのみをトンネリングします。他のすべてのトラフィックをインターネットに直接ルーティングします。
   - **クライアントレスアクセス**：［**許可**］に設定すると、Citrix Secure Accessクライアントをインストールしなくてもアプリケーションにアクセスできます。
   - **クライアントレスアクセス URL エンコーディング:クライアントレスアクセスが有効になっている場合は、内部 Web アプリケーションのアドレスをエンコードするか**、アドレスをプレーンテキストのままにすることができます。
   - **クライアントレスアクセスパーシステント Cookie**: これを に設定すると、クライアントレスアクセスモードでのパーシステント Cookie の状態が表示されます。永続的な Cookie はユーザーデバイス上に残り、HTTP 要求ごとに送信されます。
   - **高度なクライアントレス VPN モード**:高度なクライアントレス VPN モードを有効または無効にします。STRICT オプションを使用すると、アドバンスドクライアントレスモードを使用する際に、従来のクライアントレス VPN モードがブロックされます。
   - **プラグインタイプ**:単一の IP アドレスとサブネットマスク、または一定範囲の IP アドレスを使用して、ネットワークリソースにアクセスできます。無効にすると、NetScaler

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Gateway はモードをプロキシに設定し、送信元と宛先のIPアドレス、およびポート番号を構成します。

- **Webアプリケーションへのシングル・サインオン**:このオプションを有効にすると、セッションのシングル・サインオン (SSO) を設定できます。ユーザーがサーバーにアクセスすると、ユーザーのログイン資格情報は認証のためにサーバーにリダイレクトされます。
- **資格情報インデックス**:サーバーへのシングルサインオンに、一次認証資格情報と二次認証資格情報のどちらを使用するかを指定します。
- Windows**でのシングルサインオン:セッションの Windows**自動ログオンを有効または無効にします。この設定を有効にした後に VPN セッションが確立されると、ユーザーはシステムの再起動後に Windows 資格情報を使用して自動的にログオンします。
- **クライアントクリーンアッププロンプト：クライアントが開始したセッションの終了時に、NetScaler Gateway からクライアント側のキャッシュクリーンアップを**求めるメッセージが表示されるようにする場合は、このオプションを設定します。

10. タブで、次の設定を行います：

    - **デフォルトの認証アクション**:「許可」に設定すると、ユーザーが iOS および Android モバイルデバイスからネットワークリソースに接続できるようになります。ユーザーは、セキュアネットワーク内のリソースにアクセスするために完全な VPN トンネルを確立する必要はありません。

11. タブで、次の設定を有効にします：

    - **ICA プロキシ**: に設定します。
    - **Web Interfaceアドレス**:StoreFStoreFront サーバーのFQDNの後にWeb用のストアへのパスが続きます。
    - **ウェブインターフェースタイプ**:ウェブインターフェースのタイプ (IPv4/v6)。
    - **シングル・サインオン・ドメイン:ドメインのNetBIOS名**。

12. **［Create］** をクリックします。
13. 式を追加します。

    a. **［高度なポリシー］** をクリックし、 **［式エディター］** をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

b. **エクスプレッションエディタで**、 > > を選択し、パラメータ (`**CitrixReceiver**` など) を入力します。例：

```
HTTP.REQ.HEADER("User-Agent").CONTAINS("CitrixReceiver").NOT
```

このポリシーは、Citrix ADCがWebブラウザーベースの接続とCitrix Workspaceアプリベースの接続を区別するために必要です。このポリシーは、Webブラウザーベースの接続に適用されます。

WindowsまたはMac用のCitrix Workspace アプリ、およびNetScaler Gateway 上のモバイルデバイス用のセッションポリシーを作成する

1. ［**NetScaler Gateway**］> ［**ポリシー**］> ［**セッション**］ に移動します。
2. フィールドで、 をクリックします。
3. フィールドに、セッションポリシーの名前を入力します。たとえば、Receiver_Policy のようにします。
4. ［**NetScaler Gateway セッションプロファイルの構成**］**ウィンドウで、新しいセッションプロファイルの名前を入力します** 。
5. ［**クライアントエクスペリエンス**］ タブで、次の設定を有効にします：
   - **ホームページ**:**に設定
   - **分割トンネル**: **OFF**に設定
   - **クライアントレスアクセス****:On に設定****
   - **Web アプリケーションへのシングル・サインオン**:チェックボックスを選択
   - **プラグインタイプ**: **Java**に設定
6. タブで、 を に設定します。
7. タブで、次の設定を有効にします：
   - **ICA プロキシ**: に設定します。
   - **Web Interfaceアドレス：** StoreFrontサーバーのFQDNの後にストアへのパスが続きます。
   - **シングルサインオンドメイン:ドメインの** NetBIOS 名
   - **アカウント・サービス所在地:**アカウント・サービスの所在地を入力します。最後のバックスラッシュは重要です。例： `https://accounts.example.com/Citrix/Roaming/Accounts`
8. ［**Create**］ をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

9. **従来のポリシー式を使用している場合は、「式」**フィールドに次の情報を追加し、「**作成**」をクリックします。

   ```
   REQ.HTTP.HEADER User-Agent CONTAINS CitrixReceiver
   ```

10. **高度なポリシー式を使用している場合は、「式」**フィールドに次の情報を追加し、「**作成**」をクリックします。

    ```
    HTTP.REQ.HEADER("User-Agent").CONTAINS("CitrixReceiver")
    ```

    このポリシーは、Citrix ADCがWebブラウザーベースの接続とCitrix Workspaceアプリベースの接続を区別するために必要です。このポリシーは、Citrix Workspaceアプリベースの接続に適用されます。

NetScaler ADCアプライアンスで認証を構成する

NetScaler ADCアプライアンスでのLDAP認証の構成について詳しくは、 LDAP認証の構成を参照してください。

NetScaler Gateway 仮想サーバーを作成し、セッションポリシーをバインドする

1. **［NetScaler Gateway］>［仮想サーバー］** に移動し、 **［追加］** をクリックして新しい仮想サーバーを追加します。
2. 仮想サーバーを作成したら、会社の要件に基づいて、特定のセッションポリシーを仮想サーバーにバインドします。

StoreFront の認証を構成する

1. StoreFrontでNetScaler Gateway からのパススルー認証を有効にします。詳しくは、「認証サービスの構成」を参照してください。

   StoreFront は、認証コールバックサービスのNetScaler Gateway 仮想サーバーのバインド証明書（ルート証明書および中間証明書）の発行元を信頼する必要があります。

2. NetScaler Gateway をStoreFront に追加します。詳しくは、「NetScaler Gateway 接続の追加」を参照してください。

   ゲートウェイ URL は、ユーザーが Web ブラウザのアドレスバーに入力しているものと正確に一致する必要があります。

3. StoreFront ストアでリモートアクセスを有効にします。詳しくは、「NetScaler Gateway を介したストアへのリモートアクセスの管理」を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

参照ドキュメント

- タイムアウト設定を構成する

エンタープライズブックマークの高度なポリシーサポート

エンタープライズブックマーク (VPN URL) は高度なポリシーとして設定できます。

メモ：

- NetScaler Gatewayは、エンタープライズブックマーク用のHTTP、HTTPS、およびRDPプロトコルをサポートしています。
- NetScaler Gateway は、エンタープライズブックマークの絶対URLのみをサポートします。

VPN URL を高度なポリシーとして設定する

GUI について

1. VPN URL プロファイルを作成します。
    - ［構成］>［**NetScaler Gateway**］>［**ポリシー**］>［**VPN URL**］に移動します。
    - 「**VPN URL ポリシーとプロファイル**」ページで、「**VPN URL プロファイル**」タブを選択し、「**追加**」をクリックします。
    - 必須フィールドを更新し、「**作成**」をクリックします。
        - 名前:VPN URL プロファイルの名前。
        - 表示するテキスト:リンクの簡単な説明。説明はAccess Interfaceに表示されます。
        - ブックマーク:アプリケーションの Web アドレス。
        - 仮想サーバー:構成されている関連する負荷分散またはコンテンツスイッチング仮想サーバーの名前。この情報は入力しなくても構いません。
        - アイコンURL: このフィールドにアップロードされたアイコンは、デフォルトテーマを除くすべてのテーマでサポートされています。推奨最大サイズは 70 x 70 ピクセルです。透明な画像を使用することをおすすめします。この情報は入力しなくても構いません。
        - アプリケーションタイプ:URL が表すアプリケーションのタイプ (VPN、クライアントレス VPN、または SaaS) を選択します。この情報は入力しなくても構いません。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- SSO タイプ:ブックマークに設定する SSO タイプ。SSO を設定すると、ユーザーはその後のログオン時に資格情報を入力しなくてもアプリケーションにアクセスできます。次の SSO タイプがサポートされています。
  - Unified Gateway: この SSO 設定により、単一の URL からアプリケーションの複数のリソースへの安全なリモートアクセスが可能になります。
  - 自己認証：このSSO構成では、NetScaler Gateway ユーザーはアプリケーションにアクセスするためのログイン資格情報を入力するよう求められます。
  - SAMLベースの認証：このSSO構成では、NetScaler Gateway はIdPを使用してユーザーの詳細を検証し、SAMLアサーションを生成してSPに送信します。検証に合格すると、SSO は成功します。

NOTE:

If you enable clientless access, you can make sure that requests to websites go through Citrix Gateway. For example, you added a bookmark for Google. Select the Use Citrix Gateway as a reverse proxy check box. When you select this check box, website requests go from the user device to Citrix Gateway and then to the website. When you clear the check box, requests go from the user device to the website. This check box is only available if you enable clientless access.

2. VPN URL ポリシーを作成します。
   - ［構成］>［**NetScaler Gateway**］>［**ポリシー**］>［**VPN URL**］に移動します。
   - 「**VPN URL ポリシーとプロファイル**」ページで、「**VPN URL ポリシー**」タブを選択し、「**追加**」をクリックします。
   - 必須フィールドを更新し、「**作成**」をクリックします。
     - 名前:VPN URL ポリシーの名前。
     - アクション:設定した VPN URL プロファイルを選択します。ドロップダウンリストにプロファイルがない場合は、 をクリックして手順 1 を繰り返します。
     - 表現: 詳細なポリシー表現については、「ポリシーと表現」を参照してください。
3. VPN URL ポリシーをバインドポイントにバインドします。
   - ［構成］>［**NetScaler Gateway**］>［**ポリシー**］>［**VPN URL**］に移動します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 「 **VPN URL ポリシーとプロファイル** 」ページで、「 **VPN URL ポリシー** 」タブを選択します。
- **「 アクションの選択」ドロップダウンリストから「グローバルバインディング」を選択します** 。
- VPN URL ポリシーを選択します。ポリシーが表示されない場合は、 をクリックして手順 2 を繰り返します。
- **バインディングの詳細セクションで** 、VPN URL ポリシーに優先順位を割り当てます。

CLI で

VPN URL アクションの作成:

コマンドプロンプトで、次のように入力します：

```
add vpn urlAction &lt;name> -linkName &lt;string> -actualURL &lt;string>
[-vServerName &lt;string>] [-clientlessAccess ( ON | OFF )] [-comment
&lt;string>] [-iconURL &lt;URL>] [-ssotype &lt;ssotype>] [-applicationtype
&lt;applicationtype>] [-samlSSOProfile &lt;string>]
```

NetScaler Gatewayは、VPN URLアクションの以下の操作をサポートしています：

- **add**

```
add vpn urlAction &lt;name> -linkName &lt;string> -actualURL
&lt;string> [-vServerName &lt;string>] [-clientlessAccess ( ON | OFF )]
[-comment &lt;string>] [-iconURL &lt;URL>] [-ssotype &lt;ssotype>] [-
applicationtype &lt;applicationtype>] [-samlSSOProfile &lt;string>]
```

- **set**

```
set vpn urlAction &lt;name> [-vServerName &lt;string>] [-
clientlessAccess ( ON | OFF )] [-comment &lt;string>] [-iconURL
&lt;URL>] [-ssotype &lt;ssotype>] [-applicationtype
&lt;applicationtype>] [-samlSSOProfile &lt;string>]
```

- **unset**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
unset vpn urlAction &lt;name> [-vServerName] [-clientlessAccess] [-
comment] [-iconURL] [-ssotype] [-applicationtype] [-samlSSOProfile]
```

注：

クライアントレスアクセスをオンに設定すると、Webサイトへの要求がユーザーデバイスからNetScaler Gateway、次にWebサイトに送信されることを確認できます。

- **show**

```
show vpn urlAction [&lt;name>]
```

- **削除**

```
remove vpn urlAction &lt;name>
```

- **rename**

```
rename vpn urlAction &lt;name>@ &lt;newName>@
```

VPN URL ポリシーの作成:

NetScaler Gatewayは、VPN URLポリシーの以下の操作をサポートしています：

- **add**

```
add vpn urlPolicy &lt;name> -rule &lt;expression> -action &lt;string>
[-comment &lt;string>] [-logAction &lt;string>]
```

- **set**

```
set vpn urlPolicy &lt;name> [-rule &lt;expression>] [-action
&lt;string>] [-comment &lt;string>] [-logAction &lt;string>]
```

- **unset**

```
unset vpn urlPolicy &lt;name> [-comment] [-logAction]
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **show**

```
show vpn urlPolicy [&lt;name>]
```

- **削除**

```
remove vpn urlPolicy &lt;name>
```

- **rename**

```
rename vpn urlpolicy &lt;name>@ &lt;newName>@
```

- **stat**

```
stat vpn urlpolicy [&lt;name>] [-detail] [-fullValues] [-ntimes
&lt;positive_integer>] [-logFile &lt;input_filename>] [-clearstats
( basic | full )]
```

VPN URL ポリシーをバインドポイントにバインドします。

NetScaler Gateway は、VPN URLポリシーバインディングの以下の操作をサポートしています：

- **bind**

```
bind vpn vserver &lt;vserver name> -policy &lt;string> -priority
&lt;positive_integer> [-gotoPriorityExpression &lt;expression>]

bind vpn global -policyName &lt;string> -priority &lt;positive_integer>
[-gotoPriorityExpression &lt;expression>]

bind aaa user &lt;userName> -policy &lt;string> [-priority
&lt;positive_integer>] [-type &lt;type>] [-gotoPriorityExpression
&lt;expression>]

bind aaa group &lt;groupName> -policy &lt;string> [-priority
&lt;positive_integer>] [-type &lt;type>] [-gotoPriorityExpression
&lt;expression>]
```

- **unbind**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
unbind vpn vserver &lt;name> -policy &lt;string>

unbind vpn global -policyName &lt;string>

unbind aaa user &lt;name> -policy &lt;string>

unbind aaa group &lt;name> -policy &lt;string>
```

注：

バインドポイントは `aaauser`、 `aaagroup`、 `vpnvserver`、 `vpnglobal`です。

エンドポイントポリシー

Endpoint Analysis (EPA) は、ユーザーのデバイスをスキャンして、オペレーティングシステムの更新、ウイルス対策、ファイアウォール、Web ブラウザーソフトウェアの有無やバージョンレベルなどの情報を検出するプロセスです。Endpoint Analysis では、ネットワークに接続する前に、ユーザーのデバイスが要件を満たしているかどうかを判断できます。また、ユーザーが接続している間に変更がないか定期的に確認するように設定することもできます。ユーザーセッション中にユーザーデバイス上のファイル、プロセス、およびレジストリエントリをチェックして、デバイスが引き続き要件を満たしていることを確認できます。

重要：

- Endpoint Analysisは、事前に定められたコンプライアンス基準に照らしてユーザーデバイスを分析することを目的としており、エンドユーザーデバイスのセキュリティを強制または検証するものではありません。ローカル管理者による攻撃からデバイスを保護するには、エンドポイントセキュリティシステムを使用することをお勧めします。
- EPAクライアントはスタンドアロンクライアントとして使用でき、Citrix Secure Access クライアントにバンドルされています。Citrix EPAクライアントとCitrix Secure Accessクライアントは相互に独立しています。

エンドポイントポリシーの仕組み

ユーザーがログオンする前に、ユーザーデバイスが特定の要件を満たしているかどうかを確認するようにNetScaler Gateway を構成できます。これは事前認証ポリシーと呼ばれます。ポリシー内で指定したウイルス対策、ファイアウォール、スパム対策、プロセス、ファイル、レジストリエ

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ントリ、インターネットセキュリティ、またはオペレーティングシステムについて、ユーザーデバイスをチェックするようにNetScaler Gateway を構成できます。ユーザーデバイスが事前認証スキャンに失敗した場合、ユーザーはログオンできません。

事前認証ポリシーで使用されていない他の要件を確認するには、セッションポリシーを設定し、それをユーザーまたはグループにバインドできます。このタイプのポリシーは「認証後ポリシー」と呼ばれ、ウイルス対策ソフトウェアやプロセスなどの必要な基準が常に準拠していることを確認するためにユーザーセッション中に実行されます。

事前認証または認証後のポリシーを構成すると、NetScaler Gateway はEndpoint Analysisプラグインをダウンロードし、ユーザーのデバイスでスキャンを実行します。ユーザーがログオンするたびに、Endpoint Analysis プラグインが自動的に実行されます。

次の 3 種類のポリシーを使用してエンドポイントポリシーを設定できます。

- Yes または No パラメータを使用する事前認証ポリシー。このスキャンでは、ユーザーデバイスが指定された要件を満たしているかどうかが判断されます。スキャンが失敗した場合、ユーザーはログオンページで資格情報を入力できません。
- 条件付きで、SmartAccess に使用できるセッションポリシー。
- セッションポリシー内のクライアントデバイスチェック表現。ユーザーデバイスがクライアントデバイスチェック式の要件を満たしていない場合、ユーザーを隔離グループに入れるように構成できます。ユーザーデバイスがスキャンに合格すると、ユーザーは別のグループに配置され、他のチェックが必要になる場合があります。

検出された情報をポリシーに組み込んで、ユーザーデバイスに基づいてさまざまなレベルのアクセス権限を付与できます。たとえば、最新のウイルス対策ソフトウェアおよびファイアウォールソフトウェア要件を持つユーザーデバイスからリモート接続するユーザーに、ダウンロード権限を持つフルアクセスを提供できます。準拠していないデバイスから接続するユーザーには、より制限されたアクセスレベルを提供して、ユーザーがダウンロードせずにリモートサーバー上のドキュメントを編集できるようにすることができます。EPA を実行しているすべてのデバイスは非準拠デバイスとみなされます。

エンドポイント分析は、次の基本手順を実行します。

- ユーザーデバイスに関する情報の初期セットを調べ、適用するスキャンを決定します。
- 該当するすべてのスキャンを実行します。ユーザーが接続しようとすると、Endpoint Analysis プラグインは、事前認証またはセッションポリシーで指定された要件についてユーザーデバイスをチェックします。ユーザーデバイスがスキャンに合格すると、ユーザーはログオンできます。ユーザーデバイスがスキャンに失敗すると、ユーザーはログオンできなくなります。 **注:**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Endpoint Analysis のスキャンは、ユーザーセッションがライセンスを使用する前に完了します。

- ユーザーデバイスで検出されたプロパティ値を、設定したスキャンにリストされている目的のプロパティ値と比較します。
- 目的のプロパティ値が見つかったかどうかを確認する出力を生成します。

重要:

エンドポイント分析ポリシーの作成手順は、一般的なガイドラインです。1 つのセッションポリシー内に多数の設定を適用できます。セッションポリシーを構成する具体的な手順には、特定の設定を構成するための指示が含まれている場合があります。ただし、この設定は、セッションプロファイルとポリシーに含まれる多くの設定の 1 つになる場合があります。

EPA 表現のサンプル

以下は、強制終了プロセス、ファイル削除、デバイス証明書などの一部の EPA コンポーネントの表現例です。

- Windows：
  - 強制終了プロセス: `sys.client_expr(\“proc_0_perl\“) -killProcess processToKill.exe`
  - デバイス証明書: `sys.client_expr(“device-cert_0_0”)`
  - ファイルの削除: `sys.client_expr(\“proc_0_perl\“) -deletefiles “C:/removefile.txt”`
- MAC
  - 強制終了プロセス: `sys.client_expr(\“proc_0_perl\“) -killProcess processToKill.exe`
  - デバイス証明書: `sys.client_expr(“device-cert_0_0”)`
  - ファイルの削除: `sys.client_expr(\“proc_0_perl\“) -deletefiles “C:/removefile.txt”`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ユーザーログオンオプションの評価

ユーザーがログオンするときに、エンドポイント分析のスキャンをスキップするように選択できます。ユーザーがスキャンをスキップすると、NetScaler Gateway はこのアクションを失敗したエンドポイント分析として処理します。ユーザーがスキャンに失敗した場合、Web Interfaceにアクセスするか、クライアントレスアクセスを介してのみアクセスできます。

たとえば、Citrix Secure Accessエージェントを使用してユーザーにアクセスを提供するとします。プラグインを使用してNetScaler Gateway にログオンするには、ユーザーがノートンアンチウイルスなどのウイルス対策アプリケーションを実行している必要があります。ユーザーデバイスでアプリケーションが実行されていない場合、ユーザーはReceiverのみでログオンし、公開アプリケーションを使用できます。また、Outlook Web Access などの特定のアプリケーションへのアクセスを制限するクライアントレスアクセスを構成することもできます。

このログオンシナリオを実現するようにNetScaler Gateway を構成するには、制限付きセッションポリシーをデフォルトポリシーとして割り当てます。次に、ユーザーデバイスがEndpoint Analysisスキャンに合格したときに、ユーザーを特権セッションポリシーにアップグレードするように設定を構成します。この時点で、ユーザーはネットワーク層にアクセスでき、Citrix Secure Access Agent を使用してログオンできます。

制限付きセッションポリシーを最初に強制するようにNetScaler Gateway を構成するには、次の手順に従います：

- ICAプロキシを有効にしてグローバル設定を構成し、指定したアプリケーションがユーザーデバイス上で実行されていない場合は、他のすべての必要な設定を構成します。
- Citrix Secure Accessエージェントを有効にするセッションポリシーとプロファイルを作成します。
- セッションポリシーのルール部分に、次のような式を作成してアプリケーションを指定します。 `(client.application.process(symantec.exe) exists)`

  ユーザーがログオンすると、最初にセッションポリシーが適用されます。エンドポイント分析が失敗した場合、またはユーザーがスキャンをスキップした場合、NetScaler Gateway はセッションポリシーの設定を無視します（セッションポリシーの式は偽と見なされます）。その結果、ユーザは Web インターフェイスまたはクライアントレスアクセスを使用したアクセスが制限されます。エンドポイント分析に合格すると、NetScaler Gateway はセッションポリシーを適用し、ユーザーはCitrix Secure Accessエージェントに対するフルアクセス権を持ちます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

EPA スキャンをスキップする

EPA スキャンをスキップできるのは、認証後および事前認証のみです。Skip EPA は、サポートされているすべてのオペレーティングシステムのブラウザで利用できます。ユーザーは、ゲートウェイにアクセスするときに表示される ボタンをクリックする必要があります。ユーザーがスキャンをスキップすると、NetScaler Gateway はこのアクションを失敗したエンドポイント分析として処理します。ユーザーがスキャンに失敗した場合、Web Interfaceにアクセスするか、クライアントレスアクセスを介してのみアクセスできます。

「`<https://support.citrix.com/article/CTX200748>`」も参照してください。

Ubuntu でサポートされるエンドポイント分析スキャン

次のエンドポイント分析 (EPA) スキャンは、Ubuntu オペレーティングシステム用にインストールされた EPA プラグインでサポートされています。各スキャンを設定するためのサンプル式は、EPA スキャンとともに一覧表示されています。これらの式は、認証ポリシーで設定できます。

- **ファイル**
  - **存在**:sys.client_expr("file_0_/home/user/test.txt")
  - **MD5 チェックサム**:sys.client_expr ("file_0_/home/user/test.txt_md5_ce780e271debcc29f551546e8db3368f")
  - **ファイル内のテキスト (正規表現サポート): sys.client_expr (**("file_0_/home/user/test.txt_search_cloud")
- **プロセス**
  - **存在**:sys.client_expr("proc_0_perl")
  - **MD5 チェックサム**:sys.client_expr("proc_0_perl_md5_c060d3a5f97e27066cef8c116785567a")
  - **パス**:sys.client_expr("proc_0_perl_path_/usr/bin/perl")
- **ファイルシステムデバイスまたはマウントポイント名**:sys.client_expr("mountpoint_0_/sys")

高度なポリシーを使用している場合、各スキャンの式は GUI から生成できます（ > > > > > ）。

注: Linux クライアントの ページで、 を選択し、、****、** または を選択できます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

事前認証ポリシーとプロファイル

重要:

エンドポイント分析は、あらかじめ決められたコンプライアンス基準に照らしてユーザーデバイスを分析することを目的としており、エンドユーザーデバイスのセキュリティを強制または検証するものではありません。ローカル管理者による攻撃からデバイスを保護するには、エンドポイントセキュリティシステムを使用することをお勧めします。

NetScaler Gateway で認証される前にユーザーのデバイスをチェックするようにNetScaler Gateway を構成できます。ユーザーのデバイスが組織の要件を満たしていない場合、これを使用してアクセスを制限できます。デバイスチェックは、仮想サーバーに固有の個別のポリシーを使用して実装することも、次の2つの手順で説明するようにグローバルに実装することもできます。

事前認証ポリシーは、プロファイルと式で構成されます。ユーザーデバイスでのプロセスの実行を許可または拒否する式を使用するようにプロファイルを構成します。たとえば、テキストファイル clienttext.txt はユーザーのデバイスで実行されています。ユーザーがNetScaler Gateway にログオンすると、テキストファイルが実行されているかどうかに応じてアクセスを許可または拒否できます。プロセスの実行中にユーザーがログオンできないようにするには、ユーザーがログオンする前にプロセスを停止するように事前認証プロファイルを構成できます。

事前認証ポリシーには、次の設定を構成できます。

- 式。エクスプレッションを作成するのに役立つ次の設定が含まれています。
  - 式。すべてのエクスプレッションを表示します。
  - 任意の式にマッチします。選択した式のリストにある式のいずれかに一致するようにポリシーを設定します。
  - 。選択した式のリストにあるすべての式に一致するようにポリシーを設定します。
  - 表形式の表現。`OR (||) or AND (&&)`演算子を使用して、既存のエクスプレッションを含む複合エクスプレッションを作成します。
  - 高度な自由形式。エクスプレッション名と`OR (||) and AND (&&)`演算子を使用して、カスタム複合エクスプレッションを作成します。必要なエクスプレッションのみを選択し、選択したエクスプレッションのリストから他のエクスプレッションを省略します。
  - 追加。エクスプレッションを作成します。
  - 修正。既存の式を変更します。
  - 削除。選択したエクスプレッションを複合エクスプレッションリストから削除します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 名前付き式。設定済みの名前付き式を選択します。NetScaler Gateway にすでに存在する式のメニューから名前付き式を選択できます。
- 。選択した名前付き式をポリシーに追加します。
- エクスプレッションを置換。選択した名前付き式をポリシーに置き換えます。
- エクスプレッションをプレビュー。名前付きの式を選択すると、NetScaler Gateway で構成されている詳細な文字列が表示されます。

事前認証プロファイルの設定

GUI を使用して事前認証プロファイルをグローバルに設定するには

1. ［構成］タブの［**NetScaler Gateway**］をクリックし、［**グローバル設定**］をクリックします。
2. 詳細ウィンドウの で、 をクリックします。
3. ダイアログボックスで、次の設定を構成します。
   a. 「**アクション**」で、「**許可」または「拒否**」を選択します。

      エンドポイント分析の実行後、ユーザーのログオンを拒否または許可します。
   b. 「**キャンセルするプロセス**」に、プロセスを入力します。

      これは、Endpoint Analysis プラグインが停止する必要があるプロセスを指定します。
   c. に、ファイル名を入力します。

      Endpoint Analysis プラグインが削除する必要があるファイルを指定します。プロセスを削除またはキャンセルすると、エンドユーザーに通知が表示されます。

      
4. Expression では、ns_true という式をそのまま使用することも、ウイルス対策ソフトウェアやセキュリティソフトウェアなどの特定のアプリケーション用の式を作成して、「 **OK」**をクリックすることもできます。

GUI を使用して事前認証プロファイルを設定するには

1. **［Citrix Gateway］>［ポリシー］ >［認証/承認］に移動し、［事前認証EPA］をクリックします。**
2. 詳細ペインの タブで、 をクリックします。
3. に、チェックするアプリケーションの名前を入力します。
4. で または を選択します

© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. に、停止するプロセスの名前を入力します。
6. に、削除するファイルの名前**(c:\clientext.txt など) を入力し、、 の順にクリックします。

   Endpoint Analysis プラグインが削除する必要があるファイルを指定します。プロセスを削除またはキャンセルすると、エンドユーザーに通知が表示されます。

GUI を使用して事前認証プロファイルを設定する場合は、 タブの **をクリックして事前認証ポリシーを作成します** 。 ダイアログボックスで、 メニューからプロファイルを選択します** 。

事前設定済みの式を事前認証ポリシーに追加する

NetScaler Gateway には、名前付き式と呼ばれる事前構成された式が付属しています。ポリシーを設定するときは、ポリシーの名前付き式を使用できます。たとえば、事前認証ポリシーで、更新されたウイルス定義を持つ Symantec Antivirus 10 をチェックするとします。事前認証ポリシーを作成し、次の手順の説明に従って式を追加します。

事前認証ポリシーまたはセッションポリシーを作成する場合、ポリシーの作成時に式を作成できます。その後、式を使用してポリシーを仮想サーバまたはグローバルに適用できます。

次の手順では、構成ユーティリティを使用して、構成済みのウイルス対策式をポリシーに追加する方法について説明します。

事前認証ポリシーに名前付き式を追加する

1. **［Citrix Gateway］>［ポリシー］ >［認証/承認］に移動し、［事前認証EPA］をクリックします。**
2. 詳細ペインでポリシーを選択し、 をクリックします。
3. の横にある を選択し、リストからアンチウイルス製品を選択します。
4. 、、** の順にクリックします。

カスタムエクスプレッションの設定

カスタム式は、ポリシー内に作成する式です。エクスプレッションを作成するときは、エクスプレッションのパラメータを設定します。

よく使われる文字列を参照するカスタムエクスプレッションを作成することもできます。これにより、事前認証ポリシーの設定プロセスが容易になり、設定済みの式の維持も容易になります。

たとえば、Symantec antivirus 10 用のカスタム式を作成し、ウイルス定義が 3 日以上前のものでないことを確認したいとします。ポリシーを作成し、ウイルス定義を指定する式を設定します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

次の手順は、事前認証ポリシーで式を作成する方法を示しています。セッションポリシーでも同じ手順を使用できます。

事前認証ポリシーとカスタム表現の作成

1. ［**NetScaler Gateway**］>［**ポリシー**］>［**認証/承認**］に移動し、［事前**認証EPA**］をクリックします。
2. 詳細ペインで、 をクリックします。
3. ** に、ポリシーの名前を入力します。
4. 「**リクエストプロファイル**」の横にある「**新規**」をクリックします。
5. ダイアログボックスの にプロファイルの名前を入力し、 で を選択し、 をクリックします。
6. **ダイアログボックスの の横にある をクリックします。**
7. で、 を選択します。
8. 次のオプションを構成します：
    a. で、 を選択します。
    b. に、アプリケーションの名前を入力します。
    c. 「**修飾子**」で「**バージョン**」を選択します。
    d. 「**演算子**」で「**==**」を選択します。
    e. に値を入力します。
    f. 「**鮮度**」に「3」と入力し、 **「OK」**をクリックします。
9. ダイアログボックスで、、 の順にクリックします。

カスタム式を設定すると、ポリシーダイアログボックスの ボックスに追加されます。

複合式の設定

事前認証ポリシーには、1 つのプロファイルと複数の式を含めることができます。複合式を設定する場合は、演算子を使用して式の条件を指定します。たとえば、次のウイルス対策アプリケーションのいずれかを実行することをユーザデバイスに要求するように、複合式を設定できます。

- Symantec Antivirus 10
- McAfee Antivirus 11
- Sophos Antivirus 4

© 1997–2026 Citrix Systems, Inc. All rights reserved.

OR 演算子を使用して式を設定して、前述の 3 つのアプリケーションをチェックします。NetScaler Gateway がユーザーデバイス上のアプリケーションの正しいバージョンを検出すると、ユーザーはログオンできます。 ダイアログボックスの式は、次のように表示されます：

```
av_5_Symantec_10 || av_5_McAfeevirusscan_11 || av_5_sophos_4
```

複合式の詳細については、「 複合式の設定」を参照してください。

事前認証ポリシーのバインド

事前認証ポリシーを作成したら、ポリシーを適用するレベルにバインドします。事前認証ポリシーは、仮想サーバまたはグローバルにバインドできます。

事前認証ポリシーをグローバルに作成してバインドする

1. ［構成］タブの［ **NetScaler Gateway**］をクリックし、 ［ **グローバル設定**］をクリックします。
2. 詳細ウィンドウで、 をクリックします。
3. ダイアログボックスの で、 または を選択します。
4. ** に、ポリシーの名前を入力します。
5. ダイアログボックスで、 の横にある 、、、、 の順にクリックします。

事前認証ポリシーを仮想サーバーにバインドする

1. ［構成］タブの［ **NetScaler Gateway**］をクリックし、 ［ **仮想サーバー**］をクリックします。
2. 詳細ペインで仮想サーバーを選択して、**［Open］**をクリックします。
3. ［NetScaler Gateway 仮想サーバーの構成］ダイアログボックスで、［ **ポリシー** ］タブをクリックし、［ **事前認証**］をクリックします。
4. の をクリックし、 で事前認証ポリシーを選択します。
5. **［OK］** をクリックします。

事前認証ポリシーのバインド解除と削除

必要に応じて、NetScaler Gateway から事前認証ポリシーを削除できます。事前認証ポリシーを削除する前に、仮想サーバから、またはグローバルにバインド解除します。

グローバル事前認証ポリシーのバインドを解除する

1. **［Citrix Gateway］>［ポリシー］ >［認証/承認］に移動し、［事前認証EPA］をクリックします。**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. 詳細ペインでポリシーを選択し、 で をクリックします。
3. ［ **事前認証ポリシーをグローバルにバインド/バインド解除** ］ダイアログボックスで、ポリシーを選択し、［ **ポリシーのバインド解除**］、［ **OK］**の順にクリックします。

仮想サーバからの事前認証ポリシーのバインド解除

1. ［構成］タブの［ **NetScaler Gateway］をクリックし、** ［ **仮想サーバー**］をクリックします。
2. **［NetScaler Gateway 仮想サーバーの構成** ］ダイアログボックスで、［ **ポリシー** ］タブをクリックし、［ **事前認証**］をクリックします。
3. ポリシーを選択し、「 **ポリシーのバインド解除**」をクリックします。

事前認証ポリシーがバインド解除されると、NetScaler Gateway からポリシーを削除できます。

事前認証ポリシーを削除する

1. ［ **NetScaler Gateway］> ［ポリシー］> ［認証/承認**］に移動し、［事前**認証EPA**］をクリックします。
2. 詳細ペインでポリシーを選択し、 をクリックします。

事前認証ポリシーのプライオリティの設定

異なるレベルにバインドされた複数の事前認証ポリシーを持つことができます。たとえば、グローバルにバインドされている特定のウイルス対策アプリケーションをチェックするポリシーと、仮想サーバーにバインドされたファイアウォールポリシーがあるとします。ユーザーがログオンすると、仮想サーバーにバインドされているポリシーが最初に適用されます。グローバルにバインドされているポリシーが 2 番目に適用されます。

事前認証スキャンの発生順序を変更できます。NetScaler Gateway でグローバルポリシーを最初に適用するには、仮想サーバーにバインドされたポリシーの優先度番号を変更し、グローバルにバインドされたポリシーよりも高い優先度を指定します。たとえば、グローバルポリシーのプライオリティ番号を 1 に、仮想サーバポリシーのプライオリティ番号を 2 に設定します。ユーザーがログオンすると、NetScaler Gateway は最初にグローバルポリシースキャンを実行し、次に仮想サーバーポリシースキャンを実行します。

事前認証ポリシーのプライオリティを変更する

1. ［構成］タブの［ **NetScaler Gateway］をクリックし、** ［ **仮想サーバー**］をクリックします。
2. 詳細ペインで仮想サーバーを選択して、**［Open］**をクリックします。
3. 「ポリシー」タブで、「 **事前認証**」をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. ［優先度］で、ポリシーの優先度番号を入力し、［ **OK］**をクリックします。

認証ポリシーの投稿

重要:

エンドポイント分析は、あらかじめ決められたコンプライアンス基準に照らしてユーザーデバイスを分析することを目的としており、エンドユーザーデバイスのセキュリティを強制または検証するものではありません。ローカル管理者による攻撃からデバイスを保護するには、エンドポイントセキュリティシステムを使用することをお勧めします。

認証後ポリシーは、セッションをアクティブに保つためにユーザーデバイスが満たす必要がある汎用ルールのセットです。ポリシーが失敗すると、NetScaler Gateway への接続は終了します。認証後ポリシーを構成すると、条件付きに設定できるユーザー接続の設定を構成できます。

セッションポリシーを使用して、認証後のポリシーを設定します。まず、ポリシーを適用するユーザーを作成します。次に、ユーザーをグループに追加します。次に、セッション、トラフィックポリシー、およびイントラネットアプリケーションをグループにバインドします。

また、グループを承認グループとして指定することもできます。このタイプのグループでは、セッションポリシー内のクライアントデバイスチェック式に基づいてユーザーをグループに割り当てることができます。

また、ユーザーデバイスがポリシーの要件を満たしていない場合にユーザーを検疫グループに入れるように、認証後ポリシーを構成することもできます。シンプルなポリシーには、クライアントデバイスのチェック表現とメッセージが含まれます。ユーザーが検疫グループに属している場合、ユーザーはNetScaler Gateway にログオンできますが、ネットワークリソースへのアクセスは制限されます。

同じセッションプロファイルとポリシーを使用して、認可グループと検疫グループを作成することはできません。認証後ポリシーを作成する手順は同じです。セッションポリシーを作成するときは、承認グループまたは検疫グループを選択します。2 つのセッションポリシーを作成し、各ポリシーをグループにバインドできます。

認証後のポリシーは SmartAccess でも使用されます。SmartAccess 詳細については、「NetScaler Gateway でのSmartAccess 構成」を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注：

この機能は、Citrix Secure Accessエージェントでのみ動作します。ユーザーがCitrix Workspace アプリでログオンした場合、エンドポイント分析スキャンはログオン時にのみ実行されます。

認証後ポリシーを構成する

セッションポリシーを使用して、認証後ポリシーを設定します。シンプルなポリシーには、クライアントデバイスのチェック表現とメッセージが含まれます。

GUI を使用して認証後ポリシーを設定するには

1. **NetScaler Gateway > ポリシーを展開して** 、「 **セッション**」をクリックします。
2. 詳細ペインの タブで、 をクリックします。
3. ** に、ポリシーの名前を入力します。
4. 「 **リクエストプロファイル**」の横にある「 **新規**」をクリックします。
5. ** に、プロファイルの名前を入力します。
6. タブの をクリックします。
7. で、 をクリックし、** をクリックします。
8. クライアントデバイスのチェック式を設定し、「 **作成**」をクリックします。
9. の で、グループを選択します。
10. に、認証後のスキャンが失敗した場合にユーザーに受信させたいメッセージを入力します。
11. で、 をクリックし、グループを選択し、、、 の順にクリックします。
12. ダイアログボックスで、 の横にある を選択し、 を選択し、 をクリックして をクリックし、 をクリックします。

認証後スキャンの頻度を構成する

指定した間隔で認証後ポリシーを実行するようにNetScaler Gateway を構成できます。たとえば、クライアントデバイスチェックポリシーを構成し、それをユーザーデバイス上で10分ごとに実行したいとします。この頻度は、ポリシー内にカスタム式を作成することで設定できます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注：

認証後ポリシーの頻度チェック機能は、Citrix Secure Accessエージェントでのみ機能します。ユーザーがCitrix Workspace アプリでログオンした場合、エンドポイント分析スキャンはログオン時にのみ実行されます。

「 認証後ポリシーの設定」の手順に従って、クライアントデバイスチェックポリシーを設定する頻度（分単位）を設定できます。次の図は、「式の追加」(**Add Expression**) ダイアログボックスの頻度の値を入力できる場所を示しています。



検疫グループと承認グループ

ユーザーがNetScaler Gateway にログオンするときに、NetScaler Gateway またはセキュリティで保護されたネットワーク内の認証サーバーで構成するグループにユーザーを割り当てます。ユーザが認証後スキャンに失敗した場合、ユーザを検疫グループと呼ばれる制限されたグループに割り当てることができます。このグループは、ネットワークリソースへのアクセスを制限します。

また、承認グループを使用して、ネットワークリソースへのユーザーアクセスを制限することもできます。たとえば、メールサーバーとファイル共有にのみアクセスできる契約担当者のグループがあるとします。ユーザーデバイスがNetScaler Gateway で定義したデバイスチェック要件に合格すると、ユーザーは動的にグループのメンバーになることができます。

グローバル設定またはセッションポリシーを使用して、ユーザー、グループ、または仮想サーバーにバインドされた検疫および承認グループを構成します。セッションポリシー内のクライアントデバイスチェック式に基づいて、ユーザーをグループに割り当てることができます。ユーザーがグループのメンバーである場合、NetScaler Gateway はグループメンバーシップに基づいてセッションポリシーを適用します。

権限付与グループの設定

Endpoint Analysis スキャンを設定すると、ユーザーデバイスがスキャンに合格したときに、ユーザーを承認グループに動的に追加できます。たとえば、ユーザーデバイスのドメインメンバーシップをチェックする Endpoint Analysis スキャンを作成するとします。NetScaler Gateway で、ドメインに参加しているコンピューターというローカルグループを作成し、スキャンに合格したすべてのユーザーの承認グループとして追加します。ユーザーがグループに参加すると、ユーザーはグループに関連付けられたポリシーを継承します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

認可ポリシーは、グローバルにバインドすることも、仮想サーバにバインドすることもできません。ユーザーがNetScaler Gateway の別のグループのメンバーになるように構成されていない場合、承認グループを使用して、承認ポリシーのデフォルトセットを提供できます。

セッションポリシーを使用して認可グループを構成するには

1. **NetScaler Gateway > ポリシーに移動し** 、「 **セッション**」をクリックします。
2. 詳細ペインの タブで、 をクリックします。
3. ** に、ポリシーの名前を入力します。
4. 「 **リクエストプロファイル**」の横にある「 **新規**」をクリックします。
5. ** に、プロファイルの名前を入力します。
6. タブの をクリックします。
7. 「承認グループ」で、「 **グローバルをオーバーライド** 」をクリックし、ドロップダウンリストからグループを選択します。
8. 「 **追加**」をクリックし、「 **OK**」 をクリックし、「 **作成**」をクリックします。
9. ダイアログボックスで、 の横にある を選択**し**、 を選択し、 をクリックして をクリックし、**をクリック**し**ます。

セッションポリシーを作成したら、ユーザー、グループ、または仮想サーバーにバインドできます。

グローバル権限グループを構成するには

1. **NetScaler Gateway** を展開し、「 **グローバル設定**」をクリックします。
2. 詳細ペインの で、 をクリックします。
3. タブの をクリックします。
4. 「承認グループ」で、ドロップダウンリストからグループを選択します。
5. 「 **追加」をクリックし、** 「 **OK」**をクリックします。

承認グループをグローバルに、またはセッションポリシーから削除する場合は、 ダイアログボックスで、一覧から承認グループを選択し、 をクリックします。

検疫グループの設定

隔離グループを設定する場合、セッションプロファイル内の ダイアログボックスを使用してクライアントデバイスのチェック式を設定します。

検疫グループのクライアントデバイスチェック式を設定するには

1. **Citrix Gateway > ポリシーに移動し** 、「 **セッション**」をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. 詳細ペインの タブで、 をクリックします。
3. ** に、ポリシーの名前を入力します。
4. 「 **リクエストプロファイル**」の横にある「 **新規**」をクリックします。
5. ** に、プロファイルの名前を入力します。
6. タブの をクリックします。
7. で、 をクリックし、** をクリックします。
8. **クライアントエクスプレッションダイアログボックスで** 、クライアントデバイスのチェックエクスプレッションを設定し、「 **作成**」をクリックします。
9. 「 **隔離グループ**」で、グループを選択します。
10. に、問題を説明するメッセージをユーザーに入力し、 をクリックします。
11. ダイアログボックスの の横で を選択し、 を選択して をクリックします。
12. をクリックし、** をクリックします。

セッションポリシーを作成したら、ユーザー、グループ、または仮想サーバーにバインドします。

注：

Endpoint Analysis スキャンが失敗し、ユーザーが検疫グループに配置された場合、検疫グループにバインドされたポリシーは、検疫グループにバインドされたポリシーと同等またはそれ以下の優先度番号を持つユーザーに直接バインドされたポリシーがない場合にのみ有効です。

グローバル検疫グループを設定するには

1. **NetScaler Gateway** を展開し、「 **グローバル設定**」をクリックします。
2. 詳細ペインの で、 をクリックします。
3. タブの をクリックします。
4. **Client Security**で、クライアントデバイスのチェック式を設定します。
5. 「 **隔離グループ**」で、グループを選択します。
6. 「 **エラー・メッセージ**」に、問題を説明するメッセージをユーザーに入力し、「 **OK」**をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ユーザーデバイスの事前認証デバイスチェック表現

重要:

エンドポイント分析は、あらかじめ決められたコンプライアンス基準に照らしてユーザーデバイスを分析することを目的としており、エンドユーザーデバイスのセキュリティを強制または検証するものではありません。ローカル管理者による攻撃からデバイスを保護するには、エンドポイントセキュリティシステムを使用することをお勧めします。

NetScaler Gateway は、ユーザーデバイスの検証に役立つさまざまなエンドポイントコンプライアンスチェックを、ユーザーログオン中またはセッション中のその他の構成時間に行います。これらのチェックに合格したユーザーデバイスのみがNetScaler Gateway セッションを確立できます。

NetScaler Gateway で構成できるユーザーデバイスのチェックの種類は次のとおりです。

- スパム対策
- アンチウイルス
- ファイルポリシー
- インターネットセキュリティ
- オペレーティングシステム
- パーソナルファイアウォール
- プロセスポリシー
- レジストリポリシー
- サービスポリシー

ユーザーデバイス上でデバイスチェックが失敗した場合、次のチェックに合格するまで（定期的に行われるチェックの場合）、新しい接続は確立されません。ただし、既存の接続を経由するトラフィックは、引き続きNetScaler Gatewayをトンネル経由します。

構成ユーティリティを使用して、ユーザーデバイス上でチェックを実行するように設計されたセッションポリシー内の事前認証ポリシーまたはデバイスチェック式を設定できます。

ウイルス対策、ファイアウォール、インターネットセキュリティ、またはスパム対策の表現を構成する

ウイルス対策、ファイアウォール、インターネットセキュリティ、およびスパム対策ポリシーの設定は、 ダイアログボックスで行います。各ポリシーの設定は同じです。違いは、選択した値です。たとえば、ユーザーデバイスのノートンアンチウイルスバージョン 10 と ZoneAlarm Pro を

© 1997–2026 Citrix Systems, Inc. All rights reserved.

チェックする場合、セッションまたは事前認証ポリシー内に、各アプリケーションの名前とバージョン番号を指定する 2 つの式を作成します。

式の種類として Client Security を選択すると、次の項目を構成できます：

- コンポーネント:アンチウイルス、ファイアウォール、レジストリエントリなど、クライアントセキュリティの種類。
- 名前: アプリケーション、プロセス、ファイル、レジストリエントリ、またはオペレーティングシステムの名前。
- 修飾子:式がチェックするコンポーネントのバージョンまたは値。
- 演算子:値が存在するかどうか、または値と等しいかどうかを確認します。
- 値:ユーザーデバイス上のウイルス対策、ファイアウォール、インターネットセキュリティ、またはスパム対策ソフトウェアのアプリケーションバージョン。
- 頻度:認証後スキャンが実行される頻度 (分単位)。
- エラーの重み:複数の式が異なるエラー文字列を持つ場合に、ネストされた式に含まれる各エラーメッセージに割り当てられる重み。重みによって、表示されるエラーメッセージが決まります。
- 鮮度:ウイルス定義の古さを定義します。たとえば、ウイルス定義が 3 日を超えないように式を設定できます。

クライアントデバイスチェックポリシーを事前認証ポリシーまたはセッションポリシーに追加するには

1. 構成ユーティリティのナビゲーションペインで、次のいずれかの操作を行います：
    a. 構成ユーティリティの［構成］タブのナビゲーションペインで、［ **Citrix Gateway**］ > ［**ポリシー** ］を展開し、［ **セッション**］をクリックします。
    b. 構成ユーティリティの［構成］タブのナビゲーションペインで、［ **NetScaler Gateway**］ > ［**ポリシー**］ > ［**認証/承認**］の順に展開し、［事前**認証EPA**］をクリックします。
2. 詳細ペインの タブで、 をクリックします。
3. に、ポリシーの名前を入力します。
4. の横にある をクリックします。
5. ダイアログボックスの で、 を選択します。
6. 次の設定を構成します。
    a. 「コンポーネント」で、スキャンするアイテムを選択します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

b. に、アプリケーションの名前を入力します。

c. 「修飾子」で「 **バージョン**」を選択します。

d. 「演算子」で、値を選択します。

e. 「値」に、クライアント・デバイスのチェック文字列を入力し、「 **OK」**をクリックし、「 **作成**」をクリックして、「 **閉じる**」をクリックします。

サービスポリシーの設定

サービスは、ユーザーデバイス上でサイレントに実行されるプログラムです。セッションまたは事前認証ポリシーを作成するときに、セッションの確立時にユーザーデバイスが特定のサービスを実行していることを確認する式を作成できます。

サービスポリシーを設定するには

1. 構成ユーティリティのナビゲーションペインで、次のいずれかの操作を行います：

   a. 構成ユーティリティの［構成］タブのナビゲーションペインで、［ **Citrix Gateway**］ **>［ポリシー** ］を展開し、［セッション］をクリックします。

   b. 構成ユーティリティの［構成］タブのナビゲーションペインで、［ **Citrix Gateway**］ **>［ポリシー ］>［認証/承認］の順に展開し、［事前認証EPA**］をクリックします。

2. 詳細ペインの タブで、 をクリックします。
3. に、ポリシーの名前を入力します。
4. の横にある をクリックします。
5. ダイアログボックスの で、 を選択します。
6. 次の設定を構成します。

   a. 「コンポーネント」で、「サービス」を選択します。

   b. に、サービスの名前を入力します。

   c. 「修飾子」で、空白のままにするか、「バージョン」を選択します。

   d. での選択内容に応じて、次のいずれかを実行します。

      - 空白のままの場合は、「演算子」で==または!=を選択
      - 「バージョン」を選択した場合は、「演算子」の「値」に値を入力し、「OK」、「閉じる」の順にクリックします。

Windows ベースのコンピューターで利用可能なすべてのサービスの一覧と各サービスの状態は、次の場所で確認できます：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

コントロールパネル > 管理ツール > サービス

注:

各サービスのサービス名は、リストされた名前とは異なります。 ダイアログボックスを見て、サービスの名前を確認します。

プロセスポリシーの設定

セッションポリシーまたは事前認証ポリシーを作成するときに、ユーザーのログオン時にすべてのユーザーデバイスで特定のプロセスを実行するように要求する規則を定義できます。プロセスには任意のアプリケーションを使用でき、カスタマイズされたアプリケーションを含めることができます。

注:Windows ベースのコンピューターで実行されているすべてのプロセスのリストは、Windows タスクマネージャーの タブに表示されます。

プロセスポリシーを設定するには

1. 構成ユーティリティのナビゲーションペインで、次のいずれかの操作を行います：
   a. 構成ユーティリティの［構成］タブのナビゲーションペインで、［ **Citrix Gateway\］> ［ポリシー** ］を展開し、［セッション］をクリックします。
   b. 構成ユーティリティの［構成］タブのナビゲーションペインで、［ **NetScaler Gateway］> ［ポリシー］> ［認証/承認**］の順に展開し、［事前認証EPA］をクリックします。
2. 詳細ペインの タブで、 をクリックします。
3. に、ポリシーの名前を入力します。
4. の横にある をクリックします。
5. ダイアログボックスの で、 を選択します。
6. 次の設定を構成します。
   a. 「コンポーネント」で、「プロセス」を選択します。
   b. に、アプリケーションの名前を入力します。
   c. 「演算子」で「EXISTS」または「NOTEXISTS」を選択し、「OK」をクリックして。

Endpoint Analysis ポリシー（認証前または認証後）を設定してプロセスをチェックする場合、MD5 チェックサムを設定できます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ポリシーの式を作成するときに、チェックするプロセスに MD5 チェックサムを追加できます。たとえば、notepad.exe がユーザーデバイスで実行されているかどうかを確認する場合、式は次のようになります。
CLIENT.APPLICATION.PROCESS(notepad.exe_md5_388b8fbc36a8558587afc90fb23a3b00) EXISTS

オペレーティングシステムポリシーを構成する

セッションまたは事前認証ポリシーを作成すると、クライアントデバイスのチェック文字列を構成して、ユーザーのログオン時にユーザーデバイスが特定のオペレーティングシステムを実行しているかどうかを判断できます。また、特定の Service Pack または修正プログラムをチェックするように式を構成することもできます。

WindowsとMacintoshの値は次のとおりです。

オペレーティングシステム	VALUE
macOS X	macOS
Windows 8.1	win8.1
Windows 8	win8
Windows 7	win7
Windows Vista	ビスタ
Windows XP	`winxp`
Windows Server 2008	win2008
Windows Server 2003	win2003
Windows 2000 Server	win2000
Windows 64 ビットプラットフォーム	win64

GUI を使用してオペレーティングシステムポリシーを構成するには

1. ナビゲーションペインで、次のいずれかの操作を行います。
    a. **Citrix Gateway > ポリシーに移動し** 、「 **セッション**」をクリックします。
    b. **NetScaler Gateway > ポリシー > 事前認証に移動します。**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. 詳細ペインの タブで、 をクリックします。
3. ** に、ポリシーの名前を入力します。
4. 「 **アクションのリクエスト** 」で、既存のアクションを選択するか、アクションを作成します。
5. ［**Expression Editor**］ をクリックします。
6. ****で、 を選択します。
7. 次の設定を構成します。
   a. 「 **コンポーネント**」で、「 **オペレーティング・システム**」を選択します。
   b. に、オペレーティングシステムの名前を入力します。
   c. で、次のいずれかの操作を行います。
      - フィールドは空白のままにします。
      - **サービスパックを選択**
      - **修正プログラムの選択**
      - **バージョンを選択** (macOS のみ)
   d. 手順 7 での選択内容に応じて、 で次のいずれかを実行します。
      - が空白の場合は、 で EQUAL (= =)、NOTEQUAL (!=)、EXISTSまたは NOTEXISTSを選択します。
      - または を選択した場合は、演算子を選択し、 に値を入力します。
8. をクリックし、 をクリックします。

client.os `(winxp).sp` などのサービスパックを構成している場合、［ **値** ］フィールドに数字がない場合、式が無効であるため、NetScaler Gateway はエラーメッセージを返します。

オペレーティングシステムに Service Pack 3 や Service Pack 4 などのサービスパックが存在する場合は、Service Pack 4 のチェックだけを構成できます。Service Pack 4 の存在により、以前のサービスパックが存在することが自動的に示されるためです。

レジストリポリシーを構成する

セッションポリシーまたは事前認証ポリシーを作成するときに、ユーザーデバイス上のレジストリエントリが存在し、値があるかどうかを確認できます。セッションは、特定のエントリが存在するか、設定されているか、またはより高い値を持つ場合にのみ確立されます。

レジストリ式を設定する場合は、次のガイドラインに従ってください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 4つのバックスラッシュは、キーとサブキーを区切るために使われます。

  HKEY_LOCAL_MACHINE\\\\\\\SOFTWARE

- アンダースコアは、サブキーと関連する値の名前を区切るために使用されます。

  HKEY_LOCAL_MACHINE\\\\\\\SOFTWARE\\\\\\\VirusSoftware_Version

- バックスラッシュ (\\) は、次の 2 つの例のように、スペースを示すために使用されます。

  HKEY_LOCAL_MACHINE\\\\\\\SOFTWARE\\\Citrix\\\\\\\Secure\ Access\ Client_ProductVersion

  CLIENT.REG(HKEY_LOCAL_MACHINE\\\\\\\Software\\\\\\\Symantec\\\Norton\ AntiVirus_Version).VALUE == 12.8.0.4 -frequency 5

以下は、ユーザーのログオン時にCitrix Secure Accessエージェントのレジストリキーを検索するレジストリ式です。

CLIENT.REG(`secureaccess`).VALUE==HKEY_LOCAL_MACHINE\\\\\\\SOFTWARE\\\\\\\CITRIX\\\\\\\Secure\Access\Client_ProductVersion

注:

レジストリキーと値をスキャンするときに、「式」ダイアログ・ボックスで「アドバンスド・フリーフォーム」を選択し、式の先頭が CLIENT.REG で始まっている必要があります。

レジストリチェックは、次の最も一般的な 5 つのタイプでサポートされています。

- HKEY_CLASSES_ROOT
- HKEY_CURRENT_USER
- HKEY_LOCAL_MACHINE
- HKEY_USERS
- HKEY_CURRENT_CONFIG

チェックするレジストリ値には、次のタイプを使用します。

- 文字列

  文字列型の場合は、大文字と小文字の区別がチェックされます。

- DWORD

  DWORD 型の場合、値は比較され、等しくなければなりません。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 展開文字列

  バイナリやマルチストリングなどの他のタイプはサポートされていません。
- 比較演算子 '==' のみがサポートされています。
- <、> などの他の比較演算子、大文字と小文字を区別する比較はサポートされていません。
- レジストリ文字列の合計長は 256 バイト未満である必要があります。

式に値を追加できます。値には、ソフトウェアのバージョン、サービスパックのバージョン、またはレジストリに表示されるその他の値を指定できます。レジストリのデータ値がテスト対象の値と一致しない場合、ユーザーはログオンを拒否されます。

注:

サブキー内の値をスキャンすることはできません。スキャンは、名前付きの値と関連するデータ値と一致する必要があります。

レジストリポリシーを構成するには

1. 構成ユーティリティのナビゲーションペインで、次のいずれかの操作を行います：

   a. 構成ユーティリティの［構成］タブのナビゲーションペインで、［**Citrix Gateway\］> ［ポリシー** ］を展開し、［セッション］をクリックします。

   b. 構成ユーティリティの［構成］タブのナビゲーションペインで、［**NetScaler Gateway**］**>［ポリシー］>［認証/承認**］の順に展開し、［事前認証EPA］をクリックします。

2. 詳細ペインの タブで、 をクリックします。
3. に、ポリシーの名前を入力します。
4. の横にある をクリックします。
5. ダイアログボックスの で、 を選択します。
6. 次の設定を構成します。

   a. 「コンポーネント」で「レジストリ」を選択します

   b. に、レジストリキーの名前を入力します。

   c. 「修飾子」で、空白のままにするか、「値」を選択します。

   d. で、次のいずれかを実行します。

      - 修飾子が空白のままの場合は、EXISTS または NOTEXISTS を選択します。
      - で を選択した場合は、 または [!==

© 1997–2026 Citrix Systems, Inc. All rights reserved.

e. ［値］に、レジストリエディタに表示される値を入力し、［OK］、［閉じる］の順にクリックします。

複合クライアントデバイスチェック表現の設定

クライアントデバイスチェック文字列を組み合わせて、複合クライアントデバイスチェック式を作成できます。

NetScaler Gateway でサポートされているブール演算子は次のとおりです。

- と (&&)
- または (||)
- ない (!)

精度を上げるには、括弧を使用して文字列をグループ化できます。

注:

コマンドラインを使用して式を設定する場合は、複合式を作成するときに括弧を使用してデバイスチェック式をグループ化します。かっこを使用すると、クライアント式の理解とデバッグが向上します。

AND (&&) 演算子を使用したポリシーの設定

AND (&&) 演算子は、2 つのクライアントデバイスのチェック文字列を組み合わせて、両方のチェックが合格した場合にのみ複合チェックが成功するようにします。式は左から右に評価され、最初のチェックが失敗した場合、2 番目のチェックは実行されません。

AND (&&) 演算子は、キーワード 'AND' または記号 '&&' を使用して設定できます。

例：

以下は、ユーザーデバイスにバージョン 7.0 の Sophos antivirus がインストールされ、実行されているかどうかを判断するクライアントデバイスチェックです。また、Net Logon サービスが同じコンピュータで実行されているかどうかも確認します。

```
CLIENT.APPLICATION.AV(sophos).version==7.0 AND CLIENT.SVC(netlogon) EXISTS
```

この文字列は、次のように設定することもできます：

```
CLIENT.APPLICATION.AV(sophos).version==7.0 && CLIENT.SVC(netlogon) EXISTS
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

OR (\|\|) 演算子を使用したポリシーの設定

OR `(||)`演算子は、2 つのデバイスチェック文字列を組み合わせて機能します。複合チェックは、どちらかのチェックが true の場合にパスします。式は左から右に評価され、最初のチェックに合格した場合、2 番目のチェックは実行されません。最初のチェックがパスしない場合、2 番目のチェックが実行されます。

OR `(||)`演算子は、 キーワード`OR`または`||`記号を使用して設定できます 。

例：

以下は、ユーザーデバイスに`c:\\file.txt`ファイルがあるのか、それとも実行中の`putty.exe`プロセスがあるのかを判断するクライアントデバイスチェックです。

```
client.file(c:\\\\\\\\file.txt) EXISTS) OR (client.proc(putty.exe) EXISTS
```

この文字列は、次のように設定することもできます

```
client.file(c:\\\\\\\\file.txt) EXISTS) || (client.proc(putty.exe) EXISTS
```

NOT (!) 演算子を使用してポリシーを設定

NOT (!)または、否定演算子はクライアントデバイスのチェック文字列を無効にします。

例：

ファイル c:\sophos_virus_defs.dat ファイルが作成されてから 2 日以内であれば、次のクライアントデバイスチェックに合格します。

```
\!(client.file(c:\\\\\\\\sophos\_virus\_defs.dat).timestamp==2dy)
```

EPA コンポーネントとしての nFactor でのデバイス証明書

デバイス証明書は、nFactor で EPA コンポーネントとして設定できます。デバイス証明書は、EPA の一部として任意の要素として表示できます。

以下は、EPAコンポーネントとしてnFactorでデバイス証明書を構成する利点です。

- デバイス証明書の検証に失敗しても、ログオンエラーは発生しません。構成に基づいて、ログオンを続行し、アクセスを制限されたグループの下にユーザーを配置することができます。
- デバイス証明書のチェックはポリシーによって決定されるため、デバイス証明書の認証に基づいて、社内のイントラネットリソースへのアクセスを選択的に許可またはブロックできます。たとえば、デバイス証明書認証は、企業で管理されているラップトップ上でのみの Office 365 アプリケーションへの条件付きアクセスを提供するために使用できます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

デバイス証明書の検証を定期的な EPA スキャンに含めることはできません。

重要:

Windows では、デフォルトで、デバイス証明書にアクセスするための管理者権限が義務されています。管理者以外のユーザーのデバイス証明書チェックを追加するには、デバイスに EPA プラグインと同じバージョンの VPN プラグインをインストールする必要があります。

デバイス証明書を NFactor で EPA コンポーネントとして構成する

コマンドラインインターフェイスを使用して nFactor のデバイス証明書を EPA コンポーネントとして構成するには、コマンドプロンプトで次のように入力します。

```
add authentication epaAction epa-act -csecexpr sys.client_expr("device-cert_0_0") -defaultgroup epa_pass -quarantine_group epa_fail
```

Citrix ADC GUIを使用して、VPN仮想サーバーのEPAコンポーネントとしてnFactorのデバイス証明書を構成するには：

1. NetScaler GUIで、 **「構成」>「Citrix Gateway」>「仮想サーバー」**の順に選択します。
2. ［ **Citrix Gateway 仮想サーバー** ］ページで、変更する仮想サーバーを選択し、［ **編集** ］をクリックします。
3. \[**VPN 仮想サーバー** \] ページで、\[編集\] アイコンをクリックします。

   
4. \[**詳細**\] をクリックします。

   
5. \[デバイス証明書の CA\] セクションの横にある \[**追加** \] をクリックし、\[OK\] をクリックします。

   \[デバイス証明書を有効にする\] チェックボックスは選択しないでください。これを有効にすると、従来の EPA でデバイス証明書の検証が有効になります。
6. NetScaler GUIで、 **「 構成」>「セキュリティ」>「AAA」—「アプリケーショントラフィック」>「ポリシー」>「認証」>「高度なポリシー」>「アクション」>「EPA>」の順に選択します。**
7. \[**認証 EPA アクション** \] ページで、\[**追加** \] をクリックします。\[**Edit** \] をクリックすると、既存の EPA アクションを編集できます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

8. \[**認証 EPA アクションの作成** \] ページで、認証 EPA アクションを作成するために必要なフィールドの値を入力し、\[**EPA エディタ** \] リンクをクリックします。
9. \[**式エディタ**\] リストから \[**共通**\] を選択します。



10. 表示される次のリストから \[**デバイス証明書** \] を選択し、\[**完了** \] をクリックして設定を完了します。



Citrix ADC GUI を使用して、nFactor でデバイス証明書を AAA 仮想サーバの EPA コンポーネントとして構成するには、次の手順を実行します。

1. Citrix DC GUIで、 **「セキュリティ」>「AAAアプリケーショントラフィック」>「仮想サーバー」の順に**選択します。
2. ［ **Citrix Gateway 仮想サーバー** ］ページで、変更する仮想サーバーを選択し、［編集］をクリックします。
3. \[**認証仮想サーバー** \] ページで、\[編集\] アイコンをクリックします。



4. \[**詳細**\] をクリックします。



5. \[**デバイス証明書の CA** \] セクションの横にある \[**追加** \] をクリックします。



6. 追加する証明書を選択し、\[**OK** \] をクリックして構成を完了します。



7. 前のセクションで示 **した手順 6 〜 10** を繰り返して、設定を完了します。

nFactor 認証の要素としての EPA スキャン

重要:

エンドポイント分析は、あらかじめ決められたコンプライアンス基準に照らしてユーザーデバイスを分析することを目的としており、エンドユーザーデバイスのセキュリティを強制または検証するものではありません。ローカル管理者による攻撃からデバイスを保護するには、エンドポイントセキュリティシステムを使用することをお勧めします。

以下は、nFactor EPA の基本エンティティの一部です。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

EPA アクション: EPA アクションは nFactor EPA に導入されたアクションタイプです。次の内容が含まれています。

- クライアントデバイスチェック式:この式は、評価のためにゲートウェイ EPA プラグインに送信されます。
- 成功グループ:EPA の結果が true の場合、このグループは (設定されている場合) ゲートウェイセッションに継承されます。
- 検疫グループ:EPA の結果が false の場合、このグループが設定されている場合、ゲートウェイセッションに継承されます。
- KillProcess: EPA プロセスが終了しなければならないプロセスの名前を表します。
- DeleteFiles: EPA プロセスで削除する必要があるファイルへのパスをカンマで区切って指定します。

グループは、セッションの存続期間中に使用して、クライアントが特定の EPA 条件を満たしているかどうかを判断できます。 特定の要素で EPA が失敗し、最後のアクションに「検疫グループ」が含まれていない場合、そのユーザーの認証は終了します。 「検疫グループ」が存在する場合、認証は継続され、管理者は制限付きアクセスを許可するグループを確認できます。詳細については、「 EPA の実行」を参照してください。

EPA ポリシー:nFactor では、すべてのポリシーが同じ構文「認証ポリシーの追加」で追加されます。ただし、アクションのタイプによって、ポリシーが EPA ポリシーとして認定されます。

EPAファクター： EPAファクターは通常のポリシーラベルです。EPA ファクターと呼ばれるエンティティはありません。EPA ポリシーがファクタにバインドされると、EPA ファクタにする特定のプロパティが継承されます。

> **注：**
>
> このドキュメントでは、「EPA ファクター」という用語は、EPA ポリシーが適用されるファクターを指す場合によく使用されます。

EPA — 隔離: あるファクターですべてのアクションのすべてのクライアントデバイスチェック式が失敗し、最後のアクションに「Quarantine group」が含まれている場合、そのグループがセッションに追加され、NextFactor が調査されます。つまり、失敗にもかかわらず、「検疫グループ」の存在は、セッションを次の段階に認定します。ただし、特別なグループの継承により、管理者はセッションを制限されたアクセスまたは追加の認証ポリシー（OTP や SAML など）に降格させることができます。

最後のアクションで検疫グループが存在しない場合、認証は失敗して終了します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

nFactor の EPA は、次のエンティティも使用します。

- **LoginSchema :** ログオンフォームの XML 表現。ログオンフォームの「ビュー」を定義し、「ファクタ」のプロパティも持っています。
- **ポリシーラベルまたはポリシーファクター:** 認証の特定の段階で試行されるポリシーの集まりです。
- **仮想サーバーラベル:**仮想サーバーはポリシーラベルでもあります。つまり、ポリシーを仮想サーバーにバインドできます。ただし、仮想サーバーは、ユーザーアクセスのエントリポイントであるため、さまざまなポリシーラベルの集まりです。
- **次の要素:** 特定の認証ポリシーが成功したときに適用されるポリシーラベル/要素を指定するために使用されます。
- **NO_AUTHN ポリシー:**アクションが常に成功する特別なポリシー。
- **パススルーファクター:**— ログインスキーマにビューが含まれていないポリシーラベル/ファクターです。これは、NetScaler ADCアプライアンスが、ユーザーの介入なしに指定された要素で認証を続行することを示します。

詳細については、 nFactor の概念、エンティティ、および用語を参照してください。

EPA ファクター相互排他性

EPA ファクターには、1 つ以上の EPA ポリシーが含まれています。EPA ポリシーがファクタにバインドされると、そのファクタに対する通常の認証ポリシーは使用できません。この制限は、最高のユーザーエクスペリエンスを提供し、エンドポイント分析を明確に分離することです。この規則の唯一の例外は NO_AUTHN ポリシーです。NO_AUTHN ポリシーは「障害時ジャンプ」をシミュレートするために使用される特別なポリシーであるため、EPA ファクタで許可されています。

EPA の実行

任意の要素（仮想サーバーファクタを含む）で、ログオンフォームを提供する前に、NetScaler ADCアプライアンスはファクタがEPA用に構成されているかどうかを確認します。その場合、EPA シーケンスがトリガーされるように、特定の応答をクライアント (UI) に送信します。このシーケンスでは、クライアントがクライアントデバイスのチェック式を要求し、結果を送信します。ファクタ内のすべてのポリシーのクライアントデバイスチェック式は、クライアントに一度に送信されます。NetScaler ADCアプライアンスで結果が得られると、すべてのアクションの各式が順番に評価されます。EPA が成功する最初のアクションはその要素を終了し、defaultGroup (構成されている場合) はセッションに継承されます。NO_AUTHN ポリシーが検出された場合、それは自動成功と見なされます。nextFactor が指定されている場合、アプライアンスはそのファクタで続行します。それ以外の場合、認証は終了します。 この条件は、第1因子にも当てはまります。仮想サー

© 1997–2026 Citrix Systems, Inc. All rights reserved.

バーで EPA の後に認証ポリシーファクタがない場合、認証は終了します。これは、EPA の後にユーザーに常にログインページが表示される従来のポリシーの動作とは異なります。 ただし、EPAポリシーが成功しない場合、NetScaler Gateway は、そのファクタまたはカスケードの最後のEPAポリシーに対して構成された検疫グループを検索します。最後のポリシーが検疫グループで構成されている場合、そのグループがセッションに追加され、NextFactor が検査されます。NextFactor が存在する場合、認証はその要素に進みます。それ以外の場合、認証は完了します。

定期的な EPA スキャンを nFactor 認証の要素として構成する

高度なポリシーインフラストラクチャを使用して、定期的な EPA スキャンを nFactor 認証の要素として設定できます。

注：

クラシックポリシーでは、定期的な EPA は `vpn session action` のセッションポリシーの一部として設定されていました。 以下のロジックは、nFactor 認証の要素として EPA スキャンを実装する例として使用されます。



- ユーザーがNetScaler Gateway 仮想IPに接続しようとしました。
- ユーザー名とパスワードフィールドを含むログインページがユーザーにレンダリングされ、ログイン資格情報が提供されます。これらの資格情報を使用して、LDAP または AD ベースの認証がバックエンドで実行されます。成功すると、EPA スキャンを承認するためのポップアップがユーザーに表示されます。
- ユーザーが承認すると、EPA スキャンが実行され、ユーザークライアント設定の成功または失敗に基づいて、アクセスが提供されます。
- スキャンが成功すると、EPA スキャンが定期的に実行され、設定されたデバイスチェック要件が満たされているかどうかが確認されます。
- このようなチェック中に EPA スキャンが失敗すると、セッションは終了します。

前提条件

次の設定が行われていると仮定します。

- VPN 仮想サーバ、ゲートウェイ、および認証仮想サーバの設定
- LDAP サーバの設定と関連付けられたポリシー。

次のセクションでは、必要なポリシーとポリシーラベルの設定、およびポリシーとポリシーラベルの認証プロファイルへのマッピングについて説明します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CLI で

1. LDAP 認証の前に EPA スキャンを実行するアクションを作成し、EPA スキャンポリシーに関連付けます。

```
add authentication epaAction pre-ldap-epa-action -csecexpr
"sys.client_expr ("proc_2_firefox")"



add authentication Policy pre-ldap-epa-pol -rule true -action pre-ldap-
epa-action
```

   前述の式は、プロセス 'Firefox' が実行中かどうかをスキャンします。EPA クライアントは、スキャン表現の数字「2」で示されるように、2 分ごとにプロセスの存在を確認します。

2. EPA `pre-ldap-epa-label` スキャンのポリシーをホストするポリシーラベルを設定します。

```
add authentication policylabel pre-ldap-epa-label -loginSchema
LSCHEMA_INT
```

   注：

   LSCHEMA_INT はスキーマのない組み込みスキーマです (スキーマなし)。つまり、このステップではユーザーに追加の Web ページは表示されません。

3. ステップ 1 で設定したポリシーを、ステップ 2 で設定したポリシーラベルに関連付けます。これで認証メカニズムは完了です。

```
bind authentication policylabel pre-ldap-epa-label -policyName pre-
ldap-epa-pol -priority 100 -gotoPriorityExpression END
```

4. LDAP アクションとポリシーを設定します。

```
add authentication ldapAction ldap-act -serverIP 10.106.103.60
-ldapBase "dc=cgwsanity,dc=net" -ldapBindDn user1@example.net
-ldapBindDnPassword 1.cloud -ldapLoginName samAccountName
-groupAttrName memberOf -subAttributeName CN -passwdChange ENABLED
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
add authentication Policy ldap-pol -rule true -action ldap-act
```

5. SSO を有効にしたログインスキーマを作成します。

```
add authentication loginSchema ldap-schema -authenticationSchema "/
nsconfig/loginschema/LoginSchema/SingleAuth.xml" -SSOCredentials Yes
```

6. LDAP `ldap-pol-label` 認証のポリシーをホストするポリシーラベルを設定します。

```
add authentication policylabel ldap-pol-label -loginSchema ldap-schema
```

7. ステップ 5 で設定したログインスキーマを、ステップ 6 で設定したポリシーラベルにバインドします。

```
bind authentication policylabel ldap-pol-label -policyName ldap-pol
-priority 100 -gotoPriorityExpression NEXT
```

8. LDAP 認証後に EPA スキャンを実行するアクションを作成し、EPA スキャンポリシーに関連付けます。

```
add authentication epaAction post-ldap-epa-action -csecexpr
"sys.client_expr ("proc_2_chrome")"



add authentication Policy post-ldap-epa-pol -rule true -action post-
ldap-epa-action



add authentication policylabel post-ldap-epa-label -loginSchema
LSCHEMA_INT
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
bind authentication policylabel post-ldap-epa-label -policyName post-
ldap-epa-pol -priority 100 -gotoPriorityExpression
```

9. すべてをまとめて、 `pre-ldap-epa-pol` ポリシーを認証仮想サーバーに関連付けます。次のステップでは、 `ldap-pol-label` ポリシーラベルを指してEPAスキャンを実行します。

```
bind authentication vserver user.auth.test -policy pre-ldap-epa-pol
-priority 100 -nextFactor ldap-pol-label -gotoPriorityExpression NEXT



bind authentication policylabel ldap-pol-label -policyName ldap-pol
-priority 100 -gotoPriorityExpression NEXT -nextFactor post-ldap-epa-
label
```

注：

- 複数のファクターとして設定された定期的な EPA では、定期的な EPA 設定による最新のファクターが考慮されます。
- 定期スキャンは EPA プラグインを使用してのみ実行でき、ブラウザでは実行できません。
- 最初の例では、EPA がスキャンでプロセス「Firefox」を検索する最初の要素です。
- EPA スキャンが成功すると、LDAP 認証が行われ、次の EPA スキャンが行われ、プロセス「Chrome」が検索されます。
- 複数の定期スキャンが異なるファクタとして設定されている場合は、最新のスキャンが優先されます。この場合、EPA プラグインは、ログインが成功してから 2 分ごとにプロセス「Chrome」をスキャンします。

GUI 上 (nFactor ビジュアライザーを使用)

GUI の nFactor ビジュアライザーを使用して、高度な EPA スキャンをファクターとして設定できます。次の例では、最初の要素として LDAP を使用し、次の要素として EPA を使用しています。

1. nFactor フローの 1 つ目のファクターを作成します。
   - > > > に移動し、 をクリックします
   - **+** をクリックして nFactor フローを追加します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 係数を追加して をクリックします。



2. 1 つ目の要素のログインスキーマとポリシーを作成します。

   - 最初のファクタータイルで、 をクリックしてログインスキーマを追加します。ドロップダウンリストから既存の認証ログインスキーマを選択するか、ログインスキーマを作成できます。
   - 認証ログインスキーマを作成するには、「**追加**」をクリックします。認証ログインスキーマの詳細については、「nFactor 認証の設定」を参照してください。

   - をクリックして LDAP ポリシーを追加します。LDAP ポリシーがすでに作成されている場合は、同じポリシーを選択できます。 **[追加]** をクリックします。

     注:

     LDAP ポリシーが作成されていない場合は、作成できます。「 **ポリシーの選択」ドロップダウンリストの横にある「**追加**」ボタンをクリックします。「**アクション**」フィールドで「LDAP」を選択します。認証 LDAP サーバの追加の詳細については、を参照してください `https://support.citrix.com/article/CTX123782`。

3. 次のファクターを作成し、それを最初のファクターに接続します。

   - 緑色または赤色の「**+**」アイコンをクリックして、次の要素として EPA を追加します。
   - 「**次の接続要素」ページで次の要素を作成します**。
   - 「**スキーマの追加**」セクションを空白のままにすると、デフォルトではこのファクターにスキーマが適用されません。

4. 次の要素に関するポリシーを追加してください。

   - 「**ポリシーを追加**」をクリックして、認証後の EPA ポリシーとアクションを追加します。
   - 既存のポリシーのリストから選択するか、ポリシーを作成できます。既存のポリシーから選択するには、「ポリシーの選択」 **ドロップダウンリストからポリシーを選択し**、バインドの詳細を入力して、「**追加**」をクリックします。
   - ポリシーを作成するには、「**ポリシーの選択**」ドロップダウンリストの横にある「**追加**」ボタンをクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



5. nFactor フローが完了したら、 をクリックします。
6. nFactor フローを認証サーバーにバインドします。
   - > > に移動します。
   - nFactor を選択し、 をクリックします。



参照ドキュメント

- 多要素（nFactor）の概念、エンティティ、用語
- NetScaler Gateway でLDAP認証を構成する方法
- LDAP認証
- Advanced Endpoint Analysisスキャン

Advanced Endpoint Analysisスキャン

高度なエンドポイント分析（EPA）は、NetScaler Gatewayで構成されたエンドポイントセキュリティ要件についてユーザーデバイスをスキャンするために使用されます。ユーザーデバイスがNetScaler Gateway にアクセスしようとすると、管理者がNetScaler Gateway へのアクセスを許可する前に、デバイスのセキュリティ情報（オペレーティングシステム、ウイルス対策、Webブラウザーのバージョンなど）がスキャンされます。Citrix EPA クライアントのシステム要件について詳しくは、「 エンドポイント分析要件」を参照してください。

高度なEPAスキャンはポリシーベースのスキャンで、NetScaler Gateway で認証セッション用に構成できます。このポリシーは、ユーザーデバイス上でレジストリチェックを実行し、評価に基づいて、NetScaler ADCネットワークへのアクセスを許可または拒否します。

GUI または CLI を使用して高度な EPA スキャンを設定できます。

GUI について

1. EPA アクションを作成します。

   > > > > > > に移動し、 をクリックします。「 **認証 EPA アクションの作成** 」ページで、次の情報を更新し、「 **作成**」をクリックします。

   - 名前:EPA アクションの名前。
   - デフォルトグループ:EPA チェックが成功したときに選択されるデフォルトグループ。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 検疫グループ:EPA チェックが失敗したときに選択される検疫グループ。
- Kill Process: EPA プラグインによって終了されるプロセスの名前を指定する文字列。複数のプロセスはカンマで区切る必要があります。
- ファイルの削除:EPA プラグインによって削除されるファイルのパスと名前を指定する文字列。複数のファイルはカンマで区切る必要があります。
- 表現:EPA 表現形式については、 アドバンスドエンドポイント分析ポリシー表現リファレンスを参照してください 。

2. 対応する EPA ポリシーを作成します。

   > > > > > に移動し、 をクリックします。「 **認証ポリシーの作成** 」ページで、次の情報を更新し、「 **作成**」をクリックします。

   - 名前:詳細な EPA ポリシーの名前。
   - アクションタイプ:認証アクションのタイプ。
   - アクション:ポリシーが一致した場合に実行される認証アクションの名前。
   - 表現:EPA 表現形式については、 アドバンスドエンドポイント分析ポリシー表現リファレンスを参照してください 。
   - ログアクション:リクエストがこのポリシーに一致する場合に使用するメッセージログアクションの名前。最大許容長は 127 文字です。

3. 認証仮想サーバーと認証プロファイルを設定します。

   - > > に移動し、 をクリックします。
   - > > に移動し、 をクリックします。

4. 高度な EPA ポリシーを認証仮想サーバーにバインドします。

   - > > に移動し、認証仮想サーバーを選択します。
   - 「 **詳細認証ポリシー」セクションでポリシーを選択します** 。
   - 「 **ポリシーバインディング** 」セクションの「 **バインド** 」をクリックします。

5. EPA ポリシーを nFactor フローにバインドします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

高度な EPA ポリシーを nFactor フローの要素として追加する方法の詳細については、 nFactor 認証の要素としての EPA スキャンを参照してください。

CLI で

1. EPA スキャンを実行するアクションを作成します。

```
add authentication epaAction EPA-client-scan -csecexpr "sys.client_expr
("proc_2_firefox")"
```

上記の式は、プロセス「Firefox」が実行されているかどうかをスキャンします。EPA プラグインは、スキャン式の数字「2」で表される 2 分ごとにプロセスの存在をチェックします。

2. EPA アクションを高度な EPA ポリシーに関連付けます。

```
add authentication Policy EPA-check -rule true -action EPA-client-scan
```

3. 認証仮想サーバーと認証プロファイルを設定します。

```
add authentication vserver authnvsepa ssl -ip address 10.104.130.129
-port 443
```

```
add Authnprofile_EPA -authnVsName authnvsepa
```

4. 高度な EPA ポリシーを認証仮想サーバーにバインドします。

```
bind authentication vs authnvsepa -policy EPA-check -pr 1
```

EPA ライブラリをアップグレードする

NetScaler ADC GUIを使用してEPAライブラリをアップグレードするには：

1. ［**構成**］>［**NetScaler Gateway**］>［**クライアントコンポーネントの更新**］に移動します。
2. で、** リンクをクリックします。
3. 必要なファイルを選択し、 をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

重要：

- NetScaler Gateway の高可用性では、EPAライブラリをプライマリノードとセカンダリノードの両方でアップグレードする必要があります。
- NetScaler Gateway クラスタリングセットアップでは、すべてのクラスタノードでEPAライブラリをアップグレードする必要があります。

NetScaler ADC スキャン用の OPSWAT でサポートされているWindowsおよびMACアプリケーションのリストについては、`<https://support.citrix.com/article/CTX234466>`を参照してください。

高度なエンドポイント分析スキャンのトラブルシューティング

Advanced Endpoint Analysis スキャンのトラブルシューティングに役立つように、クライアントプラグインはクライアントエンドポイントシステム上のファイルにログ情報を書き込みます。これらのログファイルは、ユーザーのオペレーティングシステムに応じて、次のディレクトリにあります。

Windows Vista、Windows 7、Windows 8、Windows 8.1、Windows 10：

C:\\\ Users\\\\\ <username\ >\ AppData\\\ ローカル\\\ Citrix\\\ AGEE\\\ nsepa.txt

Windows XP:

C:\Documents と設定\ すべてのユーザー\ アプリケーションデータ\ Citrix\ AGEE\ nsepa.txt

Mac OS Xシステム:

\~/ライブラリ/アプリケーション Support/Citrix/EPAPlugin/epaplugin.log

(ここで、~ 記号は該当する macOS ユーザーのホームディレクトリパスを示します。) (ここで、~ 記号は該当する macOS ユーザーのホームディレクトリパスを示します。)

Ubuntu:

- ~/.citrix/nsepa.txt
- ~/.citrix/nsgcepa.txt

© 1997–2026 Citrix Systems, Inc. All rights reserved.

高度なエンドポイント分析ポリシー式リファレンス

このトピックでは、高度なエンドポイント分析式の形式と構成について説明します。NetScaler Gateway 構成ユーティリティは、ここに含まれる式要素を自動的に構築し、手動で構成する必要はありません。

エクスプレッションフォーマット

高度なエンドポイント分析式の形式は次のとおりです。

```
CLIENT.APPLICATION (SCAN-type_ Product-id_ Method-name _ Method-comparator_ Method-param _…)
```

各項目の意味は次のとおりです：

スキャンタイプは、分析されるアプリケーションのタイプです。

Product-ID は、分析されたアプリケーションの製品 ID です。

method-name は、分析対象の製品属性またはシステム属性です。

メソッドコンパレータは、分析に選択されたコンパレータです。

method-param は、分析される 1 つまたは複数の属性値です。

例：

client.application(ANTIVIR_2600_RTP_==_TRUE)

注:

非アプリケーションスキャンタイプの場合、式のプレフィックスは

CLIENT.APPLICATION ではなく CLIENT.SYSTEM になります。

エクスプレッション文字列

高度なエンドポイント分析でサポートされている各スキャンタイプは、式で一意の識別子を使用します。次の表は、スキャンの種類ごとの文字列を列挙したものです。

スキャンの種類	スキャンタイプの式文字列
フィッシング対策	ANTIPHI

© 1997–2026 Citrix Systems, Inc. All rights reserved.

スキャンの種類	スキャンタイプの式文字列
スパイウェア対策	ANTISPY
アンチウイルス	ANTIVIR
バックアップクライアント	BACKUP
デバイスアクセス制御	DEV-CONT
データ損失防止	DATA-PREV
デスクトップ共有	DESK-SHARE
ファイアウォール	FIREWALL
ヘルスエージェント	HEALTH
ハードディスク暗号化	HD-ENC
インスタントメッセンジャー	IM
ウェブブラウザ	BROWSER
P2P	P2P
パッチ管理	PATCH
URL フィルタリング	URL-FILT
MACアドレス	MAC
ドメインチェック	DOMAIN
レジストリスキャン	REG

注:

macOS X 固有のスキャンの場合、式はメソッドタイプの前にプレフィックス MAC-を含みます。したがって、ウイルス対策およびフィッシング対策スキャンの場合、方法はそれぞれMAC-ANTIVIRとMAC-ANTIPHIです。

例:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

client.application (MAC-ANTIVIR_2600_RTP_==_TRUE)

アプリケーションのスキャン方法

高度なエンドポイント分析式の設定では、メソッドを使用してエンドポイントスキャンのパラメータを定義します。これらのメソッドには、メソッド名、コンパレータ、および値が含まれます。次の表は、式で使用可能なメソッドを列挙したものです。

一般的なスキャン方法:

次のメソッドは、複数のタイプのアプリケーションスキャンに使用されます。

方法	説明	コンパレータ	指定可能な値
VERSION*	アプリケーションのバージョンを指定します。	<, <=, >, >=, !=, ==	バージョン文字列
AUTHENTIC**	アプリケーションが本物かどうかを確認します。	==	TRUE
有効	アプリケーションが有効になっているかどうかを確認します。	==	TRUE
RUNNING	アプリケーションが実行されているかどうかを確認します。	==	TRUE
COMMENT	コメントフィールド (スキャンでは無視されます)。式内では [] で表されます。	==	任意のテキスト

* VERSION 文字列には、1.2.3.4 のように、最大 4 つの値から成る 10 進文字列を指定できます。

**AUTHENTIC チェックは、アプリケーションのバイナリファイルの信頼性を検証します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注:

アプリケーションスキャンの種類には、汎用バージョンを選択できます。汎用スキャンを選択した場合、製品 ID は 0 になります。

Gateway には、ソフトウェアの種類ごとに汎用スキャンを設定するオプションが用意されています。汎用スキャンを使用すると、管理者はスキャンチェックを特定の製品に制限することなく、クライアントコンピュータをスキャンできます。

汎用スキャンの場合、スキャン方法は、ユーザーのシステムにインストールされている製品がそのスキャン方法をサポートしている場合にのみ機能します。特定のスキャン方法をサポートしている製品を確認するには、Citrix サポートにお問い合わせください。

固有のスキャン方法:

次のメソッドは、指定されたスキャンの種類に固有のものです。

方法	説明	コンパレータ	指定可能な値
ENABLED-FOR	選択したアプリケーションでフィッシング対策ソフトウェアが有効になっているかどうかを確認します。	`allof, anyof,noneof`	**Windowsの場合：** Internet Explorer、Mozilla Firefox、Google Chrome、Opera、Safari。**Mac用：** Safari、Mozilla Firefox、Google、Chrome、Opera

表2. スパイウェア対策とウイルス対策

方法	説明	コンパレータ	指定可能な値
RTP	リアルタイム保護がオンになっているかどうかを確認します。	==	TRUE
SCAN-TIME	**フルシステムスキャンが実行されてから何分経過したか** 。	<, <=, >, >=, !=, ==	任意の正数

© 1997–2026 Citrix Systems, Inc. All rights reserved.

方法	説明	コンパレータ	指定可能な値
VIRDEF-FILE-TIME	ウイルス**定義**ファイルが更新されてからの分数 (つまり、ウイルス定義ファイルのスタンプと現在のタイムスタンプの間の分数)。	<, <=, >, >=, !=, ==	任意の正数
VIRDEF-FILE-VERSION	定義ファイルのバージョン。	<, <=, >, >=, !=, ==	バージョン文字列
ENGINE-VERSION	エンジンバージョン。	<, <=, >, >=, !=, ==	バージョン文字列

表3. バックアップクライアント

方法	説明	コンパレータ	指定可能な値
LAST-BK-ACTIVITY	**前回のバックアップアクティビティが完了してから何分経過したか** 。	<, <=, >, >=, !=, ==	任意の正数

表4. データ損失防止

方法	説明	コンパレータ	指定可能な値
有効	アプリケーションが有効になっているかどうか、および時間保護がオンになっているかどうかを確認します。	==	TRUE

表5. ヘルスチェックエージェント

© 1997–2026 Citrix Systems, Inc. All rights reserved.

方法	説明	コンパレータ	指定可能な値
SYSTEM-COMPL	システムが準拠しているかどうかを確認します。	==	TRUE

表 6. ハードディスク暗号化

方法	説明	コンパレータ	指定可能な値
ENC-PATH	暗号化ステータスをチェックするためのPATH。	NO OPERATOR	任意のテキスト
ENC-TYPE	指定したパスの暗号化タイプかどうかを確認します。	`allof, anyof, noneof`	**次のオプションで一覧表示**:暗号化されていない、一部、暗号化、仮想、一時停止、保留中

表7. Webブラウザー

方法	説明	コンパレータ	指定可能な値
DEFAULT	デフォルトブラウザとして設定されているかどうかを確認します。	==	TRUE

表 8. パッチ管理 </caption>

方法	説明	コンパレータ	指定可能な値
SCAN-TIME	前回のパッチのスキャンが実行されてから何分経過したか。	<, <=, >, >=, !=, ==	任意の正数
MISSED-PATCH	クライアントシステムには、これらのタ	`anyof, noneof`	任意の事前選択 (Patch Manager サー

© 1997–2026 Citrix Systems, Inc. All rights reserved.

方法	説明	コンパレータ	指定可能な値
	イプのパッチがありません。		バで事前に選択されたパッチ)

テーブル 9. MACアドレス

方法	説明	コンパレータ	指定可能な値
ADDR	クライアントマシンの MAC アドレスが指定されたリストに含まれているかどうかを確認します。	`anyof, noneof`	編集可能なリスト

テーブル 10. ドメインメンバーシップ

方法	説明	コンパレータ	指定可能な値
SUFFIX	指定されたリストにクライアントマシンが存在するか、存在しないかを確認します。	`anyof, noneof`	編集可能なリスト

テーブル 11. 数値レジストリエントリ

方法	説明	コンパレータ	指定可能な値
PATH	レジストリチェックのパス。形式は次のとおりです。HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access Client\EnableAutoUpdate。特殊文字のエスケープは不要です。すべてのレジストリルートキー：HKEY_LOCAL_MACHINE、	NO OPERATOR	任意のテキスト

© 1997–2026 Citrix Systems, Inc. All rights reserved.

方法	説明	コンパレータ	指定可能な値
	HKEY_CURRENT_USER、HKEY_USERS、HKEY_CLASSES_ROOT、HKEY_CURRENT_CONFIG		
REDIR-64	64 ビットリダイレクトに従います。TRUE に設定すると、WOW リダイレクトに従います (つまり、32 ビットシステムではレジストリパスがチェックされますが、64 ビットシステムでは WOW リダイレクトパスがチェックされます)。設定されていない場合、WOW リダイレクトは実行されません (つまり、32 ビットシステムと 64 ビットシステムでは同じレジストリパスがチェックされます)。リダイレクトされないレジストリエントリの場合、この設定は無効です。64 ビットシステムでリダイレクトされるレジストリキーの一覧については、次の記事を参照してください。 `http://msdn.microsoft.com/en-us/library/`	==	TRUE

© 1997–2026 Citrix Systems, Inc. All rights reserved.

方法	説明	コンパレータ	指定可能な値
	`aa384253%28v=vs.85%29.aspx`		
VALUE	上記のパスに期待される値。このスキャンは、REG_DWORD および REG_QWORD のレジストリタイプに対してのみ機能します。	<, <=, >, >=, !=, ==	任意の数字

MAC アドレスの EPA スキャン

NetScaler ADCリリース13.0-88.x以降では、許可または特定のMACアドレスのEPAスキャン構成を構成できます。NetScaler ADCは、ポリシー式とパターンセットを使用してMACアドレスのリストを指定します。

NetScaler ADC リリース13.0-88.xより前は、許可されているすべてのMACアドレスのリストをEPA式の一部として指定する必要がありました。お客様が許可する MAC アドレスのリストが大量にある場合、すべての MAC アドレスを 1 つの式に追加するのは面倒でした。また、1 つの式に追加できる MAC アドレスの数にも制限がありました。

例：

```
add authentication epaAction epa -csecexpr q/
sys.client_expr("proc_0_notepad.exe") || sys.client_expr("proc_0_chrome")
|| sys.client_expr("proc_0_firefox") &&
sys.client_expr("sys_0_MAC_ADDR_anyof_1AC89C83BOF7,0250F20A777C[COMMENT:
MAC Address]")/
```

GUI を使用して MAC アドレスの EPA スキャンを設定します

以前はWindowsスキャンカテゴリで使用可能だったMACアドレス （式） オプションが、NetScaler ADC **GUIの共通スキャンカテゴリで使用できるようになりました** 。このオプションにより、ユーザーは許可または特定の MAC アドレスのリストの EPA スキャンを設定できます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注：

Citrix Secure Access Client 22.10.1以降のバージョンでは、NetScaler ADCがGUI上のEPAスキャン構成を処理するこの方法をサポートしています。

1. パターンセットを設定する。詳細については、「パターンセットを設定する」を参照してください。
2. パターンセットごとに、対応するポリシー式を作成します。

   エクスプレッションを設定するときに、エクスプレッションエディタで > > > > **を選択します

   高度な式の設定について詳しくは、「ポリシーでの高度なポリシー式の構成」を参照してください。
3. 前のステップで構成した式の EPA スキャンを作成します。詳細については、 高度なエンドポイント分析スキャンを参照してください。

CLI を使用して MAC アドレスの EPA スキャンを設定します

1. MAC アドレスをパターンセット内に格納します。

   コマンドプロンプトで次を入力します：

   ```
   add policy patset <name> [-comment <string>]
   ```

   Example:

   ```
   add policy patset patset1

   bind policy patset patset1 1A-C8-9C-83-BO-F7

   bind policy patset patset1 02-50-F2-0A-77-7C … and so on up to 3K
   entries.

   add policy patset patset2

   bind policy patset patset2 1A-2B-3C-4D-5E-6A

   bind policy patset patset2 1A-2B-3C-4D-5E-6B … and so on up to 3K
   ```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
entries.

\`\`\`
```

2. AAA.LOGIN.CLIENT_MAC_ADDR.equals_any()を使用して、各パターンセットに対応するポリシー式を作成します。

   コマンドプロンプトで次を入力します：

   ```
   Add policy expression &lt;name> &lt;value> [-comment &lt;string>] [-
   clientSecurityMessage &lt;string>]
   ```

   例：

   ```
   add policy expression exp1
   AAA.LOGIN.CLIENT_MAC_ADDR.equals_any("patset1")

   add policy expression exp2
   AAA.LOGIN.CLIENT_MAC_ADDR.equals_any("patset2")
   ```

3. 構成済みのポリシー式を使用して EPA スキャンを作成する

   コマンドプロンプトで次を入力します：

   ```
   add authentication epaAction &lt;name>  -csecexpr &lt;expression>
   ```

   例：

   ```
   add authentication epaAction epa -csecexpr q/
   sys.client_expr("proc_0_notepad.exe") ||
   sys.client_expr("proc_0_chrome")  || sys.client_expr("mac-addr_0_exp1")
   || sys.client_expr("mac-addr_0_exp2") ||
   sys.client_expr("proc_0_firefox")/
   ```

   事前認証ポリシーを設定し、

   ```
   add authentication Policy epapol -rule true -action epa
   ```

   事前認証ポリシーをバインドし、

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
bind authentication vserver &lt;name> -policy epapol -priority 10
-gotoPriorityExpression NEXT
```

注意事項

- 許可された MAC アドレスのリストに対する EPA スキャンの設定は、nFactor 認証フローにのみ適用されます。
- 1 つのパターンセットには 3000 個以下のエントリを保存することをお勧めします。
- MAC アドレスは、1A-2B-3C-4D-5E-6F の形式で設定する必要があります。
- EPA スキャンの形式は `mac-addr_0_<policy-expression-name>` です。この形式では、`mac-addr_0_` は静的な値であり、`mac-addr_0_` 後にポリシー式名を入力する必要があります。
- EPA スキャンは、記号 `( ||, &&)` を使用して適切に分離できます。
- 1 つのパターンセットに多数の MAC アドレスを追加するには、ファイルベースのパターンセットのインポートを使用できます。最適なパフォーマンスを得るには、最大 3000 個のエントリ/パターンセットを保存することをお勧めします。
- MAC アドレスがファイル内に存在する場合、ファイルベースのパターンセットのインポートを使用し、インポート時に適切な区切り文字を指定することで、パターンセットを作成できます。

参照ドキュメント

- パターンセットを設定する。
- ファイルベースのインポートを使用してパターンセットを作成します。

ユーザーセッションの管理

NetScaler ADC GUIで［**アクティブユーザーセッション**］**ダイアログボックスからユーザーセッションを管理できます** 。このダイアログボックスには、NetScaler Gateway 上のアクティブなユーザーセッションの一覧が表示されます。ユーザー名、グループ名、または IP アドレスを使用して、エンドユーザーまたはグループセッションを表示できます。このダイアログ・ボックスでは、アクティブなセッションを表示することもできます。セッション情報には以下が含まれます。

- ユーザー名
- ユーザーデバイスの IP アドレス
- ユーザーデバイスのポート番号

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 仮想サーバの IP アドレス
- 仮想サーバーのポート番号
- ユーザーに割り当てられたイントラネット IP アドレス

GUI を使用したユーザーセッションの管理

ユーザーセッションを表示するには

1. NetScaler ADC GUIのナビゲーションペインで、［**NetScaler Gateway**］をクリックします。
2. 詳細ウィンドウの で、 をクリックします。
3. で、次のタイプから選択します。
   - **アクティブユーザー**
   - **アクティブグループ**
   - - を選択した場合は、イントラネット IP アドレスとサブネットマスクを入力する必要があります。
4. ［**続行**］ をクリックします。

セッションリストを更新するには

NetScaler Gateway へのセッションに関する更新された情報を取得できます。

1. NetScaler ADC GUIのナビゲーションペインで、［**NetScaler Gateway**］をクリックします。
2. 詳細ウィンドウの で、 をクリックします。
3. をクリックします。

エンドユーザーまたはグループセッション、または特定のイントラネット IP アドレスを持つセッションを終了するには

ユーザーセッションとグループセッションを終了できます。また、特定のイントラネット IP アドレスとサブネットマスクを持つセッションを終了することもできます。

1. NetScaler ADC GUIのナビゲーションペインで、［**NetScaler Gateway**］をクリックします。
2. 詳細ウィンドウの で、 をクリックします。
3. で、特定のイントラネット IP アドレスを持つユーザー、グループ、またはセッションを選択し、 をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CLI を使用してユーザセッションを管理する

次の CLI コマンドを使用して、ユーザセッション、エンドユーザ、またはグループセッションを表示できます。

- `show aaa session` -指定したユーザー、グループ、IPアドレス、またはIP範囲にバインドされているすべてのNetScaler ADC認証、承認、監査、またはVPN接続を表示します。
- `show vpn icaConnection` -ICAプロキシを使用するすべてのアクティブな接続を表示します。
- `show system session` -現在のすべてのシステムセッション、または指定されたセッションに関する情報を表示します。

常時オン

NetScaler Gateway の常時接続機能により、ユーザーは常にエンタープライズネットワークに接続できます。この永続的な VPN 接続は、VPN トンネルの自動確立によって実現されます。

注

常時オン機能は、NetScaler ADC 12.0ビルド51.24以降のキャプティブポータルをサポートします。

Always On をいつ使用するのか

ユーザーの位置情報に基づいてシームレスな VPN 接続を提供し、VPN に接続していないユーザーによるネットワークアクセスを防止する必要がある場合は、Always On を使用します。

次のシナリオは、Always On の使用方法を示しています。

- 従業員がエンタープライズネットワークの外部でノートパソコンを起動し、VPN 接続を確立するための支援を必要としています。 **解決方法:** ラップトップが企業ネットワークの外部で起動されると、Always On はシームレスにトンネルを確立し、VPN 接続を提供します。
- VPN 接続を使用している従業員は、エンタープライズネットワークに移動します。従業員は企業ネットワークに切り替えられますが、VPN トンネルへの接続は維持されますが、これは望ましい状態ではありません。 **解決方法:** 従業員が企業ネットワークに移動すると、Always On は VPN トンネルを切断し、従業員をエンタープライズネットワークにシームレスに切り替えます。
- 従業員が企業ネットワークの外に移動して、ラップトップを閉じる（シャットダウンしない）。従業員は、ノートパソコンでの作業を再開する際に VPN 接続を確立するための支援を

© 1997–2026 Citrix Systems, Inc. All rights reserved.

必要としています。 **解決策:**従業員が企業ネットワークの外に移動しても、Always Onはシームレスにトンネルを確立し、VPN接続を提供します。

- 企業は、VPN トンネルに接続していないときにユーザに提供されるネットワークアクセスを規制したいと考えています。 **解決方法:** 構成に応じて、Always On はアクセスを制限し、ユーザーはゲートウェイネットワークにのみアクセスできるようにします。

Always On フレームワークを理解する

Always On は、クライアントが以前に確立した VPN トンネルにユーザを自動的に接続します。ユーザーがVPNトンネルを初めて必要とするときは、ユーザーはNetScaler Gateway URLに接続してトンネルを確立する必要があります。Always On 設定がクライアントにダウンロードされた後、この設定によって後続のトンネルの確立が推進されます。

NetScaler Gateway クライアント実行可能ファイルは、常にクライアントマシン上で実行されています。ユーザーがログオンするかネットワークが変更されると、NetScaler Gateway クライアントは、ユーザーのラップトップがエンタープライズネットワーク上にあるかどうかを判断します。場所と構成に応じて、NetScaler Gateway クライアントはトンネルを確立するか、既存のトンネルを切断します。

トンネルの確立は、ユーザーがコンピュータにログオンした後にのみ開始されます。NetScaler Gateway クライアントは、クライアントマシンの資格情報を使用してゲートウェイサーバーとの認証を行い、トンネルの確立を試みます。

トンネルの自動再確立

トンネルの自動再確立は、NetScaler Gateway によってVPNトンネルが切断されたときにトリガーされます。

注

エンドポイント分析の失敗では、NetScaler Gateway クライアントはトンネルの確立を再試行しませんが、エラーメッセージを表示します。認証に失敗した場合、NetScaler Gateway クライアントはユーザーに資格情報の入力を求めます。

シームレストンネル確立でサポートされるユーザ認証方式

サポートされているユーザー認証方法は次のとおりです。

- ユーザー名+ ADパスワード：Windowsユーザー名とパスワードが認証に使用される場合、NetScaler Gateway クライアントはこれらの資格情報を使用してトンネルをシームレスに確立します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- ユーザー証明書：認証にユーザー証明書が使用され、クライアントマシンに証明書が1つしかない場合、Citrix Secure Accessクライアントはこの証明書を使用してトンネルをシームレスに確立します。複数のクライアント証明書がインストールされている場合は、ユーザが優先証明書を選択した後にトンネルが確立されます。Citrix Secure Accessクライアントは、この優先証明書を後のトンネルに使用します。

  スマートカードがユーザー証明書を共有している場合、ストアにある証明書と比較して証明書がストアに動的にインストールされていると、自動ログオンを実行できません。
- ユーザー証明書とユーザー名+AD パスワード:この認証方法は、前述の認証方法を組み合わせたものです。

注

他のすべての認証メカニズムはサポートされますが、トンネルの確立は他の認証方式に対してシームレスではありません。その他すべての認証方法では、ユーザーの介入が必要です。

Always On の設定要件

エンタープライズ管理者は、管理対象デバイスに対して次のことを強制する必要があります。

- ユーザーは、特定の構成のプロセス/サービスを終了できないようにする必要があります。
- 特定の構成では、ユーザーがパッケージをアンインストールできないようにする必要があります。
- ユーザーは特定のレジストリエントリを変更できないようにする

注

管理対象外のデバイスの場合のように、ユーザに管理特権がある場合、この機能が期待どおりに動作しない可能性があります。

常時オン機能を有効にする際の考慮事項

Always On 機能を有効にする前に、次のセクションを確認してください。

プライマリネットワークアクセス：トンネルが確立されると、企業ネットワークへのトラフィックは分割トンネル設定に基づいて決定されます。この動作を上書きするための他の設定は提供されていません。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

クライアントマシンのプロキシ設定:クライアントマシンのプロキシ設定は、ゲートウェイサーバーへの接続時に無視されます。

> **注**
>
> Citrix ADCアプライアンスのプロキシ構成は無視されません。クライアントマシンのプロキシ設定のみが無視されます。システムでプロキシが設定されているユーザには、VPN プラグインがプロキシ設定を無視したことが通知されます。

設定値を「拒否」に設定すると、次の変更が適用されます：

- クライアント UI-プラグインのコンテキストメニューおよびプラグイン UI の および オプションが無効になります。ユーザはゲートウェイ URL を変更できません。
- ブラウザログオン-別のゲートウェイへのブラウザのログオンは許可されていません。クライアントコントロールは無効です。

常時オンの設定

常時接続を構成するには、NetScaler Gateway アプライアンスで常時接続プロファイルを作成し、プロファイルを適用します。

Always On プロファイルを作成するには:

1. NetScaler ADC GUIで、 ［**構成**］**>**［**NetScaler Gateway >**［**ポリシー**］**>**［**AlwaysOn**］**に移動します**
2. ページで、 をクリックします。
3. 「**AlwaysOn プロファイルの作成** 」ページで、次の詳細を入力します：
   - **名前** — プロフィールの名前。
   - **ロケーションベースの VPN (クライアント側のレジストリ名:LocationDetection) — 次のいずれかの設定を選択します。
     - **Remote** ：クライアントがエンタープライズネットワークにあるかどうかを検出し、エンタープライズネットワーク内にない場合はトンネルを確立できるようにします。リモートはデフォルト設定です。
     - クライアントの場所に関係なく、**クライアントが位置検出をスキップしてトンネルを確立できるようにするあらゆる場所**
   - 「**クライアント制御**」— 次の設定のいずれかを選択します：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- は、ユーザーがログオフして別のゲートウェイに接続できないようにします。 は既定の設定です。
- ：ユーザーがログオフして別のゲートウェイに接続できるようにします。

- **VPN 障害時のネットワークアクセス (クライアント側のレジストリ名:alwaysOn)** — 次のいずれかの設定を選択します。
  - は、トンネルが確立されていないときに、クライアントとの間でネットワークトラフィックが流れるようにします。 が既定の設定です。
  - は、トンネルが確立されていないときにネットワークトラフィックがクライアントとの間で流れるのを防ぎます。ただし、ゲートウェイ IP アドレスとの間のトラフィックは許可されます。

    注： モードでは、仮想サーバ、DNS、および DHCP トラフィックのみがブロック解除されます。他の Web サイト、IP アドレス範囲、または IP アドレスのブロックを解除するには、 **AlwaysOnAllowList** レジストリに、FQDN、IP アドレス範囲、または IP アドレスのセミコロン区切りのリストを設定する必要があります。 例えば、mycompany.com、mycdn.com,10.120.67.0-10.120.67.255,67.67.67.67

4. をクリックして、プロファイルの作成を終了します。

Always On プロファイルを適用するには:

1. NetScaler ADCインターフェイスで、［**構成］>［NetScaler Gateway］>［グローバル設定］**を選択します。
2. ページで、 リンクをクリックし、 タブを選択します。
3. **AlwaysOn プロファイル名ドロップダウンメニューから** 、新しく作成したプロファイルを選択し、 **OK**をクリックします。

注

セッションプロファイルでも同様の設定を行い、グループレベル、サーバレバー、またはユーザレベルでポリシーを適用できます。

IIP に関する注意事項

マシンレベルトンネルでは証明書ベースの認証が使用され、作成されるセッションには証明書の共通名がユーザー名として使用されます。そのため、デバイス証明書に一意の共通名がある場合、マシンのセッションごとにユーザー名が異なり、IIP も異なります。一意の名前を持つデバイス証

© 1997–2026 Citrix Systems, Inc. All rights reserved.

明書を生成するようにしてください。デバイス証明書の共通名としてマシン名を使用するのが理想的です。

管理者ユーザーと管理者以外のユーザーの異なる設定の動作の概要

次の表は、さまざまな設定の動作をまとめたものです。また、Always On機能に影響する可能性のある特定のユーザーアクションの可能性についても詳しく説明します。

VPN でのネットワークアクセスの失敗	クライアントコントロール	管理者以外のユーザー	管理者ユーザー
`fullaccess`	許可	トンネルは自動的に確立されます。ユーザーはログオフし、ネットワークからオフにできます。ユーザーは別のNetScaler Gateway をポイントすることもできます。	トンネルは自動的に確立されます。ユーザはログオフし、エンタープライズネットワークから離れることができます。ユーザーは別の NetScaler Gateway をポイントすることもできます。
`fullaccess`	拒否	トンネルは自動的に確立されます。ユーザーがログオフしたり、別のNetScaler Gateway をポイントしたりすることはできません。	トンネルは自動的に確立されます。ユーザーは、NetScaler Gateway クライアントをアンインストールしたり、別の NetScaler Gateway に移動したりできます。
onlyToGateway	許可	トンネルは自動的に確立されます。ユーザーはログオフできます (ネットワークアクセスなし)。ユーザーは別のNetScaler Gateway をポイントすることもできます。この場合、アクセスは新しくポイントされたNetScaler	トンネルは自動的に確立されます。ユーザーは、NetScaler Gateway クライアントをアンインストールしたり、別の NetScaler Gateway に移動したりできます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

VPN でのネットワークアクセスの失敗	クライアントコントロール	管理者以外のユーザー	管理者ユーザー
		Gateway にのみ与えられます。	
onlyToGateway	拒否	トンネルは自動的に確立されます。ユーザーがログオフしたり、別のNetScaler Gateway をポイントしたりすることはできません。	トンネルは自動的に確立されます。ユーザーは、NetScaler Gateway クライアントをアンインストールしたり、別の NetScaler Gateway に移動したりできます。

「常時オン」がダウンしているときに選択した URL を許可する

Always On がダウンしていてネットワークがロックされている場合でも、ユーザはいくつかの Web サイトにアクセスできます。管理者は **AlwaysOnAllowList** レジストリを使用して、AlwaysOn がダウンしているときにアクセスを有効にする Web サイトを追加できます。

注：

- **AlwaysOnAllowList** レジストリは、リリース 13.0 ビルド 47.x 以降でサポートされています。
- **AlwaysOnAllowList**レジストリの場所は、Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access Clientです。
- ワイルドカード URL/FQDN は、 **AlwaysOnAllowList** レジストリではサポートされていません。

AlwaysOnAllowList レジストリを設定するには

AlwaysOnAllowList レジストリに、アクセスを許可する FQDN、IP アドレス範囲、または IP アドレスのセミコロン区切りのリストを設定します。

例： example.citrix.com; 10.103.184.156; 10.102.0.0-10.102.255.100

次の図に、 **AlwaysOnAllowList** レジストリの例を示します。



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Windows ログオン前に常時接続の VPN (正式には常時接続サービス)

Windows ログオン前の AlwaysOn VPN (正式には Always On サービス) 機能を使用すると、ユーザーが Windows システムにログインする前であっても、マシンレベルの VPN トンネルを確立できます。トンネルは、マシンがシャットダウンするまでアクティブなままです。ユーザーがログオンすると、マシンレベルの VPN トンネルがユーザーレベル VPN トンネルに引き継がれます。ユーザーがログオフすると、ユーザーレベルのトンネルが破棄され、マシンレベルのトンネルが確立されます。**Windows ログオン前の常時オン VPN** は、高度な認証ポリシーのみを使用して構成できます。詳細については、「Windows ログオン前に常時接続 VPN を構成する」を参照してください。

Windows ログオン前に常にオン VPN 機能

- 管理者は、リモートで初めて作業するユーザーにワンタイムパスワードを提供できます。このワンタイムパスワードを使用して、ドメインコントローラに接続してパスワードを変更できます。
- 管理者は、ユーザーがログインする前であっても、デバイスに対する AD ポリシーをリモートで管理/適用できます。
- 管理者は、ユーザーがログオンした後のユーザーグループに基づいて、ユーザーにきめ細かなレベルの制御を提供できます。たとえば、ユーザーレベルのトンネルを使用して、特定のユーザーグループに対するリソースへのアクセスを制限または提供できます。
- ユーザートンネルは、ユーザーの要件に従って MFA 用に設定できます。
- 複数のユーザーが同じマシンを使用できます。選択的リソースへのアクセスは、ユーザープロファイルに基づいて提供されます。たとえば、複数のユーザーがキオスク内のマシンを面倒なく使用できます。
- リモートで作業しているユーザーは、ドメインコントローラに接続してパスワードを変更します。
- Windows マシンは、社内 Active Directory (AD) を使用してユーザーのログイン資格情報を確認でき、マシン上の Windows 資格情報はキャッシュされません。また、新しい企業の AD ユーザーは、マシンにシームレスにログオンできます。
- Windows マシンは、ユーザーがログインする前でも企業イントラネットの一部となり、IT 管理者はデバッグ目的で企業ネットワークからクライアントマシンにアクセスできます。
- Windows マシンの VPN トンネルは、別のユーザーがマシンにログインまたはログアウトしても、接続されたままになります。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Windows ログオン前に常時接続の VPN について理解する

Windows ログオン前の常時接続 VPN 機能のイベントのフローを次に示します。



- ユーザーがラップトップの電源を入れます。デバイス証明書をIDとして使用して、NetScaler Gateway に向けてマシンレベルのトンネルが確立されます。
- ユーザは AD クレデンシャルを使用してラップトップにログインします。
- ログイン後、ユーザーは MFA でチャレンジされます。
- 認証が成功すると、マシンレベルのトンネルはユーザレベルのトンネルに置き換えられます。
- ユーザがログアウトすると、ユーザレベルのトンネルはマシンレベルのトンネルに置き換えられます。

注意事項：

- NetScaler Gateway および VPN プラグインのバージョンは 13.0.41.20 以降である必要があります。
- クライアントマシンにインターネット接続がない場合、 **Windows ログオンの前に Always On VPN は** 、VPN トンネルを確立する前にインターネット接続が使用可能になるのを待機します。
- クライアントマシンがキャプティブポータルネットワークに接続されている場合、 **Windows ログオンの前に Always On VPN** はキャプティブポータルへのユーザの認証を待機します。ユーザーがログインしてインターネットアクセスを有効にすると、 **Windows ログオンが VPN トンネルを確立する前に Always** On VPN が実行されます。
- Windowsログオン前にVPNを常時接続する機能では、NetScaler ADC キャプティブポータルがサポートされています。
- Windows でログオン資格情報のキャッシュオプションが有効になっていない場合は、次のシナリオでユーザーはログオンできません。
  - マシンにインターネット接続がありません
  - マシンがキャプティブポータルネットワークに接続されている
- 管理者は、エンドユーザーにログオンページを表示する前に、デバイス証明書の失効ステータスを確認する必要があります。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Windows ログオン構成の前に常時接続の VPN の後の Windows 認証情報マネージャ画面

Windows ログオン前に常時オン VPN 機能を構成すると、 **Windows 資格情報マネージャーの画面が次のように変更されます** 。



ログオン画面で をクリックすると、次の情報が表示されます。

- NetScaler Gateway アイコンは、マシンがNetScaler Gateway に接続されているかどうかを示します。
- ユーザ構成モードに応じて、次のいずれかのステートメントがログオン画面に表示されます。
  - NetScaler Gateway はサービスモードで接続されています
  - NetScaler Gateway はユーザーモードで接続されています

Windows ログオン前に常時接続の VPN を構成する

このセクションでは、詳細ポリシーを使用して **Windows ログオンの前に Always On VPN** を構成するための詳細をキャプチャします。

前提条件

- NetScaler Gateway および VPN プラグインのバージョンは 13.0.41.20 以降である必要があります。
- ソリューションが機能するには、NetScaler ADC Advanced Edition以上が必要です。
- この機能は、高度なポリシーを使用してのみ設定できます。
- VPN 仮想サーバーが稼働している必要があります。

大まかな設定手順

Windows ログオン前の常時接続 VPN の構成には 、次の大まかな手順が含まれます。

1. マシンレベルトンネルのセットアップ
2. ユーザーレベルトンネルのセットアップ (オプション)
3. ユーザー認証を有効にする
   a. VPN 仮想サーバを設定し、証明書キーを仮想サーバにバインドします。
   b. 認証プロファイルを作成する
   c. 認証仮想サーバーを作成する

© 1997–2026 Citrix Systems, Inc. All rights reserved.

d. 認証ポリシーの作成

e. ポリシーを認証プロファイルにバインドします。

マシンレベルトンネル

デバイス証明書をIDとして使用して、NetScaler Gateway に向けてマシンレベルのトンネルが確立されます。デバイス証明書は、クライアントマシンのマシンストアの下にインストールする必要があります。これは、 サービスにのみ適用されます。

デバイス証明書について詳しくは、 認証にデバイス証明書を使用するを参照してください。

重要：

NetScaler Gateway アプライアンスのVPN仮想サーバーが非標準ポート（443以外）で構成されている場合、マシンレベルのトンネルは意図したとおりに機能しません。

デバイス証明書を使用してマシンレベルトンネルをセットアップする

GUI を使用したデバイス証明書ベースの認証設定

1. 「 構成 」タブで**、**「 **NetScaler Gateway」>「仮想サーバー**」に移動します。
2. Citrix Gateway 仮想サーバーページで、既存の仮想サーバーを選択し、「 **編集**」をクリックします。
3. VPN 仮想サーバーページで 、編集アイコンをクリックします。
4. 「 **デバイス証明書用 CA** 」セクションの横にある「 **追加****」をクリックし、「OK」**をクリックします。

   注: チェックボックスは選択しないでください。
5. CA 証明書を仮想サーバーにバインドするには、 セクションの をクリックします。 ページで をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注：

- デバイス証明書のサブジェクトの共通名 (CN) フィールドは空にできません。デバイスが空の CN デバイス証明書でログインしようとすると、VPN セッションはユーザ名が「anonymous」として作成されます。IIP では、複数のセッションが同じユーザー名を持つ場合、以前のセッションは切断されます。したがって、IIP を有効にすると、共通名が空であるため、機能への影響に気付くでしょう。
- クライアントに発行されたデバイス証明書に署名できる可能性のあるすべての CA 証明書（ルートおよび中間）は、手順 4 および 5 の セクションと、仮想サーバの セクションの下にバインドする必要があります** 。CA 証明書を中間/下位とリンクする方法の詳細については、「証明書のインストール、リンク、および更新」を参照してください。
- 複数のデバイス証明書が設定されている場合、有効期限が最も長い証明書が VPN 接続に対して試行されます。この証明書で EPA スキャンが正常に許可されると、VPN 接続が確立されます。この証明書がスキャンプロセスで失敗すると、次の証明書が使用されます。このプロセスは、すべての証明書が試行されるまで続きます。

6. ** をクリックして、必要な証明書を選択します。

7. 必要な CA 証明書を選択します。

8. **［Bind］** をクリックします。
9. 認証仮想サーバーを作成します。

   a. ページの で、 をクリックします。

   b. ページで、認証プロファイルの名前を指定し、 をクリックします。

   c. ページで、認証仮想サーバーの名前を入力します。IP アドレスタイプ] を として選択し、****OK**をクリックします。

   。**注:** 認証仮想サーバーは常に DOWN 状態のままです。

10. 認証ポリシーを作成します。

    a. で、認証ポリシーの内側をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

b. ページで、 の横にある をクリックします。

c. 「 認証ポリシーの作成 」ページで、

i. 事前認証ポリシーの名前を入力します。

ii. リストから を選択します。

iii. の横にある をクリックします。



d. ページで、

i. 作成する EPA アクションの名前を入力します。

ii. `sys.client_expr("device-cert_0_0")` フィールドにと入力します。

iii. **［Create］** をクリックします。



11. 「 認証ポリシーの作成 」ページで、

a. 認証ポリシーの名前を入力します。

b. フィールドに **is_aoservice** と入力します。

c. **［Create］** をクリックします。



12. ページで、 に **100** と入力し、 をクリックします。



CLI を使用したデバイス証明書ベースの認証設定

1. CA 証明書を VPN 仮想サーバーにバインドします。

```
bind ssl vserver <vServerName> -certkeyName <string> -ocspCheck
( Mandatory | Optional )
```

例

```
bind ssl vserver TestClient -CertkeyName ag51.xm.nsi.test.com -CA
-ocspCheck Mandatory
```

2. 認証仮想サーバーを追加します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
add authentication authnProfile <name>  {-authnVsName <string>}
```

例

```
add authentication authnProfile always_on -authnVsName
always_on_auth_server
```

3. 認証 EPA アクションを作成します。

```
add authentication epaAction <name> -csecexpr <expression>
```

Example

```
add authentication epaAction epa-act -csecexpr
 `sys.client_expr("device-cert_0_0")` -defaultgroup epa_pass

\`\`\`
```

4. 認証ポリシーを作成する

```
add authentication Policy &lt;name> -rule &lt;expression> -action
&lt;string>
```

例：

```
add authentication Policy always_on_epa_auth -rule is_aoservice -action
epa_auth
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

重要：

- これで、マシンレベルのトンネルの設定は完了です。Windows ログオン後にユーザーレベルトンネルを設定するには、「**ユーザーレベルトンネル**」のセクションを参照してください。
- クライアントマシンでは、デバイス証明書は.pfx 形式です。Windows では.pfx 形式が認識されるため、.pfx 証明書は Windows マシンにインストールされます。このファイルには、証明書ファイルとキーファイルが含まれています。この証明書は、仮想サーバにバインドされているドメインと同じである必要があります。.pfx とサーバーの証明書とキーは、クライアント証明書ウィザードを使用して生成できます。これらの証明書を認証局で使用して、サーバー証明書とドメインを含むそれぞれの.pfx を生成できます。証明書.pfx は、コンピューターアカウントの個人用フォルダーにインストールされます。`show aaa session`コマンドは、NetScaler ADCアプライアンス上のデバイストンネルを表示します。

ユーザーレベルトンネル

GUI を使用してマシンレベルのトンネルをユーザーレベルのトンネルに置き換える

注： 式`is_aoservice.not`は、NetScaler Gateway バージョン13.0.41.20以降から適用できます。

1. ユーザー認証のポリシーを構成します。
   a. **Citix Gateway > 仮想サーバーに移動し** 、［**詳細設定］**で［**認証プロファイル**］をクリックします。
   b. 認証プロファイルを設定します。
   c. ページで、認証ポリシーの内側をクリックします。
   d. **で をクリックし、ポリシーバインドの** を ではなく [**NEXT** 。

   e. 「**バインド** 」をクリックし、「**認証ポリシー** 」ページで認証ポリシーを選択し、「**バインドの追加**」をクリックします。

   f. ページで、 の横にある をクリックします。

   「 認証ポリシーの作成 」ページで。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

i. 作成する「認証なし」ポリシーの名前を入力します。
ii. アクションタイプを **No_Authn**として選択します。
iii. フィールドに **is_aoservice.NOT** と入力します。
iv. ［**Create**］ をクリックします。



2. **「アクションを選択」**で、「 **バインドの編集**」をクリックします。



3. ページで、 に **110**と入力します。 の横にある をクリックします。

a. ページで、ポリシーラベルのわかりやすい名前を入力し、ログインスキーマを選択して、をクリックします。
b. ** で、 をクリックし、LDAP 認証ポリシーを作成します。
c. をクリックし、 **をクリックします。**
d. をクリックし、** をクリックします。

ページの 列に、構成済みの次の要素ポリシーが表示されます。



4. LDAP ポリシーを認証ポリシーの次の要素として設定できます。

a. ページで、LDAP ポリシーの名前を入力します。
b. として を選択します
c. 設定済みの LDAP **アクションとして** Action を入力します。

注：

- ログインスキーマ XML ファイルの作成については、「ログインスキーマ XML ファイル」を参照してください。
- ポリシーラベルの作成については、 ポリシーラベルの認証を参照してください。
- LDAP 認証ポリシーの作成については、「構成ユーティリティを使用してLDAP認証を構成するには」を参照してください。

CLI を使用してマシンレベルトンネルをユーザーレベルトンネルに置き換える

1. ポリシーを認証仮想サーバにバインドする

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
bind authentication vserver &lt;name> -policy &lt;name> -priority
 &lt;positive_integer> -gotoPriorityExpression &lt;expression>
```

例

```
bind authentication vserver alwayson-auth-vserver -policy alwayson-
auth-pol -priority 100 -gotoPriorityExpression NEXT
```

2. アクションを`NO_AUTH`と式`is_aoservice.not,`として持つ認証ポリシーを追加し、ポリシーにバインドします。

```
add authentication Policy &lt;name> -rule &lt;expression> -action
&lt;string>



bind authentication vserver &lt;name> -policy &lt;name> -priority
&lt;positive_integer> -gotoPriorityExpression &lt;expression>
```

例

```
add authentication Policy alwayson-usertunnel-pol -rule
is_aoservice.not -action NO_AUTHN



bind authentication vserver alwayson-auth-vserver -policy alwayson-
usertunnel-pol -priority 110
```

3. 次の要素を追加し、ポリシーラベルを次の要素にバインドします。

```
add authentication policylabel &lt;labelName> -loginSchema &lt;string>



bind authentication  policylabel &lt;string>  -policyName &lt;string>
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
 -priority &lt;positive_integer> -gotoPriorityExpression
&lt;expression> -nextFactor &lt;string>
```

例

```
add authentication policylabel user-tunnel-auth-label -loginSchema
singleauth_alwayson



bind authentication policylabel user -policyName alwayson-usertunnel-
pol -priority 100
```

4. LDAP ポリシーを設定し、ユーザトンネルポリシーラベルにバインドします。

```


add authentication policy &lt;name>  -rule &lt;expression>  -action
&lt;string>



bind authentication vserver &lt;vserver_name> -policy &lt;string>  -
priorit < positive integer>  gotoPriorityExpression &lt;string>
```

例

```
add authentication Policy LDAP_new -rule true -action LDAP_new



bind authentication policylabel user-tunnel-auth-label -policyName
LDAP_new -priority 100 -gotoPriorityExpression NEXT
```

クライアント側の設定

`AlwaysOn, locationDetection, and suffixList registries` はオプションで、位置検出機能が必要な場合にのみ必要です。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

レジストリキーエントリにアクセスするには、**Computer>HKEY_LOCAL_MACHINE>SOFTWARE>Citrix>Secure Access Client**のパスに移動します。

レジストリキー	レジストリタイプ	値と説明
AlwaysOnService	REG_DWORD	1 => マシンレベルのトンネルを確立するが、ユーザーレベルのトンネルは確立しない。2 => マシンレベルのトンネルとユーザーレベルのトンネルを確立する
AlwaysOnURL	REG SZ	ユーザーが接続する NetScaler Gateway 仮想サーバーのURL。**例:** `https://xyz.companyDomain.com` **重要:** 1 つの URL だけがマシンレベルのトンネルとユーザーレベルのトンネルを担当します。alwaysOnUrl レジストリは、サービスレベルコンポーネントとユーザーレベルのコンポーネントの両方が動作し、設計に基づいて別のトンネル、つまりマシンレベルのトンネルとユーザーレベルのトンネルを接続するのに役立ちます
`AlwaysOn`	REG_DWORD	1 => VPN 障害時にネットワークアクセスを許可する、2=> VPN 障害時にネットワークアクセスをブロックする
AlwaysOnAllowlist	REG_SZ	マシンが厳密モードで実行されている間にホワイトリストに登録する必要がある IP アドレスまたは FQDN のセミコロン区切りのリスト。**例:** `8.8.8.8;linkedin.com`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

レジストリキー	レジストリタイプ	値と説明
UserCertCAList	REG_SZ	カンマまたはセミコロンで区切られたルート CA 名のリスト。証明書の発行者名です。Always On サービスのコンテキストで使用され、カスタマーはクライアント証明書の選択元となる CA のリストを指定できます。**例**: `cgwsanity.net;xyz.gov.in`
locationDetection	REG_DWORD	1 => 位置検出を有効にするには、0 => 位置検出を無効にする
suffixList	REG SZ	セミコロンで区切られたドメインのリストで、位置検出が有効になっているときにいつでもマシンがイントラネット上にあるかどうかを確認する役割を果たします。**Example:** `citrite.net,cgwsanity.net`

これらのレジストリエントリの詳細については、「Always On」を参照してください。

注：

常時接続サービスを構成すると、NetScaler Gateway 仮想サーバーまたはCitrix ADC で構成された常時接続プロファイルはクライアント側で無視されます。そのため、Always On サービスを設定するときは、必ず `locationDetection` VPN レジストリと `AlwaysOn` VPN レジストリも有効にしてください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

アドバンスポリシーを使用した VPN ポリシーの作成

クラシックポリシーエンジン（PE）とアドバンスポリシーインフラストラクチャ（PI）は、NetScaler ADCが現在サポートしている2つの異なるポリシー構成および評価フレームワークです。

アドバンス・ポリシー・インフラストラクチャは、強力な表現言語で構成されています。式言語は、ポリシーでのルールの定義、アクションのさまざまな部分、およびサポートされている他のエンティティの定義に使用できます。式言語は、リクエストまたはレスポンスの任意の部分を解析でき、ヘッダーとペイロードを深く調べることもできます。同じ式言語が拡張され、NetScaler ADCがサポートするすべての論理モジュールで動作します。

注:

ポリシーの作成には、高度なポリシーを使用することをお勧めします。

クラシックポリシーからアドバンスポリシーに移行する理由

高度なポリシーには豊富な式セットがあり、クラシックポリシーよりもはるかに高い柔軟性を提供します。NetScaler ADCはさまざまなクライアントに拡張および対応するため、高度なポリシーを大きく超える式をサポートすることが不可欠です。詳細については、「ポリシーと式」を参照してください。

アドバンスポリシーに追加された機能は次のとおりです。

- メッセージの本文にアクセスする機能。
- 他の多くのプロトコルをサポートします。
- システムの他の多くの機能にアクセスします。
- 基本関数、演算子、データ型の数が増えています。
- HTML、JSON、および XML ファイルの解析に対応します。
- 高速並列マルチストリングマッチング (`patsets` など) を容易にします。

アドバンスポリシーを使用して、次の VPN ポリシーを設定できるようになりました。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- セッションポリシー
- 認可ポリシー
- 交通政策
- トンネルポリシー
- 監査ポリシー

また、エンドポイント分析 (EPA) は、認証機能の nFactor として設定できます。EPA は、Gateway アプライアンスに接続しようとするエンドポイントデバイスのゲートキーパーとして使用されます。エンドポイントデバイスに ページが表示される前に、ゲートウェイ管理者が設定した適格基準に応じて、デバイスのハードウェアおよびソフトウェアの最小要件がチェックされます。Gateway へのアクセスは、実行されたチェックの結果に基づいて許可されます。以前は、EPA はセッションポリシーの一部として構成されていました。nFactor にリンクできるようになり、いつ実行できるかについて柔軟性が高まります。EPA の詳細については、「エンドポイントポリシーの仕組み」トピックを参照してください。nFactor の詳細については、 nFactor 認証のトピックを参照してください 。

ユースケース:

高度な EPA を使用した事前認証 EPA

認証前 EPA スキャンは、ユーザーがログオン資格情報を提供する前に実行されます。認証要素の1つとして事前認証EPAスキャンを使用するnFactor認証用にNetScaler Gateway を構成する方法については、 CTX224268トピックを参照してください 。

高度な EPA を使用したポスト認証 EPA

認証後 EPA スキャンは、ユーザーの資格情報が検証された後に実行されます。クラシックポリシーインフラストラクチャでは、認証後 EPA がセッションポリシーまたはセッションアクションの一部として構成されました。高度なポリシーインフラストラクチャでは、EPA スキャンは nFactor 認証の EPA 要素として構成されます。認証要素の1つとして認証後のEPAスキャンを使用するnFactor認証用にNetScaler Gateway を構成する方法については、 CTX224303のトピックを参照してください 。

高度なポリシーを使用した事前認証および認証後 EPA

EPA は認証の前に実行でき、認証後に実行できます。事前認証および認証後のEPAスキャンを使用したnFactor認証用にNetScaler Gateway を構成する方法については、 CTX231362 トピックを参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

nFactor 認証の要素としての定期的な EPA スキャン

従来のポリシーインフラストラクチャでは、定期的な EPA スキャンがセッションポリシーアクションの一部として構成されていました。高度なポリシーインフラストラクチャでは、nFactor 認証の EPA 要素の一部として設定できます。

定期的な EPA スキャンを nFactor 認証の要素として構成する方法の詳細については、CTX231361 トピックをクリックしてください。

トラブルシューティング：

トラブルシューティングの際には、次の点に留意する必要があります。

- 同じタイプのクラシックポリシーとアドバンスポリシー（セッションポリシーなど）は、同じエンティティ/バインドポイントにバインドできません。
- プライオリティは、すべての PI ポリシーで必須です。
- VPN のアドバンスポリシーは、すべてのバインドポイントにバインドできます。
- 同じ優先度を持つアドバンスポリシーは、単一のバインドポイントにバインドできます。
- 設定されている認可ポリシーのいずれも選択されない場合は、VPN パラメータで設定されたグローバル認可アクションが適用されます。
- 認可ポリシーでは、認可ルールが失敗しても、認可アクションは取り消されません。

クラシックポリシーでよく使用される高度なポリシーに相当する式:

クラシックポリシー式	高度なポリシー式
ns_true	true
ns_false	false
REQ.HTTP	HTTP.REQ
RES.HTTP	HTTP.RES
HEADER "foo"	HEADER("foo")
CONTAINS "bar"	.CONTAINS("bar") [Note use of “..”]
REQ.IP	CLIENT.IP
RES.IP	SERVER.IP

© 1997–2026 Citrix Systems, Inc. All rights reserved.

クラシックポリシー式	高度なポリシー式
SOURCEIP	SRC
DESTIP	DST
REQ.TCP	CLIENT.TCP
RES.TCP	SERVER.TCP
SOURCEPORT	SRCPORT
DESTPORT	DSTPORT
STATUSCODE	STATUS
REQ.SSL.CLIENT.CERT	CLIENT.SSL.CLIENT_CERT

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SSL VPN 仮想サーバを使用した DTLS VPN 仮想サーバの構成

NetScaler Gateway用のDTLS VPN仮想サーバーは、構成済みのSSL VPN仮想サーバーと同じIPアドレスとポート番号を使用して構成できます。DTLS VPN 仮想サーバを設定すると、高度な DTLS 暗号と証明書を DTLS トラフィックにバインドして、セキュリティを強化できます。 リリース 13.0 ビルド 47.x から、以前サポートされていた DTLS 1.0 プロトコルに加えて、DTLS 1.2 プロトコルがサポートされます。

重要：

- デフォルトでは、既存の SSL VPN 仮想サーバの DTLS 機能は ON に設定されています。DTLS VPN 仮想サーバーを作成する前に、サーバーの機能を無効にします。
- DTLSゲートウェイ仮想サーバー用のSNIは、NetScaler Gateway リリース13.0ビルド64.x以降でサポートされています。
- NetScaler ADCリリース13.0ビルド79.x以降、この`helloverifyrequest`パラメータはデフォルトで有効になっています。DTLS プロファイルで`helloverifyrequest`パラメータを有効にすると、攻撃者またはボットがネットワークスループットを圧倒し、アウトバウンド帯域幅の枯渇につながるリスクを軽減できます。つまり、DTLS DDoS 増幅攻撃を軽減するのに役立ちます。 `helloverifyrequest` パラメータの詳細については、 DTLS プロファイルを参照してください。
- UDPトラフィックを処理する場合、バックエンドサーバーが大量のトラフィックをプッシュすると、NetScaler ADCアプライアンスのメモリ消費量が増加します。その結果、クライアント側のTCP MUX接続のため、NetScaler ADCアプライアンスはこのトラフィックをクライアントにプッシュできません。このような場合は、DTLSプロトコルを使用することをお勧めします。

注意事項

- NetScaler Gateway アプライアンス上の DTLS VPN 仮想サーバーは、リリース13.0ビルド58.xから構成できます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- NetScaler Gateway アプライアンスでDTLS VPN仮想サーバーを構成する前に、アプライアンスにSSL VPN仮想サーバーを構成しておく必要があります。
- DTLS VPN 仮想サーバは、設定された SSL VPN 仮想サーバの IP アドレスとポート番号を使用します。
- DTLS ハンドシェイクが失敗すると、接続は TLS にフォールバックします。
- DTLS だけを使用するには、DTLS トラフィックに DTLS 暗号だけをバインドすることで、TLS を無効にできます。
- TCP トラフィックが VPN 上でトンネリングされる場合、DTLS 多重化はサポートされません。

GUI を使用して DTLS VPN 仮想サーバーを構成する

1. ［構成］タブで、［ **NetScaler Gateway**］**>**［**仮想サーバー**］に移動します。
2. **NetScaler Gateway仮想サーバーページで**、既存のSSL VPN仮想サーバーを選択し、「編集」をクリックします**。
3. **「VPN 仮想サーバー」ページで、編集アイコンをクリックし、「DTLS」チェックボックスをオフにし、「OK」をクリックします。**
4. **> に戻り、 をクリックします。**
5. 「 **基本設定**」で、次のフィールドに値を入力し、 **「OK」**をクリックします。
   - 名前-DTLS VPN 仮想サーバーの名前
   - プロトコル- DTLS を選択
   - IP アドレス — SSL VPN 仮想サーバーの IP アドレスを入力します
   - ポート — SSL VPN 仮想サーバーのポート番号を入力します
6. **NetScaler Gateway仮想サーバーページで**、以前に追加した仮想サーバーを選択し、「編集」をクリックします**。
7. で、矢印アイコンをクリックして必要な証明書キーを選択します。
8. 「 **サーバー証明書のバインド」>「サーバー証明書の選択**」で、既存のSSL証明書キーを選択するか、作成します。
9. ページで をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注：

- DTLS 1.2 を使用するには、「SSL パラメータ」の下の編集アイコンをクリックし、「**DTLS** 1.2」チェックボックスを選択します。
- サーバ名表示（SNI）は、DTLS タイプの VPN 仮想サーバでサポートされます。

CLI を使用して DTLS VPN 仮想サーバーを設定します

コマンドプロンプトで、次の一連のコマンドを入力します：

```
set vpn vserver <ssl vpnvserver name> -dtls off

add vpn vserver <dtls vpnvserver name> dtls <ssl vpn vserver IP> <ssl vpn vserver port>

bind ssl vservser <dtls vpnvserver name> -certkeyName <existing ssl cert key or newly created cert key>
```

DTLS 1.0 は通常どおりに動作します。DTLS 1.2 を使用するには、次のコマンドを入力します：

```
set ssl vserver < dtls vpnvserver name > -dtls12 ENABLED
```

例

```
set vpn vserver vpnvserver  -dtls off

add vpn vserver vpnvserver_dtls dtls 10.108.45.220 443

bind ssl vservser vpnvserver_dtls -certkeyName sslcertkey

set ssl vserver vpnvserver_dtls -dtls12 ENABLED
```

DTLS タイプ VPN 仮想サーバーの SNI を有効にするには、次のコマンドを入力します。

```
set ssl vserver <vServerName>@ [-SNIEnable ( ENABLED | DISABLED )
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
bind ssl vservser <dtls vpnvserver name> -certkeyName <existing ssl cert
key or newly created cert key> <-SNICert>
```

例

```
set ssl vserver _XD_10.106.40.225_443_DTLS -sniEnable eNABLED

bind ssl vserver _XD_10.106.40.225_443_DTLS -certkeyName "Insight/
*.insight.net.cer_CERT_" -snICert
```

サポートされている DTLS VPN 仮想サーバーパラメーター

DTLS タイプの VPN 仮想サーバーでは、次のパラメーターのみがサポートされます。

- Ipaddress
- ポート
- 状態
- ダブルホップ
- downstateflush
- コメント
- Appflowlog
- Icmpvsrresponse

サポートされていない DTLS VPN 仮想サーバーパラメーター

次のパラメータは、DTLS タイプの VPN 仮想サーバーではサポートされていません。

- LinuxEPAPluginUpgrade
- WindowsEPAPluginUpgrade
- maxAAAUsers
- icaProxySessionMigration
- loginOnce
- cginfraHomePageRedirect
- logoutOnSmartcardRemoval

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- L2Conn
- MacEPAPluginUpgradeRHIstate
- icaOnly
- maxLoginAttempts
- failedLoginTimeout
- vserverFqdn
- deviceCert
- rdpServerProfileName
- pcoipVserverProfileName
- tcpProfileName
- netProfile
- authnProfile
- Listenpriority
- Listenpolicy
- ipset
- certkeyNames

XenAppおよびXenDesktopウィザードを使用してDTLS仮想サーバーを構成します

1. 「 **Citrix 製品との統合** 」の「 **XenAppとXenDesktop**」をクリックします。
2. **XenAppおよびXenDesktopのセットアップウィザードで、［StoreFront］を選択し、［続行］をクリックします。**
3. **NetScaler Gateway 設定ページで**、「 **このVPN vServerのDTLSリスナーを構成する」チェックボックスを有効にして、「続行** 」をクリックします**。

   DTLS リスナーの設定が完了しました。
4. 「サーバー証明書」で、「 **ファイルを選択** 」をクリックしてサーバー証明書を選択し、「 **続行**」をクリックします。
5. 証明書ファイルとキーファイル名を指定し、 をクリックします。
6. **StoreFront** セクションで、次のように必須パラメータの値を指定し、「 **続行**」をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

7. 「**認証**」セクションで、次のように必須パラメータの値を指定し、「**接続をテスト**」をクリックします。

   サーバーが到達可能であることを確認し、 の値と を指定して、 をクリックします。

8. をクリックして設定を完了します。

制限事項

- DTLS 1.2 は、Windows クライアントでのみサポートされています。
- DTLS を使用した VPN 仮想サーバは IPv6 アドレスをサポートしていません。
- SSL ポリシーと SSL プロファイルは、DTLS VPN 仮想サーバではサポートされていません。また、VPN 仮想サーバポリシーのバインドはサポートされていません。
- NetScaler Gateway DTLS VPN仮想サーバーは、次の機能をサポートしていません。ただし、NetScaler Gateway SSL VPN仮想サーバーは次の機能をサポートしています。
  - コンテンツスイッチング仮想サーバを備えた Unified Gateway
  - UDP MUX
  - UDPビデオ
  - UDPオーディオ
  - PCOIP
- DTLS VPN 仮想サーバーの統計に関連する`stat vpn vserver`コマンドはサポートされていません。
- HSM キーは DTLS 仮想サーバーではサポートされていません。
- クラスタ構成はサポートされていません。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix製品との統合

NetScaler Gateway のインストールと構成を担当するシステム管理者は、Citrix Endpoint Management、StoreFront、およびWeb Interfaceをサポートするようにアプライアンスを構成できます。

ユーザーは、内部ネットワークまたはリモートの場所からEndpoint Managementに直接接続できます。ユーザーが接続すると、Web、SaaS、モバイルアプリにアクセスできます。また、ShareFileにあるドキュメントを任意のデバイスからサポートすることもできます。

NetScaler Gateway を介したサーバーファームへのユーザー接続を許可するには、StoreFront またはWeb Interface、およびNetScaler Gateway の設定を構成します。ユーザーが接続すると、公開アプリケーションと仮想デスクトップにアクセスできます。

NetScaler Gateway とEndpoint Management、StoreFront、およびWeb Interfaceを統合するための構成手順は、次のことを前提としています。

- NetScaler Gateway はDMZに存在し、既存のネットワークに接続されています。
- NetScaler Gateway はスタンドアロンアプライアンスとして展開され、リモートユーザーは NetScaler Gateway に直接接続します。
- StoreFront、Endpoint Management、Citrix Virtual Apps、Citrix Virtual DesktopsおよびWeb Interfaceは、セキュリティで保護されたネットワーク内にあります。
- ShareFile はEndpoint Management で設定されています。 [ShareFile の詳細については、「ShareFile」トピックおよび「 ユーザーアクセス用の ShareFile の構成 」トピックを参照してください。](http://docs.citrix.com/en-us/sharefile.html)

StoreFront とEndpoint Managementの展開方法は、モバイルデバイスに提供するアプリによって異なります。ユーザーがMDX Toolkitでラップされたアプリにアクセスできる場合、Endpoint Managementはセキュアネットワーク内のStoreFrontの前に配置されます。MDXアプリへのアクセスを提供していない場合、StoreFront はセキュリティで保護されたネットワーク内のEndpoint Managementの前に配置されます。

ユーザーがアプリケーション、デスクトップ、ShareFileに接続する方法

展開環境に Citrix Endpoint Management がある場合、ユーザーは次の方法で接続できます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 内部ネットワークのリソースへの完全なVPNトンネルを確立するCitrix Gateway プラグイン。セッションプロファイルを作成して、Windows用のCitrix Gateway プラグインまたはMac用のCitrix Gatewayプラグインを選択します。ユーザーがプラグインを使用してログオンすると、エンドポイントの分析スキャンをユーザーデバイスで実行できます。

注

：エンドポイント分析スキャンをMacコンピューターで実行できるようにするには、Citrix Gateway 10.1、Build 120.1316.e以降をインストールする必要があります。

- Citrix Workspace アプリを使用して、ShareFileからEndpoint Management を介してウェブ、SaaS、エンタープライズアプリケーション、Webリンク、およびドキュメントに接続します。ユーザーがCitrix Workspace アプリでログオンすると、Citrix Gateway は接続をEndpoint Management にルーティングします。Citrix Workspace アプリが接続を確立すると、ユーザーのアプリケーションとドキュメントがCitrix Workspace アプリに表示されます。 ユーザーがCitrix Workspace アプリでログオンし、Endpoint Management に直接接続する場合は、Citrix Gateway でクライアントレスアクセスを有効にする必要があります。この展開では、StoreFront は必要ありません。
- Citrix Workspace アプリを使用して、StoreFront またはWeb Interfaceを介して公開アプリケーションおよび仮想デスクトップに接続できます。ユーザーがCitrix Workspace アプリでログオンすると、Citrix Gateway はStoreFront またはWeb Interfaceへの接続をルーティングします。Citrix Workspace アプリが接続を確立すると、ユーザーアプリケーションとデスクトップがCitrix Workspace アプリに表示されます。
- Secure Hub は、Endpoint Management を介してモバイルデバイスからWorxMailやWorxWebなどのiOSおよびAndroidアプリに接続します。ユーザーは、Secure Hub にログオンすると、Endpoint Management で設定したモバイルアプリにアクセスできます。Citrix Gateway がMicro VPN接続を確立すると、ユーザーのモバイルアプリがSecure Hub ウィンドウに表示されます。ユーザーはSecure Hub からアプリを起動できます。一部のアプリでは、ユーザーがモバイルデバイスにアプリをダウンロードしてインストールする必要があります。

前述のシナリオのいずれかで、ユーザーがCitrix Gateway 経由で接続する場合は、次の操作を行います。

- ユーザーは、Citrix GatewayプラグインまたはCitrix Workspaceアプリを使用してログオンします。 初めてログオンするには、ユーザーがWebブラウザーを開き、Citrix GatewayまたはCitrix Workspace アプリの完全修飾ドメイン名（FQDN）を入力します。 モバイルデバイスを持つユーザーは、Secure Hub を使用してログオンします。
- ログオンページで、ユーザーは自分の資格情報を入力し、認証されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 認証後、ユーザーセッションは、展開環境に応じてStoreFront またはEndpoint Management にリダイレクトされます。
- StoreFront とEndpoint Management の両方を展開する場合、Citrix Gateway は展開の最初のサーバーに接続します。たとえば、Endpoint Management でMDXモバイルアプリを構成する場合、Endpoint Management 背後にStoreFront を展開します。MDXモバイルアプリケーションへのアクセスを提供しない場合は、StoreFront の背後にEndpoint Management を展開します。
- ユーザーのデスクトップ、ドキュメント、Web、SaaS、Windowsベースのアプリケーションはすべて Citrix Workspace アプリまたはSecure Hub に表示されます。

Exchange、ファイル共有、内部Webサイトなど、内部ネットワーク上の他のリソースにアクセスする必要がある場合は、Citrix Gateway プラグインを使用してログオンすることもできます。たとえば、ユーザーがネットワーク内の Microsoft Exchange サーバーに接続する場合、ユーザーは自分のコンピュータで Outlook を起動します。セキュアな接続は、Citrix Gateway に接続するCitrix Gatewayプラグインを使用して行われます。SSL VPN トンネルが Exchange Server に作成され、ユーザは自分の電子メールにアクセスできます。

重要

・Citrix Gateway仮想サーバーで認証を構成することをお勧めします。Citrix Gateway で認証を無効にすると、認証されていないHTTPリクエストが、内部ネットワークのWeb Interface、StoreFront またはEndpoint Management を実行しているサーバーに直接送信されます。

NetScaler Gateway とStoreFront の統合

Citrix Virtual Apps and Desktops ウィザードは、StoreFront とNetScaler Gatewayを統合するために使用されます。この統合により、NetScaler Gateway を介して、ホストされた仮想デスクトップ（XenDesktop）およびホストされるWindows仮想アプリケーション（XenApp）に簡単にアクセスできます。

NetScaler Gateway とStoreFront の統合では、Citrix Virtual Apps and Desktops ウィザードのワークフローが次の機能で強化されました。

- **サポートされているStoreFrontで構成されたストアの取得：サポートされているStoreFront** で構成されたストアは、ワンクリックで取得できます。この検索方法は、手動による介入を回避し、ヒューマンエラー（タイプミス）を回避するのに役立ちます。
- **StoreFront 構成ファイルのエクスポートサポート：** StoreFront 構成ファイルはNetScaler Gateway でエクスポートできます。その後、StoreFront 構成ファイルをダウンロードして、サポートされているStoreFront サーバーにインポートできます。ファイルがインポートされると、StoreFront はNetScaler統合を完了します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **認証サーバーとしてのStoreFront ：認証サービスの認証サーバーとしてStoreFront** を使用する高度な認証アクションを導入することにより、認証が簡素化されます。

注：認証サーバーは、Citrix Virtual Apps and Desktops以外の展開にも使用できます。

StoreFront で使用するようにNetScaler Gatewayを構成する方法

前提条件

NetScalerとStoreFront を統合するには、次の情報が必要です。

- NetScaler Gateway 仮想サーバーのIPアドレス
- StoreFrontサーバーの完全修飾ドメイン名 (FQDN)
- NetScaler Gateway のサーバー証明書
- 認証サーバーの詳細

また、次の点も確認してください。

- NetScaler GatewayとStoreFront の間のファイアウォールポートが開いている
- StoreFront はLANアクセスできる

NetScaler Gateway GUIを使用してStoreFront とNetScaler Gateway を統合するには：

1. タブをクリックします。
2. ［**Citrix 製品との統合**］で、［**XenApp およびXenDesktop**］をクリックします。
3. **「始める」をクリックします。**
4. **StoreFront** を選択して［**続行**］**をクリックします。**
5. ［NetScaler Gateway］領域の次のフィールドに値を入力し、［**続行**］**をクリックします。**
   - **ゲートウェイFQDN** — NetScaler Gateway の完全修飾ドメイン名
   - **ゲートウェイIPアドレス** — NetScaler Gateway のIPアドレス
   - **ポート** — NetScaler Gateway のポート
6. 領域で次のファイルをインポートし、 をクリックします。**証明書ファイル** -NetScaler Gateway のサーバー証明書。
7. **StoreFront** 領域に次の情報を入力し、［**続行**］をクリックします。
   - **StoreFront URL** — StoreFront サーバーのURL

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Receiver for Webパス** -StoreFront ですでに構成されているReceiver for Webサイトへのパス
- **既定の Active Directory ドメイン** -内部ネットワークのシングルサインオンアプリケーションに使用されるシングルサインオンドメイン
- **Secure Ticket Authority URL** — Secure Ticket Authority URL。通常、配信コントローラーに存在します。

  注：［**ストアの取得**］を選択すると、NetScaler GatewayはStoreFront に接続し、StoreFront で構成されているすべてのストア情報を返します。次に、ドロップダウンメニューから優先ストアを選択できます。［**ストアの取り出し**］オプションは、最新の StoreFront サーバーでのみ機能します。

8. 新しい認証設定を使用すると、ユーザーは認証ポリシーを作成することも、既存の認証ポリシーを使用することもできます。

   ドメインベースの認証ポリシーを作成するには、の次のフィールドに値を入力し、 をクリックします。

9. **認証タイプの選択-** ドロップダウンメニューからドメインを選択します。
10. または を選択します。

    - **IP アドレス** — ドメインサーバの IP アドレス
    - **Port** ：ドメインサーバのポート
    - **ベース DN** -ユーザーが配置されているベース DN
    - **サービスアカウント** -Active Directory のクエリに使用するアカウント
    - **Password** -ドメインサーバーへのログオンに必要なパスワード
    - **Time out** ：ドメインディレクトリが検索される期間
    - **サーバーログオン名属性** -NetScalerアプライアンスが外部ドメインサーバーまたはAcActive Directory を照会するために使用する名前属性。

    必要に応じて、 をクリックして、サーバーが到達可能であり、有効な資格情報が提供されていることを確認できます。

    注:既存の認証ポリシーを使用するには、「 認証タイプの選択 」 リストから必要な認証タイプを選択し、前述の情報を入力します。

11. ［NetScaler Gateway の設定］ページで、［**完了**］**をクリックします。**
12. をクリックします。**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

StoreFront GUIで必要な構成手順は次のとおりです。

1. `Gatewayconfig.zip` ファイルをStoreFront にコピーします。
2. をクリックします。
3. ［ **NetScaler Gateway の管理** ］を選択し、［ **NetScaler Gateway の管理** ］ウィンドウの［ **ファイルからインポート** ］リンクをクリックします。
4. ［ **NetScaler構成のインポート** ］ウィンドウの［ **ファイルの選択** ］領域で、［ **次へ**］をクリックします。
5. **［ログオンの種類の選択］** 領域で、必要に応じて、StoreFront がNetScaler Gateway **に接続するためのコールバックURLを指定し** 、［ **次へ**］をクリックします。
6. で、 をクリックします。
7. で をクリックします。
8. **［完了］**をクリックします。

NetScaler Gateway をCitrix Virtual Apps and Desktops 統合する

公開リソースおよびデータへのアクセスを管理するには、StoreFrontサーバーを展開および構成します。リモートアクセスの場合は、NetScaler GatewayをStoreFrontの前に追加することをお勧めします。

注

Citrix Virtual Apps and DesktopsをNetScaler Gatewayと統合する方法の詳細な構成手順については、StoreFront のドキュメントを参照してください。

次の図は、NetScaler Gateway を含むCitrix の簡略化されたCitrix itrix展開の例を示しています。NetScaler GatewayはStoreFrontと通信して、Citrix Virtual Apps and Desktopsが配信するアプリやデータを保護します。ユーザーデバイスはCitrix Workspaceアプリを実行してセキュリティで保護された接続を構築し、アプリ、デスクトップ、ファイルにアクセスします。



ユーザーは、NetScaler Gatewayを使用してログオンおよび認証を行います。NetScaler Gatewayは、DMZで展開およびセキュリティ保護されます。2要素認証が構成されます。ユーザーの資格情報に基づいて、ユーザーに該当のリソースおよびアプリケーションが提供されます。アプリケーションとデータは適切なサーバー上に存在します（図には表示されていません）。セキュリティ上機微なアプリケーションとデータについては、別のサーバーが使用されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix Endpoint Management、Citrix Virtual Apps and Desktopsを使用した展開

ユーザーは、ネットワークでホストされている Windows、Web、SaaS、モバイルアプリケーション、および仮想デスクトップに接続できます。NetScaler Gateway、Citrix Endpoint Management、およびCitrix Virtual Apps and Desktopsを使用して、リモートユーザーおよび内部ユーザーにアプリケーションおよびデスクトップへのアクセスを提供できます。NetScaler Gateway はユーザーを認証し、Citrix WorkspaceアプリまたはSecure Hubを使用してユーザーがアプリケーションにアクセスできるようにします。

ユーザーは、Citrix WorkspaceアプリおよびStoreFrontを使用して、Citrix Virtual Appsで公開されているWindowsベースのアプリおよびCitrix Virtual Desktopsで公開された仮想デスクトップに接続します。

Citrix Endpoint Managementには、ユーザーがWeb、SaaS、およびMDXアプリケーションに接続できるようにするCitrix Endpoint Managementが含まれています。Endpoint Managementを使用すると、シングルサインオン（SSO）用のウェブ、SaaS、およびMDXアプリケーションを、ShareFileドキュメントとともに管理できます。Endpoint Managementは内部ネットワークにインストールします。リモートユーザーは、NetScaler Gateway を介してEndpoint Managementに接続し、アプリケーションとShareFileデータにアクセスします。リモートユーザーは、NetScaler Gateway プラグイン、Citrix Workspace アプリ、またはSecure Hubのいずれかを使用して接続し、アプリケーションおよびShareFileにアクセスできます。内部ネットワークにいるユーザーは、Citrix Workspace アプリを使用してEndpoint Managementに直接接続できます。次の図は、Endpoint Management とStoreFront を使用して展開されたNetScaler Gateway を示しています。

展開環境で、Endpoint ManagementからMDXアプリケーションにアクセスし、StoreFront からWindowsベースのアプリケーションにアクセスできる場合は、次の図に示すように、StoreFront Endpoint Managementを展開します：

図1：StoreFront の前にEndpoint Management 機能を備えたNetScaler Gatewayを展開する



展開環境でMDXアプリケーションへのアクセスが提供されない場合、次の図に示すように、StoreFront はEndpoint Managementの前に配置されます。

図2：Endpoint Management StoreFront を使用したNetScaler Gateway の展開



展開ごとに、StoreFront およびEndpoint Managementは内部ネットワークに存在し、NetScaler GatewayはDMZに存在する必要があります。Endpoint Managementの展開について詳しくは、「

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Endpoint Managementのインストール 」トピックを参照してください。 StoreFrontの展開について詳しくは、「 StoreFront のトピック」を参照してください。

Citrix Endpoint Management 環境の設定を構成する

Citrix Endpoint Management用NetScaler ADCウィザードの指示に従って、Citrix Endpoint Management展開環境用のNetScaler ADC機能を構成できます。このウィザードを使用すると、次のことができます。

- **マイクロ VPN をセットアップします。**このシナリオでは、リモートユーザーは内部ネットワークのアプリケーションとデスクトップにアクセスできます。
    - Citrix Endpoint ManagementのMAM専用モードでは、認証にNetScaler Gateway を使用する必要があります。
    - MDMの展開では、モバイルデバイスVPNとしてNetScaler Gatewayをお勧めします。
    - ENT展開の場合、ユーザーがMDM登録をオプトアウトすると、デバイスは従来のMAMモードで動作し、NetScaler Gateway FQDNを使用して登録します。
- **証明書ベースの認証を構成します。**Citrix Endpoint Managementのデフォルトの構成は、ユーザー名とパスワードの認証です。Citrix Endpoint Management環境への登録とアクセスのためのセキュリティレイヤーを追加するには、証明書ベースの認証の使用を検討してください。
- **Citrix Endpoint Management サーバーの負荷を分散します。**NetScaler ADC負荷分散は、複数のCitrix Endpoint Managementサーバーを使用している場合、またはCitrix Endpoint ManagementがDMZまたは内部ネットワーク内にある場合（したがって、デバイスからNetScaler ADC、Citrix Endpoint Managementへのトラフィックフロー）、すべてのCitrix Endpoint Managementデバイスモードで必要です。このシナリオでは、NetScalerアプライアンスはユーザーデバイスとCitrix Endpoint Managementサーバーの間のDMZに配置され、モバイルデバイスからCitrix Endpoint ManEndpoint Management サーバーに送信される暗号化されたデータの負荷を分散します。
- **電子メールフィルタリングを使用して Microsoft Exchange サーバーの負荷を分散します。**このシナリオでは、NetScaler ADCアプライアンスは、ユーザーデバイスとCitrix Endpoint Management NetScaler ADCコネクタ（XNC）の間、およびユーザーデバイスとMicrosoft Exchange CASサーバーの間にあります。ユーザーデバイスからのすべての要求はNetScaler Gateway アプライアンスに送信され、XNCと通信してデバイスに関する情報を取得します。XNCからの応答に応じて、NetScaler ADCアプライアンスは、ホワイトリストに登録されたデバイスから内部ネットワークのサーバーに要求を転送するか、ブラックリストに登録されたデバイスからの接続をドロップします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **要求されたコンテンツのタイプに基づいて、ShareFile StorageZones コネクタの負荷を分散します。**このシナリオでは、ストレージゾーン Controller 環境に関する基本情報の入力を求められ、次の処理を行う構成が生成されます。
  - ストレージゾーン Controller 間でトラフィックを負荷分散します。
  - StorageZones コネクタのユーザー認証を提供します。
  - ShareFile のアップロードおよびダウンロードの URI 署名を検証します。
  - NetScaler ADCアプライアンスでSSL接続を終了します。

ShareFileの構成の詳細については、「ストレージゾーンController用のNetScaler ADC 構成」を参照してください。

重要：

Citrix Endpoint Managementウィザードを使用する前に、次のCitrix Endpoint Managementの展開に関する記事を参照して、設計および展開に関する情報と推奨事項を確認してください。

Citrix Endpoint Management 統合
NetScaler GatewayおよびNetScaler ADCとの統合
MDXアプリのSSOとプロキシの考慮事項
認証
Citrix Endpoint Management用NetScaler ADCウィザードは一度だけ使用できます。テスト環境、開発環境、本番環境など、複数のCitrix Endpoint Managementインスタンスを使用する場合は、追加の環境用にNetScaler ADCを手動で構成する必要があります。次のサポート記事には、ウィザードによって実行されるコマンドの一覧と、それらのコマンドを実行してNetScaler ADCインスタンスを作成する方法が記載されています。
NetScaler ADC上のCitrix Endpoint Management ウィザードによって生成されるコマンド-SSLブリッジ
NetScaler ADC上のCitrix Endpoint Management ウィザードによって生成されるコマンド-SSLオフロード

NetScaler機能のライセンス要件

次のNetScaler ADC機能を有効にするには、ライセンスをインストールする必要があります：

- Citrix Endpoint ManagementのMDM負荷分散には、NetScaler ADC標準ライセンスが必要です。
- StorageZonesを使用したShareFile負荷分散には、NetScaler ADC標準ライセンスが必要です。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Exchange負荷分散には、NetScaler ADCライセンスまたは統合キャッシュライセンスを追加したアドバンスドライセンスが必要です。

NetScaler for Citrix Endpoint Management ウィザード

このセクションでは、NetScaler for Citrix Endpoint Managementウィザードを使用して次の例を説明します：

- 内部ネットワーク内のCitrix Endpoint Managementで管理されるリソースへのリモートユーザー接続用のマイクロVPNアクセスをセットアップする
- 証明書ベースの認証を構成します。パブリック SSL 証明書の取得とインストールの詳細については、「 証明書のインストールと管理」を参照してください。
- Citrix Endpoint Managementサーバーの負荷分散を構成します。

ウィザードを使用するには、次の手順に従います：

1. NetScaler GUIで、［ 構成 ］タブをクリックし**、**［ **Citrix 製品との統合** ］セクションの［ **XenMobile** ］をクリックします。
2. Citrix Endpoint Managementのバージョンを選択し、［ **始める**］をクリックします。
3. 構成する機能を選択します。このウィザードは 1 回しか使用できないため、後続の設定は手動で実行する必要があります。この手順では、 **NetScaler Gateway経由のアクセス （ENTまたはMAMモードで**実行されているCitrix Endpoint Management 用） およびCitrix EnEndpoint Management **サーバーの負荷**分散の設定を選択することを前提としています。
4. **NetScaler Gateway**構成ページで 、外部側 のNetScaler GatewayのIPアドレス、ポート、 および仮想サーバー名の値を入力します。
5. ［ **NetScaler Gatewayのサーバー証明**書］ページの ［ **証明書ファイル**］で、［ **ローカル** ］または［**アプライアンス**］から証明書ファイルを選択します。
   - ローカル:コンピュータ上の証明書を選択します
   - アプライアンス： NetScaler Gateway（アプライアンス） 上の証明書を選択します。
6. ページの で、 を選択し、証明書プロファイルの名前を入力します。

   次の手順では、証明書ポリシーがすでにあることを前提しています。

   証明書ポリシーを作成する必要がある場合は、 をクリックします。Citrix Endpoint Management 証明書画面で、既存のサーバー証明書を選択するか、新しい証明書をインストールします。複数のCitrix Endpoint Management サーバーを実行している場合は、それぞれに証

© 1997–2026 Citrix Systems, Inc. All rights reserved.

明書を追加します。サーバーログオン名属性には、必要に応じてユーザープリンシパル名またはSAMAccountNameを指定します。

7. 2 **要素**認証を有効にするには 、「2 段階認証」をクリックします。クライアント証明書認証に続いて、2 次認証タイプとして LDAP または RADIUS を指定します。
8. で、二次認証方法を選択します。

   - クライアント証明書をプライマリ認証タイプとして使用すると、LDPA（または RADIUS）をセカンダリ認証タイプとして構成するオプションがあります。

     クライアント証明書認証のみを使用する場合は、 を のままにして、 をクリックします。

     クライアント証明書+ドメイン (LDAP) 認証を使用するには、 を **LDAP** に変更し、認証サーバーの設定を行います。

9. **Citrix Endpoint Managementの［アプリケーション管理］設定を構成します。**

   - **Citrix Endpoint Management FQDNを入力します。**これは MAM の負荷分散 FQDN です。
   - Citrix Endpoint **Managementサーバーの負荷分散を行う仮想サーバーのMAM専用内部負荷分散IPアドレスを入力します。**NetScaler Gateway は、このMAM負荷分散仮想IPを介してCitrix Endpoint Managementと通信します。
   - これはSSLオフロード展開であるため、［**Citrix Endpoint Managementサーバーとの通信**］で［**HTTP**］を選択します。
   - フィールドは自動的に に設定されます。

   展開で分割トンネリングが必要な場合は、 を選択します。分割トンネリングを有効にする場合は、次に、イントラネットアプリケーションバインディングを構成します。

   デフォルトでは、Secure Webアクセスは内部ネットワークにトンネリングされます。つまり、Secure Webはすべてのネットワークアクセスに対してアプリケーションごとのVPNトンネルを使用して内部ネットワークに戻り、NetScaler ADCアプライアンスは分割トンネル設定を使用します。

10. NetScaler Gateway でユーザー接続の傍受ルールを構成するには、 **イントラネットアプリケーションバインドを構成する必要があります。** をクリックして、バインドを追加します。

11. ネットワークアクセスを許可するためのパラメータを入力し、 をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

12. Citrix Endpoint Management 証明書を追加します。これは MAM 負荷分散仮想サーバーに使用されます。



13. ［**Citrix Endpoint Managementサーバー**］で、［**サーバーの追加**］をクリックして、**負荷分散仮想IPにバインドするCitrix Endpoint ManagementのIPアドレスを追加します。**



NetScalerダッシュボードで、NetScaler GatewayとCitrix Endpoint Management 負荷分散が構成されていることを確認します。



ユーザー証明書でユーザープリンシパル名（UPN）の代わりにSamAccount属性を使用する場合は、「クライアント証明書認証用のNetScaler Gateway の手動構成」の説明に従って証明書プロファイルを構成します。

Citrix Endpoint ManagementまたはCitrixXenMobile Serverの負荷分散サーバーを構成する

Citrix Endpoint Management用NetScaler ADCウィザードを初期セットアップに使用した後、このセクションの説明に従って、NetScaler Gateway 構成ユーティリティを使用して負荷分散を構成します。Citrix Endpoint Management の場合は、SSLオフロードを使用します。Citrix Endpoint Managementサーバーについては、NetScaler Gateway およびNetScaler ADCとの統合の「展開の概要」の下にある負荷分散モードの推奨事項を必ず参照してください。

NetScaler ADC VIPでSSLブリッジモードを使用するには

Citrix Endpoint ManagementがDMZにある場合は、SSLブリッジモードを使用します。SSLブリッジモードでCitrix Endpoint ManagementとNetScaler ADC VIPの負荷分散を行うと、インターネットトラフィックはCitrix Endpoint Managementサーバーに直接流れ、そこで接続が終了します。SSLブリッジモードはセットアップとトラブルシューティングが最も簡単なモードです。

1. SSLブリッジモードを構成する前に、**［Citrix Endpoint Managementアプリケーション管理の設定］**に移動し、［**Citrix Endpoint Managementサーバーとの通信**］が［**HTTPS**］であることを確認します。



2. 構成ユーティリティにログオンした後、 タブの で、 をクリックします。
3. の に、サーバーの名前を入力します。
4. に、仮想サーバーのIPアドレスを入力し、 をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. ［**Citrix Endpoint Management MDMサーバーの負荷分散**］ページで、手順3と4を繰り返し、［**作成**］をクリックします。
6. 設定が正しいことを確認し、 をクリックします。



7. 負荷分散の設定を確認するには、 > に移動します。



NetScaler ADC VIPでSSLオフロードモードを使用するには

Citrix Endpoint Management にSSLオフロードを使用します。また、オンプレミスのCitrix Endpoint Managementが内部ネットワークにある場合は、セキュリティ標準を満たすために必要に応じてSSLオフロードを使用します。SSLオフロードモードでCitrix Endpoint ManagementとNetScaler ADC VIPの負荷分散を行うと、インターネットトラフィックはNetScaler ADCアプライアンスに直接流れ、そこで接続が終了します。その後、NetScaler Gateway は、アプライアンスからCitrix Endpoint Managementへの新しいセッションを確立します。SSL オフロードモードは、セットアップとトラブルシューティングの際に、より複雑になります。

1. SSLオフロードモードを構成する前に、 **［Citrix Endpoint Managementアプリケーション管理の設定］** に移動し、［ **Citrix Endpoint Managementサーバーとの通信** ］が［ **HTTP**］であることを確認します。



2. 構成ユーティリティにログオンします。 タブの で、 をクリックします。
3. の に、サーバーの名前を入力します。
4. に、仮想サーバーのIPアドレスを入力し、 をクリックします。
5. ［**Citrix Endpoint Management MDMサーバーの負荷分散**］ページで、手順3と4を繰り返し、［**作成**］をクリックします。
6. 設定を確認し、 をクリックします。
7. サーバー証明書の追加を求めるメッセージが表示されたら、サーバー証明書を選択し、 をクリックします。



8. CA 証明書を指定し、 をクリックします。



9. 同じCitrix Endpoint Management IPアドレスを保持します。 **［完了］** をクリックします。



© 1997–2026 Citrix Systems, Inc. All rights reserved.

10. 負荷分散の設定を確認するには、 > に移動します。



電子メールセキュリティフィルタを使用した Microsoft Exchange の負荷分散サーバーを構成する

1. タブの で、 をクリックします。
2. の に、サーバーの名前を入力します。
3. に、仮想サーバーの IP アドレスを入力します。
4. **［Port］ボックスにポート番号を入力します。さらにポートを追加するには、プラス記号 (+)** をクリックし、ポート番号を入力します。
5. **［続行］** をクリックします。



6. ［ **証明書］**で、既存の証明書を選択するか、コンピューター（**ローカル**）またはNetScaler ADCアプライアンス（**アプライアンス**）にある証明書をインストールします。
7. **［続行］** をクリックします。



8. で、仮想サーバーの名前、IP アドレス、およびポート番号を入力します。次に、 をクリックします。



［ **完了**］をクリックすると、Citrix Endpoint Management NetScaler ADCコネクタ（XNC）ActiveSyncフィルタリングを構成するためのフィールドが表示されます。

Citrix Endpoint Management を構成する NetScaler ADCコネクタ（XNC）ActiveSyncフィルタリング

Citrix Endpoint Management NetScaler ADCコネクタ（XNC）は、ActiveSyncクライアントのデバイスレベルの承認サービスを提供します。NetScaler ADCは、Exchange ActiveSyncプロトコルのリバースプロキシとして機能します。Citrix Endpoint Management内で定義されたポリシーと、XNCによってローカルに定義されたルールの組み合わせにより、承認が制御されます。

1. ［ **Citrix Endpoint Management NetScaler ADCコネクタ（XNC）ActiveSyncフィルタリング**］で、［ **コールアウトプロトコル**］で［ **HTTP** ］または［ **https**］を選択します。
2. に、Citrix Endpoint Management NetScaler ADCコネクタのIPアドレスを入力します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. に、HTTP ネットワークトラフィックの場合は **9080** 、HTTPS ネットワークトラフィックの場合は **9443** と入力し、 をクリックします。

   設定が表示されます。

Citrix 業務用モバイルアプリでモバイルデバイスからのアクセスを許可する

NetScaler ADC for XenMobile ウィザードでは、サポートされているデバイスからNetScaler Gateway を介して内部ネットワークのモバイルアプリおよびリソースにユーザーが接続できるようにするために必要な設定を構成します。ユーザーは、マイクロVPNトンネルを確立するセキュアハブ（以前のCitrix Secure Hub）を使用して接続します。ユーザーが接続すると、VPNトンネルがNetScaler Gateway に開かれ、内部ネットワークのXenMobile に渡されます。ユーザーは、XenMobile MobileからWeb、モバイル、およびSaaSアプリケーションにアクセスできます。

複数のデバイスで同時にNetScaler Gateway に接続するときに、ユーザーが単一のユニバーサルライセンスを使用できるようにするには、仮想サーバーでセッション転送を有効にします。詳細については、 仮想サーバーでの接続タイプの構成を参照してください。

XenMobile 用NetScaler ADCウィザードを使用した後に構成を変更する必要がある場合は、この記事のセクションを参照してガイダンスを参照してください。設定を変更する前に、変更の影響を理解していることを確認してください。詳しくは、 XenMobile の展開に関する記事を参照してください 。

NetScaler Gateway でSecure Browse を構成する

Secure Browseは、グローバル設定の一部として、またはセッションプロファイルの一部として変更できます。セッションポリシーは、ユーザー、グループ、または仮想サーバーにバインドできます。Secure Browse を設定する場合は、クライアントレスアクセスも有効にする必要があります。ただし、クライアントレスアクセスでは、Secure Browse を有効にする必要はありません。クライアントレスアクセスを設定するときは、 を に設定します。

Secure Browse をグローバルに設定するには：

1. 構成ユーティリティの［ **構成** ］タブのナビゲーションペインで、［ **Citrix Gateway** ］を展開し、［ **グローバル設定**］をクリックします。
2. 詳細ペインの で、 をクリックします。
3. ［ **グローバルNetScaler Gateway 設定** ］ダイアログボックスの［セキュリティ］タブで、［ **Secure****Browse**］をクリックし、［**OK］**をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

セッションポリシーおよびプロファイルでSecure Browseを構成するには：

1. 構成ユーティリティの［**構成**］タブのナビゲーションペインで、［**Citrix Gateway**］>［**ポリシー**］を展開し、［**セッション**］をクリックします。
2. 詳細ウィンドウで、次のいずれかの操作を行います：
   - 新しいセッションポリシーを作成する場合は、 をクリックします。
   - 既存のポリシーを変更する場合は、ポリシーを選択して をクリックします。
3. ポリシーで、プロファイルを作成するか、既存のプロファイルを変更します。これを行うには、次のいずれかを実行します：
   - 「**リクエストプロファイル**」の横にある「**新規**」をクリックします。
   - 「**リクエストプロファイル**」の横にある「**変更**」をクリックします。
4. タブで、 の横にある をクリックし、 を選択します。
5. 次のいずれかを行います：
   - 新しいプロファイルを作成する場合は、 をクリックし、ポリシーダイアログボックスで式を設定し、、 の順にクリックします。
   - 既存のプロファイルを変更する場合は、選択後に「**OK**」 を 2 回クリックします。

Secure Browse モードでSecure Webのトラフィックポリシーを構成するには、次の手順を実行します。

次の手順に従って、Secure WebトラフィックをSecure Browse モードでプロキシサーバ経由でルーティングするようにトラフィックポリシーを構成します。

1. 構成ユーティリティの［**構成**］タブで、［**NetScaler Gateway**］>［**ポリシー**］の順に展開し、［**トラフィック**］をクリックします。
2. 右側のペインで、 タブをクリックし、 をクリックします。
3. にプロファイルの名前を入力し、 として を選択し、残りの設定はそのままにします。
4. ［**Create**］ をクリックします。
5. タブをクリックし、 をクリックします。
6. にプロファイルの名前を入力し、 として を選択します。 このトラフィックプロファイルは HTTP と SSL の両方用です。クライアントレス VPN トラフィックは、宛先ポートまたはサービスタイプに関係なく、設計上 HTTP トラフィックです。したがって、トラフィックプロファイルでは、SSL トラフィックと HTTP トラフィックの両方を **HTTP** として指定します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

7. に、 **プロキシサーバーの**IP アドレスを入力します。 に、プロキシサーバーのポート番号を入力します。
8. ［**Create**］ をクリックします。
9. タブをクリックし、 をクリックします。
10. **トラフィックポリシーの名前を入力し** 、 で、ステップ 3 で作成したトラフィックプロファイルを選択します。 **次の式を入力し** 、 をクリックします。

    ```
    REQ.HTTP.HEADER HOST contains ActiveSyncServer || REQ.HTTP.HEADER User-Agent CONTAINS WorxMail || REQ.HTTP.HEADER User-Agent CONTAINS com.zenprise || REQ.HTTP.HEADER User-Agent CONTAINS Citrix Secure Hub || REQ.HTTP.URL CONTAINS AGServices || REQ.HTTP.URL CONTAINS StoreWeb
    ```

    このルールは、ホストヘッダーに基づいてチェックを実行します。プロキシからのアクティブ同期トラフィックをバイパスするには、**`ActiveSyncServer`**を適切なActive Syncサーバ名で置き換えます。
11. タブをクリックし、 をクリックします。 **トラフィックポリシーの名前を入力し** 、 で、ステップ 6 で作成したトラフィックプロファイルを選択します。 **次の式を入力し** 、 をクリックします。

    (REQ.HTTP.HEADER User-Agent CONTAINS Mozilla || REQ.HTTP.HEADER User-Agent CONTAINS com.citrix.browser || REQ.HTTP.HEADER User-Agent CONTAINS WorxWeb) && REQ.TCP.DESTPORT == 80
12. タブをクリックし、 をクリックします。 **トラフィックポリシーの名前を入力し** 、 で、ステップ 6 で作成したトラフィックプロファイルを選択します。 **次の式を入力し** 、 をクリックします。

    (REQ.HTTP.HEADER User-Agent CONTAINS Mozilla || REQ.HTTP.HEADER User-Agent CONTAINS com.citrix.browser || REQ.HTTP.HEADER User-Agent CONTAINS WorxWeb) && REQ.TCP.DESTPORT == 443
13. ［ **NetScaler Gateway**］ **>** ［**仮想サーバー**］に移動し、右側のペインで仮想サーバーを選択して、［ **編集**］をクリックします。
14. 行で、 をクリックします。
15. ** メニューから、 を選択します。
16. ［**続行**］ をクリックします。
17. で、 ****の横にある をクリックします。
18. ステップ 10 で作成したポリシーを選択し、 **OK**をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

19. ［**Bind**］ をクリックします。
20. で、 をクリックします。
21. で、 をクリックします。
22. で、 ** メニューの横にある をクリックしてポリシーリストを表示します。
23. ステップ 11 で作成したポリシーを選択し、［ **OK］**をクリックします。
24. ［**Bind**］ をクリックします。
25. で、 をクリックします。
26. で、 をクリックします。
27. で、 ** メニューの横にある をクリックしてポリシーリストを表示します。
28. ステップ 12 で作成したポリシーを選択し、［ **OK］**をクリックします。
29. ［**Bind**］ をクリックします。
30. ［**閉じる**］ をクリックします。
31. ［**完了**］ をクリックします。

必ずXenMobileコンソールでSecure Web（WorxWeb）アプリを構成してください。［ **構成**］ > ［**アプリ**］の順に選択し、Secure Webアプリを選択して［ **編集**］をクリックし、次の変更を行います。

- ページで、 を ****に変更します。
- **iOS** ページで、 を ****に変更します。
- ページで、 を ****に変更します。

アプリケーションと MDX トークンのタイムアウトを構成する

ユーザーがiOSまたはAndroidデバイスからログオンすると、アプリケーショントークンまたはMDXトークンが発行されます。トークンはSecure Ticket Authority (STA) に似ています。

トークンをアクティブにする秒数または分数を設定できます。トークンの有効期限が切れると、ユーザーはアプリケーションやウェブページなどの要求されたリソースにアクセスできなくなります。

トークンのタイムアウトはグローバル設定です。この設定を構成すると、NetScaler Gateway にログオンするすべてのユーザーに適用されます。

1. 構成ユーティリティの［ **構成** ］タブのナビゲーションペインで、［ **Citrix Gateway** ］を展開し、［ **グローバル設定**］をクリックします。
2. 詳細ペインの で、 をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. ［**グローバルNetScaler Gateway 設定**］ダイアログボックスの［**クライアントエクスペリエンス**］タブで、［**詳細設定**］をクリックします。
4. タブの に、トークンの有効期限が切れるまでの秒数を入力します。デフォルトは **100** 秒です。
5. ［**MDXトークンのタイムアウト (分)**］に、トークンの有効期限が切れるまでの分数を入力し、［**OK］**をクリックします。デフォルトは **10** 分です。

モバイルデバイスのエンドポイント分析を無効にする

エンドポイント分析を設定する場合は、エンドポイント分析スキャンが Android または iOS モバイルデバイスで実行されないようにポリシー式を設定する必要があります。エンドポイント分析スキャンは、モバイルデバイスではサポートされていません。

エンドポイント分析ポリシーを仮想サーバにバインドする場合は、モバイルデバイス用のセカンダリ仮想サーバを作成する必要があります。事前認証ポリシーまたは認証後ポリシーをモバイルデバイス仮想サーバーにバインドしないでください。

事前認証ポリシーでポリシー式を構成する場合は、Android または iOS を除外する User-Agent 文字列を追加します。ユーザーがこれらのデバイスのいずれかからログオンし、デバイスタイプを除外すると、エンドポイント分析は実行されません。

たとえば、次のポリシー式を作成して、User-Agent に Android が含まれているかどうか、アプリケーション virus.exe が存在しないかどうかを確認し、事前認証プロファイルを使用してプロセス keylogger.exe が実行されている場合はプロセスを終了します。ポリシー式は次のようになります。

REQ.HTTP.HEADER User-Agent NOTCONTAINS Android && CLIENT.APPLICATION.PROCESS(keylogger.exe) contains || CLIENT.APPLICATION.PROCESS (virus.exe) contains

事前認証ポリシーとプロファイルを作成したら、ポリシーを仮想サーバにバインドします。ユーザーが Android または iOS デバイスからログオンすると、スキャンは実行されません。ユーザーが Windows ベースのデバイスからログオンすると、スキャンが実行されます。

事前認証ポリシーの設定の詳細については、 エンドポイントポリシーの設定を参照してください 。

Android デバイスの DNS サフィックスを使用して DNS クエリをサポートする

ユーザーがAndroidデバイスからマイクロVPN接続を確立すると、NetScaler Gateway はスプリットDNS設定をユーザーデバイスに送信します。NetScaler Gateway は、構成するスプリットDNS

© 1997–2026 Citrix Systems, Inc. All rights reserved.

設定に基づくスプリットDNSクエリをサポートします。NetScaler Gateway は、アプライアンスに構成したDNSサフィックスに基づくスプリットDNSクエリもサポートできます。ユーザーがAndroidデバイスから接続する場合は、NetScaler Gateway でDNS設定を構成する必要があります。

スプリット DNS は、次のように動作します。

- スプリット DNS を に設定すると、Android デバイスはすべての DNS リクエストをローカル DNS サーバに送信します。
- **スプリットDNSをリモートに設定すると**、すべてのDNS要求は、解決のためにNetScaler Gateway（リモートDNSサーバー）で構成されたDNSサーバーに送信されます。
- スプリット DNS を に設定すると、Android デバイスは DNS リクエストタイプをチェックします。
  - DNS 要求タイプが「A」でない場合、DNS 要求パケットはローカルおよびリモート DNS サーバの両方に送信されます。
  - DNSリクエストタイプが「A」の場合、Androidプラグインはクエリ FQDNを抽出し、そのFQDNをNetScaler ADCアプライアンスに構成されたDNSサフィックスリストと照合します。DNS 要求の FQDN が一致すると、DNS 要求はリモート DNS サーバーに送信されます。FQDN が一致しない場合、DNS 要求はローカル DNS サーバーに送信されます。

次の表は、タイプ A のレコードとサフィックスリストに基づいて動作するスプリット DNS をまとめたものです。

スプリット DNS 設定	タイプAのレコードですか	接尾辞リストに載ってるの？	DNS リクエストの送信先
ローカル	はいまたはいいえの両方	はいまたはいいえの両方	ローカル
リモート	はいまたはいいえの両方	はいまたはいいえの両方	リモート
両方	いいえ	-	両方
両方	はい	はい	リモート
両方	はい	いいえ	ローカル

DNS サフィックスを設定するには、次の手順を実行します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. 構成ユーティリティの［**構成**］タブのナビゲーションペインで、［**Citrix Gateway**］>［**ポリシー**］を展開し、［**セッション**］をクリックします。
2. 詳細ペインの タブで、セッションポリシーを選択し、 をクリックします。
3. 「**リクエストプロファイル**」の横にある「**変更**」をクリックします。
4. タブで、 をクリックします。
5. 「**イントラネット IP DNS サフィックス**」の横にある「**グローバルを上書き**」をクリックし、DNS サフィックスを入力して「**OK**」を 3 回クリックします。

NetScaler Gateway でスプリットDNSをグローバルに構成するには：

1. 構成ユーティリティの［**構成**］タブのナビゲーションペインで、［**Citrix Gateway**］を展開し、［**グローバル設定**］をクリックします。
2. 詳細ペインの で、 をクリックします。
3. 「**クライアントエクスペリエンス**」タブで、「**詳細設定**」をクリックします。
4. ［**全般**］タブの［**スプリット DNS**］で［**両方**］、［**リモート**］、または［**ローカル**］を選択し、［**OK］**をクリックします

NetScaler Gateway のセッションポリシーでスプリットDNSを構成するには：

1. 構成ユーティリティの［**構成**］タブのナビゲーションペインで、［**Citrix Gateway**］>［**ポリシー**］を展開し、［**セッション**］をクリックします。
2. 詳細ペインの タブで、 をクリックします。
3. ** に、ポリシーの名前を入力します。
4. 「**リクエストプロファイル**」の横にある「**新規**」をクリックします。
5. ** に、プロファイルの名前を入力します。
6. 「**クライアントエクスペリエンス**」タブで、「**詳細設定**」をクリックします。
7. ［**全般**］タブで、［**スプリット DNS**］の横にある［**グローバルを上書き**］をクリックし、［**両方**］、［**リモート**］、または［**ローカル**］を選択して［**OK**］
8. ダイアログボックスで、 の横にある 、、、、** の順にクリックします。

Citrix Endpoint Managementのドメインおよびセキュリティトークン認証を構成する

RADIUSプロトコルを使用して、LDAP資格情報とワンタイムパスワードによる認証をユーザーに要求するようにCitrix Endpoint Managementを構成できます。このセクションでは、その2要素認証の種類に必要なNetScaler Gateway 構成について説明します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

前提条件

Citrix Endpoint Management用NetScaler ADCウィザードをまだ実行していない場合は、「Citrix Endpoint Management環境の設定を構成する」の「 *NetScaler for Citrix Endpoint Management ウィザード*」セクションを参照してください。NetScaler ADC構成に次のものが含まれていることを確認します。

- **LDAP ポート番号** = **636** （セキュア LDAP 接続のデフォルトポート）
- **サーバーログオン名属性** = **samAccountName** または **userPrincipalName** （要件に応じて）

ドメインとセキュリティトークンの認証を構成するには

1. **［NetScaler Gateway］>［仮想サーバー］**に移動します。仮想サーバーを選択し、 をクリックします。
2. をクリックします。**
3. **「CA 証明書の選択」で証明書を選択し**、「 **OK」**をクリックし、「 **バインド**」をクリックして、「 **完了**」をクリックします。
4. > > に移動し、プロファイルを選択して をクリックします。
5. タブをクリックします。
6. 「 **認証情報インデックス**」で「 **セカンダリ**」を選択します。
7. **［OK］** をクリックします。
8. > > に移動し、 タブをクリックして、 をクリックします。
9. Citrix Endpoint Management とCitrix Virtual Apps and Desktops に別々のNetScaler Gateway VIPを使用するには、次の式を使用してください。

   REQ.HTTP.HEADER User-Agent CONTAINS `CitrixReceiver`
10. > > に移動し、 タブをクリックします。
11. をクリックし、RADIUS サーバの詳細を入力して、 をクリックします。
12. に移動し、 をクリックします。
13. ポリシーの を入力します。「 **サーバ** 」ドロップダウンメニューから、作成した RADIUS サーバ名を選択します。
14. **「式」に「REQ.HTTP.HEADER ユーザーエージェントにはCitrixReceiver が含まれています」と入力し、「作成」をクリックします。**
15. 仮想サーバーを選択し、 をクリックします。
16. で をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

17. ポリシーを選択し、 をクリックして、 をクリックします。
18. 行で、 をクリックして RADIUS 認証を追加します。
19. の から を選択します。
20. ［**Bind**］ をクリックします。
21. 前に作成した RADIUS 認証ポリシーを選択し、 をクリックします。
22. ［**OK**］ をクリックします。
23. LDAP をセカンダリ認証ポリシーとして追加するには、 行で をクリックします。
24. ****から を選択します。
25. ****から、 を選択します。
26. ****から、LDAP ポリシーを選択します。
27. ポリシーを選択し、［ **OK**］をクリックします。
28. ［**Bind**］ をクリックします。
29. ［**完了**］ をクリックします。
30. 作成したポリシーのプライオリティが最も高いことを確認します。これにより、モバイルユーザー以外のユーザーに対してさらに多くのポリシーが追加された場合でも、そのユーザーの優先度が最高になります。詳細については、 認証ポリシーの優先度の設定を参照してください。

クライアント証明書またはクライアント証明書とドメイン認証を構成する

NetScaler ADC for Citrix Endpoint Managementウィザードを使用して、NetScaler ADC証明書のみの認証または証明書とドメイン認証を使用する場合にCitrix Endpoint Managementに必要な構成を実行できます。Citrix Endpoint Management用NetScaler ADCウィザードは一度だけ実行できます。ウィザードの使用について詳しくは、「 Citrix Endpoint Management環境の設定を構成する」を参照してください。

ウィザードを既に使用している場合は、この記事の手順を使用して、クライアント証明書認証またはクライアント証明書とドメイン認証に必要な追加の構成を行います。

MAM専用モードのデバイスのユーザーがデバイス上の既存の証明書を使用して認証できないようにするには、この記事の後半の「NetScaler ADC証明書失効リスト（CRL）」を参照してください。

GUIを使用してクライアント証明書認証用にNetScaler Gateway を構成する

1. **Traffic Management > Load Balancing > Virtual Servers**に移動します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. **SSL タイプの仮想サーバーを選択し、 セクションで を に設定します。
3. ［**NetScaler Gateway**］>［**仮想サーバー**］に移動します。
4. **SSL**タイプの仮想サーバを選択し、 をクリックします。
5. セクションで、 アイコンをクリックします。
6. を選択し、 で を選択します。
7. 認証証明書ポリシーを作成して、Citrix Endpoint ManagementがSecure HubからNetScaler Gateway **に提供されたクライアント証明書からユーザープリンシパル名またはsAMAccountを抽出できるようにします** 。
8. ［**NetScaler Gateway**］>［**ポリシー**］>［**認証**］>［**証明書**］に移動します。
9. タブをクリックし、 をクリックします。
10. 証明書プロファイルの次のパラメータを設定します。

    Authentication Type：**CERT**

    2 要素: **OFF** (証明書のみの認証)

    ユーザー名フィールド:件名: **CN**

    Group Name Field：**SubjectAltName:PrincipalName**
11. 証明書認証ポリシーのみをNetScaler Gateway **仮想サーバーのプライマリ認証としてバインドします** 。
12. ルートCA証明書をバインドして、NetScaler Gateway に提示されたクライアント証明書の信頼を検証します。

GUIを使用してクライアント証明書とドメイン認証用にNetScaler Gateway を構成する

1. **Traffic Management > Load Balancing > Virtual Servers**に移動します。
2. **SSL タイプの仮想サーバーを選択し、 セクションで を に設定します。
3. **NetScaler Gateway > ポリシー > 認証 > 証明書に移動します**。
4. タブをクリックし、 をクリックします。
5. **プロファイルの名前を入力し** 、 を に設定し、 から を選択します。
6. タブをクリックし、 をクリックします。
7. **ポリシーの名前を入力し** 、 から証明書プロファイルを選択し、 **を設定して をクリックします。
8. に移動し、タイプ **SSL**の仮想サーバーを選択して、 をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

9. の横にある をクリックして、証明書認証を追加します。
10. 認証方法を選択するには、「**ポリシーの選択**」で「**証明**書」を選択し、「**タイプの選択**」で「プライマリ」を選択**し**ます。これにより、証明書認証が LDAP 認証タイプと同じ優先順位のプライマリ認証としてバインドされます。
11. で、 ** をクリックし、以前に作成した証明書ポリシーを選択します。
12. 前に作成した証明書ポリシーを選択し、［**OK］**をクリックします。
13. を **100** に設定し、 をクリックします。以降の手順で LDAP 認証ポリシーを設定する場合は、同じプライオリティ番号を使用します。
14. の行で、 をクリックします。
15. ポリシーを選択し、 ドロップダウンメニューから をクリックします。
16. 証明書ポリシーに指定したのと同じ 値を入力します。 **［Bind］** をクリックします。
17. **［閉じる］** をクリックします。
18. **SSL パラメータ**セクションの編集アイコンをクリックします 。
19. 「**クライアント認証**」チェックボックスを選択し、「**クライアント証明**書」で「**必須**」を選択し、「**OK**」をクリックします。
20. **［完了］** をクリックします。

Citrix ADC証明書失効一覧（CRL）

Citrix Endpoint Managementは、サードパーティの認証局の証明書失効リスト（CRL）のみをサポートしています。Microsoft CAが構成されている場合、Citrix Endpoint ManagementはNetScaler ADCを使用して失効を管理します。クライアント証明書ベースの認証を構成する場合、NetScaler ADC証明書失効一覧（CRL）設定 **［Enable CRL Auto Refresh］** を構成する必要があるかどうか検討します。この手順を使用すると、MAMのみモードのデバイスのユーザーがデバイス上の既存の証明書を使用して認証できなくなります。Citrix Endpoint Managementは、新しい証明書を再発行します。これは、失効したユーザー証明書がユーザー証明書を生成することを制限しないためです。この設定は、CRLが期限切れのPKIエンティティを確認する場合、PKIエンティティのセキュリティを強化します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Microsoft Intune グレーション

Microsoft Intune とNetScaler Gatewayの統合により、NetScaler Gateway およびIntune が提供するクラス最高のアプリケーションアクセスおよびデータ保護ソリューションが提供されます。

電子メール、カレンダー、連絡先、メモ作成、ドキュメント編集、リモートアクセスなど、さまざまなプラットフォーム間で一元管理できる、安全な生産性向上アプリケーションの最も完全なスイートを入手できます。Intune とNetScaler Gatewayの統合は、世界クラスのモバイルデバイス管理（MDM）機能を提供しますが、NetScaler Gateway クライアント側のテクノロジーは、これらのIntune の啓発されたアプリケーションが、NetScaler Gatewayを介して企業のデータとアプリケーションに安全にアクセスできるようにします。

この統合により、NetScaler Gateway はIntune からコンプライアンスデータをプルし、条件付きアクセスポリシーを有効にすることができます。条件付きアクセスポリシーにより、NetScaler Gateway は、デバイスの機能などに基づいてアクセスを制御するためのより細かい制御を提供します。たとえば、管理者は、「カメラ」が無効になっているデバイスのみにアクセス権を付与するポリシーを作成できます。

NetScaler Gateway 仮想サーバーが構成されると、NetScaler Gateway はAzure Active Directory ライブラリ（ADAL）トークン認証をサポートします。構成時に、Citrix Network-Only ラッパーまたはSDKでラップされたモバイルアプリケーションは、アプリがAADから直接フェッチできるADALトークンを使用してNetScaler Gateway にアクセスします。

Citrix マイクロVPNとMicrosoft Endpoint Managerとの統合

NetScaler Gateway のお客様は、Microsoft Endpoint Manager（Intune）でマイクロVPNを使用できます。Citrix Micro VPNとMicrosoft Endpoint Management との統合により、アプリはオンプレミスのリソースにアクセスできます。

Citrix Micro VPNテクノロジーは、VPNトンネルが常にアクティブであるとは限らないため、データ転送コストを削減し、セキュリティを簡素化するオンデマンドVPNを提供します。代わりに、必要なときにのみアクティブになるため、リスクが軽減され、デバイスのパフォーマンスが最適化され、ユーザーエクスペリエンスが向上します。これは、モバイルバッテリーの寿命を向上させるのにも役立ちます。Citrix スのマイクロVPNテクノロジーは、モバイルユーザーに内部ビジネス

© 1997–2026 Citrix Systems, Inc. All rights reserved.

リソースへの安全なアクセスを提供すると同時に、最高のユーザーエクスペリエンスを提供します。

Micro VPN は、次のユースケースでのみサポートされています。

- Intune モバイルアプリケーション管理 (MAM) のみ
- Intune モバイルデバイス管理 (MDM) とモバイルアプリケーション管理 (MAM)

重要：

SSL VPN機能を利用するには、マイクロVPNにはNetScaler Gateway AdvancedまたはPremiumエディション（VPX 3000以上）とCitrix Endpoint Management の使用権限が必要です。Citrix Endpoint Management の資格を取得すると、Microsoft Edge モバイルブラウザ（iOSおよびAndroid）上のマイクロVPN SDKが引き続きサポートされます。詳細については、営業、アカウント、またはパートナーの担当者にお問い合わせください。

Microsoft Endpoint ManagerとのCitrixマイクロVPN統合の設定について詳しくは、「Microsoft Endpoint ManagerでマイクロVPNを使用するためのNetScaler Gateway のセットアップ」を参照してください。

統合 Intune MDM ソリューションを使用する場合

次のシナリオは、統合された Intune MDM ソリューションの使用方法を示しています。

- 新しい顧客が、オンプレミスのNetScaler Gateway 展開でIntune をオンボーディングすることにしました
- 既存のNetScaler Gateway ユーザーがIntune でモバイルデバイス管理を追加したいと考えています
- 既存のIntune ユーザーは、モバイルデバイスまたはアプリケーションが、企業DMZ内のNetScaler Gateway 物理アプライアンスまたは仮想アプライアンスを使用して、企業ネットワーク内にあるデータにアクセスすることを許可したいと考えています。

注

iOS および Android クライアントのみがサポートされています。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler Gateway MDM と Intune の統合を理解する

以下は、Intune との典型的なNetScaler Gateway MDM統合におけるイベントのフローの例です。

1. Intune でモバイルデバイスを登録します。
2. 企業が承認したアプリケーションとデバイスポリシーがデバイスにプッシュされます。
3. デバイスから SharePoint (オンプレミスアプリケーション) を参照します。
4. ブラウザ要求はNetScaler Gateway に送信されます。
5. NetScaler Gateway アプライアンスは、デバイスの登録ステータスをIntune で確認します。
6. 準拠しているデバイスが正常に登録されると、SharePoint アクセスが許可されます。



デバイスが条件付きアクセスポリシーを満たしていない場合、NetScaler Gateway VPNクライアントはエラーメッセージを表示します。このメッセージは、デバイスから Intune がホストするページへのリンクを提供し、デバイスのコンプライアンス状態を登録または修復するオプションをユーザーに提供します。

注:

管理者は、ユーザーがデバイス上のさまざまな証明書を区別できるように、証明書を Intune にプッシュするときに次のことを確認する必要があります。

- 証明書にはサブジェクトの概要が必要です。
- 異なる証明書のサブジェクトサマリーは区別する必要があります。

単一要素ログイン用のNetScaler Gateway 仮想サーバーのネットワークアクセス制御デバイスチェックを構成する

このトピックでは、Microsoft Intune eが提供するネットワークアクセスコンプライアンス（NAC）セキュリティを使用して、モバイルデバイス（iOSおよびAndroid）から内部ネットワークに接続するようにNetScaler Gateway を構成する方法について説明します。ユーザーがiOSまたはAndroid VPNクライアントからNetScaler Gateway に接続しようとすると、ゲートウェイはまずデバイスが管理対象デバイスであり、準拠しているデバイスであるかどうかをIntune サービスで確認します。

- 管理対象:デバイスは Intune 企業ポータルクライアントを使用して登録されます。
- 準拠:Intune MDM サーバーからプッシュされた必須ポリシーが適用されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

デバイスが管理対象で準拠している場合にのみ、VPN セッションが確立され、ユーザに内部リソースへのアクセスが提供されます。

注：

- このセットアップでは、バックエンドのNetScaler Gateway がIntune サービスと通信します。SSLプロファイルは、NetScaler Gateway への着信接続を処理します。NetScaler Gateway バックエンド通信は、バックエンドクラウドサービス（Intune）のSNI要件をすべて処理します。
- DTLSゲートウェイ仮想サーバー用のSNIは、NetScaler Gateway リリース13.0ビルド64.x以降でサポートされています。
- Intune NAC チェックは、アプリごとの VPN またはデバイス全体の VPN でも、VPN プロファイルが Intune 管理ポータル（現在は Microsoft エンドポイントマネージャと呼ばれる）によってプロビジョニングされている場合にのみサポートされます。これらの機能は、エンドユーザが追加した VPN プロファイルではサポートされません。NAC チェックを使用するには、エンドユーザーデバイスの Intune 管理者によって Microsoft Endpoint Manager からデバイスに VPN プロファイルが展開されている必要があります。

ライセンス

この機能を使用するには、Citrix エンタープライズエディションのライセンスが必要です。

システム要件

- NetScaler Gateway リリース11.1ビルド51.21以降
- iOS VPN — 10.6 以降
- Android VPN — 2.0.13 以降
- Microsoft
  - Azure AD アクセス (テナント権限と管理者権限を持つ)
  - Intune が有効なテナント
- ファイアウォール サブネット IP アドレスから `https://login.microsoftonline.com` および `https://graph.windows.net` (ポート 53 およびポート 443) へのすべての DNS および SSLトラフィックに対するファイアウォールルールを有効にします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

前提条件

- 既存の認証ポリシーはすべて、クラシックポリシーから高度なポリシーに変換する必要があります。クラシックポリシーから高度なポリシーに変換する方法については、`<https://support.citrix.com/article/CTX131024>`を参照してください。
- Azure Portalで NetScaler Gateway アプリケーションを作成します。詳しくは、「Azure Portalでの NetScaler Gateway アプリケーションの構成」を参照してください。
- 次のアプリケーション固有の情報を使用して、作成したNetScaler Gateway アプリケーションでOAuthポリシーを構成します。
  - クライアント ID/アプリケーション ID
  - クライアントシークレット/アプリケーションキー
  - Azure テナント ID

参照ドキュメント

- このドキュメントでは、NetScaler Gateway のセットアップ構成について説明します。Citrix SSOクライアント（iOS/Android）の構成のほとんどはIntune 側で行われる。NAC 用の Intune VPN 設定の詳細については、`<https://docs.microsoft.com/en-us/mem/intune/protect/network-access-control-integrate>`を参照してください。
- iOS アプリの VPN プロファイルを設定するには、「`<https://docs.microsoft.com/en-us/mem/intune/configuration/vpn-settings-ios>`」を参照してください。
- Azure Portalで NetScaler Gateway アプリケーションをセットアップするには、「Azure Portalでの NetScaler Gateway アプリケーションの構成」を参照してください。

ゲートウェイ展開用に nFactor を搭載した NetScaler Gateway 仮想サーバーを追加するには

1. ［**NetScaler Gateway**］>［**仮想サーバー**］に移動します。

2. **［追加］** をクリックします。
3. 「**基本設定**」領域に必要な情報を入力し、 **「OK」**をクリックします。

4. を選択します。

5. 必要なサーバー証明書を選択し、 をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



6. ［**続行**］ をクリックします。
7. ［**続行**］ をクリックします。
8. ［**続行**］ をクリックします。
9. **の横にあるプラスアイコンをクリックし、 リストから を選択し、 リストから を選択して をクリックします。**
10. の横にあるプラスアイコン ****をクリックします。
11. ［**NetScaler Gateway セッションポリシーの作成** ］ページで、セッションポリシーの名前を入力します。
12. ［ **プロファイル** ］の横にあるプラスアイコン をクリックし、［ **NetScaler Gateway セッションプロファイルの作成** ］ページでセッションプロファイルの名前を入力します。
13. タブで、 の横にあるチェックボックスをクリックし、リストから を選択します。
14. の横にあるチェックボックスをクリックし、リストから を選択します。
15. をクリックし、 の横にあるチェックボックスをオンにし、その値を に設定します。
16. タブで、 の横にあるチェックボックスをクリックし、リストから を選択します。
17. タブで、 の横にあるチェックボックスをクリックし、一覧から を選択します。
18. **「 作成」をクリックします。**
19. ［**NetScaler Gateway セッションポリシーの作成** ］ページの［ **式** ］領域で、修飾式を構成します。
20. ［**Create**］ をクリックします。
21. ［**Bind**］ をクリックします。
22. で を選択します。



23. プラスアイコン をクリックし、認証プロファイルの名前を入力します。



24. プラスアイコン をクリックして、認証仮想サーバを作成します。



25. ［ **基本設定** ］領域で認証仮想サーバーの名前とIPアドレスの種類を指定し、［ **OK］ **をクリックします。IP アドレスタイプは、 **アドレス指定不可にもできます** 。



26. をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

27. ビューで、プラスアイコン をクリックして認証ポリシーを作成します。

28. として を選択し、プラスアイコン をクリックして NAC の OAuth アクションを作成します。

29. **クライアント ID**、**クライアントシークレット**、および**テナント ID**を使用して OAuth アクションを作成します。

    注：

    - **クライアントID**、 **クライアントシークレット**、および**テナントIDは** 、Azure Portalで NetScaler Gateway アプリケーションを構成した後に生成されます。
    - クライアントID/アプリケーションID、クライアントシークレット/アプリケーションシークレット、およびAzureテナントIDの情報は、後でNetScaler Gateway でOAuthアクションを作成する際に必要になるため、書き留めておきます。

    アプライアンスに適切な DNS ネームサーバが設定されていて、解決して到達できることを確認します。

    - `https://login.microsoftonline.com/,`
    - `https://graph.windows.net/`, \- *.manage.microsoft.com。

30. **OAuth アクションの認証ポリシーを作成します。**

    規則:

    ```
    http.req.header("User-Agent").contains("NAC/1.0")&&
    ((http.req.header("User-Agent").contains("iOS") &&
    http.req.header("User-Agent").contains("NSGiOSplugin")) ||
    (http.req.header("User-Agent").contains("Android") &&
    http.req.header("User-Agent").contains("CitrixVPN")))
    ```

31. プラスアイコン をクリックして NextFactor ポリシーラベルを作成します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

32. プラスアイコン をクリックして、ログインスキーマを作成します。

    ☐

33. 認証スキーマとして**`noschema`**を選択し、 をクリックします。

    ☐

34. 作成したログインスキーマを選択したら、 をクリックします。

    ☐

    をクリックします](/ja-jp/netscaler-gateway/media/intune_18.jpg)

35. ** で、ユーザログイン用の既存の認証ポリシーを選択するか、プラスアイコン をクリックして認証ポリシーを作成します。 認証ポリシーの作成について詳しくは、 [高度な認証ポリシーの構成およびLDAP認証の設定を参照してください](/en-us/citrix-adc/13/aaa-tm/authentication-methods/citrix-adc-aaa-advanced-authentication-policy.html)。

    ☐

36. **［Bind］** をクリックします。

    ☐

    をクリックします](/ja-jp/netscaler-gateway/media/intune_21.jpg)

37. **［完了］** をクリックします。

    ☐

38. **［Bind］** をクリックします。

    ☐

    をクリックします](/ja-jp/netscaler-gateway/media/intune_23.jpg)

39. **［続行］** をクリックします。

    ☐

40. **［完了］** をクリックします。

    ☐

41. **［Create］** をクリックします。

    ☐

42. **［OK］** をクリックします。

    ☐

43. **［完了］** をクリックします。

    ☐

© 1997–2026 Citrix Systems, Inc. All rights reserved.

認証ログインスキーマを認証仮想サーバーにバインドして、VPN プラグインが /cgi/login 要求の一部としてデバイス ID を送信するように指示するには

1. > > に移動します。

2. 以前に選択した仮想サーバを選択し、 をクリックします。

3. の をクリックします。

4. をクリックしてバインドします。

5. をクリックして、NAC デバイスチェック用の既存のビルドインログインスキーマポリシーを選択してバインドします。

6. 認証展開に適した必要なログインスキーマポリシーを選択し、 をクリックします。

   前に説明した展開では、NAC OAuth アクションポリシーとともに単一要素認証（LDAP）が使用されるため、 **lschema_single_factor_deviceid** が選択されています。

7. ［**Bind**］ をクリックします。

   をクリックします](/ja-jp/netscaler-gateway/media/a_intune_7.jpg)

8. ［**完了**］ をクリックします。

トラブルシューティング

一般的な問題

問題	解像度
アプリを開くと、「ポリシーの追加が必要です」というメッセージが表示されます。	Microsoft Graph API でポリシーを追加する

© 1997–2026 Citrix Systems, Inc. All rights reserved.

問題	解像度
ポリシーの競合がある	アプリごとに許可されるポリシーは 1 つだけです。
アプリが内部リソースに接続できない	正しいファイアウォールポートが開いていること、テナント ID が正しいことなどを確認します。

NetScaler Gatewayの問題

問題	解像度
NetScaler Gatewayは `login.microsoftonline.comandgraph.windows.net` に到達できません。	NS Shell から、次のMicrosoft Web サイトにアクセスできるかどうかを確認します。cURL-v-k `<https://login.microsoftonline.com>` 。次に、NetScaler Gateway でDNSが構成されているかどうかを確認します。また、ファイアウォールの設定が正しいことを確認します(DNS 要求がファイアウォールされている場合)。
OAuthActionを設定すると、ns.logにエラーが記録される。	Intuneのライセンスが有効であること、およびAzureのゲートウェイアプリに適切な権限のセットが設定されているかを確認します。
Sh OAuthActionコマンドでOAuthのステータスが完了と表示されない。	DNS設定とAzureのゲートウェイアプリに設定されている権限を確認します。
AndroidまたはiOSデバイスで2要素認証のプロンプトが表示されない。	2要素デバイスIDログオンスキーマが認証仮想サーバーにバインドされているかを確認します。

NetScaler Gateway OAuthのステータスとエラー状態

ステータス	エラー状態
AADFORGRAPH	シークレットが無効、URLが未解決、接続タイムアウト

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ステータス	エラー状態
MDMINFO	`*manage.microsoft.com`はダウンまたは到達不能です
GRAPH	グラフエンドポイントがダウンしており到達不能
CERTFETCH	DNSエラーのため「トークンエンドポイント：`<https://login.microsoftonline.com>`」と通信できない。この構成を検証するには、シェルプロンプトに移動し、cURL `<https://login.microsoftonline.com>`と入力します。このコマンドは検証が必要です。

注: OAuth ステータスが成功すると、ステータスは「完了」と表示されます。

Intune 構成チェック

［**Citrix SSOの基本iOS VPN構成**］>［**ネットワークアクセス制御（NAC）を有効にする**］で、［**同意する**］チェックボックスをオンにします。そうでない場合、NAC チェックは機能しません。

Azure Portalでの NetScaler Gateway アプリケーションの構成

次のセクションでは、Azure PortalでNetScaler Gateway アプリケーションを構成する手順を示します。

前提条件

- Azure グローバル管理者の認証情報
- Intune ライセンスが有効になっている
- Intune 統合の場合は、Azure Portalで NetScaler Gateway アプリケーションを作成する必要があります。
- NetScaler Gateway アプリケーションが作成されたら、次のアプリケーション固有の情報を使用して、NetScaler Gateway でOAuthポリシーを構成します。
    - クライアント ID/アプリケーション ID

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- クライアントシークレット/アプリケーションキー
- Azure テナント ID

- NetScaler Gateway は、アプリクライアントIDとクライアントシークレットを使用してAzureと通信し、NACコンプライアンスをチェックします。

Azure で NetScaler Gateway アプリを作成するには

1. portal.azure.com にログインします
2. をクリックします。
3. をクリックし、 をクリックします。



4. ページで、アプリケーション名を入力し** 、 をクリックします。



5. ［**認証**］に移動し、［**URIの追加**］をクリックし、NetScaler Gateway のFDQNを入力して、［**保存**］をクリックします。



6. ページに移動して、クライアント ID、テナント ID、およびオブジェクト ID を取得します。



7. に移動し、 をクリックします。



注:

`https://login.microsoftonline.com`、`https://graph.microsoft.com`、または`https://graph.windows.com`サービスエンドポイントを呼び出すすべての Azure AD アプリケーションでは、ゲートウェイが NAC API を呼び出すには、API 権限を割り当てる必要があります。利用可能な API 権限は次のとおりです。

- Application.Read.All
- Application.ReadWrite.All
- application.ownedBy
- Directory.Read.All

優先されるパーミッションは **Application.Read.All**です。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

詳細については、以下を参照してください。`<https://techcommunity.microsoft.com/t5/intune-customer-success/support-tip-intune-service-discovery-api-endpoint-will-require/ba-p/2428040>`

8. タイルをクリックして、Microsoft Graph の API 権限を設定します。



9. タイルをクリックします。



10. 次の権限を選択し、 をクリックします。

    - メール
    - `openid`
    - Profile
    - Directory.AccessAsUser.All
    - User.Read
    - User.Read.All
    - User.ReadBasic.All



INTUNE NAC チェックのアクセス許可:

`https://login.microsoftonline.com`、`https://graph.microsoft.com`、`https://graph.windows.com` またはサービスエンドポイントを呼び出すすべての Azure AD アプリケーションでは、ゲートウェイが NAC API を呼び出せるように API 権限を割り当てる必要があります。利用可能な API 権限は次のとおりです。

- Application.Read.All
- Application.ReadWrite.All
- application.ownedBy
- Directory.Read.All

優先されるパーミッションは **Application.Read.All**です。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

詳細については、 `<https://techcommunity.microsoft.com/t5/intune-customer-success/support-tip-intune-service-discovery-api-endpoint-will-require/ba-p/2428040>`

注:

お客様が NAC チェックに Intune アクションのみを使用している場合、必要な権限は Microsoft Graph の **Application.Read.All** だけです。

11. **Intune** タイルをクリックして、Intune の API パーミッションを設定します。



12. タイルと タイルをクリックして、それぞれ Get_Device_Compliance と Get_Data_Warehouse のアクセス許可を追加します。



13. 次の権限を選択し、 をクリックします。

    - get_device_Compliance-アプリケーションのアクセス許可
    - Get_Data_Warehouse-委任されたアクセス許可

    注:

    Intune NAC チェックでは、必要な権限は **get_device_Compliance**だけです。



14. 次のページには、設定された API 権限が一覧表示されます。



15. に移動し、 をクリックします。



16. ページで、説明を入力し、 を選択して、 をクリックします。



17. 次の画面は、設定されたクライアントシークレットを示しています。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

（注

）クライアントシークレットは、生成時に一度だけ表示されます。表示されたクライアントシークレットをローカルにコピーします。Intune 用のNetScaler Gateway アプライアンスでOAuthアクションを構成するときに、新しく登録されたアプリに関連付けられたクライアントIDと同じクライアントシークレットを使用します。



Azure Portalのアプリケーション構成はこれで完了です。

Azure ADAL トークン認証について

以下は、一般的なNetScaler Gateway-Microsoft ADALトークン認証のイベントのフローです。

1. iOS または Android でアプリを起動すると、アプリは Azure に接続します。ユーザーは、ユーザーの資格情報を使用してログオンするように求められます。ログオンに成功すると、アプリは ADAL トークンを取得します。

2. このADALトークンは、ADALトークンを検証するように構成されたNetScaler Gatewayに提示されます。

3. NetScaler Gateway は、ADALトークンの署名をMicrosoftの対応する証明書で検証します。

4. 検証が成功すると、NetScaler Gateway はユーザーのプリンシパル名（UPN）を抽出し、アプリケーションVPNに内部リソースへのアクセスを許可します。

Microsoft ADALトークン認証用のNetScaler Gateway 仮想サーバーの構成

Microsoft ADALトークン認証を監視するようにNetScaler Gateway 仮想サーバーを構成するには、次の情報が必要です：

- **certEndpoint**: ADAL トークン検証用の JSON ウェブキー (JWK) を含むエンドポイントの URL。
- **対象ユーザー**：アプリがADALトークンを送信するCitrix ADC仮想サーバーのFQDN。
- **発行者**:AAD 発行者の名前。既定で値が設定されます。
- **tenantID**: Azure ADAL 登録のテナント ID。
- **クライアントID**: ADAL 登録の一部としてゲートウェイアプリに付与される一意の ID。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **クライアントシークレット**:ADAL 登録の一部としてゲートウェイアプリに与えられるシークレットキー。
- **resourceURI**: リソース URI をキャプチャするためのオプションのパラメータです。構成されていない場合、NetScaler ADCはAzure商用リソースURIを使用します。

コマンドラインインターフェイスを使用して、次の手順を実行します。

1. OAuth アクションを作成します。

```
add authentication OAuthAction <oauth-action-name> -OAuthType <INTUNE>
–clientid <clientID> -clientsecret <client-secret> -audience <audience
name> -tenantid <tenantID> -issuer <issuer-name> -userNameField <upn>
-certEndpoint <certEndpoint-name> -resourceURI <name of resource URI>
```

2. 新しく作成した OAuth アクションに関連付ける認証ポリシーを作成します。

```
add authentication Policy <policy-name> -rule <true> -action <oauth
intune action>
```

3. 新しく作成した OAuth を AuthVs にバインドします。

```
bind authentication vserver <auth-vserver> -policy <oauth-intune-
policy> -priority 2 -gotoPriorityExpression END
```

4. ログインスキーマを作成します。

```
add authentication loginSchema <loginSchemaName> -authenticationSchema
<authenticationSchema”location”>

add authentication loginSchemaPolicy <loginSchemaPolicyName> -rule true
-action <loginSchemaName>
```

5. AuthVs をログインスキーマでバインドします。

```
bind authentication vserver <auth-vs> -policy <oauth-pol> -priority 2
-gotoPriorityExpression END
```

6. 認証プロファイルを追加し、VPN 仮想サーバに割り当てます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
add authnprofile <nfactor-profile-name> -authnvsName <authvserver>

set vpn vserver <vserver-name> -authnprofile <nfactor-profile-name>
```

設定例

```
add authentication OAuthAction tmp-action -OAuthType INTUNE -clientid id
1204 -clientsecret a -audience "[http://hello](http://hello/)" -tenantid
xxxx -issuer "[https://hello](https://hello/)" -userNameField upn
-certEndpoint https://login.microsoftonline.com/common/discovery/v2.0/keys
--resourceURI htpps://api.manage.microsoft.com



add authentication Policy oauth-intune-pol -rule true -action tmp-action

bind authentication vserver auth-vs-for-gw1-intune -policy oauth-pol
-priority 2 -gotoPriorityExpression END



add authentication loginSchema oauth-loginschema -authenticationSchema "/
nsconfig/loginschema/LoginSchema/OnlyOAuthToken.xml"



add authentication loginSchemaPolicy oauth-loginschema-pol -rule true
-action oauth-loginschema`



bind authentication vserver auth-vs-for-gw1-intune -policy oauth-
loginschema-pol -priority 2 -gotoPriorityExpression END



add authnprofile nfactor-prof-intune -authnvsName auth-vs-for-gw1-intune



set vpn vserver gw1-intune-authnprofile nfactor-prof-intune
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Microsoft Endpoint ManagerでマイクロVPNを使用するようにNetScaler Gateway をセットアップする

Citrix Micro VPNとMicrosoft Endpoint Management との統合により、アプリはオンプレミスのリソースにアクセスできます。詳しくは、 Citrix マイクロVPNとMicrosoft Endpoint Managerの統合を参照してください。

システム要件

- NetScaler Gateway バージョン
  - 13.0
  - 12.1.50.x またはそれ以降
  - 12.0.59.x またはそれ以降

  NetScaler Gatewayの最新バージョンは、NetScaler Gatewayダウンロードページからダウンロードすることもできます。
- Windows 7以降を実行しているWindowsデスクトップ（Androidアプリのラッピングにのみ対応）
- Microsoft
  - Azure ADアクセス（テナントの管理者特権あり）
  - Intune対応のテナント
- ファイアウォール規則
  - NetScaler Gateway サブネットIPから`*.manage.microsoft.com`、`https://login.microsoftonline.com`および`https://graph.windows.net`（ポート443）へのSSLトラフィックに対するファイアウォールルールを有効にする
  - NetScaler Gateway は、前述のURLを外部で解決できる必要があります。

前提条件

- **Intune 環境:** Intune 環境がない場合は、セットアップします。手順については、 Microsoft のドキュメントを参照してください。
- **エッジブラウザーアプリ:** マイクロ VPN SDK は、iOS および Android 用の Microsoft Edge アプリと Intune Managed Browser アプリに統合されています。Managed Browserについて詳しくは、MicrosoftのManaged Browserのページを参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Citrix Endpoint Management 資格**：Microsoft Edge モバイルブラウザ（iOSおよびAndroid）でマイクロVPN SDKを引き続きサポートするには、アクティブなCitrix Endpoint Management資格が必要です。詳細については、営業、アカウント、またはパートナーの担当者にお問い合わせください。

Azure Active Directory (AAD) アプリケーションのアクセス許可を付与する

1. NetScaler Gateway がAADドメインで認証することを許可することを、Citrixマルチテナント AADアプリケーションに同意します。Azure グローバル管理者は、次の URL にアクセスして同意する必要があります。

   `<https://login.windows.net/common/adminconsent?client_id=b6a53a76-5d50-499e-beb3-c8dbdad5c40b&redirect_uri=https://www.citrix.com&state=consent>`。

2. Citrix マルチテナント AAD アプリケーションに同意して、モバイルアプリケーションが NetScaler Gateway Micro VPNで認証できるようにします。このリンクは、Azure グローバル管理者が の既定値を から に変更した場合にのみ必要です。 この設定は、Azure Portalの > > **の下にあります。 Azure グローバル管理者は、次の URL にアクセスして同意 (テナント ID を追加) する必要があります。 `<https://login.microsoftonline.com/[tenant_id]/adminconsent?client_id=9215b80e-186b-43a1-8aed-9902264a5af7>`

NetScaler Gateway をマイクロVPN用に構成する

IntuneでマイクロVPNを使用するには、NetScaler GatewayでAzure Active Directoryが認証されるように設定する必要があります。このユースケースでは、既存のNetScaler Gateway仮想サーバーは利用できません。 まず、Azure ADがオンプレミスのActive Directoryと同期するように設定します。この手順は、IntuneとNetScaler Gatewayとの間の認証を適切に行うために必要です。

スクリプトのダウンロード:.zip ファイルには、スクリプトの実装手順を含む readme が含まれています。スクリプトに必要な情報を手動で入力し、NetScaler Gateway でスクリプトを実行してサービスを構成する必要があります。スクリプトファイルは、 ［Citrix Downloads］ページからダウンロードできます。

重要：

NetScaler Gateway の構成が完了し、OAuthステータスがCOMPLETE以外に表示される場合は、「トラブルシューティング」セクションを参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Microsoft Edge Browserの設定

1. `<https://endpoint.microsoft.com/>`にサインインし、 **［Intune］ > ［モバイルアプリ］** の順に移動します。
2. 通常どおり Edge アプリを公開し、アプリ構成ポリシーを追加します。
3. **［管理］** の **［アプリ構成ポリシー］** をクリックします。
4. **［追加］** をクリックし、作成するポリシーの名前を入力します。 で、 を選択します。
5. をクリックします。**
6. ポリシーを適用するアプリ（Microsoft Edge または Intune 管理対象ブラウザ）を選択し、［ **OK］**をクリックします。
7. **［構成設定］** をクリックします。
8. フィールドに、次の表に示すいずれかのポリシーの名前を入力します。
9. **［値］** フィールドに、対象のポリシーに適用する値を入力します。フィールドの外をクリックすると、ポリシーがリストに追加されます。ポリシーは複数追加できます。
10. **［OK］** をクリックしてから **［追加］** をクリックします。

ポリシーのリストにポリシーが追加されます。

名前（IOSまたはANDROID）	VALUE	説明
MvpnGatewayAddress	`https://external.companyname.com`	NetScaler Gateway の外部 URL
MvpnNetworkAccess	mvpnNetworkAccessTunneledWebSSOor Unrestricted	mvpnNetworkAccessTunneledWebSSOがトンネリングのデフォルトです
MvpnExcludeDomains	除外するドメイン名のカンマ区切りリスト	オプションです。既定値は [空白] です

注:

Web SSO は設定でSecure Browse の名前です。動作は同じです。

- **mvpnNetworkAccess** -mvpnNetworkAccessTunneledWebSSOを使用すると、NetScaler Gateway（トンネルウェブSSOとも呼ばれる）を介したHTTP/HTTPSリダイレクトが可能になります。ゲートウェイは HTTP 認証チャレンジにインラインで応答し、シングルサインオン (SSO) エクスペリエンスを提供します。ウェブ SSO を使用するには、このポリシーを **mvpnNetworkAccessTunneledWebSSO**に設定します。フルトンネルリダイレクションは現

© 1997–2026 Citrix Systems, Inc. All rights reserved.

在サポートされていません。マイクロ VPN トンネリングをオフのままにするには、 を使用します。

- **mvpnExcludeDomains** -NetScaler Gateway リバースWebプロキシ経由のルーティングから除外されるホスト名またはドメイン名のカンマ区切りのリスト。NetScaler Gateway 構成のスプリットDNS設定でドメインまたはホストが選択される場合がありますが、ホストまたはドメイン名は除外されます。

  注：

  - このポリシーは、 **MVPN ネットワークアクセスのトンネリング WebSSO 接続にのみ適用されます** 。 `MvpnNetworkAccess` が **Unrestricted**の場合、このポリシーは無視されます。
  - このポリシーは、NetScaler Gatewayがリバース分割トンネリング用に設定されているトンネルWeb SSOモードにのみ適用されます。

トラブルシューティング

一般的な問題

問題	解像度
アプリを開くと、「ポリシーの追加が必要です」というメッセージが表示されます。	Microsoft Graph API でポリシーを追加する
ポリシーの競合がある	アプリごとに許可されるポリシーは 1 つだけです。
アプリをラップすると、「アプリのパッケージ化に失敗しました」というメッセージが表示されます。完全なメッセージについては、次の表を参照してください。	アプリは Intune SDK と統合されています。Intune でアプリをラップする必要はありません
アプリが内部リソースに接続できない	正しいファイアウォールポートが開いていること、テナント ID が正しいことなどを確認します。

アプリのパッケージ化に失敗しました。エラーメッセージ:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

アプリのパッケージ化に失敗しました。
com.microsoft.intune.mam.appPackager.utils.appPackageException: このアプリにはすでに MAM SDK が統合されています。
com.microsoft.intune.mam.appPackager.appPackager.appPackagerApp (appPackager.java: 113)
com.microsoft.intune.mam.appPackager.Packager.PackagerMain.mainInternal (packagerMain.java: 198) com.microsoft.intune.mam.appPackager.Packager.PackagerMAIN.main (packagerMain.MAIN .java:56) アプリケーションはラッピングできません。

NetScaler Gatewayの問題

問題	解像度
NetScaler Gatewayは `login.microsoftonline.comandgraph.windows.net` に到達できません。	NS Shell から、次のMicrosoft Web サイトにアクセスできるかどうかを確認します。cURL-v-k `<https://login.microsoftonline.com>` 。次に、NetScaler Gateway でDNSが構成されているかどうかを確認します。また、ファイアウォールの設定が正しいことを確認します (DNS 要求がファイアウォールされている場合)。
OAuthActionを設定すると、ns.logにエラーが記録される。	Intuneのライセンスが有効であること、およびAzureのゲートウェイアプリに適切な権限のセットが設定されているかを確認します。
Sh OAuthActionコマンドでOAuthのステータスが完了と表示されない。	DNS設定とAzureのゲートウェイアプリに設定されている権限を確認します。
AndroidまたはiOSデバイスで2要素認証のプロンプトが表示されない。	2要素デバイスIDログオンスキーマが認証仮想サーバーにバインドされているかを確認します。

NetScaler Gateway OAuthのステータスとエラー状態

ステータス	エラー状態
AADFORGRAPH	シークレットが無効、URLが未解決、接続タイムアウト

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ステータス	エラー状態
MDMINFO	`*manage.microsoft.com`はダウンまたは到達不能です
GRAPH	グラフエンドポイントがダウンしており到達不能
CERTFETCH	DNSエラーのため「トークンエンドポイント：`<https://login.microsoftonline.com>`」と通信できない。この設定を検証するには、shell に移動して cURL `<https://login.microsoftonline.com>`と入力します。このコマンドは検証が必要です。

注: OAuth ステータスが成功すると、ステータスは「完了」と表示されます。

Azure AD グラフの拡張サポート

Azure AD Graph は廃止されたため、新しいアプリケーションをトリガーする顧客は、Azure AD Graph で使用可能だった以前の権限を使用できません。ただし、既存のアプリケーションを使用していて、Azure AD Graph の古い権限をしばらく使用したいお客様は、ゲートウェイアプライアンスでいくつかの構成変更を行うことで引き続き使用できます。この構成は、NetScaler Gateway リリース13.1-27.xx以降でサポートされています。

NetScaler Gateway アプライアンスで次の構成変更を行います。

1. コマンドプロンプトで、次のコマンドを実行します。

   ```
   shell nsapimgr_wr.sh -ys call=”ns_intune_enable_old_endpoints”
   ```

2. **セキュリティ > AAA アプリケーショントラフィック > ポリシー > 認証 > 詳細ポリシー > アクション > OAUTH アクションに移動します。**

   a. 既存の OAuth サーバーを選択します。

   b. **［詳細］** クリックします。

   c. **グラフエンドポイントで**、URL が図に表示されているものと同じであることを確認します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HDX Enlightened Data Transport サポート

NetScaler Gateway のEnlightened Data Transport（EDT）サポートにより、Citrix WorkCitrix Workspace アプリを実行しているユーザーに、仮想デスクトップの高精細なセッション内ユーザーエクスペリエンスが保証されます。

また、Citrix Workspace アプリとVDA間のEDT終了のためのDTLS 1.0によるエンドツーエンドの暗号化も容易になります。詳細については、 DTLS プロトコルのサポートを参照してください。

EDT対応のNetScaler Gateway は、LANとWANの両方の状態で優れたユーザーエクスペリエンスを提供します。EDT を使用すると、一方から他方へのローミング時に管理設定やユーザー設定は必要ありません。この利点は、パケット損失が中程度の高遅延ネットワークで最も顕著であり、ユーザーエクスペリエンスは通常、代替案と遅れます。

Enlightened Data Transport サポートを使用する場合

次のシナリオは、EDTが有効なNetScaler Gateway の使用を示しています。

- ユーザーは、ビジネスリソースにリモートアクセスしながら、LAN 環境と同じくらい優れたエクスペリエンスを望んでいます。
- ユーザーは、輻輳、高いパケット損失、および高遅延のためにネットワークの品質が低下するWi-Fi およびセルラーネットワーク上で、リッチな仮想アプリケーションおよびデスクトップユーザーエクスペリエンスを望んでいます。

EDTを使用する際は、以下の点に留意すべきである。

- 仮想サーバレベルの DTLS ノブは、デフォルトで有効になっています。
- DTLS を使用した IPv6 はサポートされていません。
- アプライアンスは、ReceiverとVDA間のEDTトラフィックのダブルホップ機能用に構成できるようになりました。詳細については、[ダブルホップ DMZ での展開] をクリックしてください。

注: EDT は、リリース 12.1 ビルド 49.xx 以降の MPX FIPS プラットフォームでサポートされています。Intel Coleto SSL チップベースの MPX デバイスでは、リリース 12.1 ビルド 51.16 以降から EDT がサポートされています。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

EDTおよびHDX InsightをサポートするようにNetScaler Gatewayを構成

ゲートウェイを通過する EDT トラフィックは、エンドツーエンドの可視性を持つようになりました。リアルタイムと履歴の両方の可視性データの可用性により、NetScaler ADMはさまざまなユースケースをサポートできます。

次のシナリオがサポートされています。

シナリオ	EDTサポート
Citrix Gateway	はい
高可用性（HA）を備えたNetScaler Gateway	はい
高可用性（HA）最適化機能を備えたNetScaler Gateway	はい
Unified Gateway を搭載したNetScaler ADC	はい
GSLBを搭載したNetScaler Gateway	はい
NetScaler Gateway とクラスター	はい
Citrix Workspace アプリからNetScaler Gateway へのDTLS暗号化	はい
NetScaler Gateway のデュアルSecure Ticket Authority（STA）	はい
NetScaler Gateway ICA セッションタイムアウト	はい
NetScaler Gateway マルチストリーム ICA	いいえ
NetScaler Gateway セッション画面の保持性（ポート2598）	はい
NetScaler Gateway ダブルホップ	はい
NetScaler ADCからVDAへのDTLS暗号化	はい
HDX Insight	はい

© 1997–2026 Citrix Systems, Inc. All rights reserved.

シナリオ	EDTサポート
IPv6モードのNetScaler Gateway	いいえ
NetScaler Gateway SOCKS (ポート1494)	いいえ
Citrix ADC ピュア LAN プロキシ (注記を参照)	いいえ

注：

Citrix ADC LANプロキシがLANユーザーモードまたはトランスペアレントモードで構成されている場合、EDTはサポートされません。ただし、TCP はサポートされています。詳しくは、次のトピックを参照してください：

- アウトバウンドICAプロキシの構成
- SOCKSを使用したCitrix ADCによるLANユーザー向けのHDX Insight 分析の収集

Enlightened Data Transport をサポートするようにNetScaler Gateway を構成する

Enlightened Data Transport (EDT) を使用する場合、EDT によって使用される UDP 接続を暗号化するには、データグラムトランスポート層セキュリティ (DTLS) を有効にする必要があります。DTLS パラメータは、ゲートウェイ VPN 仮想サーバレベルで有効にする必要があります。また、Gateway VPN仮想サーバーとユーザーデバイス間のトラフィックを暗号化するには、Citrix Virtual Apps and Desktopsコンポーネントを正しくアップグレードして構成する必要があります。

注：

仮想サーバーがDTLS接続を受信するには、NetScaler Gateway フロントエンド仮想サーバー用に構成されたUDPポート（ポート443など）をDMZで開く必要があります。DTLSとCGPは、EDTがNetScaler Gatewayと互換性を持つための前提条件です。

GUIを使用してEDTをサポートするようにNetScaler Gateway を構成するには

1. NetScaler Gatewayを展開して、StoreFrontと通信しCitrix Virtual Apps and Desktopsのユーザーを認証するように構成します。
2. NetScaler ADC GUIの［構成］タブで、［**NetScaler Gateway**］を展開し、［**仮想サーバー**］を選択します。

   
3. をクリックして VPN 仮想サーバーの基本設定を表示し、DTLS 設定の状態を確認します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



4. その他の設定オプションを表示するには、 をクリックします。



5. データグラムプロトコルの通信セキュリティを提供するには、 を選択します。［**OK**］ をクリックします。VPN 仮想サーバーの 領域に、DTLS フラグが **True**に設定されていることが示されます。



CLIを使用してEDTサポート用にNetScaler Gateway を構成するには

```
set vpn vserver vs1 -DTLS ON
```

HDX InsightをサポートするようにNetScaler Gatewayを構成する

HDX Insightは、NetScaler ADCを通過する仮想アプリケーションおよびデスクトップへのHDXトラフィックのエンドツーエンドの可視性を提供します。また、管理者は、リアルタイムのクライアントおよびネットワーク遅延メトリック、履歴レポート、エンドツーエンドのパフォーマンスデータを表示し、パフォーマンスの問題のトラブルシューティングを行うことができます。

GUIを使用してHDX InsightをサポートするようにNetScaler Gateway を構成するには

1. タブで、 > > に移動し、 をクリックします。



2. ページで、次のフィールドに入力し、 をクリックします。 Name — コレクタの名前

   IP アドレス：コレクタの IPv4 アドレス

   Port：コレクタがリッスンするポート

   ネットプロファイル-コレクタに関連付けるネットプロファイル。プロファイルに定義されている IP アドレスは、このコレクタの AppFlow トラフィックの送信元 IP アドレスとして使用されます。このパラメーターを設定しない場合、NetScaler ADC IP（NSIP）アドレスがソースIPアドレスとして使用されます。

   トランスポート — コレクタのトランスポートタイプ。



3. > > に移動し、 をクリックします。



© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. ページで、次のフィールドに入力し、 をクリックします。 AppFlow アクション名 — アクションの名前

   コメント — アクションに関するコメント

   「コレクタ」— AppFlow アクションに関連付けるコレクタの名前を選択します。

   — ログに記録するトランザクションタイプ。

   
5. > > に移動し、 をクリックします。

   
6. ページで、次のフィールドに入力し、 をクリックします。

   ：ポリシーの名前。

   Action — ポリシーに関連付けるアクションの名前。

   UNDEF-未定義のイベントが発生したときに、このポリシーに関連付けられる AppFlow アクションの名前。

   Expression：トラフィックが評価される式またはその他の値。ブール式でなければなりません。

   コメント — このポリシーに関するコメント。

   
7. ［ **NetScaler Gateway**］**>**［**仮想サーバー**］に移動し、仮想サーバーを選択して［ **編集**］をクリックします。

   
8. ページを下にスクロールし、 セクションで をクリックします。

   
9. 画面の ドロップダウンメニューで、 を選択します。 ドロップダウンメニューで、 または を選択し、 をクリックします。

   
10. で強調表示された矢印をクリックします。

    
11. **AppFlow ポリシーを選択し** 、 をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

12. 最後に をクリックします。



CLIを使用してHDX Insightサポート用にNetScaler Gateway を構成するには、次のコマンドを入力します

```
add appflow collector col3 -IPAddress&lt;ip_mas>

add appflow action act1 &lt;action_name>

add appflow policy &lt;policy_name> true &lt;action_name>

bind vpn Vserver &lt;vserver_name>  -pol &lt;policy_name> - priority101
END -type &lt;ICA_Request>
```

非 NSAP HDX セッションの HDX Insightを無効にする

NetScaler ADCアプライアンスでは、NSAP HDX以外のセッションに対してHDX Insightを無効にできるようになりました。

コマンドプロンプトで入力します：

```
set ica parameter HDXInsightNonNSAP (YES | NO )
```

デフォルトでは、非NSAPセッションのHDX Insightは有効になっています。

L7 遅延しきい値処理

HDX InsightのL7遅延しきい値処理機能は、アプリケーションレベルでエンドツーエンドのネットワーク遅延の問題をアクティブに検出し、プロアクティブなアクションを実行します。L7レイテンシーしきい値処理機能は、ライブレイテンシーモニタリングを実行してスパイクを検出し、レイテンシーが最小観測レイテンシを超えた場合に通知をHDX Insightに送信します。

以前は、クライアント側とサーバー側の平均L7遅延値は、60秒ごとにHDX Insightに送信されていました。この間隔内に見られるスパイクはすべて平均化されているため、検出されませんでした。また、これらのスパイクを検出するためのライブレイテンシーモニタリングはありませんでした。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

L7 レイテンシは L4 レイテンシとどう違うのですか

ネットワークの待ち時間がキャプチャされ、L4 レベルでも表示されます。これらのレイテンシは TCP レイヤーから計算され、ICA トラフィックの解析を必要としません。したがって、これらは比較的入手しやすく、CPU 負荷も少なくなります。ただし、L4 レイテンシの主な欠点は、エンドツーエンドのレイテンシを理解することです。パスにTCPプロキシがある場合、L4レイテンシーはNetScaler ADCからTCPプロキシへのレイテンシーのみをキャプチャします。これにより、情報が不完全になり、問題のデバッグが困難になる可能性があります。

L7 レイテンシは ICA トラフィックの解析によって計算されます。L7レイテンシーの計算はICAレイヤーで行われるため、中間プロキシによってレイテンシ値が不完全になることはありません。したがって、はエンドツーエンドの遅延検出を提供します。

次の図は、TCP プロキシを使用する場合と使用しない場合の、展開の種類を示しています。



ICA RTT と L7 のレイテンシー計算の違い

ICA RTTは、Citrix Workspace アプリからVirtual Delivery Agent（VDA）への合計ラウンドトリップ時間を表します。L7 レイテンシは、クライアント側とサーバー側のレイテンシに関する詳細な詳細を提供します。L7クライアントの待ち時間は、Citrix WorkspaceアプリとNetScaler Gatewayの間の遅延です。L7サーバーの遅延は、NetScaler GatewayとVDAの間の遅延です。

注

：サーバーのサーバー側のL7遅延計算は、Citrix Virtual Apps and Desktopsバージョン7.13以降でのみサポートされています。

CLI を使用した L7 遅延しきい値の設定

1. ICA 遅延プロファイルを追加します。

```
add ica latencyprofile <name> [-l7LatencyMonitoring ( ENABLED |
DISABLED )] [-l7LatencyThresholdFactor <positive_integer>] [-
l7LatencyWaitTime <positive_integer>] [-l7LatencyNotifyInterval
<positive_integer>] [-l7LatencyMaxNotifyCount <positive_integer>]
```

2. ICA アクションを追加します。

```
add ica action <name> [-latencyprofileName <string>]
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. ICA ポリシーを追加します。

```
add ica policy <name> -rule <expression> -action <string> [-
comment<string>] [-logAction <string>
```

4. ICAポリシーをVPNサーバーまたはICAグローバルバインドポイントにバインドします。

```
bind ica global -policyName <string> -priority <positive_integer> [-
gotoPriorityExpression <expression>] [-type ( ICA_REQ_OVERRIDE |
ICA_REQ_DEFAULT )]
```

または

```
bind vpn vserver <name> -policy <string>  [-priority
<positive_integer>]
```

または

```
bind cr vserver <name> -policy <string> [-priority <positive _integer>]
```

引数

- **レイテンシーモニタリング**：L7 しきい値モニタリングを有効または無効にするパラメータ。このパラメーターを有効にすると、設定した条件が満たされたときに通知がHDX Insightに送信されます。

  デフォルト値: 無効

- **latencyThresholdFactor：しきい値を超えたため**、HDX Insightに通知を送信する必要があると判断するために、アクティブなレイテンシーが最小観測レイテンシよりも大きくなければならない係数。

  デフォルト値:4

  最小値:2

  最大値:65535

- **latencyWaitTime**：遅延しきい値を超えた後、HDX Insightに通知を送信するためにアプライアンスが待機する時間（秒）。

  デフォルト値:20

© 1997–2026 Citrix Systems, Inc. All rights reserved.

最小値:1

最大値:65535

- **latencyNotifyInterval**： 待機時間が経過した後、アプライアンスが後続の通知をHDX Insightに送信する時間間隔（秒）。

  デフォルト値:20

  最小値:1

  最大値:65535

- **latencyMaxNotifyCount**：レイテンシーがしきい値を上回る間隔内にHDX Insightに送信できる通知の最大数。

  デフォルト値：5

GUI を使用した L7 遅延しきい値の設定

1. ［ **構成** ］>［ **NetScaler Gateway** ］>［ **ポリシー**］ >［ **ICA**］に移動します。
2. タブを選択し、 をクリックします。
3. ** ページで、次の手順を実行します。

   - を選択して、L7 しきい値モニタリングを有効にします。
   - ［ **L7 しきい値係数**］に、HDX Insightに通知を送信するために、アクティブなレイテンシーが観測された最小レイテンシを超える必要がある値を入力します。
   - ［ **L7 Latency Wait**Time］に、しきい値を超えた後にHDX Insightに通知を送信するまでアプライアンスが待機する時間を秒単位で入力します。
   - ［ **L7遅延通知間隔**］に、待機時間が経過した後にアプライアンスが後続の通知をHDX Insightに送信する時間を秒単位で入力します。
   - ［ **L7レイテンシーの最大通知数**］に、レイテンシーがしきい値を超える間隔内にHDX Insightに送信できる通知の最大数を入力します。 **注:** L7 遅延の最大通知カウントは、しきい値を超えると適用され、アクティブな遅延がしきい値を下回るとリセットされます。これらの通知の周期性は、通知間隔によって制御されます。

4. ［**Create**］ をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

重要：

L7 遅延しきい値パラメーターを構成したら、HDX Insight を構成する必要があります。詳しくは、「HDX InsightをサポートするようにNetScaler Gateway を構成する」を参照してください。

NetScaler ADMでL7レイテンシーパラメーターを表示する

NetScaler ADMでL7レイテンシーパラメーターを表示するには、 > > または > > に移動します。



L7 クライアントのレイテンシー値を計算する時間間隔を指定するパラメーター

Citrix ADCリリース13.0ビルド83.17以降では、L7クライアントの遅延値を計算する時間間隔を秒単位で指定できます。この構成は、L7レイテンシーを有効にしていて、セッションのICAレイテンシーが誤って64,000ミリ秒と記録されている場合に必要です。

CLI を使用してレイテンシー頻度を設定するには

コマンドプロンプトで次を入力します：

```
set ica parameter -L7LatencyFrequency <positive_integer>
```

例：

```
set ica parameter -L7LatencyFrequency 5
```

L7 レイテンシー周波数を表示するには、コマンドプロンプトで次のように入力します：

```
show ica parameter
```

L7 レイテンシー周波数を設定解除または無効にするには、コマンドプロンプトで次のように入力します：

```
unset ica parameter -L7LatencyFrequency
```

注:デフォルトでは、L7 クライアントの遅延はパケットごとに計算されます。
`L7LatencyFrequency` パラメーターのデフォルト値は 0、最小値は 0、最大値は 60 です。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CLI を使用してレイテンシー頻度を設定するには

1. > > に移動します。
2. **L7遅延頻度**に、L7クライアントの遅延値を計算する時間間隔を入力します。



L7 レイテンシ測定モデルと L7 レイテンシしきい値レポートモデル

L7 レイテンシー測定モデル

L7レイテンシ測定モジュールでは、クライアント側とサーバー側の平均L7レイテンシー値が60秒ごとにHDX Insightに送信されます。その結果、この間隔内に見られるスパイクは平均化されるため、検出されないままになります。また、L7 レイテンシ測定モジュールにはライブレイテンシモニタリング機能はありません。

次の図は、L7 レイテンシー測定モデルのサンプルを示しています。



L7 遅延しきい値レポートモデル

L7 レイテンシーしきい値レポートモデルには、スパイクを検出するライブレイテンシーモニタリング機能があります。レイテンシーが観測された最小レイテンシーを超えると、通知がHDX Insightに送信されます。

しきい値を超えると、遅延の増加が検出されます。設定したしきい値の待機時間が経過すると、HDX Insightに通知が送信されます。後続の通知は、待機時間が経過してもしきい値係数を超過した後もHDX Insightに送信されます。 待機時間が経過する前にレイテンシ値がしきい値係数を下回った場合、HDX Insightに通知は送信されません。

次の図は、L7 遅延しきい値レポートモデルの例を示しています。



次のパラメータは、実行時に構成できます。

- しきい値監視 (ON/OFF)
- しきい値係数
- しきい値の待機時間
- 通知間隔
- 最大通知数

© 1997–2026 Citrix Systems, Inc. All rights reserved.

RDPプロキシ

RDPプロキシ機能は、NetScaler Gateway の一部として提供されます。一般的な展開では、RDP クライアントはリモートユーザーのマシンで実行されます。NetScaler Gateway アプライアンスは DMZ内に展開され、RDPサーバーファームは社内ネットワークにあります。

リモートユーザー。

1. NetScaler Gateway パブリックIPアドレスに接続する
2. SSL VPN 接続を確立します。
3. 認証する
4. NetScaler Gateway アプライアンスを介してリモートデスクトップにアクセスします。

RDP プロキシ機能は、クライアントレス VPN および ICA プロキシモードでサポートされます。

注：

NetScaler Gateway は、リモートデスクトップセッションホスト（RDSH）、リモートアプリ、RDSマルチユーザー、RDPセッション、またはRDPアプリをサポートしていません。

次のRDPプロキシ機能は、NetScaler Gateway を介してリモートデスクトップファームへのアクセスを提供します。

- クライアントレス VPN または ICA プロキシモード（フルトンネルなし）を介して RDP トラフィックを保護します。
- NetScaler Gateway を介したRDPサーバーへのSSO（シングルサインオン）。また、必要に応じて SSO を無効にするオプションも用意されています。
- 強制（SmartAccess）機能。NetScaler ADC管理者は、NetScaler Gateway 構成を通じて特定のRDP機能を無効にできます。
- すべてのニーズに対応するシングル/ステートレス（デュアル）ゲートウェイソリューション（VPN/ICA/RDP/Citrix Endpoint Management）。
- RDP 用のネイティブ Windows MSTSC クライアントとの互換性は、カスタムクライアントを必要としません。
- Microsoftが提供している既存の RDP クライアントを MACOSX、iOS、Android で使用する。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

次の図は、展開の概要を示しています。



クライアントレス VPN を介した導入

このモードでは、RDP リンクは Gateway ホームページまたはポータルで、ブックマークとして、`add vpn url`構成または外部ポータルを介して公開されます。ユーザーは、これらのリンクをクリックして、リモートデスクトップにアクセスできます。

ICA プロキシを介した展開

このモードでは、`wihome`パラメータを使用して、Gateway VIP でカスタムホームページを設定します。このホームページは、ユーザーがアクセスできるリモートデスクトップリソースの一覧を使用してカスタマイズできます。このカスタムページは、NetScaler ADCでホストすることも、外部の場合は既存のGatewayポータルページのiFrameにすることもできます。

どちらのモードでも、ユーザーがプロビジョニングされたRDPリンクまたはアイコンをクリックすると、対応するリソースのHTTPSリクエストがNetScaler Gateway に到着します。Gateway は、要求された接続の RDP ファイルコンテンツを生成し、クライアントにプッシュします。ネイティブ RDP クライアントが呼び出され、ゲートウェイ上の RDP リスナーに接続します。ゲートウェイは、強制 (SmartAccess) をサポートすることによって RDP サーバーへの SSO を実行します。ゲートウェイは、NetScaler ADC構成に基づいて特定のRDP機能へのクライアントアクセスをブロックし、RDPクライアントとサーバー間のRDPトラフィックをプロキシします。

強制の詳細

NetScaler ADC管理者は、NetScaler Gateway 構成を通じて特定のRDP機能を構成できます。NetScaler Gateway は、重要なRDPパラメータに対して「RDP強制」機能を提供します。NetScaler ADCは、クライアントがブロックされたパラメータを有効にできないようにします。ブロックされたパラメータが有効の場合、RDP 強制機能はクライアント対応パラメータよりも優先され、適用されません。

重要：

強制機能は、SSO が有効な場合にのみ適用できます。

強制用にサポートされている RDP パラメータ

次のリダイレクトパラメータの強制がサポートされています。これらのパラメータは、RDP クライアントプロファイルの一部として設定できます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- クリップボードのリダイレクト
- プリンタのリダイレクト
- ディスクドライブのリダイレクト
- COM ポートのリダイレクト
- PNP デバイスのリダイレクト

接続フロー

接続フローは、次の 2 つのステップに分けることができます。

- RDP リソースの列挙と RDP ファイルのダウンロード。
- RDP 接続の起動。

前述の接続フローに基づいて、2 つの展開ソリューションがあります。

- ステートレス（デュアル）ゲートウェイソリューション-RDP リソースの列挙と RDP ファイルのダウンロードはAuthenticator Gatewayを介して行われますが、RDP 接続の起動は RDP リスナーゲートウェイを介して行われます。
- 単一ゲートウェイソリューション-RDP リソースの列挙、RDP ファイルのダウンロード、および RDP 接続の起動は、同じゲートウェイを介して行われます。

ステートレス (デュアル) ゲートウェイの互換性

次の図は、展開を示しています。



- ユーザはAuthenticator Gateway VIP に接続し、クレデンシャルを提供します。
- ゲートウェイへのログインに成功すると、ユーザーはホームページまたは外部ポータルにリダイレクトされ、ユーザーがアクセスできるリモートデスクトップリソースが列挙されます。
- ユーザーが RDP リソースを選択すると、Authenticator Gateway VIP は、ユーザーがクリックした公開リソースを示す形式`https://vserver-vip/rdpproxy/rdptarget/listener`で要求を受信します。この要求には、ユーザーが選択した RDP サーバーの IP アドレスとポートに関する情報が含まれます。
- Authenticator Gatewayは /rdpproxy/ 要求を処理します。ユーザはすでに認証されているため、このリクエストには有効な Gateway Cookie が付属しています。
- `RDPTarget`および`RDPUser`情報は STA サーバに保存され、STA チケットが生成されます。STA サーバに保存された情報は、設定済みの事前共有キーを使用して暗号化されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Authenticator Gatewayは、ゲートウェイ仮想サーバ上に設定されている STA サーバの 1 つを使用します。

- /rdpproxy/ 要求で取得された「リスナー」情報は、`.rdp file`に「`fulladdress`」 としてに追加され、STAチケット（STA AuthId が前に付く）は`.rdp file`に「`loadbalanceinfo`」として追加されます。
- `.rdp file`がクライアントエンドポイントに返送されます。
- ネイティブ RDP クライアントが起動し、`RDPListener Gateway`に接続します。STA チケットを最初のパケットで送信します。

  `RDPListener`ゲートウェイは STA チケットを検証し、`RDPTarget`および`RDPUser`情報を取得します。使用する STA サーバは、`loadbalanceinfo`に存在する「AuthID」を使用して取得されます。
- ゲートウェイセッションは、承認/監査ポリシーを格納するために作成されます。ユーザーのセッションが存在する場合、そのセッションは再利用されます。
- `RDPListener`ゲートウェイは、`RDPTarget`に接続し、CREDSSP を使用してシングルサインオンします。

重要：

- ステートレス RDP プロキシの場合、STA サーバは RDP クライアントによって送信された STAチケットを検証して`RDPTarget/RDPUser`情報を取得します。VPN 仮想サーバーに加えて STA サーバーをバインドする必要があります。

シングルゲートウェイの互換性

次の図は、展開を示しています。



重要：

単一ゲートウェイ展開の場合、STA サーバーは必要ありません。Authenticator Gatewayは、`RDPTarget`およびCitrix 認証、承認、および監査セッションCookieを安全にエンコードし、`.rdp file`で`loadbalanceinfo`として送信します 。RDP クライアントがこのトークンを最初のパケットで送信すると、Authenticator Gatewayは`RDPTarget`情報をデコードし、セッションを検索し、`RDPTarget`に接続します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

シングルリスナーのサポート

- RDP トラフィックと SSL トラフィックの両方に対応する単一リスナー。
- RDPファイルのダウンロードとRDPトラフィックは、NetScaler ADCアプライアンスの同じ2つのタプル（IPとポート）を介して処理できます。

RDP プロキシのライセンス要件

プレミアムエディション、アドバンスドエディション

注:

RDP プロキシ機能は、Gateway プラットフォームライセンスのみ、または Standard エディションのみをお持ちのお客様にはご利用いただけません。

RDP プロキシを有効にするには、次のコマンドを使用します。

```
enable feature rdpProxy
```

ブックマーク

ポータルを介した RDP リンク生成。ユーザーの RDP リンクを構成したり、外部ポータルを使用して RDP リンクを公開したりする代わりに、`targerIP:Port`を提供して独自の URL を生成するオプションをユーザーに与えることができます。ステートレス RDP プロキシ展開の場合、管理者は RDP クライアントプロファイルの一部として、RDP リスナー情報を FQDN: ポート形式で含めることができます。これは`rdpListener`オプションの下で行われます。この構成は、デュアルゲートウェイモードのポータル経由の RDP リンク生成に使用されます。

ブックマークを作成する

1. RDP リソースにアクセスするためのポータルページにブックマークを作成します (actualURL は`rdp`://で始まります)。
2. VPN URL を追加 `<urlName> <linkName>  <actualURL>`
   - URLは次の形式にする必要があります。`rdp://<TargetIP:Port>`
   - ステートレス RDP プロキシモードの場合、URL は次の形式である必要があります。`rdp://<TargetIP:Port>/<ListenerIP:Port>`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- URL は、次の形式でポータルに公開されます。 `https://<VPN-VIP>/rdpproxy/<TargetIP:Port>` `https://<VPN-VIP>/rdpproxy/<TargetIP:Port>/<ListenerIP:Port>`

3. ブックマークをユーザー、グループ、VPN 仮想サーバー、または VPN グローバルにバインドします。

RDP プロキシで有効にする機能とモード

```
-  enable ns feature ssl


-  enable ns feature sslvpn


-  enable ns feature rdpproxy


-  enable mode usnip
```

RDP プロキシの概要設定手順

ステートレス RDP プロキシ設定に関連する次の高レベルのステップ。

- RDP サーバープロファイルを作成する
- RDP クライアントプロファイルを作成する
- 仮想サーバーを作成してバインドする
- ブックマークを作成する
- セッションプロファイルまたはポリシーを作成または編集する
- ブックマークをバインドする

クライアントプロファイルを構成する

Authenticator Gatewayでクライアントプロファイルを設定します。次に、設定例を示します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
add rdpClient profile <name> [-addUserNameInRdpFile ( YES | NO )] [-
audioCaptureMode ( ENABLE | DISABLE )] [-keyboardHook <keyboardHook>] [-
multiMonitorSupport ( ENABLE | DISABLE )] [-psk <string>] [-
rdpCookieValidity <positive_integer>] [-rdpCustomParams <string>] [-
rdpFileName <string>] [-rdpHost <optional FQDN that will be put in the RDP
file as 'fulladdress>] [-rdpUrlOverride ( ENABLE | DISABLE )] [-
redirectClipboard ( ENABLE | DISABLE )] [-redirectComPorts ( ENABLE |
DISABLE )] [-redirectDrives ( ENABLE | DISABLE )] [-redirectPnpDevices
( ENABLE | DISABLE )] [-redirectPrinters ( ENABLE | DISABLE )] [-
videoPlaybackMode ( ENABLE | DISABLE )]
```

RDP クライアントプロファイルを VPN 仮想サーバに関連付けます。

これは、SessionAction+SessionPolicy を設定するか、グローバル VPN パラメータを設定することによって行うことができます。

例：

```
add vpn sessionaction <actname> -rdpClientprofile <rdpprofilename>



add vpn sessionpolicy <polname> NS_TRUE <actname>



bind vpn vserver <vservername> -policy <polname> -priority
<prioritynumber>
```

または

```
set vpn parameter –rdpClientprofile <name>
```

サーバープロファイルを構成する

リスナーゲートウェイでサーバプロファイルを設定します。

```
add rdp ServerProfile <profilename> -rdpIP <IPV4 address of the RDP
listener> -rdpPort <port for terminating RDP client connections> -psk <key
to decrypt RDPTarget/RDPUser information, needed while using STA>`
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

`rdp ServerProfile` は VPN 仮想サーバ上で設定する必要があります。

```
add vpn vserver v1 SSL <publicIP> <portforterminatingvpnconnections>
-rdpServerProfile <rdpServer Profile>`
```

CLI を使用した RDP プロキシの設定

CLI を使用した RDP プロキシ設定の例を次に示します。

- ターゲット情報を含むユーザの VPN URL を追加します。

```
add aaa user Administrator –password freebsd123$%^


add vpn url rdp RdpLink rdp://rdpserverinfo


add dns addrec rdpserverinfo 10.102.147.132


bind aaa user Administrator  –urlName rdp
```

- VPN 接続用の RDP クライアントおよびサーバプロファイルを設定します。

```
add rdp clientprofile p1 –psk citrix -redirectClipboard ENABLE


add rdp serverprofile p1 -rdpIP 10.102.147.134 -psk citrix


add vpn vserver mygateway SSL  10.102.147.134 443 –rdpserverprofile p1


set vpn parameter -clientlessVpnMode ON -defaultAuthorizationAction
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
ALLOW -rdpClientProfileName p1



add ssl certKey gatewaykey -cert rdp_rootcert.pem  -key rdp_rootkey



bind ssl vserver mygateway -certkeyName gatewaykey
```

- NetScaler ADCからターゲットに接続するためのSNIPを追加します。

```
add ns ip 10.102.147.135  255.255.255.0 –type SNIP
```

GUI を使用した RDP プロキシの設定

1. ［**NetScaler Gateway**］>［**ポリシー**］に移動し、［**RDP**］を右クリックして［**機能を有効にする**］をクリックします。
2. ナビゲーションペインで をクリックします。右側の タブを選択し、 をクリックします。
3. クライアントプロファイルの名前を入力し、設定します。

   
4. ［RDPホスト］フィールドに、RDPプロキシリスナーに解決されるFQDNを入力します。これは通常、NetScaler Gateway アプライアンスのFDQNと同じFQDNです。
5. 「**事前共有キー**」にパスワードを入力し、 **「OK」**をクリックします。

   
6. サーバプロファイルの名前を入力します。
7. このプロファイルをバインドするゲートウェイ仮想サーバーの IP アドレスを入力します。
8. RDP クライアントプロファイルに設定したのと同じ事前共有キーを入力します。［**Create**］をクリックします。

   
9. クライアントレスアクセスポータルページでRDPブックマークを追加する場合は、左側で［**NetScaler Gateway**］、［**リソース**］、［**ブックマーク**］の順に展開します。
10. 右側の をクリックします。
11. ブックマークに名前を付けます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

12. URL には、 **IP または DNS を使用して rdp: //myrdpServer**と入力します。
13. ［**NetScaler Gateway をリバースプロキシとして使用**］を選択し、［**作成**］をクリックします。
14. 要件に従ってブックマークを作成します。

    ▢
15. セッションプロファイルを作成または編集します。 **［NetScaler Gateway］>［ポリシー］>［セッション］** に移動します。
16. タブで、 を に設定します。または、認可ポリシーを使用してアクセスを制御することもできます。

    ▢
17. タブで、前に作成した RDP クライアントプロファイルを選択します。

    ▢
18. ブックマークを使用する場合は、 タブで、 を に設定します。

    ▢
19. タブで、 **がオフになっていることを確認します。**

    ▢
20. ゲートウェイ仮想サーバーを変更または作成します。
21. ** セクションで、 をクリックします。

    ▢
22. RDP サーバプロファイルリストを使用して、前に作成した RDP サーバプロファイルを選択します。

    ▢
23. 下にスクロールします。 がオフになっていることを確認します。

    ▢
24. 証明書をバインドします。
25. 認証ポリシーをバインドします。
26. RDP クライアントプロファイルが設定されているセッションポリシー/プロファイルをバインドします。

    ▢

© 1997–2026 Citrix Systems, Inc. All rights reserved.

27. ブックマークは、NetScaler Gateway 仮想サーバー、または認証、承認、および監査グループにバインドできます。NetScaler Gateway 仮想サーバーにバインドするには、右側の［詳細設定］セクションで、［ **公開アプリケーション**］をクリックします。

    ☐

28. 左側の セクションで、 をクリックします。

    ☐

29. ブックマークをバインドします。

    ☐

30. このNetScaler Gateway 仮想サーバーには［ICAのみ］が指定されていないため、NetScaler Gateway ユニバーサルライセンスが正しく構成されていることを確認してください。左側で、**［NetScaler Gateway］** を展開し、［ **グローバル設定**］をクリックします。

    ☐

31. 右側の をクリックします。

    ☐

32. ** をライセンス制限に変更します。

    ☐

33. DNS を使用して RDP サーバーに接続する場合は、アプライアンスで DNS サーバーが設定されていることを確認します（ > > ）**。

    ☐

34. FQDN の代わりに短い名前を使用する場合は、DNS **サフィックスを追加します (> >)**。

    ☐

35. ゲートウェイに接続してログオンします。

    ☐

36. を構成した場合は、 をクリックします。

    ☐

37. アドレスバーを **/rdpProxy/myrdpServer**に変更できます。IP アドレス (rdpproxy/192.168.1.50 など) または DNS 名 (/rdpproxy/myserver) を入力できます。

    ☐

38. ダウンロードした`.rdp file`を開きます。

    ☐

© 1997–2026 Citrix Systems, Inc. All rights reserved.

39. 現在接続しているユーザーを表示するには、［**NetScaler Gateway ポリシー］>［RDP］の順に選択します。**右側には タブがあります。



SSO を無効にするオプション

RDPプロキシを使用したSSO（シングルサインオン）機能は、NetScaler ADCトラフィックポリシーを構成することで無効にできます。これにより、ユーザーは常に資格情報の入力を求められます。SSO が無効になっていると、RDP 強制 (SmartAccess) は機能しません。

例：

```
add vpn trafficaction <TrafficActionName> HTTP -SSO OFF
```

トラフィックポリシーは、要件に従って設定できます。次に、2 つの例を示します。

- すべてのトラフィックに対して SSO を無効にするには、次の手順を実行します。

```
add vpn trafficpolicy <TrafficPolicyName>  "url contains rdpproxy"
<TrafficActionName>
```

- 送信元/宛先 IP/FQDN に基づいて SSO を無効にするには

```
add vpn trafficPolicy <TrafficPolicyName>
 "HTTP.REQ.URL.CONTAINS("rdpproxy") && CLIENT.IP.SRC.EQ(<IP>)"
<TrafficActionName>

bind vpnvserver rdp -policy <TrafficPolicyName> -priority 10
```

ステートレス RDP プロキシ

ステートレス RDP プロキシは RDP ホストにアクセスします。ユーザーが別のNetScaler Gateway Authenticatorで認証すると、NetScaler Gateway上の`RDPListener`を介してアクセスが許可されます。NetScaler Gateway用に`RDPListener`に必要な情報は、STAサーバーに安全に保存されます。STAサーバーは、NetScaler Gateway およびアプリケーション列挙サーバーが到達できる限り、どこにでも配置できます。詳細については、`<https://support.citrix.com/article/CTX101997>`を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

接続フロー

RDP プロキシフローには 2 つの接続が含まれます。最初の接続は、NetScaler Gateway VIPへのユーザーのSSL VPN接続と、RDPリソースの列挙です。

2番目の接続は、NetScaler Gateway 上のRDPリスナー（RDPIPおよびrdpPortを使用して構成）へのネイティブRDPクライアント接続と、その後のRDPクライアントのサーバーパケットへの安全なプロキシです。



1. ユーザはAuthenticator Gateway VIP に接続し、クレデンシャルを提供します。
2. ゲートウェイへのログインに成功すると、ユーザーはホームページ/外部ポータルにリダイレクトされます。このポータルには、ユーザーがアクセスできるリモートデスクトップリソースが列挙されます。
3. ユーザーが RDP リソースを選択すると、Authenticator Gateway VIP によって、ユーザーがクリックした公開リソースを示す形式`https://AGVIP/rdpproxy/ip:port/rdptargetproxy`で要求が受信されます。この要求には、ユーザーが選択した RDP サーバーの IP およびポートに関する情報が含まれます。
4. Authenticator Gatewayは /rdpproxy/ 要求を処理します。ユーザはすでに認証されているため、この要求には有効なゲートウェイ Cookie が付属しています。
5. `RDPTarget`と`RDPUser`の情報は STA サーバに保存され、STA チケットが生成されます。情報は XML BLOB として格納され、設定済みの事前共有キーを使用してオプションで暗号化されます。暗号化されている場合、BLOB は base64 でエンコードされて格納されます。Authenticator Gatewayは、ゲートウェイ仮想サーバ上に構成されている STA サーバの 1 つを使用します。
6. XML BLOB の形式は次のとおりです。

```
<Value name=”IPAddress”>ipaddr</Value>\n<Value name=”Port”>port</
Value>n



<Value name=”`Username`”>username</Value>\n<Value name=”Password”>pwd</
Value>
```

7. /rdpproxy/ リクエストで取得された`rdptargetproxy`は'`fulladdress`' として配置され、STA チケット (STA AuthID の前に) が`loadbalanceinfo`として.rdp ファイルに配置されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

8. `.rdp`ファイルはクライアントのエンドポイントに送り返されます。
9. ネイティブ RDP クライアントが起動し、`RDPListener Gateway`に接続します。STA チケットは最初の x.224 パケットで送信されます。
10. `RDPListener Gateway`はSTAチケットを検証し、`RDPTarget`および`RDPUser`情報を取得します。使用する STA サーバは、`loadbalanceinfo`に存在する「AuthID」を使用して取得されます。
11. Gateway セッションは、承認/監査ポリシーを格納するために作成されます。ユーザーのセッションが存在する場合、そのセッションは再利用されます。
12. `RDPListener Gateway`は`RDPTarget`に接続し、CREDSSP を使用してシングルサインオンします。

前提条件

- ユーザーはNetScaler Gateway Authenticatorで認証されます。
- 最初の /rdpproxy URL と RDP クライアントは、別の`RDPListener Citrix Gateway`に接続されています。
- STA サーバを使用するAuthenticator Gatewayは、`RDPListener Gateway`情報を安全に渡します。

CLI を使用したステートレス RDP プロキシの設定

- `rdpServer`プロファイルを追加します。サーバプロファイルは`RDPListener Gateway`で設定されます。

  注：

  - RDPSServer プロファイルが VPN 仮想サーバーで設定されると、変更できません。また、同じ ServerProfile を別の VPN 仮想サーバーで再利用することはできません。

  ```
  add rdpServer Profile [profilename] -rdpIP [IPV4 address of the RDP
  listener] -rdpPort [port for terminating RDP client connections] -psk
  [key to decrypt RDPTarget/RDPUser information, needed while using STA].
  ```

  次のコマンドを使用して、VPN 仮想サーバーの RDP サーバープロファイルを設定します。

  ```
  add vpn vserver v1 SSL [publicIP] [portforterminatingvpnconnections]
  -rdpServerProfile [rdpServer Profile]
  ```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

例

```
add vpn vserver v1 SSL 1.1.1.1 443 -rdpServerProfile rdp_server_prof
```

重要：

- 同じ STA サーバーを RDP 認証ゲートウェイとリスナーゲートウェイの両方にバインドする必要があります。
- ステートレス RDP プロキシの場合、STA サーバーは RDP クライアントから送信された STA チケットを検証して RDP ターゲットサーバーと RDP ユーザーの情報を取得します。VPN 仮想サーバーに加えて STA サーバーをバインドする必要があります。次の例では、RDP ターゲットサーバーは 1.1.1.0 で、RDP リスナーゲートウェイ仮想サーバー 1.1.1.2 です。

```
add vpn url url4 RDP2 "rdp://1.1.1.0/1.1.1.2:443"
```

次のコマンドを使用して、オーセンティケータ Gateway のクライアントプロファイルを設定します。

```
add rdpClient profile <name> -rdpHost <optional FQDN that will be put in
the RDP file as ‘fulladdress’> [-rdpUrlOverride ( ENABLE | DISABLE )] [-
redirectClipboard ( ENABLE | DISABLE )] [-redirectDrives ( ENABLE |
DISABLE )]



        [-redirectPrinters ( ENABLE | DISABLE )] [-keyboardHook
<keyboardHook>] [-audioCaptureMode ( ENABLE | DISABLE )] [-
videoPlaybackMode ( ENABLE | DISABLE )]



        [-rdpCookieValidity <positive_integer>][-multiMonitorSupport
( ENABLE | DISABLE )] [-rdpCustomParams <string>]
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

—rdpHost設定は、単一のゲートウェイ展開で使用されます。`psk`のみは必須の引数であり、RDP リスナーゲートウェイの RDP サーバープロファイルに追加された PSK と同じである必要があります。

- RDP プロファイルを VPN 仮想サーバに関連付けます。

RDP プロファイルを関連付けるには、SessionAction+SessionPolicy を設定するか、グローバル VPN パラメータを設定します。

例:

```
add vpn sessionaction <actname> -rdpClientprofile <rdpprofilename>



add vpn sessionpolicy <polname> NS_TRUE <actname>



bind vpn vserver <vservername> -policy <polname> -priority
<prioritynumber>
```

または

```
set vpn parameter –rdpClientprofile <name>
```

GUI を使用してステートレス RDP プロキシを構成する

ステートレス RDP プロキシの設定には、次の高レベルの手順が含まれます。詳細な手順については、「RDP プロキシの設定」を参照してください。

- RDP サーバープロファイルを作成する
- RDP クライアントプロファイルを作成する
- 仮想サーバーの作成
- ブックマークを作成する
- セッションプロファイルまたはポリシーを作成または編集する
- ブックマークをバインドする

© 1997–2026 Citrix Systems, Inc. All rights reserved.

重要：

ステートレス RDP プロキシの場合は、VPN 仮想サーバーに加えて STA サーバーをバインドする必要があります。

接続カウンタ

新しい接続カウンタ ns_rdp_tot_curr_active_conn が追加されました。これは、使用中のアクティブな接続数の記録を保持します。これは、NetScaler ADCシェルの `nsconmsg` コマンドの一部として表示できます。これらのカウンタを表示する CLI コマンドは、後で追加される予定です。

アップグレードノート

以前VPN仮想サーバー上で構成されていた rdpIP と rdpPort は、rdpServerProfile の一部です。`rdp Profile` の名前が `rdp ClientProfile` に変更され、パラメータ clientSSL が削除されます。したがって、以前の設定は機能しません。

RDP 接続リダイレクト

NetScaler Gateway アプライアンスは、接続ブローカーまたはセッションディレクトリの存在下でのRDP接続リダイレクトをサポートするようになりました。RDP プロキシ通信では、クライアントからサーバーへの接続ごとに排他的な URL が必要なくなりました。代わりに、プロキシは単一の URL を使用して RDP サーバーファームに接続し、管理者のメンテナンスと構成のオーバーヘッドを削減します。

注意点：

- RDP 接続リダイレクトは、SSO が有効になっている場合にのみサポートされ、シングルゲートウェイモードとステートレスモードまたはデュアルゲートウェイモードの両方でサポートされます (SmartAccess)。
- RDP プロキシ機能は、IP Cookie をサポートするトークンベースのリダイレクトでのみサポートされます。IP ベースのルーティングトークン「msts=」は、 機能が無効になっている場合、Windows セッションブローカまたは接続ブローカによって返されます。
- ［**IP アドレスリダイレクトを使用する**］設定を無効にすると、次の場所でトークンベースのリダイレクトを有効にできます。 `Computer Configuration > Policies > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host > RD Connection Broker` 。
- 接続ブローカマシンではなく、RDSH マシンで 設定を無効にします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- RDP プロキシ接続用の専用リダイレクタを設定できます。

前提条件

- RDPサーバープロファイルを作成して、NetScaler Gateway 仮想サーバーで3389リスナーを有効にします。 RDP するマシンが RDS 接続ブローカインフラストラクチャのメンバーでない場合は、3389 リスナーは必要ありません。
- NetScaler Gateway アプライアンスでRDP接続リダイレクトを有効にして、接続ブローカーの存在下でRDPプロキシをサポートします。

接続ブローカの存在下で RDP プロキシを展開する

接続ブローカの存在下の RDP プロキシは、次の 2 つの方法で展開できます。

- RD 接続ブローカーの負荷分散に参加している RD セッションホストサーバーを使用する。
- RDP 負荷分散機能がある場合。

RD 接続ブローカーの負荷分散に参加している RD セッションホストサーバーの場合：

この場合、RDP URL リンクは、RDP サーバの 1 つを宛先サーバとして指すように設定できます。このサーバは、リダイレクタとして機能します。また、ファーム内の RDP サーバーの 1 つを宛先サーバーとして使用することもできます (この場合、サーバーは RDP セッションを受け入れません)。

RDP 負荷分散機能が存在する場合：

接続ブローカーの負荷分散が有効になっていない場合は、NetScaler ADCでRDP負荷分散機能を利用して、接続ブローカーの存在下でRDPセッションの必要な負荷分散を実行できます。この場合、RDP URL リンクは、RDP ロードバランサを宛先サーバとして設定する必要があります。RDPロードバランサーは、RDPプロキシと同じNetScaler Gateway アプライアンス上に置くことができます。詳細については、「RDP サーバーの負荷分散」を参照してください。

CLI を使用して、接続ブローカの存在下で RDP プロキシを構成する

コマンドプロンプトで次を入力します：

```
add rdpserverprofile <Name> -psk <string> -rdpRedirection ( ENABLE |
DISABLE )
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
add rdpserverprofile serverProfileName -psk “secretString” -rdpRedirection
ENABLE
```

NetScaler ADC GUIを使用してRDP接続リダイレクトを構成する

1. **NetScaler Gateway > ポリシー > RDP**に移動します。
2. を右クリックして、RDP **リダイレクト機能を有効または無効にします** 。

LDAP 属性に基づいて RDP URL を設定

NetScaler Gateway アプライアンスは、LDAPサーバー属性からRDPサーバー（IP/FQDN）のリストを取得するように構成できます。取得したリストに基づいて、アプライアンスはユーザーがアクセスできるサーバーの RDP URL を表示します。

CLI を使用して LDAP 属性に基づいて RDP URL を入力するには

コマンドプロンプトで入力します：

```
add rdpclientprofile <Name> –rdpUrlLinkAttribute <string>



add rdpclientprofile clientProfileName –rdpUrlLinkAttribute
rdpServerAttribute
```

前の例では、rdpServerAttribute は、LDAP サーバー上の特定のユーザーの RDP サーバーの詳細に対応しています。

注：LDAP サーバから LDAP 属性の詳細を取得するには、LDAPアクションを次のように `pUrlLinkAttribute` で設定したのと同じ文字列で設定する必要があります。

```
add authentication ldapAction dnpg_ldap -serverIP <IP address>-ldapBase
<"domain name"> -ldapBindDn <username> -ldapLoginName sAMAccountName
-ldapbindDnpassword <password>



add authentication ldapAction dnpg_ldap -serverIP 10.102.39.101 -ldapBase
"dc=dnpg-blr,dc=com" -ldapBindDn sqladmin@dnpg-blr.com -ldapLoginName
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
sAMAccountName -ldapbindDnpassword xxxx

add authentication ldapPolicy dnpg_ldap_pol ns_true dnpg_ldap

bind vpn vs vserver<name> -pol dnpg_ldap_pol

set ldapaction dnpg_ldap -attributes "rdpServerAttribute"

set rdpclientprofile ldap -rdpLinkAttribute rdpServerAttribute
```

LDAP サーバ設定

LDAP サーバで、次の手順を実行します。

1. **特定のユーザーに移動します。**
2. で、、 の順にクリックします。**
3. **ユーザ名を右クリックし** 、 をクリックします。**
4. 必要な属性 (DisplayName) の値を変更し、 **「OK」をクリックします。**

GUI を使用して LDAP 属性に基づいて RDP URL を入力するには

1. **NetScaler Gateway > ポリシー > RDP**に移動します。
2. ページで、 タブをクリックし、RDP リンク属性を構成するクライアントプロファイルを選択します。
3. ** ページの に、LDAP 属性名を入力します。

   注: LDAP 属性値は、カンマ区切りのリストにすることができます。

RDP プロキシで RDP ファイル名をランダム化する

RDP URL をクリックすると、RDP ファイルがダウンロードされます。 **RDP URL** を再度クリックすると、同じ名前の新しい RDP ファイルがダウンロードされ、新しいファイルを既存のファイルに置き換えるポップアップが表示されます。これを回避するために、管理者は RDP ファイル名を

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ランダム化することを選択できます。ファイル名は現在、time () 関数の出力を \<rdpFileName\>_\<`outputof` time()>.rdpの形式で追加することでランダム化されます。これにより、ファイルをダウンロードするたびに、アプライアンスは一意の RDP ファイル名を生成します。

RDP プロキシを使用した RDP ファイル名のランダム化のサポートを構成する

コマンドプロンプトでコマンドラインインターフェイスを使用して RDP プロキシを使用した RDP ファイル名のランダム化のサポートを構成するには、次のように入力します：

```
    add rdpclientprofile <profileName> -rdpfileName <filename> -
randomizeRDPFilename <YES/NO>



    add rdpclientprofile clientProfileName -rdpfileName testRDP -
randomizeRDPFilename YES
```

NetScaler ADC GUIを使用して、RDPプロキシを使用したRDPファイル名のランダム化のサポートを構成するには：

1. **Citrix Gateway** > **ポリシー** > **RDP**に移動します。
2. ページで、 タブをクリックし、RDP ファイル名のランダム化機能を構成するクライアントプロファイルを選択します。
3. ページで、 フィールドの横のメニューで を選択します。

RDP ファイルの名前を設定する

RDP ファイルをダウンロードすると、設定したファイル名でローカルに保存できます。

RDP ファイルの名前を設定する

CLI を使用して RDP ファイルの名前を設定するには、コマンドプロンプトで次のように入力します：

```
set rdpclientprofile <Name> -rdpfilename <filename>.rdp
```

GUI を使用して RDP ファイルの名前を設定するには：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. **Citrix Gateway** > **ポリシー** > **RDP**に移動します。
2. ページで、 タブをクリックします。ランダム化 RDP ファイル名機能を設定するクライアントプロファイルを選択します。
3. ページで、 フィールドに RDP プロファイルの名前を入力します** 。ファイルの名前は、次の形式で指定する必要があります。名前には最大 31 文字を使用できます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

送信ICAプロキシのサポート

NetScaler Gateway のアウトバウンドICAプロキシサポートにより、ネットワーク管理者は、ReceiverとNetScaler Gatewayが異なる組織に展開されている場合でも、SmartControl機能を利用することができます。

次のシナリオは、アウトバウンドICAプロキシソリューションの使用方法を示しています。

ReceiverとNetScaler Gatewayが異なる組織に展開されている場合、ネットワーク管理者は、ICAセッションに関連する機能を制御する必要があります。

アウトバウンドICAプロキシのサポートについて

SmartControl機能をレシーバを持つエンタープライズ組織であるA社に導入するには、LANプロキシとして機能するNetScaler ADCアプライアンスを追加する必要があります。NetScaler ADC LANプロキシはSmartControlを強制し、トラフィックをB社のNetScaler Gatewayにプロキシします。この展開シナリオでは、レシーバはトラフィックをNetScaler ADC LANプロキシに転送します。これにより、A社のネットワーク管理者はSmartControlを強制できます。次の図に、展開を示します。

このシナリオでは、LANプロキシとNetScaler Gateway 間のトラフィックはSSL経由です。

注：

NetScaler Gateway でクライアント証明書ベースの認証を有効にしないでください。

NetScaler ADC LANプロキシでのSSLサポート

リリース13.0ビルドxx.xxから、Citrix Workspace アプリとNetScaler ADC LANプロキシ間のトラフィックは、SSL経由でもサポートされています。Citrix Workspace アプリは、SSL経由でLANプロキシに送信するトラフィックを暗号化します。LAN プロキシでの SSL サポートは、既存の展開と共存できます。

Citrix WorkspaceアプリとNetScaler ADC LANプロキシ間のSSLを介したトラフィック暗号化を有効にするには、NetScaler ADC LANプロキシで以下を実行する必要があります。

- VPN 仮想サーバーで認証を無効にし、ダブルホップを有効にします。
- Windows クライアント上のホストを VPN 仮想サーバの IP アドレスに設定します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- SNI と証明書の検証を有効にします。
- 適切な CA 証明書を追加し、グローバルに有効にします。

アウトバウンドICAプロキシの構成

アウトバウンドICAプロキシ構成には、NetScaler ADC LANプロキシとNetScaler Gatewayの構成が含まれます。

ICAアウトバウンドプロキシ用のNetScaler ADC LANプロキシを構成する

CLIを使用してアウトバウンドICAプロキシを構成するには、次の手順を実行します。

- VPN 仮想サーバーを追加します。

```
add vpn vserver <name> <serviceType> [<IPAddress> [-range
<positive_integer>] [-ipset <string>]] [<port>] [-state ( ENABLED |
DISABLED )] [-authentication ( ON | OFF )] [-doubleHop ( ENABLED |
DISABLED )]
```

- VPN パラメータを設定します。

```
set vpn parameter[-backendServerSni ( ENABLED | DISABLED )][-
backendCertValidation ( ENABLED | DISABLED )]
```

- SSL 証明書とキーのペアを追加します。

```
add ssl certKey ca_cert_verify -cert <certificate name>
```

- SSL 証明書とキーのペアをグローバルにバインドします。

```
bind vpn global -cacert ca_cert_verify
```

例:

```
-  add vpn vserver ssl_lan_proxy SSL 65.219.17.34 443 -authentication OFF
- doubleHop ENABLED
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
-  set vpn parameter backendserverSni ENABLED backendcertValidation
ENABLED



-  add ssl certKey dnpg_ca -cert dnpg_ca_cert.cer



-  bind vpn global -cacert dnpg_ca
```

NetScaler Gateway の ICA プロキシを構成する

NetScaler Gateway の ICA プロキシの構成について詳しくは、

`<https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/deploying-netscaler-gateway-in-ica-proxy-mode.pdf>` を参照してください。

注： NetScaler ADC LANプロキシでのSSLサポートの場合、NetScaler Gateway 構成を変更する必要はありません。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler Gateway 対応の PCoIP プロキシサポート（VMware Horizon View）

NetScaler Gateway 12.0は、PC-over-IP（PCoIP）プロトコルをサポートしています。PCoIP は、VMware Horizon Viewを含むいくつかの非Citrix VDIソリューションのリモート表示プロトコルです。PCoIPは、Citrix HDX/ICAプロトコルとMicrosoft RDPプロトコルに似ています。PCoIP は UDP ポート 4172 を使用します。

PCoIPがNetScaler Gatewayを介してプロキシされると、NetScaler Gatewayは、Viewセキュリティサーバーや VMwareアクセスポイントなどの従来のPCoIPリモートアクセスソリューションを置き換えることができます。

次のシナリオは、NetScaler Gateway 対応の VMware Horizon View ソリューションの使用を示しています。

- VMware Horizon PCoIP ユーザーは、Horizon View セキュリティサーバまたは VMware アクセスポイントを展開せずに、NetScaler Gateway を介して VMware Horizon View デスクトッププールおよびアプリケーションプールにリモートでアクセスする必要があります。
- PCoIPユーザーは、NetScaler Gateway を介して他のPCoIPベースの仮想デスクトップソリューションにリモートアクセスします。

注

NetScaler Gateway は、リモートアクセスソリューションとして展開されます。

VMware Horizon View 用の NetScaler Gateway 有効な PCoIP プロキシの構成

前提条件

バージョン -NetScaler ADC 12.0以上

ユニバーサルライセンス -PCoIPプロキシは、NetScaler Gateway のクライアントレスアクセス機能を使用します。つまり、すべてのNetScaler Gateway 接続には、NetScaler Gateway ユニバーサ

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ルのライセンスが必要です。NetScaler Gateway 仮想サーバーで、［**ICAのみ**］がオフになっていることを確認します。

Horizon View インフラストラクチャ -Horizon View の内部インフラストラクチャの機能NetScaler Gateway なしで内部で Horizon View エージェントに接続できることを確認します。NetScaler ADC が接続をプロキシする View 接続サーバで、Horizon View **HTTP (S) セキュアトンネルおよび ****PCoIP セキュアゲートウェイが有効になっていないことを確認します** 。 VMware Horizon ビューの次のバージョンがサポートされています。

- 接続サーバ:7.0.1以降
- Horizon クライアント:4.2.0 以降 (Windows および Mac)

ファイアウォールポート:

次の事項に留意してください。

- UDP 4172 および TCP 443 は、Horizon View クライアントから NetScaler Gateway VIP に開かれている。
- UDP 4172 は、NetScaler ADC SNIP からすべての内部の Horizon View エージェントに対して開いている必要があります。
- PCoIPプロキシは、NATの背後に展開されたNetScaler ADCでサポートされています。考慮すべき重要なポイントは次のとおりです：
  - サポートは VPN 仮想サーバーの FQDN パラメータ設定に基づきます
  - パブリックにアクセス可能な FQDN のみをサポートし、IP はサポートしない
  - 443 ポートと 4172 ポートのみをサポート
  - スタティック NAT である必要がある

証明書 -NetScaler Gateway 仮想サーバーの有効な証明書。

認証 — クラシック構文を使用する LDAP 認証ポリシー/サーバ。

Unified Gateway (オプション) — Unified Gateway の場合は、PCoIP 機能を追加する前にUnified Gateway を作成します。

RfWebUI ポータルのテーマ -Horizon View へのWebブラウザアクセスでは、NetScaler Gateway 仮想サーバを RfWebUI テーマで構成する必要があります。

Horizon View クライアント -NetScaler ADC RfWebUI ポータルを使用して Horizon 公開アイコンにアクセスする場合でも、Horizon View クライアントをクライアントデバイスにインストールする必要があります。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

VMware Horizon View の PCoIP プロキシをサポートするようにNetScaler Gateway を構成するには：

1. ［**構成**］>［**NetScaler Gateway ポリシー**］>［**PCoIP**］に移動します。
2. ページで、仮想サーバープロファイルと PCoIP プロファイルを作成します** 。
   a. 仮想サーバープロファイルを作成するには、 タブで、 をクリックします。
   b. 仮想サーバプロファイルの名前を入力します。
   c. View 接続サーバへのシングルサインオンに使用する Active Directory ドメイン名を入力し、 をクリックします。** **注：** NetScaler Gateway 仮想サーバーごとにサポートされる Active Directoryドメインは1つだけです。また、ここで指定したドメイン名が Horizon View クライアントに表示されます。
   d. をクリックします。
   e. PCoIP プロファイルを作成するには、 タブで をクリックします。
      i. PCoIP プロファイルの名前を入力します。
      ii. 内部 VMware Horizon View 接続サーバの接続 URL を入力し、 をクリックします。
   f. ［構成］>［**NetScaler Gateway**］>［**ポリシー**］>［**セッション**］に移動します。
   g. 右側の タブを選択します。
   h. ［**NetScaler Gateway セッションポリシーとプロファイル** ］ページで、NetScaler Gateway セッションプロファイルを作成または編集します。
      i. NetScaler Gateway セッションプロファイルを作成するには、［**追加**］をクリックして名前を入力します。
      ii. NetScaler Gateway セッションプロファイルを編集するには、プロファイルを選択し、［**編集**］をクリックします。
   i. タブで、 の値が に設定されていることを確認します。
   j. タブで、 の値が に設定されていることを確認します。
   k. タブで、必要な PCoIP プロファイルを選択し、 をクリックします。このタブから PCoIP プロファイルを作成または編集することもできます。
   l. 「 **作成****」または「OK」** をクリックして、セッションプロファイルの作成または編集を終了します。
   m. セッションプロファイルを作成した場合は、対応するセッションポリシーも作成する必要があります。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

i. ［構成］>［**NetScaler Gateway**］>［**ポリシー**］>［**セッション**］に移動します。

ii. 右側の タブを選択します。

iii. をクリックし、セッションポリシーの名前を指定し、 **メニューから必要なセッションプロファイル名を選択します** 。

iv. デフォルトの構文を使用してセッションポリシーを作成する場合は、 領域に「true」(引用符なし) と入力し、 をクリックします。注:Unified Gateway のデフォルトはクラシック構文です。

v. クラシック構文を使用してセッションポリシーを作成する場合は、まず をクリックします。次に、 領域に「ns_true」(引用符なし) と入力し、 をクリックします。

n. 作成したPCoIP仮想サーバープロファイルとセッションポリシーをNetScaler Gateway 仮想サーバーにバインドします。

i. ［**NetScaler Gateway**］>［**仮想サーバー**］に移動します。

ii. 右側で、新しいNetScaler Gateway **仮想サーバーを追加するか** 、既存のNetScaler Gateway **仮想サーバーを編集します** 。

iii. 既存のNetScaler Gateway 仮想サーバーを編集する場合は、［ **基本設定** ］セクションで鉛筆アイコンをクリックします。

iv. 追加と編集の両方で、 セクションの をクリックします。

v. **PCoIP 仮想サーバープロファイルメニューを使用して** 、必要な PCoIP 仮想サーバープロファイルを選択します。

vi. 下にスクロールして、 がオフになっていることを確認します。次に、 **「OK」をクリックして「**基本設定** 」セクションを閉じます。

vii. 新しいNetScaler Gateway 仮想サーバーを作成する場合は、 **証明書をバインドし、** LDAP認証ポリシーをバインドします。

viii. セクションまでスクロールダウンし、プラスアイコンをクリックします。

ix. **「タイプの選択」** ページのデフォルトは「 **セッションおよび要求**」です。 **［続行］** をクリックします。

x. セクションで、 をクリックします。

xi. PCoIP プロファイルが設定されている必要なセッションポリシーを選択し、 をクリックします。

xii. ページで、 をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

xiii. Web ブラウザを使用して VMware Horizon View に接続する場合は、右側の ****の下にある セクションを追加します。Horizon View Client のみを使用して NetScaler Gateway に接続している場合は、この手順を実行する必要はありません。

xiv. **ポータル・テーマ・メニューを使用して** 「 **RfWebUI** 」を選択し、 **「OK」**をクリックします。

xv. Horizon View の公開済みアイコンが rfWebI ポータルに追加されます。

注：

VMware は、RDP 以外のプロトコルを使用する場合、2 つ以上のプロトコルを使用します。これにより、2 つの異なるバックエンドサーバー間で要求の負荷が分散される可能性があります。この問題を解決するには、すべてのプロトコルで単一の永続性グループを設定して、すべての接続を同じCitrix 仮想サーバー上に維持します。

USB リダイレクトを有効にする手順

クライアントマシンに接続されている USB デバイスは、仮想デスクトップおよびアプリケーションからアクセスできます。USB リダイレクトを有効にする手順は次のとおりです。

1. VMware Horizon 管理者コンソールにログインします。
2. > **に移動します。
3. タブを選択します。
4. 一覧表示された接続サーバを選択し、 をクリックします。
5. タブで、 の下にある オプションを選択します。［外部URL］フィールドにNetScaler Gateway **の外部URLを入力します** 。

Unified Gateway のコンテンツスイッチング式の更新

NetScaler Gateway 仮想サーバーがUnified Gateway（コンテンツスイッチング仮想サーバー）の背後にある場合は、PCoIP URLパスを含めるようにコンテンツスイッチング式を更新する必要があります。

1. NetScaler ADC GUIで、 ［ **構成**］ **>**［ **トラフィック管理**］ **>**［ **コンテンツスイッチング**］ **>**［ **ポリシー**］に移動します。
2. 「式」 **領域の下に次の式を追加し** 、 **「OK」**をクリックします。

||http.req.url.path.eq（「/broker/xml」）|| http.req.url.path.contains（「/broker/resources」）|| http.req.url.path.eq（「/pcoip-client」）||http.req.url.path.contains（「/ice-tunnel」）

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PCoIP ゲートウェイを使う

1. 接続するには、クライアントデバイスに Horizon View Client がインストールされている必要があります。インストールが完了したら、Horizon View クライアントのユーザーインターフェイスを使用して NetScaler Gateway に接続するか、NetScaler Gateway RfWebUI ポータルページを使用して Horizon から公開されたアイコンを表示できます。
2. アクティブなPCoIP接続を表示するには、 **NetScaler Gateway >［PCoIP］に移動します。**
3. 右側で、 タブに切り替えます。アクティブなセッションは、ユーザー名、Horizon View クライアント IP、および Horizon View エージェントの宛先 IP のデータとともに表示されます。
4. 接続を終了するには、 タブを右クリックし、 をクリックします。または、 をクリックして、すべての PCoIP 接続を終了します。

VMware Horizon View 接続サーバの構成

NetScaler Gateway 経由でPCoIPプロキシをサポートするには：

1\. **VMware Horizon 管理者コンソールにログインします。**

2\. —> ** —> に移動します。

3\. タブを選択します。

4\. 一覧表示された接続サーバを選択し、 をクリックします。

5\. タブで、 の オプションの選択を解除します。

6\. ［ **OK］をクリックして［**接続サーバ設定の編集］ ウィンドウを閉じます。

7\. リストされているすべての接続サーバで、4 〜 6 の手順を実行します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler Gateway の送信プロキシサポートのプロキシ自動構成

プロキシ自動構成（PAC）をサポートするようにNetScaler Gateway アプライアンスを構成すると、PACファイルのURLがクライアントブラウザーにプッシュされます。クライアントからのトラフィックは、PAC ファイルで定義された条件に従ってそれぞれのプロキシにリダイレクトされます。

次に、送信プロキシ用の PAC の一般的なユースケースをいくつか示します。

- クライアントトラフィックを処理する複数のプロキシサーバーを構成する。
- サブネット間でプロキシトラフィックの負荷分散を行うため。

CLIを使用して送信プロキシのPACをサポートするようにNetScaler Gateway グローバルパラメーターを構成する

コマンドプロンプトで入力します：

```
set vpn parameter -proxy BROWSER -autoProxyUrl <URL>
```

CLIを使用してセッションプロファイルでPACをサポートするようにNetScaler Gateway を構成する

コマンドプロンプトで入力します：

```
add vpn sessionAction <name> -proxy BROWSER -autoProxyUrl <URL>
```

どこ;

- **URL** — プロキシサーバーの URL
- **Name** ：VPN セッションアクションの名前

© 1997–2026 Citrix Systems, Inc. All rights reserved.

GUIを使用して送信プロキシのPACをサポートするように NetScaler Gateway グローバルパラメーターを構成する

1. **構成 > NetScaler Gateway > グローバル設定に移動します。**
2. ページで 、 をクリック し、 タブを選択し ます** 。
3. タブで、 を選択し、 タブを選択します**。
4. タブ**で を選択 し、 を選択 します。
5. フィールドに、必要な PAC ファイルの URL を入力します。
6. ［**Create**］ をクリックします。

GUIを使用してセッションプロファイルでPACをサポートするようにNetScaler Gateway を構成する

1. **構成 > NetScaler Gateway > ポリシー > セッションに移動します。**
2. ［NetScaler Gateway **セッションポリシーとプロファイル**］ページで、NetScaler Gateway セッションプロファイルを作成します。
3. タブを選択し、 をクリックして名前を入力します。
4. タブで、 を選択し、 タブを選択します。
5. 「**プロキシ** 」タブで 「 **ブラウザ**」を選択し、「 **自動構成を使用**」を選択します。
6. フィールドに、必要な PAC ファイルの URL を入力します。
7. ［**Create**］ をクリックします。
8. ［**Create**］ をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SameSite Cookie属性の構成サポート

`SameSite`属性は、Cookie をクロスサイトコンテキストに使用するか、同一サイトコンテキストにのみ使用できるかをブラウザに示します。アプリケーションがクロスサイトコンテキストでアクセスされる場合は、HTTPS 接続を介してのみアクセスできます。詳細については、 RFC6265を参照してください。

2020年2月まで、`SameSite`属性はNetScaler ADCアプライアンスで明示的に設定されていませんでした。ブラウザはデフォルト値 (None) を使用しました。`SameSite`属性の設定なしは、NetScaler Gateway および NetScaler ADC AAA 展開には影響しませんでした。

Google Chrome 80 などの特定のブラウザのアップグレードでは、Cookie のデフォルトのクロスドメイン動作に変更があります。 `SameSite` この属性は、次のいずれかの値に設定できます。Google Chromeのデフォルト値はLaxに設定されています。他のブラウザーの特定のバージョンでは、`SameSite`属性のデフォルト値がまだ None に設定されている場合があります。

- **なし**:ブラウザーが安全な接続でのみクロスサイトコンテキストで Cookie を使用することを示します。
- **Lax**: ブラウザが同一サイトコンテキストのリクエストに Cookie を使用することを示します。クロスサイトコンテキストでは、GETリクエストなどの安全なHTTPメソッドのみがCookieを使用できます。
- **厳格**:Cookie は同じサイトコンテキストでのみ使用します。

クッキーに`SameSite`属性がない場合、Google Chrome は `SameSite` = Lax の機能性を前提としています。 その結果、ブラウザーによって Cookie を挿入する必要があるクロスサイトコンテキストを持つ iframe 内の展開では、Google Chrome はクロスサイト Cookie を共有しません。その結果、Web サイト内の iframe が読み込まれないことがあります。

`SameSite` Cookie属性を設定する

`SameSite` という名前の新しいクッキー属性が、VPN および NetScaler ADC AAA 仮想サーバに追加されます。この属性は、グローバルレベルおよび仮想サーバレベルで設定できます。

`SameSite`属性を設定するには、次の手順を実行する必要があります。

1. 仮想サーバの`SameSite`属性を設定する

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. クッキーを`patset`にバインドする（ブラウザがクロスサイトクッキーをドロップした場合、ブラウザによってドロップされる）

CLIを使用した`SameSite`属性の設定

仮想サーバレベルで`SameSite`属性を設定するには、次のコマンドを使用します。

```
set vpn vserver VP1 -SameSite  [ STRICT | LAX | None ]

set aaa vserver VP1 -SameSite  [ STRICT | LAX | None ]
```

グローバルレベルで`SameSite`属性を設定するには、次のコマンドを使用します。

```
set vpn param VP1 -SameSite  [ STRICT | LAX | None ]

set aaa param VP1 -SameSite  [ STRICT | LAX | None ]
```

注：仮想サーバーレベルの設定は、グローバルレベル設定よりも優先されます。
`SameSite`Cookie属性を仮想サーバーレベルで設定することをお勧めします。

CLI を使用したへの `patset` Cookie のバインド

ブラウザーがクロスサイト Cookie をドロップした場合、その Cookie 文字列を既存の`ns_cookies_SameSite patset`にバインドして、`SameSite`属性が Cookieに追加されるようにすることができます。

例:

```
bind patset ns_cookies_SameSite "NSC_TASS"

bind patset ns_cookies_SameSite "NSC_TMAS"
```

GUI を使用して sameSite 属性を設定する

仮想サーバレベルで`SameSite`属性を設定するには、次の手順を実行します。

1. ［**NetScaler Gateway**］**>**［**仮想サーバー**］に移動します。
2. 仮想サーバを選択し、 をクリックします。
3. セクションで編集アイコンを選択し、 をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



4. **SameSite**で、必要に応じてオプションを選択します。



グローバルレベルで`SameSite`属性を設定するには、次の手順を実行します。

1. ［**NetScaler Gateway**］>［グローバル設定］>［グローバル設定の変更］に移動します。
2. **［セキュリティ］** タブをクリックします。
3. **`SameSite`**で、必要に応じてオプションを選択します。



© 1997–2026 Citrix Systems, Inc. All rights reserved.

CloudBridge によるネットワークトラフィックの最適化

ユーザーがCitrix Gateway プラグインを使用してログオンする場合、CloudBridgeプラグインを使用して接続を最適化できます。このプラグインは、CloudBridgeからユーザーデバイスにインストールされます。CloudBridgeプラグインを使用して接続が最適化されると、ネットワークトラフィックはCitrix Gateway を介して圧縮され、高速化されます。接続でCloudBridgeを有効にすると、Citrix Gateway のTCP圧縮ポリシーが無効になります。

CloudBridgeプラグインがデプロイされ、Citrix Gateway プラグインと連動します。

Citrix Gateway は、リピータープラグインのバージョン5.5および6.1と、CloudBridgeプラグインのバージョン6.2および7.0をサポートしています。

CloudBridgeの最適化とフロー制御は、動的なコンテンツ変更を必要とするCitrix Gateway の最適化機能よりも優先されます。HTTPトラフィックに対してCloudBridge最適化が有効になっている場合、次のCitrix Gateway 機能は使用できません。

- Webアプリケーションへのシングル・サインオン
- ファイルタイプの関連付け
- ウェブ認証

Web アプリケーションへのシングルサインオンを許可するには、HTTP でアクセラレーションを無効にします。これを行うには、コマンドラインを使用します。Citrix Gateway シリアルコンソールにログオンし、コマンドプロンプトで次のように入力します。

add vpn trafficAction ssoact http -SSO ON

Citrix Gateway で設定されたHTTPポート宛てのネットワークトラフィックは、CloudBridgeの最適化から自動的に除外されます。これがデフォルトの設定です。HTTP ポートで CloudBridge 最適化のトラフィックポリシーを設定すると、トラフィックポリシーが適用され、ネットワークトラフィックは CloudBridge によって最適化されます。ただし、Citrix Gateway の最適化機能は、そのポリシーの影響を受けるすべてのトラフィックに対して無効になります。CloudBridgeは、他のCitrix Gateway 機能に影響を与えることなく、非HTTPポート宛てのネットワークトラフィックを高速化できます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

トラフィックポリシーを使用して、CloudBridge プラグインを使用するようにユーザー接続を設定します。その後、ポリシーをユーザー、グループ、仮想サーバー、またはグローバルにバインドできます。ポリシーは、ポリシーをバインドする場所に基づいて、またはポリシーに付与された優先順位番号に基づいて優先順位付けされます。

トラフィックポリシーを作成するには

1. 構成ユーティリティの［構成］タブのナビゲーションペインで［Citrix Gatewayポリシー］を展開し、［トラフィック］をクリックします。
2. 詳細ウィンドウで、\[**追加**\] をクリックします。
3. \[**名前\]** に、ポリシーの名前を入力します。
4. \[プロファイルの要求\] の横にある \[**新規**\] をクリックします。
5. \[**名前\]**に、プロファイルの名前を入力します。
6. \[**ブランチリピーター**\] で \[**オン**\] を選択し、\[**作成**\] をクリックします。
7. \[**トラフィックポリシーの作成** \] ダイアログボックスの \[式の **追加** \] の横で、CloudBridge アクセラレーションを有効にするトラフィックタイプを表す式を選択または入力します。\[式の **追加** \] をクリックし、\[**作成** \] をクリックして、\[**閉じる** \] をクリックします。

式を追加するときは、CloudBridge が高速化するように設定されているのと同じ IP アドレスとポート範囲を使用するネットワーク式を選択します。CloudBridgeアクセラレーションを実行するには、Citrix Gateway で設定されたトラフィックの種類が、CloudBridgeで設定されたサービスクラスポリシーと一致している必要があります。

すべての TCP トラフィックは、CloudBridge アクセラレーションの恩恵を受けています。シングルサインオンの使用を計画している場合は、アクセラレーションによってシングルサインオンが無効になるため、HTTP トラフィックを加速しないでください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ゲートウェイ UX 構成での RfWebUI ペルソナ

RFWebIペルソナは、NetScaler Gateway を介してログオンするNetScaler Gateway ユーザーに新しいログオンおよびポータルページを提供するテーマです。ポータルでは、Receiver、StoreFront、およびCitrix Endpoint Managementユーザーに、これらの製品のいずれかに直接アクセスする場合と同じGUIが表示されます。

RfWebUI ペルソナを使用する時は

Webアプリケーション、サービスとしてのソフトウェア（SaaS）アプリケーション、仮想Windowsアプリケーション、デスクトップなど、さまざまなCitrix製品によって提供されるすべてのアプリケーションの単一ペインビューが必要な場合は、NetScaler Gateway のRfWebUI Personaを使用します。

次のシナリオは、RfWebUI ペルソナの使用方法を示しています。

- ユーザーがGatewayを使用してStoreFront にアクセスすると、Gatewayなしで製品にアクセスしたときに表示されるGUIとは異なるGUIが見つかります。

  解決方法： ユーザーがゲートウェイを使用してStoreFront にアクセスすると、RfWebUIテーマは、Gatewayを使用せずに製品にアクセスしたときと同様のユーザーインターフェイスを提供します。
- ユーザーがGatewayを使用してCitrix Workspace アプリ、StoreFront、およびCitrix Endpoint Managementアプリケーションにアクセスし、アプリケーションが論理的にグループ化されていないため、目的のアプリケーションを見つけるのに苦労します。

  解決策： RfWebUIペルソナは、Receiver、StoreFront、Citrix Endpoint Managementなどのさまざまな製品によって提供されるアプリケーションの論理的なバンドルを作成することにより、単一のペインビューのユーザーエクスペリエンスを提供します。

RfWebUI ペルソナによって提供される機能

新しい RfWebUI は次の機能を提供します。

- GO

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- アプリケーションの集約
- ユーザー構成リモートデスクトッププロトコル (RDP) プロキシリンク
- お気に入りのアプリケーション

GO

GO： Go 機能は、クライアントレス VPN を介して Web ページへのアクセスを提供します。ユーザーは「 **ブックマーク** 」タブの「 **URL** 」セクションに URL を入力し、「 **GO**」をクリックするだけです。

現在、 **移動機能は** Outlook Web アプリケーション (OWA) と SharePoint の URL のみをサポートしています。

注: タブは、 `clientlessAccessVPNMode` セッションポリシーのパラメータが の場合にのみ表示されます。

アプリケーションの集約

アプリケーションの集約: RfWebUI テーマは、異なる製品によって提供されるアプリケーションを説明的なバナーの下にバンドルすることにより、単一ペインビューを提供します。たとえば、NetScaler ADC管理者によって構成されたすべてのVPN URLは、 **WebおよびSaaSアプリケーションという名前のバンドルに含まれ、 ユーザー固有のWebブックマークは個人用ブックマークの下にあります。**Citrix Virtual Apps and Desktops アプリケーションバンドルがStoreFront で構成されている場合、NetScaler Gateway の単一ペインビューにもこれらのバンドルが表示されます。

ユーザ設定の RDP プロキシリンク

ユーザーは RDP プロキシリンクを個人用ブックマークとして追加できます。個人用ブックマークは、 タブの下に表示されます。

次の RDP モードがサポートされています。

- シングルゲートウェイ
- ステートレス (デュアル) ゲートウェイ

注: RDPプロキシリンクを追加できるのは、 `RDPclientprofile` が設定されている場合だけです。RDP 構成の詳細については、 RDP Proxy のドキュメントを参照してください 。

お気に入りのアプリケーション

ユーザーは、アプリケーション名の横にある リンクをクリックして、 および **の下に表示されている目的のアプリケーションを タブに追加できます** 。一度追加されたアプリケーションは、 タブの

© 1997–2026 Citrix Systems, Inc. All rights reserved.

下に表示されます。また、［**お気に入り**］タブ内のアプリケーションの横にある［**削除**］リンクをクリックして、［**お気に入り**］タブから削除することもできます。

RfWebUI ペルソナを有効にする際の考慮事項

RfWebUI ペルソナは、以下を完全にはサポートしていません。

ファイル共有機能: SMB ファイル共有にアクセスするためのファイル共有機能はサポートされていません。 **メールホーム：メールホームVPNパラメーターは、NetScaler Gateway ポータルの埋め込みビューとしては使用できません。RfWebUI の APPS タブにあるWeb および SaaS アプリバンドル内のアプリケーションとしてアクセスできます 。 Java クライアント:** SSL トンネルを確立するためのブラウザベースの Java クライアントは、このテーマでは使用できません。

RfWebUI ペルソナの設定

RfWebUI ペルソナを適用するには：

1. NetScaler ADCインターフェイスで、［**構成**］**>**［**NetScaler Gateway ポータルのテーマ**］に移動します。
2. ページで、 チェックボックスをオンにします。
3. ページの右上隅にある アイコンをクリックします。
4. ダイアログボックスで、 をクリックします。

RfWebUI 設定パラメーター

NetScaler Gateway ポータルの全体的な動作は、ローカルNetScaler Gateway 構成ファイルとStoreFront ファイルの2つの構成ファイルの影響を受けます。

展開環境に応じて、"plugins.xml「ファイルのプロパティを変更して、NetScaler Gateway ポータルの動作を変更できます。このファイルは、`/var/netscaler/logon/themes/<custom_theme>/plugins.xml`のリクエストであるブラウザの設定ファイルとして表示されます。

ログオン中は、NetScaler Gateway 構成ファイルが使用されます。ただし、StoreFront に接続すると、StoreFront は新しい構成を送信し、以前の構成は上書きされます。この動作は、クライアントレス VPN と ICA では異なります。

ICAの場合、StoreFront 構成が常に優先されますが、NetScaler Gateway 構成の影響を受けるクライアントレスVPNの一部の動作は、新しい構成がStoreFront から更新された後でも保持されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

次の表に、クライアントレス VPN および ICA よりも優先される設定を記述するパラメータを示します。

コンフィグタイプ	サブコンフィグタイプ	パラメーター	クライアントレス VPN	ICA	説明
クライアントレス VPN のセッション/認証マネージャ for ICA	-	loginFormTimeout	Citrix Gateway	-	ログオンページのタイムアウト時間を分単位で定義します
プラグインアシスタント	-	enabled	StoreFront	StoreFront	プラグインアシスタントを有効または無効にする
プラグインアシスタント	-	upgradeAtLogin	StoreFront	StoreFront	ログイン時にプラグインのアップグレードを促す
プラグインアシスタント	-	showAfterLogin	Citrix Gateway	StoreFront	ログイン後にプラグインプロンプトを表示します
プラグインアシスタント	-	showOnlyIfRequiredByApps	Citrix Gateway	StoreFront	アプリで必要な場合、ログイン後にプラグインプロンプトを表示します
プラグインアシスタント	macOS/win32	path	Citrix Gateway	StoreFront	プラグインのダウンロードパス

© 1997–2026 Citrix Systems, Inc. All rights reserved.

コンフィグタイプ	サブコンフィグタイプ	パラメーター	クライアントレス VPN	ICA	説明
					を定義します
プラグインアシスタント	protocolHandler	enabled	Citrix Gateway	StoreFront	プラグインを起動する前にプロトコルハンドラページを切り替える
プラグインアシスタント	protocolHandler	platforms	Citrix Gateway	StoreFront	プラグインでサポートされるプラットフォームを識別します
プラグインアシスタント	-	skipDoubleHopCheckWhenDisabled	• NetScaler Gateway	StoreFront	ICAパススルーのダブルホップNetScaler Gateway構成チェックを切り替えます
ユーザーインターフェイス	-	frameOptions	-	-	-
ユーザーインターフェイス		autoLaunchDesktop	StoreFront	StoreFront	デスクトップ起動を有効または無効にする
ユーザーインターフェイス	workspaceControl	enabled	StoreFront	StoreFront	ワークスペースコントロールを有効または無効にする

© 1997–2026 Citrix Systems, Inc. All rights reserved.

コンフィグタイプ	サブコンフィグタイプ	パラメーター	クライアントレス VPN	ICA	説明
ユーザーインターフェイス	workspaceControl	autoReconnectAtLogon	StoreFront	StoreFront	可能であれば、前のセッションを自動再接続するように切り替えます
ユーザーインターフェイス	workspaceControl	logoffAction	StoreFront	StoreFront	Citrix Workspace のログオフ動作を定義します
ユーザーインターフェイス	workspaceControl	showReconnectButton	StoreFront	StoreFront	**再接続ボタンを表示または非表示にする**
ユーザーインターフェイス	workspaceControl	showDisconnectButton	StoreFront	StoreFront	**切断ボタンを表示または非表示にする**
ユーザーインターフェイス	workspaceControl	showDesktopsView	StoreFront	StoreFront	[デスクトップ] ビューを表示または非表示にする
ユーザーインターフェイス	workspaceControl	showappsView	StoreFront	StoreFront	アプリビューを表示または非表示にする
ユーザーインターフェイス	workspaceControl	defaultView	StoreFront	StoreFront	デスクトップビューまたはアプリビューのい

© 1997–2026 Citrix Systems, Inc. All rights reserved.

コンフィグタイプ	サブコンフィグタイプ	パラメーター	クライアントレス VPN	ICA	説明
					ずれかを選択します
ユーザーインターフェイス	receiverConfiguration	enabled	StoreFront	StoreFront	受信機の構成を切り替える
ユーザーインターフェイス	receiverConfiguration	showOnlyIfRequiredByApps	Citrix Gateway	Citrix Gateway	アプリが必要とする場合は受信機プロンプトを表示する
ユーザーインターフェイス	receiverConfiguration	downloadURL	StoreFront	StoreFront	受信者のURLをダウンロードする
ユーザーインターフェイス	appShortcuts	enabled	StoreFront	StoreFront	アプリのショートカットタブを有効または無効にする
ユーザーインターフェイス	appShortcuts	allowSessionReconnect	StoreFront	StoreFront	セッションの再接続を許可する

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler Gateway ポータルのカスタマイズ

カスタムプラグインを使用したゲートウェイポータルのカスタマイズ

NetScaler Gateway RFWebIフレームワークは、カスタムプラグインを追加してゲートウェイポータルをカスタマイズする機能を提供します。これらのカスタムプラグインは、ゲートウェイフローに新しいページ全体を追加する場合など、ゲートウェイに大規模な機能を追加するために使用できます。その他のユースケースでは、ゲートウェイテーマ用のカスタムスクリプトファイルに、`/var/netscaler/logon/themes/<custom_theme>/script.js`という場所にあるコードを追加できます。

1. カスタムプラグインを追加するには、その場所`/var/netscaler/logon/LogonPoint/plugins/ns-gateway/`に JavaScript ファイルを作成します。たとえば、`/var/netscaler/logon/LogonPoint/plugins/ns-gateway/`には次のプラグインがあります。

   - ns-nfactor.js
   - nsg-epa.js
   - nsg-setclient.js

   プラグイン名は、`<plugin_name>`.js の形式で入力することをお勧めします。

   これらのプラグインファイルはすべて、機能に必要な RfWebUI フレームワークによって取得されます。

2. プラグインファイルを作成したら、次のコードを例として使用して、プラグインを RfWebUI フレームワークに登録します。

```
(function ($) {

            CTXS.ExtensionAPI.addPlugin( {

                        Name : “plugin name”,

                        initialize: function() {}
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
            });

    })(jQuery);
```

各項目の意味は次のとおりです。

name は、プラグインに付けられた名前です。これは、プラグインの識別子として使用されます。

initialize は、プラグインの初期化に使用されるパラメータとして関数を取ります。

3. プラグインを登録する `CTXS.ExtensionAPI.addPlugin()` 関数に、プラグイン名と初期化関数を入力します。 追加したプラグインの名前と場所は、その場所 `/var/netscaler/logon/themes/<custom_theme>/plugins.xml` の plugins.xml ファイルに登録する必要があります。
4. プラグインコードを記述したら、新しく追加したプラグインの名前と場所を、その場所 `/var/netscaler/logon/themes/<custom_theme>/plugins.xml` の `plugins.xml` ファイルに登録する必要があります。プラグインは、 `plug-in` タグで登録する必要があります。

```
<plugins>

<plugin name="nsg-epa" src="plugins/ns-gateway/nsg-epa.js"/>

<plugin name="nsg-setclient" src="plugins/ns-gateway/nsg-setclient.js"/
>

<plugin name="ns-nfactorn" src="plugins/ns-gateway/ns-nfactor.js"/>

</plugins>
```

5. RfWebUI がプラグインを識別して取得できるように、プラグインの名前と src を入力します。

設定例

次の構成例を使用して、カスタムプラグインを追加して、NetScaler Gateway ログオンページにフッターを追加できます。

1. 次の場所に JavaScript プラグインファイルを作成します。 `/var/netscaler/logon/LogonPoint/plugins/ns-gateway/.`
2. プラグインに ns-footer.js `/var/netscaler/logon/LogonPoint/plugins/ns-gateway/ns-footer.js` という名前を付けます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. 登録されたプラグインに次のコードを RfWebUI に追加し、初期化関数でゲートウェイにフッターを追加します。

```
(function ($) {

CTXS.ExtensionAPI.addPlugin({

    name: "ns-footer", // Name of plugin - must match name sent in
configuration

    initialize: function () {

        CTXS.Extensions.beforeLogon = function (callback) {

            $("#customExplicitAuthBottom").append("<div style='text-
align:center;color:white;font-size:15px;'><br>Disclaimer<BR><BR>"+

                " Access to this website is restricted to employees of
Login Consultants<BR></div>");

            callback();

        };

    }

});

})(jQuery);
```

4. ファイルを保存します。
5. その場所 `var/netscaler/logon/themes/<custom_theme>/plugins.xml` の plugins.xml に nameと src を追加します。

```
<plugins>

<plugin name="nsg-epa" src="plugins/ns-gateway/nsg-epa.js" />

<plugin name="nsg-setclient" src="plugins/ns-gateway/nsg-
setclient.js" />

<plugin name="ns-nfactor" src="plugins/ns-gateway/ns-nfactor.js" />
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
<plugin name="ns-footer" src="plugins/ns-gateway/ns-footer.js" />

</plugins>
```

6. プラグインを追加するカスタムテーマを設定します。
7. `flush cache contentgroup loginstaticobjects`コマンドを使用してキャッシュをフラッシュします。
8. ポータル画面をリロードします。 フッターがNetScaler Gateway ログインページに追加されます。

ログインスキーマの作成とカスタマイズ

ログインスキーマは、フォームベース認証の構造を提供する XML ファイルです。 ユーザーは、基本的な HTML フォームに似た一連のユーザーインターフェイス構造を使用して、幅広い認証フォームを使用できます。

nFactor 認証では、認証要素は連鎖されます。各ファクタは、異なるログインスキーマページまたはファイルを持つことができます。一部の認証シナリオでは、ユーザーに複数のログオン画面を表示することができます。また、1 つのログインスキーマで複数のファクタに渡すことができる情報を収集して、後者のファクタが別のログインスキーマを表示する必要がないようにすることもできます。

ログインスキーマのXMLファイルは、`/nsconfig/loginschema/LoginSchema`のNetScaler ADC アプライアンスに含まれています。

ログインスキーマプロファイルの作成

1. **セキュリティ > AAA > ログインスキーマに移動します。**
2. タブをクリックし、 をクリックします。
3. で、鉛筆アイコンをクリックします。

4. **LoginSchema** フォルダをクリックして、フォルダ内のファイルを表示します。
5. ファイルの 1 つを選択し、必要に応じて変更を実行します。

   - 右上の ボタンをクリックして、ラベルを変更します。
   - 言語を選択してスキームを編集します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



注: 変更後に変更を保存すると、変更内容を含む新しいスキーマ XML ファイルが作成されます。

6. 右上の をクリックして、変更したスキーマ XML を選択します。
7. ログインスキーマ名を入力し、 をクリックします。

   注: 既に入力された認証情報は他の場所で使用できます。たとえば、StoreFrontへのシングルサインオンには、ユーザー名とパスワードのいずれかを使用できます。 をクリックして、インデックスに一意の値を入力できます。これらの値は1 ～ 16の範囲です。
   REQ.USER.ATTRIBUTE (#) という式を使用して、トラフィックポリシーまたはプロファイルでこれらのインデックス値を参照できます。



8. をクリックして、ログインスキーマプロファイルを作成します。

ログインスキーマプロファイルを認証、承認、および監査仮想サーバーにバインドする

ログインスキーマプロファイルを認証、承認、および監査仮想サーバーにバインドするには、最初にログインスキーマポリシーを作成する必要があります。ログインスキーマポリシーは、ログインスキーマプロファイルを認証ポリシーラベルにバインドするときには必要ありません。

ログインスキーマポリシーを作成してバインドするには、次の手順に従います。

1. **セキュリティ > AAA > ログインスキーマに移動します。**
2. タブをクリックし、 をクリックします。
3. 「**プロファイル**」で、以前に作成したログインスキーマプロファイルを選択します。
4. 「**ルール**」に、デフォルトの構文式を入力し、「**作成**」をクリックします。

管理 UI からのポータルのカスタマイズ

管理者は、カスタムテーマを作成してポータルテーマをカスタマイズし、ユーザーポータルのルックアンドフィールをパーソナライズできます。カスタムテーマは、RfWebUI、Default、X1、および GreenBubble テーマに基づいて作成できます。

カスタムテーマを作成するには:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. ［構成］タブで、［ **NetScaler Gateway**］**>**［**ポータルテーマ** ］に移動し、［ **追加**］をクリックします。
2. カスタムテーマの名前を入力します。
3. で、必要に応じてベーステーマを選択します。**RfWebUI** はデフォルトで選択されています。
4. ［**OK**］ をクリックします。
5. 「 **Look &** Feel」セクションで、ホームページの要件に従って属性を変更し、「 **OK」**をクリックします。

次の図に、RfWebUI ベースのカスタムテーマを示します。

リンクをクリックすると、編集する内容を選択しやすくするために、セクション名を含むグラフィカルなページが表示されます。

共通属性

［ **共通属性** ］セクションには、すべてのNetScaler Gateway ログオンページに共通する構成可能な設定が表示されます。

リンクをクリックすると、共通の設定可能な各パラメータが表示されます。

同様に、 **Default**に基づくカスタムテーマの場合、次の図はホームページで使用可能な設定を示しています。 **注:** この構成は x1 と GreenBubble では異なります。

文字列のカスタマイズ

管理 UI では、ゲートウェイポータルのホームページの外観と外観に加えて、すべてのページで文字列のカスタマイズも可能です。

文字列をカスタマイズするには、次の手順を実行します。

1. 文字列を編集する言語を選択します。選択した言語で文字列が表示されます。既定では、 が選択されています。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注: 選択した言語では、ポータル・テーマ言語は定義されません。これは、文字列がカスタマイズされる言語です。

2. 右側の ****に、文字列のカスタマイズに使用できるページが一覧表示されます。

   - ログインページ
   - EPA ページ
   - EPA エラーページ
   - 環境保護庁後のページ
   - ページ
   - ホームページ

3. 文字列をカスタマイズするページを選択し、「編集」アイコンをクリックします。文字列のカスタマイズがあらかじめ入力されたフォームが表示されます。
4. フィールドを選択し、必要に応じて文字列を追加または編集します。
5. をクリックして、カスタムポータルテーマの作成を完了します。テーマは、 **NetScaler Gateway > から後で編集できます。

注: セクションに以前に選択した言語の文字列が引き続き表示される場合は、言語が変更されたときにセクションが既に開かれていた可能性があります。この場合は、セクションを閉じて言語を選択し、 からページを再度開きます。

次のスクリーンショットは、各ページで使用できるカスタマイズ可能な文字列のセットを示しています。

ログインページ:



環境保護庁ページ:



EPA エラーページ:



環境保護庁後のページ:



ページ:



ホームページ:



© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler Gateway VPN 分割トンネルのOffice365用に最適化

組織はリモートワークオプションに以前よりも迅速に適応しているため、トラフィック負荷の増加時にシームレスな接続を可能にするために、リモートアクセスインフラストラクチャを最適化する必要があります。

重要：

Microsoft では、公開されているIPv4およびIPv6のアドレス範囲を使用して分割トンネリングを構成することにより、主要なOffice 365サービスを宛先とするトラフィックをVPN接続の範囲から除外することを推奨しています。パフォーマンスを最大限に高め、VPN 容量を最も効率的に使用するには、次のアプリケーションに関連する専用 IP アドレス範囲へのトラフィックを VPN トンネルの外部に直接ルーティングする必要があります。

- Office 365 Exchange Online
- SharePoint Online
- Microsoft Teams (Microsoft のドキュメントでは「最適化」カテゴリと呼ばれています)

この推奨事項の詳細については、 Microsoft のガイダンスを参照してください 。
NetScaler Gateway でのMicrosoftの推奨は、分割トンネルのリバース構成を使用して、Microsoftが提供するIPアドレスのリストをO365トラフィック用にインターネットに直接ルーティングすることで実現されます。

設定には以下が含まれます。これらの設定は、GUI または CLI を使用して手動で実行できます：

- 分割トンネルをリバース構成に設定します。詳細については、「 分割トンネリングオプション 」を参照してください。
- リソースへのユーザーアクセス用にイントラネットアプリケーションを構成します。

GUI を使用した設定

GUI を使用して分割トンネリングを設定するには

1. 「構成」タブで、「 **Citrix Gateway」>「グローバル設定」**に移動します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. 詳細ウィンドウの で、 をクリックします。
3. タブの で、 を選択します。
4. ［**OK**］ をクリックします。



GUI を使用して VPN イントラネットアプリケーションを作成するには

1. 「構成」タブで、「 **Citrix Gateway」>「グローバル設定」**に移動します。
2. 詳細ウィンドウの で、リンクをクリックします。
3. ページで、、 の順にクリックします。



4. ** に、プロファイルの名前を入力します。
5. 「 **プロトコル**」で、ネットワークリソースに適用するプロトコルを選択します。
6. で、 と を選択します。
7. に、O365 トラフィック用にインターネットに直接ルーティングする必要がある IP アドレスを入力します。IP アドレスの一覧については、IP アドレスの一覧を参照してください。
8. に、ネットマスク IP アドレスを入力します。



9. ［**Create**］ をクリックしてから、 ［**Close**］ をクリックします。

注: すべての IP アドレスに対してこの手順を繰り返します。

CLI を使用した設定

- 分割トンネルをリバースに設定するには、コマンドプロンプトで; と入力します。

```
set vpn parameter -splitTunnel REVERSE
```

- VPN イントラネットアプリケーションを追加するには、コマンドプロンプトで; と入力します。

```
add vpn intranetApplication intranetapp1 ANY 13.107.6.152 -netmask
255.255.255.254 -destPort 1-65535 -interception TRANSPARENT
```

注: すべての IP アドレスに対してこの手順を繰り返します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- イントラネットアプリケーションをバインドするには、コマンドプロンプトで次のように入力します。

```
bind vpn global -intranetApplication intranetapp1
```

Office 365 サービス (EXO、SPO、およびMicrosoft Teams) の IP アドレスのリスト

参考: `<https://docs.microsoft.com/en-us/office365/enterprise/urls-and-ip-address-ranges>`

Microsoftからの注記: *COVID-19 の状況に対するMicrosoftの対応の一環として、MicrosoftはURLとIPアドレスの計画変更に関する一時的なモラトリアムを宣言しました。このモラトリアムは、顧客の IT チームが、自宅勤務の Office 365 シナリオで推奨されるネットワーク最適化を実装する際に、自信を持ってシンプルに実装できるようにすることを目的としています。2020 年 3 月 24 日から 2020 年 6 月 30 日まで、このモラトリアムでは、主要な Office 365 サービス (Exchange Online、SharePoint Online、およびMicrosoft Teams) の IP 範囲と カテゴリに含まれる URL への変更が停止されます。*

IPv4 アドレス範囲

104.146.128.0/17

13.107.128.0/22 13.107.136.0/22

13.107.18.10/31 13.107.6.152/31

13.107.64.0/18 131.253.33.215/32

132.245.0.0/16 150.171.32.0/22

150.171.40.0/22 191.234.140.0/22

204.79.197.215/32 23.103.160.0/20

40.104.0.0/15 40.108.128.0/17

40.96.0.0/13 52.104.0.0/14

52.112.0.0/14 52.96.0.0/14

52.120.0.0/14|

© 1997–2026 Citrix Systems, Inc. All rights reserved.

IPv6 アドレス範囲

2603:1006::/40

2603:1016::/36 2603:1026::/36

2603:1036::/36 2603:1046::/36

2603:1056::/36 2603:1096::/38

2603:1096:400::/40 2603:1096:600::/40

2603:1096:a00::/39 2603:1096:c00::/40

2603:10a6:200::/40 2603:10a6:400::/40

2603:10a6:600::/40 2603:10a6:800::/40

2603:10d6:200::/40 2620:1ec:4::152/128

2620:1ec:4::153/128 2620:1ec:c::10/128

2620:1ec:c::11/128 2620:1ec:d::10/128

2620:1ec:d::11/128 2620:1ec:8f0::/46

2620:1ec:900::/46 2620:1ec:a92::152/128

2620:1ec:a92::153/128 2a01:111:f400::/48

2620:1ec:8f8::/46 2620:1ec:908::/46

2a01:111:f402::/48

© 1997–2026 Citrix Systems, Inc. All rights reserved.

UDP トラフィックのサービスタイプサポート

UDPのタイプ（ToS）のサポートにより、送信者によってUDPパケットのToS値が構成されると、NetScaler Gateway はパケットが宛先に到達するまでその値を保持します。設定値と宛先ネットワークの設定に基づいて、宛先ネットワークは UDP パケットを優先された発信キューに配置します。

（

注

）ToS 情報を使用して、各 IP パケットに優先順位を割り当て、高スループット、高信頼性、低遅延などの特定の処理を要求できます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

サーバー名表示拡張機能の設定

NetScaler Gateway アプライアンスは、バックエンドサーバーに送信されるSSL「クライアントこんにちは」パケットにサーバー名表示（SNI）拡張を含めるように構成できるようになりました。SNI 拡張は、バックエンドサーバーが SSL ハンドシェイク中に要求される FQDN を識別し、それぞれの証明書で応答するのに役立ちます。

注

複数の SSL ドメインが同じサーバーでホストされている場合は、SNI サポートを有効にします。

GUIを使用してSNIをサポートするようにNetScaler Gateway を構成するには：

1. NetScaler GUIで、［**構成**］>［**Citrix NetScaler**］>［**グローバル設定**］の順に移動します。
2. リンクをクリックし、 メニューから を選択します。

コマンドラインインターフェイスを使用してSNIをサポートするようにNetScaler Gateway を構成するには、コマンドプロンプトで次のように入力します。

```
set vpn parameter backendServerSni <ENABLED><DISABLED>
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SSL ハンドシェイク中のサーバ証明書の検証

NetScaler Gateway アプライアンスは、SSLハンドシェイク中にバックエンドサーバーから提供されたサーバー証明書を検証するように構成できるようになりました。

構成ユーティリティを使用して送信プロキシのPACをサポートするようにNetScaler Gateway グローバルパラメーターを構成するには

CA 証明書をバインドする

1. ［ **構成** ］ > ［**NetScaler Gateway**］ > ［**NetScaler Gateway ポリシーマネージャー** ］ > ［ **証明書のバインド**]に移動します。****
2. 画面で、 アイコンをクリックします。
3. 画面で、 をクリックし、 をクリックします。
4. **フィールドで証明書ファイル名を選択し** 、 をクリックします。
5. ** 画面で、証明書を選択し、 をクリックします。
6. ［**完了**］ をクリックします。

証明書の検証を有効にします。

1. ［ **NetScaler Gateway**］ **>［グローバル設定］に移動します。**
2. をクリックします。****
3. **バックエンドサーバー証明書の検証ドロップダウンメニューから** 「 **有効** 」を選択し、 ** 「OK」**をクリックします。

コマンドラインでサーバー証明書をサポートするようにNetScaler Gateway グローバルパラメーターを構成するには

コマンドプロンプトで、次のコマンドを入力します：

```
bind vpn global cacert DNPGCA1
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
set vpn parameter backendcertValidation ENABLED
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

テンプレートを使用した簡略化されたSaaS アプリ設定

NetScaler Gateway でのシングルサインオンによるSaaSアプリの構成は、一般的なSaaSアプリのテンプレートドロップダウンメニューをプロビジョニングすることで簡素化されます。構成するSaaS アプリは、メニューから選択できます。テンプレートには、アプリケーションの構成に必要な情報の大部分があらかじめ入力されています。ただし、顧客固有の情報は引き続き提供する必要があります。

注：

SaaSアプリを構成して公開するには、NetScaler Gateway で構成して公開し、次にアプリケーションサーバーで構成して公開します。

次のセクションの手順は、テンプレートを使用してNetScaler Gateway でアプリを構成して公開するのに役立ちます。次に、アプリケーションサーバー上で構成して公開する方法を説明するセクションに進みます。

テンプレートを使用したアプリの構成と公開-NetScaler Gateway 固有の構成

次の設定では、テンプレートを使用してアプリケーションを設定および発行する方法の例としてAWS Console アプリケーションを使用しています。

開始する前に、次のものが必要です：

- AWS コンソールの管理者アカウント
- NetScaler Gateway の管理者アカウント

AWS コンソールの設定手順は次のとおりです。

1. アプリケーションカタログを使用して AWS コンソールを設定します。
2. AWS コンソール IdP メタデータをNetScaler ADC からエクスポートします。
3. IdP を AWS コンソールに設定します。

ステップ 1: アプリケーションカタログで AWS コンソールを設定する

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. **Unified Gateway > 認証をクリックします。**

   画面が表示されます。
2. セクションで、 アイコンをクリックします。次に、プラスアイコンをクリックします。 ウィンドウが表示されます。

   
   
3. から を選択します。

   
4. ドロップダウンリストから を選択します。

   
5. アプリケーションテンプレートに適切な値を入力します。

   
6. 次の SAML 設定の詳細を入力し、 をクリックします。

   サービスプロバイダー ID — `<https://signin.aws.amazon.com/saml>`

   署名証明書名 — IdP 証明書を選択する必要があります

   発行者名 — 発行者名は選択に従って入力できます

   属性 1 — `https://aws.amazon.com/SAML/Attributes/Role`

   属性 1 式 `- Role ARN, IdP ARN`（ステップ 3 を参照）
7. ［完了］ をクリックします。

ステップ 2: AWS コンソール IdP メタデータをNetScaler Gateway からエクスポートします。

1. **Unified Gateway > 認証をクリックします。**
2. 下にスクロールして、 をクリックします。 ウィンドウが表示されます。 をクリックします。

   
3. **メタデータは別のウィンドウで開きます 。 IdP メタデータファイルを保存する**

ステップ 3: IdP を AWS コンソールに設定します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

テンプレートを使用したアプリの構成と公開-アプリサーバー固有の構成

次のリンクは、テンプレートを使用して一般的な SaaS アプリを構成および公開するための具体的なガイダンスを提供する PDF ドキュメントを開きます。

- 15Five
- Absorb
- Accompa
- Adobe Captivate Prime
- Adobe Creative Cloud
- Aha
- AlertOps
- Allocadia
- Ariba
- Assembla
- AWS Console
- BambooHR
- Base CRM
- BitaBIZ
- BlueJeans
- Blissbook
- Bonusly
- Box
- Bugsnag
- Buildkite
- CakeHR
- Cardboard
- Cedexis
- Celoxis
- Cisco Meraki
- ClearSlide

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- CloudCheckr
- ConceptShare
- Concur
- Confluence
- Contactzilla
- Convo
- Circonus
- Dashlane
- Datadog
- Deskpro
- Deputy
- DigiCert
- DocuSign
- Domo
- Dropbox
- Duo
- eFront
- Ekarda
- Envoy
- ERP
- Expensify
- EZOfficeInventory
- EZRentOut
- Favro
- Federated Directory
- Feedly
- Fivetran
- Flatter Files
- Flowdock
- Freshdesk

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Front
- G-Suite
- GitHub
- GlassFrog
- GotoMeeting
- HappyFox
- Helpjuice
- Help Scout
- Hoshinplan
- Humanity
- Igloo
- Illumio
- Image Relay
- iMeet Central
- InteractGo
- iQualify One
- Jira
- Kanban Tool
- Keeper Security
- Kentik
- Kentik
- Kissflow
- KnowBe4
- KnowledgeOwl
- Kudos
- LaunchDarkly
- Lifesize
- Litmos
- LiquidPlanner
- LogDNA

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Mango
- Manuscript
- Marketo
- Mingle
- Mixpanel
- MuleSoft
- MyWebTimesheets
- New Relic
- Nmbrs
- Nuclino
- Office365
- OneDesk
- OpsGenie
- Orginio
- PagerDuty
- Panorama9
- ParkMyCloud
- Peakon
- People HR
- Pingboard
- Pipedrive
- PlanMyLeave
- PlayVox
- Podio
- ProdPad
- Proto.io
- Proxyclick
- PurelyHR
- Quandora
- Rackspace

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- RealtimeBoard
- Remedyforce
- Robin
- Rollbar
- Salesforce
- Samanage
- Samepage
- Sentry
- ServiceDesk Plus
- ServiceNow
- Shufflrr
- Skeddly
- Skills Base
- Slack
- Slemma
- Sli.do
- Smartsheet
- Spoke
- Spotinst
- SproutVideo
- StatusCast
- Status Hero
- StatusHub
- Statuspage
- Sumo Logic
- Supermood
- Syncplicity
- Tableau
- Targetprocess
- Teamphoria

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Testable
- TestFairy
- TextExpander
- TextMagic
- ThousandEyes
- Thycotic Secret server
- Tinfoil Security
- Trisotech
- Trumba
- TwentyThree
- UniFi
- UserEcho
- UserVoice
- Velpic
- VictorOps
- VIDIZMO
- Visual Paradigm
- Weekdone
- Wepow
- When I Work
- Workday
- Workpath
- Workplace
- Workstars
- Workteam
- XaitPorter
- Ximble
- `XMatters`
- Yodeck
- Zendesk

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- ZIVVER
- Zoho One
- ZIVVER
- Zoom

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Web Interfaceを使用したNetScaler Gateway の展開

NetScaler Gateway を展開してCitrix Virtual Apps and Desktops へのセキュアなリモートアクセスを提供する場合、NetScaler GatewayはWeb InterfaceおよびSecure Ticket Authority（STA）と互換性があり、サーバーファームでホストされている公開アプリケーションおよびデスクトップへのアクセスを提供します。

NetScaler Gateway をDMZに展開することは、NetScaler Gateway がサーバーファームで動作する場合に最も一般的な構成です。この構成では、NetScaler Gateway は、Web Interfaceを介して公開リソースにアクセスするWebブラウザーおよびCitrix Workspace アプリに、安全な単一アクセスポイントを提供します。このセクションでは、この展開オプションの基本的な側面について説明します。

組織のネットワークの構成によって、NetScaler Gateway がサーバーファームで動作する場合の展開先が決まります。次の2つのオプションが使用できます：

- 組織が単一のDMZで内部ネットワークを保護している場合は、DMZにNetScaler Gateway を展開します。
- 組織が2つのDMZで内部ネットワークを保護している場合は、ダブルホップDMZ構成の2つのネットワークセグメントそれぞれに1つのNetScaler Gateway を展開します。詳細については、「ダブルホップDMZでのNetScaler Gateway の展開」を参照してください。 注：セキュアネットワーク内の2番目のNetScaler Gateway アプライアンスを使用して、ダブルホップDMZを構成することもできます。

DMZにNetScaler Gateway を展開してサーバーファームへのリモートアクセスを提供する場合は、次の3つの展開オプションのいずれかを実装できます。

- DMZのNetScaler Gateway の背後にWeb Interfaceを展開します。この構成では、次の図に示すように、NetScaler Gateway とWeb Interfaceの両方がDMZに展開されます。最初のユーザー接続はNetScaler Gateway に送信され、Web Interfaceにリダイレクトされます。 図1：DMZのNetScaler Gateway
  
- NetScaler Gateway をDMZのWeb Interfaceと並行して展開します。この構成では、NetScaler Gateway とWeb Interfaceの両方がDMZに展開されますが、最初のユーザー接続はNetScaler Gateway ではなくWeb Interfaceに送信されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- DMZにNetScaler Gateway を展開し、内部ネットワークにWeb Interfaceを展開します。この構成では、NetScaler Gateway はユーザーの要求を認証してから、要求をセキュアネットワーク内のWeb Interfaceに中継します。Web Interfaceは認証を実行しませんが、STAと対話してICAファイルを生成し、ICAトラフィックがNetScaler Gateway を介してサーバーファームにルーティングされるようにします。

Web Interfaceを配置する場所は、次のようなさまざまな要因によって異なります。

- 認証。ユーザーがログオンすると、NetScaler Gateway またはWeb Interfaceのいずれかがユーザー資格情報を認証できます。Web Interface をネットワークに配置する場所は、ユーザの認証先を部分的に決定する要素です。
- ユーザーソフトウェア。ユーザーは、NetScaler Gateway プラグインまたはCitrix Workspaceアプリのいずれかを使用してWeb Interfaceに接続できます。Citrix Workspaceアプリのみを使用してユーザーがアクセスできるリソースを制限したり、NetScaler Gateway プラグインを使用してユーザーにより大きなネットワークアクセスを提供したりできます。ユーザーの接続方法およびユーザーに接続を許可するリソースは、Web Interface をネットワーク内のどこに展開するかを決定するのに役立ちます。

Web Interface をセキュアなネットワークに展開する

この展開では、Web Interface はセキュアな内部ネットワークに存在します。NetScaler GatewayはDMZにあります。NetScaler Gateway は、Web Interfaceに要求を送信する前にユーザー要求を認証します。

セキュリティで保護されたネットワークにWeb Interfaceを展開するときは、NetScaler Gatewayで認証を構成する必要があります。

Citrix Virtual Apps and Desktops でWeb Interfaceを展開する場合、セキュリティで保護されたネットワークにWeb Interfaceを展開することが、デフォルトの展開シナリオです。Desktop Delivery Controllerをインストールすると、カスタムバージョンのWeb Interfaceもインストールされます。

重要

：Web Interfaceがセキュアネットワークにある場合は、NetScaler Gateway で認証を有効にする必要があります。ユーザーはNetScaler Gateway に接続し、資格情報を入力して、Web Interfaceに接続します。認証を無効にすると、認証されていない HTTP 要求は、Web Interface を実行しているサーバーに直接送信されます。NetScaler Gateway での認証の無効化は、Web InterfaceがDMZにあり、ユーザーがWeb Interfaceに直接接続する場合にのみ推奨されます。

図1：セキュアネットワーク内に配置された Web インターフェイス



© 1997–2026 Citrix Systems, Inc. All rights reserved.

DMZ内のNetScaler Gateway と並行してWeb Interfaceを展開する

この展開では、Web InterfaceとNetScaler Gateway の両方がDMZに存在します。ユーザーは、WebブラウザーまたはCitrix Workspace アプリを使用してWeb Interfaceに直接接続します。ユーザ接続は、最初に認証のために Web インターフェイスに送信されます。認証後、接続はNetScaler Gateway を介してルーティングされます。ユーザーは Web Interface に正常にログオンすると、サーバーファーム内の公開アプリケーションまたはデスクトップにアクセスできます。ユーザーがアプリケーションまたはデスクトップを起動すると、Web Interfaceは、Secure Gatewayを実行しているサーバーであるかのように、NetScaler Gatewayを介してICAトラフィックをルーティングするための命令を含むICAファイルを送信します。Web Interfaceによって配信されるICAファイルには、セキュア・チケット・オーソリティー (STA) によって生成されたセッション・チケットが含まれています。

Citrix Workspace アプリがNetScaler Gateway に接続すると、チケットが表示されます。NetScaler Gateway はSTAに接続してセッションチケットを検証します。チケットがまだ有効な場合、ユーザーのICAトラフィックはサーバーファーム内のサーバーに中継されます。次の図は、この展開を示しています。

図1：NetScaler Gateway と並行してインストールされたWeb Interface

Web InterfaceがDMZでNetScaler Gateway と並行して実行されている場合、NetScaler Gatewayで認証を構成する必要はありません。Web インターフェイスはユーザを認証します。

DMZのNetScaler Gateway の背後にWeb Interfaceを展開する

この構成では、NetScaler Gateway とWeb Interfaceの両方がDMZに展開されます。ユーザーがCitrix Workspace アプリでログオンすると、最初のユーザー接続はNetScaler Gateway に送信され、Web Interfaceにリダイレクトされます。すべてのHTTPSおよびICAトラフィックを単一の外部ポート経由でルーティングし、単一のSSL証明書を使用する必要がある場合、NetScaler Gateway はWeb Interfaceのリバースプロキシとして機能します。

図1：NetScaler Gateway の背後にあるWeb Interface

Web InterfaceがDMZのNetScaler Gateway の背後に展開されている場合、アプライアンスで認証を構成できますが、必須ではありません。どちらもDMZに存在するため、NetScaler Gateway またはWeb Interfaceのいずれかにユーザーを認証させることができます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Web Interfaceの機能

NetScaler Gateway のWeb Interfaceを構成する前に、Citrix Virtual Apps WebサイトとCitrix Virtual Appsサービスサイトの違いを理解する必要があります。

- **Citrix Virtual Apps の Web サイト。**Web Interfaceは、Citrix Virtual Apps Webサイトを作成および管理する機能を提供します。ユーザーは、Web ブラウザーとプラグインを使用して、公開リソースとストリーム配信アプリケーションにリモートでアクセスします。
- **Citrix Virtual Apps サービスサイト。**Citrix Virtual Apps は、柔軟性と構成の容易さを追求して設計されたプラグインです。Web InterfaceでCitrix Virtual Apps ServicesサイトでCitrix Virtual Apps Servicesを使用すると、公開リソースをユーザーのデスクトップと統合できます。ユーザーは、デスクトップまたは メニューのアイコンをクリックするか、コンピュータデスクトップの通知領域をクリックして、リモートアプリケーション、ストリーム配信アプリケーション、リモートデスクトップおよびコンテンツにアクセスします。オーディオ、表示、ログオンの設定など、ユーザーがアクセスおよび変更できる構成オプションを決定できます。

  注：
  このオプションを選択すると、仮想デスクトップへのアクセスはサポートされません。

詳しくは、Citrix 製品ドキュメントを参照してください。

Web Interfaceのサイトのセットアップ

Web Interfaceをセキュアネットワークに展開し、NetScaler Gateway で認証を構成する場合、ユーザーがNetScaler Gateway に接続すると、アプライアンスはユーザーを認証します。

重要：

NetScaler Gateway を構成する前に、Web Interfaceをインストールして構成します。詳しくは、Citrix 製品ドキュメントの「Web Interface」ドキュメントを参照してください。

Web Interface サイトを作成する手順は次のとおりです：

- ユーザーのログオン方法を選択します。Webブラウザ、NetScaler Gateway プラグイン、またはCitrix Workspace アプリからログオンできます。詳細については、「Web インターフェイスの機能」を参照してください。
- ユーザーの認証元を特定します。NetScaler Gateway またはWeb Interface。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注：

Web Interfaceがセキュアネットワークにある場合は、NetScaler Gateway 上の仮想サーバーで認証を有効にします。認証を無効にすると、認証されていない HTTP 要求は、Web Interface を実行しているサーバーに直接送信されます。NetScaler Gateway での認証の無効化は、Web InterfaceがDMZにあり、ユーザーがWeb Interfaceに直接接続する場合にのみ推奨されます。

NetScaler Gateway に有効なサーバー証明書をインストールしてください。証明書の操作の詳細については、「 証明書のインストールと管理」を参照してください。

重要：

Web InterfaceをNetScaler Gateway 10.1で正常に動作させるには、Web Interfaceを実行しているサーバーがNetScaler Gateway 証明書を信頼し、仮想サーバーの完全修飾ドメイン名（FQDN）を正しいIPアドレスに解決できる必要があります。

Web インターフェイス 5.4 サイトの作成

Citrix Web Interface管理コンソールは、Microsoft管理コンソール（MMC）3.0スナップインであり、Microsoftインターネットインフォメーションサービス（IIS）でホストされているCitrix Virtual Apps Webサイトおよびcitrix仮想アプリケーションサービスサイトを作成および構成できます。Web Interface サイトの種類が左側のウィンドウに表示されます。中央の結果ウィンドウには、左ペインで選択したサイトタイプコンテナ内で使用可能なサイトが表示されます。

Citrix Web Interface管理コンソールを使用すると、日常的な管理タスクをすばやく簡単に実行できます。 ペインには、現在使用可能なタスクが一覧表示されます。左ペインで選択したアイテムに関連するタスクが上部に表示され、結果ウィンドウで選択したアイテムに対して実行可能なアクションが表示されます。

コンソールを使用する場合、コンソールを使用して変更をコミットすると、設定が有効になります。その結果、一部の Web Interface 設定の値が現在の設定に関連せず、対応する設定が WebInterface.conf のデフォルト値にリセットされると、無効になることがあります。サイトの WebInterface.confファイルと config.xml ファイルのバックアップを定期的に作成することをお勧めします。

Citrix Web Interface管理コンソールは、Microsoftインターネットインフォメーションサービス用のWeb Interfaceをインストールすると自動的にインストールされます。［スタート］>［すべてのプ

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ログラム］>［Citrix］>［管理コンソール］>［Citrix Web Interface管理］の順にクリックして、コンソールを実行します。

注

：Web Interfaceをインストールするサーバー上にMMC 3.0が存在することを確認します。これは、Citrix Web Interface管理コンソールをインストールするための前提条件です。MMC 3.0 は、Web インターフェイスをホストするためにサポートされているすべての Windows プラットフォームで既定で利用できます。

設定ファイルの使用

次の構成ファイルを編集して、Web Interface サイトを構成できます。

- Web Interface構成ファイル：Web インターフェイスの設定ファイル WebInterface.conf を使用すると、多くの Web インターフェイスのプロパティを変更できます。Microsoft インターネットインフォメーションサービス (IIS) と Java アプリケーションサーバーの両方で使用できます。このファイルを使用して、日常的な管理タスクを実行し、さらに多くの設定をカスタマイズできます。WebInterface.conf の値を編集し、更新したファイルを保存して変更を適用します。WebInterface.confを使用したWeb Interfaceの構成について詳しくは、Citrix 製品ドキュメントの［テクノロジー］ノードにあるWeb Interfaceのドキュメントを参照してください。
- Citrix オンラインプラグイン構成ファイル。Web Interfaceサーバー上の config.xml ファイルを使用して、Citrix オンラインプラグインを構成できます。

Citrix Web Interface管理コンソールを使用したサイトの構成

Citrix Web Interface管理コンソールは、Microsoft管理コンソール（MMC）3.0スナップインであり、Microsoftインターネットインフォメーションサービス（IIS）でホストされているCitrix Virtual Apps WebサイトおよびCitrix仮想アプリケーションサービスサイトを作成および構成できます。Web Interface サイトの種類が左側のウィンドウに表示されます。中央の結果ウィンドウには、左ペインで選択したサイトタイプコンテナ内で使用可能なサイトが表示されます。

Citrix Web Interface管理コンソールを使用すると、日常的な管理タスクをすばやく簡単に実行できます。 ペインには、現在使用可能なタスクが一覧表示されます。左ペインで選択したアイテムに関連するタスクが上部に表示され、結果ペインで選択したアイテムに対して実行可能なアクションが下に表示されます。

コンソールを使用する場合、コンソールを使用して変更をコミットすると、設定が有効になります。その結果、一部の Web Interface の設定は、その値が現在の設定に関連せず、WebInterface.conf で対応する設定がデフォルト値にリセットされた場合に無効になることがあり

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ます。サイトのWebInterface.confファイルと config.xml ファイルのバックアップを定期的に作成することをお勧めします。

Citrix Web Interface管理コンソールは、Microsoft IIS用Web Interfaceをインストールすると自動的にインストールされます。［スタート］>［すべてのプログラム］>［Citrix］>［管理コンソール］>［Citrix Web Interface管理］の順にクリックして、コンソールを実行します。

注：Web Interfaceをインストールするサーバー上にMMC 3.0が存在することを確認する必要があります。これは、Citrix Web Interface管理コンソールをインストールするための前提条件です。MMC 3.0 は、Web インターフェイスをホストするためにサポートされているすべての Windows プラットフォームで既定で利用できます。

Web InterfaceでのNetScaler Gateway 設定の構成 5.4

展開環境でNetScaler Gateway を使用するには、アプライアンスをサポートするWeb Interfaceを構成する必要があります。これを行うには、Citrix Web Interface管理コンソールで［ Secure Access ］タスクを使用します。

Web InterfaceでNetScaler Gateway 設定を構成するには

1. **Windowsの［スタート ］メニューで、［ すべてのプログラム］、［Citrix］、［管理コンソール］、［Citrix Web Interface管理］の順にクリックします。**
2. Citrix Web Interface管理コンソールの左側のペインで、［ **Citrix Virtual Apps ウェブサイト］または［Citrix Virtual Apps サービスサイト］のいずれかをクリックし、** 結果ペインでサイトを選択します。
3. **アクション**ペインで 、「 セキュアアクセス」をクリック**します。**
4. ページで、次のいずれかの操作を行います。
   - をクリックして、新しいアクセスルートを追加します。
   - リストから既存のルートを選択し、 をクリックします。
5. リストから、次のいずれかのオプションを選択します。
   - Citrixサーバーの実際のアドレスをNetScaler Gateway に送信する場合は、［NetScaler Gateway**ダイレクト**］を選択します。
   - Citrix Virtual Apps サーバーの代替アドレスをNetScaler Gateway に送信する場合は、［ **代替ゲートウェイ**］を選択します。

   注：Citrix Virtual Desktops 仮想デスクトップは、代替アドレスが使用されているとアクセスできません。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- NetScaler Gateway に付与されるアドレスを、Web Interfaceで設定されたアドレス変換マッピングによって決定する場合は、［**変換されたゲートウェイ**］を選択します。

6. クライアントネットワークを識別するネットワークアドレスとサブネットマスクを入力します。 **ボタンと ボタンを使用して、アクセスルートを優先順に [ユーザデバイスアドレステーブル（User device addresses**
7. ゲートウェイアドレス変換を使用していない場合は、ステップ 10 に進みます。ゲートウェイアドレス変換を使用している場合は、 ページで次のいずれかを実行します。

   - 「 **追加** 」をクリックして、新しい住所翻訳を追加します。
   - リストから既存のアドレス変換を選択し、 をクリックします。

   8\.「 **アクセスタイプ」領域で**、次のオプションのいずれかを選択します：

   - NetScaler Gateway で変換されたアドレスを使用してCitrixサーバーに接続する場合は、［**ゲートウェイルート変換**］を選択します。
   - ［ユーザーデバイスアドレス］表でクライアント変換ルートを構成し、CitrixクライアントとNetScaler Gateway の両方で変換後のアドレスを使用してCitrixサーバーに接続する場合は、［ユーザーデバイスとゲートウェイのルート変換］を選択します。

8. Citrix サーバーの内部ポートと外部（変換済み）ポートとアドレスを入力し、［**OK**］ 、［**次へ**］の順にクリックします。 NetScaler Gateway がCitrix サーバーに接続すると、外部ポート番号とアドレスが使用されます。作成するマッピングが、サーバファームで使用されているアドレッシングのタイプと一致することを確認します。
9. ［ゲートウェイ設定の指定］ページで、クライアントが使用する必要があるNetScaler Gateway アプライアンスの完全修飾ドメイン名（FQDN）とポート番号を指定します。FQDN は、ゲートウェイにインストールされている証明書にあるものと一致する必要があります。
10. クライアントが自動的に再接続を試みる間、切断されたセッションを開いたままにしておくには、［ **セッション保持を有効にする** ］を選択します。
11. セッション画面の保持を有効にし、2つのSecure Ticket Authority（STA）サーバーから同時にチケットを発行する場合は、［ **2つのSTAからチケットを要求する** ］を選択します。このオプションを有効にすると、Web Interfaceは2つの異なるSTAからチケットを取得します。これにより、セッション中に1つのSTAが使用できなくなっても、ユーザー・セッションが中断されることはありません。何らかの理由で Web Interface が 2 つの STA に接続できない場合は、単一の STA を使用するようにフォールバックします。 **［次へ］** をクリックします。
12. ページで、次のいずれかの操作を行います。

    - をクリックして、Web インターフェイスで使用できる STA の URL を指定します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- リストからエントリを選択し、 をクリックします。

および ボタンを使用して、STAを優先順に配置します。 STA は、Citrix XML サービスに含まれています（`http\[s\]://servername.domain.com/scripts/ctxsta.dll` など）。

フォールトトレランスには、複数の STA を指定できます。ただし、この目的のために外部ロードバランサーを使用しないことをお勧めします。

13. を選択して、STA間の負荷分散を有効にするかどうかを選択します。

    負荷分散を有効にすると、サーバー間で接続を均等に分散できるため、サーバーが過負荷になることはなくなります。

14. を選択して、到達不能な STAをバイパスする必要がある時間の長さを指定します。

    Web Interface は、STA URL リストのサーバ間でフォールトトレランスを提供するため、通信エラーが発生した場合、障害が発生したサーバは指定された期間バイパスされます。

Web インターフェイス 5.3 サイトの作成

Web Interface 5.3サイトを作成するときに、Webブラウザ、Citrix Workspaceアプリ、またはCitrix デスクトップのCitrix Workspace アプリのいずれかを使用してログオンするようにユーザーに要求できます。Citrix Web Interface管理コンソールを使用して、複数のWeb Interfaceサイトを作成できます。

Web Interface 5.3 を使用した Web Interface に対しては、スマートカードを使用したシングルサインオンのみを有効にできます。このバージョンのWeb Interfaceは、Citrix Virtual Apps 4.5、5.0、および6.0で実行できます。

Web Interface 5.3 は、次のオペレーティングシステムで動作します。

- Windows Server 2003
- Windows Server 2008
- Windows Server 2008 R2

注

- Citrix Virtual Apps 6.0 は、Windows Server 2008 R2 でのみ動作します。

Web Interface 5.3のサイトを作成するには

1. 「**スタート**」>「**すべてのプログラム**」>「**Citrix**」>「**管理コンソール**」>「**Citrix Webインターフェイス管理**」をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. 左側のペインで、［Citrix Virtual Apps ウェブサイト］を選択します。ユーザは Web ブラウザを使用して Web インターフェイスにログオンします。
3. メニューの をクリックします。
4. 既定のインターネットインフォメーションサービス (IIS) サイトとパスをそのままにして、 をクリックします。

   デフォルトのサイトパスは /Citrix/Citrix Virtual Appsです。または、パスを指定できます。

   注

   ：デフォルトのパスを使用する既存のCitrix Virtual Apps Webサイトがある場合は、新しいサイトを区別するために適切な増分が追加されます。

5. で、次のいずれかを選択します：

   - Web インターフェイスで、Web インターフェイスを使用してユーザを認証します。

     Web Interfaceが非武装地帯（DMZ）のNetScaler Gateway と並行してスタンドアロンサーバーとして展開されている場合は、このオプションを選択します。

   - Access Gateway で、NetScaler Gateway アプライアンスを使用してユーザーを認証します。

     このオプションを選択すると、NetScaler Gateway はユーザーを認証し、アプライアンスでWeb Interfaceが構成されている場合は、Web Interfaceへのシングルサインオンを開始します。

   注

   ：SmartAccess がNetScaler Gateway で構成されている場合、この設定により、Citrix Virtual Apps and Desktops でSmartAccess が有効になります。

6. **［次へ］** をクリックします。
7. 手順5では、［認証サービスのURL］に、NetScaler Gateway 認証サービスのURLへのWebアドレス（`https://access.company.com/CitrixAuthService/AuthService.asmx` など）を入力し、［ **次へ**］をクリックします。
8. で、 **ユーザーのログオン方法を選択します。**

   - **エクスプリシット。**ユーザーは Web ブラウザを使用してログオンします。
   - **スマートカード。**ユーザーはスマートカードを使用してログオンします。

9. **［次へ］** をクリックします。
10. 手順 8 で を選択した場合は、次のいずれかを選択します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- ユーザに PIN の入力を求めます。ユーザーは、公開アプリケーションまたはデスクトップを起動するときに、暗証番号 (PIN) を入力します。
- ユーザーは、公開アプリケーションまたはデスクトップを起動するときに PIN を入力する必要はありません。

概要画面に設定が表示されます。

11. をクリックして Web Interface サイトを作成します。サイトが正常に作成されると、Web Interface で残りの設定を構成するように求められます。ウィザードの指示に従って構成を完了します。

Web Interface 5.3でのNetScaler Gateway 設定の構成

Web Interface5.3サイトを作成したら、Citrix Web Interface管理を使用してNetScaler Gateway の設定を構成できます。

NetScaler Gateway のWeb Interface5.3設定を構成するには

1. 「**スタート**」>「**すべてのプログラム**」>「**Citrix**」>「**管理コンソール**」>「**Citrix Webインターフェイス管理**」をクリックします。
2. ［Citrix Web Interface管理］の左側のペインで、［**Citrix Virtual Apps Webサイト**］をクリックします。
3. アクションペインで、「**Secure Access**」をクリックします。
4. **［セキュアアクセス設定の編集］**ダイアログボックスの**［追加］**をクリックします。
5. **アクセスルートの追加ダイアログボックスで** 、ユーザーデバイスのアドレスとサブネットマスクを入力し、「**アクセス方法**」で「**Gateway direct**」を選択し、「**OK」**をクリックして「**次へ**」をクリックします。ユーザーデバイスアドレスとサブネットマスクを指定しない場合、Gateway direct オプションはすべてのユーザーデバイスに適用されます。 オプションは、内部ネットワークの外部から接続するユーザーデバイスに適していますが、 オプションは、内部ネットワーク内から接続するユーザーデバイスに適しています。
6. に、NetScaler Gateway の完全修飾ドメイン名（FQDN）を入力します。これは、NetScaler Gateway 証明書で使用されているのと同じFQDNである必要があります。
7. **［Port］**ボックスにポート番号を入力します。デフォルトは 443 です。
8. セッションの保持を有効にするには、 をクリックし、 をクリックします。
9. 「**Secure Ticket Authority URL**」で、「**追加**」をクリックします。
10. 「**Secure Ticket Authority URL**」に、Citrix Virtual AppsでXMLサービスを実行しているマスターサーバーの名前を入力し、「**OK」**をクリックし、「**完了**」をクリックします。たとえば、`http://Citrix Virtual Appssrv01/Scripts/CtxSta.dll`と入力します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Web Interfaceで設定を構成したら、NetScaler Gateway で設定を構成できます。

単一サイトへのCitrix Virtual Apps and Desktops の追加

Citrix Virtual Apps and Desktopsを実行している場合は、両方のアプリケーションを1つのWeb Interfaceサイトに追加できます。この構成では、Citrix Virtual Apps and Desktops のいずれかから同じSecure Ticket Authority（STA）サーバーを使用できます。

注

: Citrix Virtual Desktops はWeb Interfaceをサポートしています。Web インターフェイスの最低限必要なバージョンは 5.0 です。

Web Interface 5.3または5.4を使用している場合は、Web Interface管理コンソールを使用して、Citrix Virtual Apps and Desktops サイトを組み合わせます。

注

: サーバーファームが異なるドメインにある場合は、ドメイン間で双方向の信頼を確立する必要があります。

Web Interface 5.3または5.4を使用してCitrix Virtual Apps and Desktops を単一のサイトに追加するには

1. > > > > をクリックします。
2. 左側のペインで、［**Citrix Virtual Apps のWebサイト**］を選択します。
3. ウィンドウで、サイトを右クリックし、 をクリックします。
4. ダイアログボックスで、 をクリックします。
5. サーバーファームの設定を完了し、［**OK**］ を 2 回クリックします。

Citrix Virtual Desktops を使用するときに最適なエクスペリエンスを実現するには、WebInterface.conf構成ファイルで［ユーザーインターフェイスのブランド］設定を［デスクトップ］に変更します。

NetScaler Gateway を介したユーザー接続のルーティング

Citrix Virtual Apps and Desktops では、NetScaler Gateway 経由でルーティングされる接続のみを受け入れるようにサーバーを構成できます。Citrix XenApp 6.5では、Citrix AppCenterでNetScaler Gateway経由で接続をルーティングするポリシーを構成します。Citrix Virtual Desktops 7.1 では、Citrix Studio を使用して設定を構成します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix XenApp 6.5サーバーのプロパティを構成して、NetScaler Gateway 経由でルーティングされた接続のみを受け入れるようにするには

1. スタート > 管理ツール > Citrix > 管理コンソール > Citrix AppCenter をクリックします。
2. ［NetScalerリソース］> Citrix Virtual Apps］>［ファーム名］の順に展開します。ここで、FarmNameはサーバーファームの名前です。
3. をクリックします。
4. 中央のウィンドウで、 または をクリックし、 をクリックします。
5. ウィザードの にポリシーの名前を入力し、 をクリックします。
6. で、 をクリックします。
7. **の の横にある をクリックします。
8. ［ **設定の追加-接続アクセス制御** ］ダイアログボックスの［ **値］で、［Citrix Access Gateway 接続のみ］を選択し** 、［ **OK］**をクリックします。
9. を 2 回クリックし** 、 をクリックします。Citrix Virtual Apps によってポリシーが作成されます。

NetScaler Gateway を介してルーティングされた接続のみを受け入れるようにCitrix 仮想デスクトップサーバーのプロパティを構成するには

デリバリーグループのマシンへのアクセスを制限できます。NetScaler Gateway を介して行われるユーザー接続をフィルタリングするSmartAccessを使用して、ユーザーのアクセスを制限できます。このタスクは、Studioの［ポリシー］ノード、 またはクイックリファレンスの表で説明されているポリシー設定を使用して実行できます。

1. Studioの［デリバリーグループ］で、制限するデリバリーグループを選択します。
2. ［デリバリーグループの編集］をクリックし、［アクセスポリシー］をクリックします。
3. ［アクセスポリシー］ページで、［NetScaler Gateway を介した接続］を選択します。NetScaler Gateway を介した接続のみが許可されます。
4. これらの接続のサブセットを選択するには、 を選択します。
   a. NetScaler Gateway サイトを定義します。
   b. デリバリーグループの許可されたユーザーアクセスのシナリオを定義するSmartAccess文字列を追加、編集、または削除します。SmartAccess の構成について詳しくは、「NetScaler Gateway でのSmartAccess 構成」を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Web インターフェイスとの通信の設定

NetScaler Gateway を構成して、Citrix Virtual Apps and Desktopsで実行されているWeb Interfaceと通信できます。これを行うには、NetScaler Gateway で仮想サーバーを構成します。次に、署名付きサーバー証明書と認証、セッション、事前認証、および認証後のポリシーを仮想サーバーにバインドします。NetScaler Gateway は、仮想サーバーのIPアドレスを使用して、ユーザー接続をWeb Interfaceにルーティングします。

公開アプリケーションウィザードを使用すると、ユーザー接続をWeb Interfaceにルーティングするように NetScaler Gateway を構成できます。NetScaler Gateway は、ユーザー接続にSecure Ticket Authority（STA）を使用します。

公開アプリケーションとデスクトップのポリシーの構成

Citrix Virtual Apps and Desktops サーバーとの通信を確立するには、サーバーを認識するように NetScaler Gateway を構成する必要があります。設定をグローバルに構成することも、ユーザー、グループ、または仮想サーバーにバインドされたポリシーを使用することもできます。

NetScaler Gateway でWeb Interfaceをグローバルに構成するには

1. ナビゲーションペインにある、［Configuration］タブの構成ユーティリティで、［NetScaler Gateway］を展開し、［Global Settings］をクリックします。
2. 詳細ペインの で、 をクリックします。
3. ［グローバルNetScaler Gateway 設定］ダイアログボックスの［クライアントエクスペリエンス］タブで、次の操作を行います。

   a. 「プラグイン・タイプ」で「Java」を選択します。

   b. で、 を選択します。

   注

   ：iOS向けCitrix WorkspaceアプリやAndroid向けCitrix Workspace アプリなど、VPN対応のCitrix Workspace Citrix Workspace アプリをサポートするには、手順3を実行します。モバイルCitrix Workspace アプリをサポートするには、アクセスゲートウェイ10、ビルド69.6、またはアクセスゲートウェイ10、ビルド71.6014.e以上をインストールする必要があります。Access Gateway 9.3 を実行している場合は、この手順を実行する必要はありません。

4. タブで、 の横にある を選択します。
5. ［Web Interfaceアドレス］の横に、Web Interfaceの Web アドレスを入力し、［ **OK］**をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Web Interface のセッションポリシーを構成するには

セッションポリシーを構成し、それを仮想サーバーにバインドして、Web Interface へのアクセスを制限できます。

1. 構成ユーティリティの［ 構成 ］タブのナビゲーションペインで、［ NetScaler Gateway ポリシー ］を展開し、［ セッション］をクリックします。
2. 詳細ペインの タブで、 をクリックします。
3. ダイアログボックスの に、ポリシーの名前を入力します。
4. 「リクエストプロファイル」の横にある「 新規」をクリックします。
5. ダイアログボックスの に、プロファイルの名前を入力します。
6. タブで、次の操作を行います。
    a. プラグイン・タイプの横にある「グローバルを上書き」を選択し、「Java」を選択します。
    b. の横にある を選択し、 を選択します。
7. ［ICAプロキシ］の横にある［グローバル上書き］をクリックして［オン］を選択します
8. の横にある をクリックし、Web インターフェイスの Web アドレスを入力して、 をクリックします。
9. ダイアログボックスで、 の横にある を選択し、 を選択し、 をクリックして をクリックし、 をクリックします。

セッションポリシーを作成したら、ポリシーを仮想サーバーにバインドします。

セッションポリシーを仮想サーバーにバインドするには

1. 構成ユーティリティの［構成］タブのナビゲーションペインで、［ NetScaler Gateway ］を展開し、［ 仮想サーバー］をクリックします。
2. 詳細ペインで仮想サーバーを選択し、 をクリックします。
3. タブで、、 の順にクリックします。
4. リストからセッションポリシーを選択し、優先度番号（オプション）を入力して、［OK］をクリックします。

公開アプリケーションウィザードで設定を構成する

Web Interfaceを使用してNetScaler Gateway を構成するには、次の情報が必要です。

- Citrix Virtual Apps and Desktops を実行しているサーバーのIPアドレス。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Web Interface を実行しているサーバーの完全修飾ドメイン名 (FQDN)。
- NetScaler Gateway で構成された仮想サーバー。
- SmartAccess 用に設定されたセッションポリシー。
- Web インターフェイスフェールオーバーを設定している場合は、Web インターフェイスを実行している追加サーバの IP アドレス。

公開アプリケーションウィザードを使用して Web Interface の設定を構成するには

1. 構成ユーティリティで、［構成］タブをクリックし、ナビゲーションペインで［ NetScaler Gateway］をクリックします。
2. 詳細ウィンドウの で、 をクリックします。
3. をクリックし、ウィザードの指示に従います。

公開アプリケーションウィザード内から Secure Ticket Authority (STA) を構成してアクティブ化できます。公開アプリケーションウィザードを完了すると、設定はグローバルにバインドされます。

NetScaler Gateway でのSecure Ticket Authority 構成

Secure Ticket Authority（STA）は、Citrix Virtual Apps上の公開アプリケーションおよびCitrix Virtual Desktops上の公開デスクトップに対する接続要求に応答して、セッションチケットを発行します。これらのセッションチケットは、公開リソースへのアクセスに対する認証と承認の基礎を形成します。

STA はグローバルにバインドすることも、仮想サーバにバインドすることもできます。仮想サーバを構成するときに、STA を実行している複数のサーバを追加することもできます。

NetScaler Gateway とSTA間の通信をセキュリティで保護する場合は、STAを実行しているサーバーにサーバー証明書がインストールされていることを確認してください。

一般的なNetScaler Gateway GSLB展開では、再接続の問題を回避するために、（各サイトの）すべてのゲートウェイ仮想サーバーを同じバックエンドSTAサーバーで構成する必要があります。

STA をグローバルにバインドするには

1. ［ **NetScaler Gateway］>［グローバル設定］**に移動します。
2. 詳細ペインの で、Secure Ticket Authority が使用する **STA サーバーのバインド/**バインド解除をクリックします 。
3. ダイアログボックスで、 をクリックします。
4. ［ **STA サーバーの構成** ］ダイアログボックスで、STA サーバーの URL を入力し、［ **作成**］、［ **OK］**の順にクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. ダイアログボックスの に、STA を実行しているサーバーの IP アドレスまたは完全修飾ドメイン名 (FQDN) を入力し、 をクリックします。

注

. STA を実行している複数のサーバをリストに追加できます。Web Interfaceに表示されるSTAは、NetScaler Gateway で構成されているSTAと一致する必要があります。複数のSTAを構成する場合は、NetScaler Gateway とSTAを実行しているサーバーとの間で負荷分散を使用しないでください。

STA を仮想サーバーにバインドするには

1. ［**NetScaler Gateway**］>［**仮想サーバー**］に移動します。
2. 詳細ペインで、仮想サーバーを選択し、 をクリックします。
3. 「**公開アプリケーション**」タブの「Secure Ticket Authority」で、「**追加**」をクリックします。
4. ダイアログボックスで、STA サーバーの URL を入力し、 をクリックします。
5. ステップ 4 を繰り返して STA サーバーを追加し、「**OK**」をクリックします。

参照ドキュメント

- STAについて詳しくは、「NetScaler GatewaySecure Ticket Authority」の記事を参照してください。
- Cloud Connector をSecure Ticket Authority（STA）サーバーとして使用するようにNetScaler Gateway を構成する方法の詳細については、「Cloud Connector をSTAとして使用するようにNetScaler Gateway を構成するにはどうすればよいですか」を参照してください。

NetScaler Gateway での追加のWeb Interface設定の構成

NetScaler Gateway をWeb Interface環境に展開する場合は、次のオプションタスクを実行できます。

- Web Interfaceフェイルオーバーの構成Web Interfaceを実行しているセカンダリサーバーにフェイルオーバーするようにNetScaler Gateway を構成します。
- Web Interfaceを使用したスマートカードアクセスの構成 Citrix Workspace アプリとスマートカード認証を使用して、Web Interfaceに直接ログオンするようにユーザーセッションを構成します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Web インターフェイスフェールオーバーの設定

公開アプリケーションウィザードを使用して、Web Interfaceを実行しているセカンダリサーバーにフェイルオーバーするようにNetScaler Gateway を構成できます。

Web インターフェイスフェールオーバーにより、プライマリ Web インターフェイスに障害が発生しても、ユーザ接続をアクティブのままにできます。フェールオーバーを設定するときは、システム IP アドレス、マッピング IP アドレス、または仮想サーバの IP アドレスに加えて、新しい IP アドレスを定義します。新しい IP アドレスは、システムまたはマッピング IP アドレスと同じサブネット上にある必要があります。

NetScaler Gateway でWeb Interfaceフェイルオーバーを構成すると、新しいIPアドレスに送信されるネットワークトラフィックはすべてプライマリWeb Interfaceに中継されます。公開アプリケーションウィザードで選択した仮想サーバーは、ネットワークアドレス変換 (NAT) IP アドレスとして機能します。実際の IP アドレスは、Web インターフェイスの IP アドレスです。プライマリ Web インターフェイスに障害が発生すると、ネットワークトラフィックはセカンダリ Web インターフェイスに送信されます。

Web インターフェイスフェールオーバーを設定するには

1. 構成ユーティリティで、［構成］タブをクリックし、ナビゲーションペインで［ NetScaler Gateway］をクリックします。
2. 詳細ウィンドウの で、 をクリックします。
3. をクリックし、仮想サーバーを選択して、 をクリックします。
4. ページで、 をクリックします。
5. の に、プライマリ Web インターフェイスの IP アドレスを入力します。
6. に、プライマリ Web インターフェイスのポート番号を入力します。
7. に、フェイルオーバー用の新しい IP アドレスを入力します。
8. に、仮想サーバーのポート番号を入力します。
9. の に、Web インターフェイスを実行しているサーバーの IP アドレスを入力するか、一覧からサーバーを選択します。
10. 「Web Interface サーバーポート」に Web インターフェイスのポート番号を入力し、「OK」をクリックします。
11. をクリックし、指示に従ってウィザードを完了します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Web インターフェイスを使用したスマートカードアクセスの構成

スマートカード認証を使用するようにWeb Interfaceを構成すると、ユーザーのログオン方法に応じて、NetScaler Gateway を統合するために次の展開シナリオを構成できます：

- ユーザーがCitrix Workspace アプリとスマートカード認証を使用してWeb Interfaceに直接ログオンする場合、Web InterfaceはDMZ内のNetScaler Gateway と並列である必要があります。Web Interface を実行しているサーバーも、ドメインメンバーである必要があります。

  このシナリオでは、NetScaler Gateway とWeb Interfaceの両方がSSLターミネーションを実行します。Web Interface は、ユーザー認証、公開アプリケーションの表示、公開アプリケーションの起動など、セキュリティで保護された HTTP トラフィックを終了します。NetScaler Gateway は、着信ICA接続のSSLを終了します。
- ユーザーがNetScaler Gateway プラグインを使用してログオンすると、NetScaler Gateway が初期認証を実行します。NetScaler Gateway がVPNトンネルを確立すると、ユーザーはスマートカードを使用してWeb Interfaceにログオンできます。このシナリオでは、DMZまたはセキュアネットワーク内のNetScaler Gateway の背後にWeb Interfaceをインストールできます。

注

: NetScaler Gateway は、クライアント証明書を使用した認証にスマートカードを使用することもできます。

詳細については、「スマートカード認証の構成」を参照してください。

Web Interface でのアプリケーションおよび仮想デスクトップへのアクセスの構成

ReceiverではなくNetScaler Gateway プラグインを使用して、公開アプリケーションおよび仮想デスクトップにユーザーがアクセスできるようにNetScaler Gateway を構成できます。アプリケーションとデスクトップへのアクセスを構成するには、NetScaler Gateway の構成を「Receiverのみを使用してNetScaler Gateway に接続する」から、Web InterfaceへのシングルサインオンでNetScaler Gatewayプラグインを使用した接続を有効にする構成に変更します。たとえば、すべてのユーザーがNetScaler Gateway プラグインを使用して接続し、Web Interfaceをホームページとして使用するようにNetScaler Gateway を構成します。このシナリオでは、Web Interface へのシングルサインオンがサポートされています。

アプリケーションやデスクトップへのアクセスに加えて、ユーザーは、VPN トンネルを介してネットワーク接続を行うユーザーデバイスにインストールされたアプリケーションを実行することもできます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

設定を開始するには、次のガイドラインに従ってください。

- Web インターフェイスサイトを作成します。
- アクセス制御の詳細設定を構成します。
- SmartAccess 構成します。
- NetScaler Gateway でエンドポイント分析を構成します。
- Citrix Virtual Apps and Desktopsでポリシーとフィルターを構成します。
- ユーザーがNetScaler Gateway プラグインを使用してログオンし、公開アプリケーションと仮想デスクトップにアクセスするようにNetScaler Gateway を構成します。

詳しくは、Citrix 製品ドキュメントの以下のトピックを参照してください。

- Web インターフェイスサイトの設定。
- SmartAccess がCitrix Virtual Apps and Desktops どのように機能するのか
- エンドポイントポリシーの設定
- Citrix Virtual Apps ポリシーとフィルターの構成
- Citrix Virtual Desktops でポリシーとフィルターを構成するには 5
- Web Interfaceと通信するためのNetScaler Gateway の構成

Citrix Virtual Apps and Desktops へのユーザーログオンを構成するときは、最初にセッションプロファイルを作成して、NetScaler Gateway for Windows プラグインを選択します。次に、Citrix Virtual Apps、Citrix Virtual Desktops、およびWeb Interfaceにアクセスするためのイントラネットアプリケーションのプロファイルを作成します。

アプリケーションおよびデスクトップにアクセスするためのNetScaler Gateway プラグインのグローバル設定を構成するには

1. ナビゲーションペインにある、［Configuration］タブの構成ユーティリティで、［NetScaler Gateway］を展開し、［Global Settings］をクリックします。
2. 詳細ペインの で、 をクリックします。
3. タブで、 の横にある を選択します。
4. に、Web インターフェイスサイトの URL を入力します。これがユーザーのホームページになります。
5. に、Active Directory ドメイン名を入力します。
6. ［クライアントエクスペリエンス］タブで、［プラグインの種類］の横にある［Windows/Mac OS X］を選択し、［OK］をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

イントラネットアプリケーションを構成するには

1. 構成ユーティリティの［構成］タブのナビゲーションペインで、［**NetScaler Gateway**］> ［**リソース**］の順に展開し、［イントラネットアプリケーション］をクリックします。
2. 詳細ペインで、［Add］ をクリックします。
3. に、アプリケーションの名前を入力します。
4. をクリックします。
5. で、、、または を選択します。
6. で、 と を選択します。たとえば、172.16.100.0 とサブネットマスク 255.255.255.0 と入力して、172.16.100.x サブネット上のすべてのサーバーを表します。Web Interface、Citrix Virtual Apps、およびユーザーが接続する他のすべてのサーバーのIPアドレスは、イントラネットアプリケーションとして定義されたサブネットの1つにある必要があります。

   イントラネットアプリケーションを作成したら、グローバルにバインドすることも、仮想サーバーにバインドすることもできます。
7. に、内部ネットワークを表す IP アドレスとサブネットマスクを入力し、、 の順にクリックします。

   イントラネットアプリケーションを作成したら、グローバルにバインドすることも、仮想サーバーにバインドすることもできます。

イントラネットアプリケーションをグローバルにバインドするには

1. ナビゲーションペインにある、［Configuration］タブの構成ユーティリティで、［NetScaler Gateway］を展開し、［Global Settings］をクリックします。
2. 詳細ペインの［イントラネットアプリケーション］で、［ NetScaler Gateway Plug-in for Java のセキュアネットワーク内のTCPアプリケーションへのマッピングの作成］をクリックします。
3. ダイアログボックスで、 をクリックします。
4. ［使用可能］で、1つ以上のイントラネットアプリケーションを選択し、矢印をクリックしてイントラネットアプリケーションを［構成済み］に移動し、［OK］をクリックします。

イントラネットアプリケーションを仮想サーバーにバインドするには

1. 構成ユーティリティの［構成］タブのナビゲーションペインで、［ NetScaler Gateway ］を展開し、［ 仮想サーバー］をクリックします。
2. 詳細ペインで仮想サーバーを選択し、 をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. NetScaler Gateway 仮想サーバーの構成ダイアログボックスで、「イントラネットアプリケーション」タブをクリックします。
4. 「使用可能なアプリケーション名」で、イントラネットアプリケーションを選択し、「追加」をクリックして、「OK」をクリックします。

ユーザーがNetScaler Gateway プラグインを使用してログオンすると、VPNトンネルが確立され、受信側またはWeb Interfaceのいずれかがホームページとして使用されます。

SmartAccess 設定

SmartAccessをCitrix Virtual Apps and Desktopsとともに使用すると、公開アプリケーションと仮想デスクトップをインテリジェントにユーザーに配信できます。

SmartAccessを使用すると、NetScaler Gateway セッションポリシーを使用して、サーバー上の公開アプリケーションおよびデスクトップへのアクセスを制御できます。公開リソースにアクセスするための条件として、事前認証および認証後のチェックを他の条件とともに使用します。その他の条件には、Citrix Virtual Apps and Desktopsポリシーで制御できるすべての条件（プリンターの帯域幅制限、ユーザーデバイスドライブのマッピング、クリップボード、オーディオ、プリンターマッピングなど）が含まれます。ユーザーがNetScaler Gateway チェックに合格するかどうかに基づいて、Citrix Virtual Apps and Desktopsポリシーを適用できます。

NetScaler Gateway は、Web Interface、ICAプロキシアクセス、クライアントレスアクセス、およびNetScaler Gateway アクセスで使用できるのと同じオプションを使用して、Citrix 仮想デスクトップを配信できます。

この機能は、NetScaler GatewayコンポーネントをWeb InterfaceおよびCitrix Virtual Apps and Desktopsと統合することによって実現されます。この統合により、Web Interface に対する高度な認証とアクセス制御オプションが提供されます。詳しくは、Citrix 製品ドキュメントの［テクノロジー］ノードにあるWeb Interfaceのドキュメントを参照してください。

サーバーファームへのリモート接続には、NetScaler Gateway プラグインは必要ありません。ユーザーはCitrix Workspace アプリに接続できます。ユーザーは、NetScaler Gateway プラグインを使用してログオンし、NetScaler Gateway のデフォルトのホームページであるAccess Interfaceを介して公開アプリケーションと仮想デスクトップを受信できます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SmartAccess がCitrix Virtual Apps and Desktops どのように機能するのか

SmartAccessを構成するには、Web Interface/StoreFrontでNetScaler Gateway 設定を構成し、NetScaler Gateway でセッションポリシーを構成する必要があります。公開アプリケーションウィザードを実行すると、SmartAccess 用に作成したセッションポリシーを選択できます。

SmartAccess を設定すると、この機能は次のように動作します。

1. ユーザが Web ブラウザで仮想サーバの Web アドレスを入力すると、設定した事前認証ポリシーがユーザデバイスにダウンロードされます。
2. NetScaler Gateway は、事前認証およびセッションポリシー名をフィルターとしてWeb Interface/StoreFrontに送信します。ポリシー条件が true に設定されている場合、ポリシーは常にフィルタ名として送信されます。ポリシー条件が満たされない場合、フィルタ名は送信されません。これにより、エンドポイント分析の結果に基づいて、公開アプリケーションとデスクトップの一覧と、Citrix Virtual Apps and Desktopsを実行しているコンピューター上の有効なポリシーを区別できます。
3. Web Interface/StoreFrontは、Citrix Virtual Apps and Desktops サーバーに接続し、公開リソースリストをユーザーに返します。フィルタが適用されたリソースは、フィルタの条件が満たされない限り、ユーザーのリストに表示されません。

SmartAccess エンドポイント分析は、NetScaler Gateway で構成できます。エンドポイント分析を構成するには、 **ICAプロキシ設定を有効にするセッションポリシーを作成し** 、クライアントセキュリティ文字列を構成します。

ユーザーがログオンすると、エンドポイント分析ポリシーは、NetScaler Gateway で構成したクライアントセキュリティ文字列を使用して、ユーザーデバイスのセキュリティチェックを実行します。

たとえば、Sophos Antivirus の特定のバージョンを確認するとします。式エディタでは、クライアントセキュリティ文字列は次のように表示されます。

```
client.application.av(sophos).version == 10.0.2
```

セッションポリシーを構成したら、ユーザー、グループ、または仮想サーバーにバインドします。ユーザーがログオンすると、SmartAccess ポリシーチェックが開始され、ユーザーデバイスに Sophos Antivirus のバージョン 10.0.2 以降がインストールされているかどうかが検証されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SmartAccessエンドポイント分析チェックが成功すると、Web Interface/StoreFrontポータルがクライアントレスセッションに表示されます。それ以外の場合は、Access Interfaceが表示されます。

SmartAccess のセッションポリシーを作成する場合、セッションプロファイルには設定がないため、ヌルプロファイルが作成されます。この場合、NetScaler Gateway はSmartAccess用にグローバルに構成されたWeb Interface/StoreFront URLを使用します。

Citrix Virtual Apps ポリシーとフィルターの構成

NetScaler Gateway でセッションポリシーを作成したら、Citrix Virtual Apps を実行しているコンピューターでポリシーとフィルターを構成します。ポリシーとフィルタは、エンドポイント分析の設定に従ってユーザに適用されます。

Citrix Virtual Apps ポリシーとフィルターの構成について詳しくは、「 デリバリーグループの管理 」を参照してください。

SmartAccess のセッションポリシーを構成するには

1. 構成ユーティリティの［構成］タブのナビゲーションペインで、［ NetScaler Gateway］> ［ポリシー ］を展開し、［セッション］をクリックします。
2. 詳細ペインの タブで、 をクリックします。
3. ダイアログボックスの に、ValidEndpoint などのポリシーの名前を入力します。
4. で をクリックし、 にプロファイルの名前 (Null など) を入力し、 をクリックします。
5. ダイアログボックスで、クライアントセキュリティ式を作成し、、 の順にクリックします。

クライアントセキュリティ式は、有効なエンドポイントと無効なエンドポイントを区別するために使用されます。エンドポイントの分析結果に基づいて、公開アプリケーションまたはデスクトップへのさまざまなレベルのアクセスを提供できます。

セッションポリシーを作成したら、グローバルにバインドするか、仮想サーバーにバインドします。

Citrix Virtual Apps でのユーザーデバイスマッピングの構成

Citrix Virtual Apps を実行しているコンピューター上のポリシーに適用されるNetScaler Gatewayフィルターを使用できます。フィルターを使用すると、エンドポイントの分析結果に基づいて、ユーザーデバイスドライブのマッピング、プリンターマッピング、クリップボードマッピングなどのCitrix Virtual Apps の機能にアクセスできます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix Workspace アプリは、ユーザーデバイス上のデバイスのマッピングをサポートしているため、ユーザーはユーザーセッション内で外部デバイスにアクセスできます。ユーザーデバイスマッピングは、次の機能を提供します：

- ローカルドライブとポートへのアクセス
- ユーザーセッションとローカルクリップボード間のデータ転送をカットアンドペーストする
- ユーザーセッションからのオーディオ (システムサウンドと.wav ファイル) の再生

ログオン中、ユーザーデバイスは、使用可能なユーザードライブと COM ポートをサーバーに通知します。Citrix XenApp 6.5では、ユーザーードライブはサーバーにマップされ、ユーザーデバイスのドライブ文字が使用されます。マップされたクライアント側デバイスは、そのセッションを実行中のユーザーだけが使用できます。マッピングは、ユーザーがログオフしたときに削除され、ユーザーが次回ログオンしたときに再作成されます。

XML サービスを有効にしたら、ユーザーデバイスマッピングのポリシーを構成する必要があります。

SmartAccess フィルターに基づいてユーザーデバイスマッピングポリシーを適用するには、サーバーで次の 2 つのポリシーを作成します。

- ユーザーデバイスマッピングを無効にし、すべてのNetScaler Gateway ユーザーに適用される制限付きICAポリシー。
- ユーザーデバイスマッピングを有効にし、 エンドポイント分析セッションポリシーを満たすユーザーのみに適用される完全なICAポリシー注:フィルター処理された非制限ICAポリシーは、制限付きICAポリシーよりも高い優先度を付与する必要があります。これにより、ユーザーに適用されたときに非制限ポリシーが適用されます。は、ユーザデバイスマッピングを無効にするポリシーを上書きします。

Citrix XenApp 6.5で制限ポリシーと非制限ポリシーを構成するには、Citrix AppCenterを使用します。

Citrix XenApp 6.5 で制限の厳しいポリシーを構成するには

1. スタート > 管理ツール > 管理コンソール > Citrix AppCenter をクリックします。
2. 左側のペインで［Citrix Virtual Apps］を展開し、サーバーを展開し、［ポリシー］をクリックします。
3. ペインで、 タブをクリックし、 をクリックします。
4. にポリシーの名前を入力し、 をクリックします。
5. で、 をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

6. の で、 をクリックします。
7. ［設定の追加］ダイアログボックスで、［無効］、［OK］、［次へ］の順にクリックします。
8. で、 をクリックします。
9. の で、 をクリックします。
10. 「 新規フィルター 」ダイアログで、「 追加」をクリックします。
11. で をクリックします。
12. で、 を選択します。
13. に、仮想サーバー名を入力します。
14. ［アクセス条件］で、NetScaler Gateway で構成されているセッションポリシー名を入力または選択し、［OK］を2回クリックし、［次へ］、［作成］の順にクリックしてウィザードを完了します。

Citrix XenApp 6.5で非制限ポリシーを構成するには

1. スタート > 管理ツール > 管理コンソール > Citrix AppCenter をクリックします。
2. 左側のペインで［Citrix Virtual Apps］を展開し、サーバーを展開し、［ポリシー］をクリックします。
3. ペインで、 タブをクリックし、 をクリックします。
4. にポリシーの名前を入力し、 をクリックします。
5. で、 をクリックします。
6. の で、 をクリックします。
7. ［有効］、［OK］、［次へ］の順にクリックします。
8. で、 をクリックします。
9. の で、 をクリックします。
10. 「 新規フィルター 」ダイアログで、「 追加」をクリックします。
11. で をクリックします。
12. で、 を選択します。
13. に、仮想サーバー名を入力します。
14. ［アクセス条件］で、NetScaler Gateway で構成されているセッションポリシー名を入力または選択し、［OK］を2回クリックし、［次へ］、［作成］の順にクリックしてウィザードを完了します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

検疫アクセス方法としてのCitrix Virtual Apps 有効化

NetScaler Gateway でエンドポイント分析を構成している場合、エンドポイントスキャンに合格したユーザーは、NetScaler Gateway で構成したすべてのリソースにアクセスできます。エンドポイントスキャンに失敗したユーザーを検疫グループに入れることができます。これらのユーザーは、Citrix Virtual Apps からのみ公開アプリケーションにアクセスできます。エンドポイント分析スキャンの成功または失敗によって、ユーザが使用できるアクセス方法が決まります。

たとえば、エンドポイント分析スキャンを作成して、ユーザーのログオン時にメモ帳がユーザーデバイスで実行されているかどうかを確認します。メモ帳が実行されている場合、ユーザーは NetScaler Gateway プラグインを使用してログオンできます。メモ帳が実行されていない場合、ユーザーは公開アプリケーションの一覧のみを受け取ります。

制限付きユーザーアクセスを構成するには、NetScaler Gateway で検疫グループを作成します。セッションプロファイル内に検疫グループを作成し、そのプロファイルをセッションポリシーに追加します。

検疫グループのセッションポリシーおよびエンドポイント分析スキャンの作成

Citrix Virtual Apps を検疫アクセス方法として有効にするには、検疫グループとして使用するグループをNetScaler Gateway 上に作成します。次に、グループを選択するセッションポリシーを作成します。

セッションポリシーを作成したら、ポリシーを検疫グループにバインドします。ポリシーを設定し、グループにバインドしたら、結果をテストします。たとえば、ユーザーが正常にログオンするには、メモ帳がユーザーデバイスで実行されている必要があります。メモ帳が実行されている場合、ユーザーはNetScaler Gateway プラグインを使用してログオンできます。メモ帳が実行されていない場合、ユーザーはCitrix Workspace アプリでログオンできます。

エンドポイント分析ポリシーの設定の詳細については、 エンドポイントポリシーの設定を参照してください。

エンドポイント分析スキャンを作成し、検疫グループを追加するには

1. 構成ユーティリティの［構成］タブのナビゲーションペインで、［ NetScaler Gateway］> ［ポリシー ］を展開し、［セッション］をクリックします。
2. 詳細ペインの タブで、 をクリックします。
3. ダイアログボックスの に、ポリシーの名前を入力します。
4. 「リクエストプロファイル」の横にある「 新規」をクリックします。
5. ダイアログボックスの に、プロファイルの名前を入力します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

6. タブで、 をクリックします。
7. ダイアログボックスの で、 をクリックし、 をクリックします。
8. ダイアログボックスで、 の横にある をクリックします。
9. で、 を選択します。
10. 「コンポーネント」で、「プロセス」を選択します。
11. に notepad.exe と入力し、、 の順にクリックします。
12. ［セキュリティの設定-詳細］ダイアログボックスの［隔離グループ］で、隔離グループを選択し、［作成］、［OK］、［作成］の順にクリックします。
13. ダイアログボックスで、 の横にある を選択し、、、 の順にクリックします。

SmartAccess 向けの Citrix Virtual Desktops の構成

NetScaler Gateway を使用すると、Citrix Virtual Desktops はリモートユーザーに安全なデスクトップを提供できます。Citrix Virtual Desktops は、NetScaler Gateway のSmartAccess機能を使用して、デスクトップをインテリジェントに配信できます。Citrix Virtual Desktops デリバリーサービスコンソールを使用してデスクトップグループを作成する場合は、アクセス制御用のポリシーとフィルターを構成します。

公開デスクトップを配信するようにNetScaler Gateway を構成するには、Web Interface、ICAプロキシアクセス、クライアントレスアクセス、およびNetScaler Gateway アクセスで使用できるのと同じオプションを使用します。

セッションポリシーを作成し、［**公開アプリケーション**］タブで設定を構成するときは、Citrix Virtual Desktops Web InterfaceサイトのWebアドレスを使用してください。ポリシーを作成したら、そのポリシーを仮想サーバーにバインドします。次に、設定を構成しないヌルセッションプロファイルを作成します。Web インターフェイスの設定は、グローバル設定から継承されます。

Citrix Virtual Desktops で SmartAccess のセッションポリシーを構成するには

NetScaler Gateway でSmartAccessを構成して、Citrix Virtual Desktops にアクセスするには、仮想サーバーにバインドされたセッションポリシーを作成します。

GUI を使用して SmartAccess と Citrix Virtual Desktops のセッションポリシーを構成するには：

1. ［構成］タブで、［**NetScaler Gateway**］>［**ポリシー**］>［**セッション**］に移動します。
2. タブをクリックし、 をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. ［**NetScaler Gateway セッションポリシーの作成**］ページで、［Citrix Virtual DesktopPolicy］などのポリシーの名前を入力します。
4. **［プロファイル］** で、 **［追加］** をクリックします。
5. ［**NetScaler Gateway セッションプロファイルの作成**］ページで、プロファイルの名前（Citrix Virtual DesktopsProfile など）を入力します。
6. タブで、 の横にある をクリックし、 を選択します。
7. ［ **Web Interfaceアドレス**］で、［ **グローバル上書き** ］をクリックし、Citrix Virtual Desktops Web InterfaceサイトのURLを入力します。
8. で、 をクリックし、ドメイン名を入力して をクリックします。
9. **Citrix セッションポリシーの作成** ］ページの［式］で、 **式を追加します**。

また、仮想サーバーにバインドされたヌルセッションポリシーを作成する必要があります。セッションプロファイルには設定が含まれていないため、ヌルプロファイルになります。セッションポリシーで、True Value 式を追加し、ポリシーを保存します。

両方のセッションポリシーを作成したら、両方のポリシーを仮想サーバーにバインドします。

Citrix Virtual Desktops でポリシーとフィルターを構成するには 5

Citrix Virtual Desktops 5の設定は、Citrix Studioまたはグループポリシーエディターを使用して構成できます。Citrix 仮想デスクトップでNetScaler Gateway 設定を構成する場合は、NetScaler Gateway 仮想サーバー名とセッションポリシー名を使用します。次に、定義されたフィルタを満たす接続を許可するようにアクセス制御を設定します。SmartAccess ポリシーを使用することもできます。

1. Citrix Virtual Desktops サーバーで、［ **スタート］>［すべてのプログラム］>［Citrix］>［Citrix Studio］**の順にクリックします。
2. 左側のペインで［HDXポリシー］をクリックして展開し、中央ペインの［ユーザー］タブをクリックします。
3. 「 ユーザー」で、「 新規」をクリックします。
4. ダイアログボックスの に、 に名前を入力します。
5. を 2 回クリックします。
6. ダイアログボックスの タブの で、 をクリックし、 をクリックします。
7. 「 新規フィルター 」ダイアログで、「 追加」をクリックします。
8. 「 新規フィルター要素 」ダイアログの「 接続タイプ」で、「 With Access Gateway」を選択します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NetScaler Gateway ポリシーを考慮せずにNetScaler Gateway を介して行われる接続にポリシーを適用するには、AGファーム名とアクセス条件にデフォルトのエントリを残します。

9. 既存のNetScaler Gateway ポリシーに基づいてNetScaler Gateway を介して行われる接続にポリシーを適用する場合は、次の手順を実行します。

   a. AG ファーム名に、仮想サーバー名を入力します。

   b. アクセス条件に、エンドポイント分析ポリシーまたはセッションポリシーの名前を入力します。

   重要：

   Citrix Virtual Desktops は、NetScaler Gateway 仮想サーバー、エンドポイント分析ポリシー、またはセッションポリシー名を検証しません。情報が正しいことを確認します。

10. 「 OK」 を 2 回クリックし、「 次へ」をクリックして、「 作成」をクリックします。

Desktop Delivery Controller を STA として追加するには

Citrix Virtual Desktops とのICA接続を確立するには、Desktop Delivery Controller のIPアドレスを Secure Ticket Authority（STA）として仮想サーバーに追加します。

GUIを使用してDesktop Delivery Controller をSTAとして追加するには、次の手順に従います。

1. 「構成」タブで、「 **Citrix Gateway」>「仮想サーバー**」に移動します。
2. 詳細ペインで、仮想サーバーを選択し、 をクリックします。
3. 「 **公開アプリケーション** 」タブの「Secure Ticket Authority」で、「 **追加**」をクリックします。
4. ダイアログボックスで、STA サーバーの URL を入力し、 をクリックします。
5. ステップ 4 を繰り返して STA サーバーを追加し、「 **OK**」をクリックします。

SmartControl の設定

SmartControlを使用すると、管理者は詳細なポリシーを定義して、NetScaler Gateway 上のCitrix Virtual Apps and Desktopsのユーザー環境属性を構成および適用できます。SmartControl を使用すると、管理者はこれらのサーバータイプの各インスタンスではなく、1 つの場所からこれらのポリシーを管理できます。

SmartControl は、NetScaler Gateway の ICA ポリシーによって実装されます。各ICAポリシーは、ユーザー、グループ、仮想サーバー、およびグローバルに適用できる式とアクセスプロファイルの組み合わせです。ICAポリシーは、セッション確立時にユーザーが認証された後に評価されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

次の表に、SmartControl で適用できるユーザー環境属性を示します：

クライアントドライブを接続する	ユーザーがログオンしたときのクライアントドライブへの既定の接続を指定します。
ConnectClientLPTPorts	ユーザーのログオン時にクライアントからの LPT ポートの自動接続を指定します。LPT ポートはローカルプリンタポートです。
ClientAudioRedirection	クライアントコンピューターにインストールされているサウンドデバイスを介してオーディオを送信するために、サーバーでホストされているアプリケーションを指定します。
ClientClipboardRedirection	クライアントデバイス上のクリップボードアクセスを指定および構成し、クリップボードをサーバにマップします。
ClientCOMPortRedirection	クライアントへの COM ポートリダイレクトおよびクライアントからの COM ポートリダイレクトを指定します。COM ポートは通信ポートです。COM ポートはシリアルポートです。
ClientDriveRedirection	クライアントとのドライブリダイレクトを指定します。
Multistream	指定したユーザのマルチストリーム機能を指定します。
ClientUSBDeviceRedirection	クライアントとの間の USB デバイスのリダイレクトを指定します（ワークステーションホストのみ）。
`Localremotedata`	Citrix Workspace アプリのHTML5ファイルアップロードのダウンロード機能を指定します。
ClientPrinterRedirection	ユーザーがセッションにログオンしたときにサーバーにマップされるクライアントプリンターを指定します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ポリシー

ICAポリシーは、アクション、アクセスプロファイル、式、およびオプションでログアクションを指定します。 タブでは、次のコマンドを使用できます。

- 追加
- 編集
- 削除
- Show Bindings
- ポリシーマネージャ
- アクション

追加

1. ［**NetScaler Gateway**］>［**ポリシー** ］に移動し、［ **ICA**］をクリックします。



2. 詳細ペインの タブで、 をクリックします。
3. ダイアログボックスで、ポリシーの名前を入力します。



4. の横で、次のいずれかの操作を行います。
   - **** アイコンをクリックして、既存のアクションを選択します。詳細については、(#common-processes) の を参照してください。
   - アイコンをクリックして、アクションを作成します。詳細については、(#common-processes) の を参照してください。
   - **鉛筆アイコンは無効です** 。
5. エクスプレッションを作成します。
6. **ログアクションを作成します**。詳細については、「 ログアクションの作成」を参照してください。
7. ボックスにメッセージを入力します。コメントはメッセージログに書き込まれます。この情報は入力しなくても構いません。
8. 「 **作成**」をクリックします。

編集

1. ［**NetScaler Gateway**］>［**ポリシー** ］に移動し、［ **ICA**］をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. リストから ICA ポリシーを選択します。
3. 詳細ペインの タブで、 をクリックします。
4. ポリシー名を確認します。



5. **アクションを修正するには**、次のいずれかを実行します。
   - **** アイコンをクリックして、**既存のアクションを修正します**。詳細については、(#common-processes) の を参照してください。
   - **アイコンをクリックしてアクションを作成します**。詳細については、(#common-processes) の を参照してください。
   - **鉛筆アイコンをクリックして** を修正します。
6. **必要に 応じてエクスプレッションを 修正してください**。詳細については、(#common-processes) の を参照してください。
7. **ログアクションを修正するには** 、次のいずれかを実行します。
   - をクリックして、**ログアクションを作成します**。
   - **鉛筆アイコンをクリックして** 、監査メッセージを設定します。
8. 必要に応じてコメントを修正します。
9. 「**OK」**をクリック します。

削除

1. ［**NetScaler Gateway**］>［**ポリシー** ］に移動し、［ **ICA**］をクリックします。
2. リストから目的のICAポリシーを選択します。
3. 詳細ペインの タブで、 をクリックします。
4. をクリックして、ポリシーを削除することを確認します。

バインディングを表示

1. ［**NetScaler Gateway**］>［**ポリシー** ］に移動し、［ **ICA**］をクリックします。
2. リストから ICA ポリシーを選択します。
3. 詳細ウィンドウの タブで、 をクリックします。

ポリシーマネージャ

1. ［**NetScaler Gateway**］>［**ポリシー** ］に移動し、［ **ICA**］をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. リストから目的のICAポリシーを選択します。
3. 詳細ペインの タブで、 をクリックします。
4. ダイアログボックスで、次のいずれかのポリシーを選択します。
   - グローバルを上書き
   - VPN 仮想サーバー
   - キャッシュリダイレクト仮想サーバー
   - デフォルトグローバル
5. ダイアログボックスで、メニューからバインドポリシーを選択します。
6. VPN 仮想サーバーまたはキャッシュリダイレクト仮想サーバーのいずれかを選択した場合は、メニューを使用してサーバーに接続します。
7. をクリックします。



バインディングを追加

1. を選択すると、この画面が表示されます。
2. バインドをアタッチするポリシーを選択します。
3. を選択します。



ポリシーバインディング

1\. を選択すると、この画面が表示されます。

- アイコンを クリック**** して、既存のポリシーを選択します。詳細については、「既存のポリシーを選択する」を参照してください。
- **+**アイコンをクリックしてポリシーを作成します。詳細については、「ポリシーの作成」を参照してください。



ポリシーのバインド解除

1. バインド解除するポリシーを選択し、 ボタンをクリックします。



2. 「完了」をクリック します

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. ポップアップ画面の「**はい**」(Yes) ボタンをクリックして、選択したエンティティのバインドを解除することを確認します。

バインドNOPOLICY

1. NOPOLICY を必要とするポリシーを選択し、 ボタンをクリックします。



2. 「完了」をクリック し**ます**

編集

ICA ポリシーマネージャーから編集できます。

1. **編集するポリシーを選択し、 を選択します。**



2. 、**、**の編集を行うことができます。**



バインディングを編集

1. ポリシーを選択した状態で、 をクリックします。
2. 目的のポリシーを編集していることを確認します。このポリシー名は編集できません。



3. 必要に応じて を設定します。
4. 必要に応じて Goto式を設定します。
5. ボタンをクリックします。

ポリシーの編集

1. ポリシーを選択した状態で、 をクリックします。
2. ポリシーの を確認し、目的のポリシーを編集していることを確認します。このフィールドは編集できません。



3. アクションポリシーを修正するには、次のいずれかを実行します。

   - **** アイコンをクリックして、既存のアクションを選択します。詳細については、(#common-processes) の を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- アイコンをクリックして、アクションを作成します。詳細については、(#common-processes) の を参照してください。
- **鉛筆アイコンをクリックして** 、アクセスプロファイルを変更します。詳細については、(#common-processes) の を参照してください。

4. 必要に応じてエクスプレッションを修正してください。詳細については、(#common-processes) の を参照してください。
5. メニューから目的のメッセージタイプを選択します。ログアクションを作成するには、次のいずれかを実行します。

- アイコンをクリックして、アクションを作成します。詳細については 、ログアクションの作成を参照してください。
- **鉛筆アイコンをクリックして** 、監査メッセージの設定アクションを修正します。詳細については、「 監査メッセージアクションの設定」を参照してください。

6. ICA ポリシーに関するコメントを入力します。
7. 編集が完了したら、 **「OK」** をクリックします。

アクションを編集

1. ポリシーを選択した状態で、 をクリックします。
2. を確認して、目的のアクションを編集していることを確認します。このフィールドは編集できません。
3. の横で、次のいずれかの操作を行います。

- ****アイコンをクリックして、別のアクセスプロファイルを選択します。詳細については、「アクションの設定」を参照してください。
- **+**アイコンをクリックして、新しいチャンネルプロファイルを選択します。アクセスプロファイルを作成します。
- **鉛筆アイコンをクリックして** 、アクセスプロファイルを変更します。詳細については、(#common-processes) の を参照してください。

4. をクリックします**。

アクション

> コマンドを使用して、アクションの名前を変更します。

1. リストから目的の ICA アクションを選択します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. タブで、 をクリックします。メニューから を選択します。



3. アクションの名前を変更します。
4. **［OK］**をクリックします

アクション

アクションは、ポリシーをアクセスプロファイルと接続します。 タブでは、次のコマンドを使用できます。

- 追加
- 編集
- 削除
- アクション

追加

1. **［NetScaler Gateway］>［アクション**］に移動し、［ **ICA**］をクリックします。



2. 詳細ウィンドウの タブで、 をクリックします。



- ****アイコンをクリックして、既存のアクセスプロファイルを選択します。詳細については、(#common-processes) の を参照してください。
- **+** アイコンをクリックして、アクセスプロファイルを作成します。詳細については、「」を参照してください。(#creating-an-access-profile-with-the-gui)。
- この画面では、 **鉛筆アイコンは無効になっています** 。

3. **［Create］** をクリックします。



編集

1. リストから目的のICAポリシーを選択します。



2. 詳細ウィンドウの タブで、 をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

アクションの設定

1. を確認して、目的のアクションを編集していることを確認します。このフィールドは編集できません。
2. の横で、次のいずれかの操作を行います。
   - **** をクリックして、既存のアクセスプロファイルを選択します。詳細については、(#common-processes) の を参照してください。
   - をクリックして、アクセスプロファイルを作成します。詳細については、「アクセスプロファイルの作成」を参照してください。
   - **鉛筆アイコンをクリックして** 、 アクセスプロファイルを設定します。
3. ［**OK**］ をクリックします。



削除

1. ［**NetScaler Gateway**］**>**［**アクション** ］に移動し、［ **ICA**］をクリックします。
2. リストから目的の ICA アクションを選択します。
3. 詳細ペインの タブで、 をクリックします。



4. をクリックして、ポリシーを削除する を確認します。

アクション

> コマンドを使用して、アクションの名前を変更します。

1. ［**NetScaler Gateway**］**>**［**アクション** ］に移動し、［ **ICA**］をクリックします。
2. リストから目的の ICA アクションを選択します。
3. 詳細ウィンドウの タブで、 をクリックします。



4. メニューから > を選択します。
5. アクションの名前を変更します。
6. **［OK］**をクリックします

アクセスプロファイル

ICA プロファイルは、ユーザー接続の設定を定義します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

アクセスプロファイルは、ユーザーデバイスがポリシー式の条件を満たす場合に、ユーザーの Citrix Virtual Apps and Desktops 環境のICAに適用されるアクションを指定します。GUIを使用して、ICAポリシーとは別にICAプロファイルを作成し、そのプロファイルを複数のポリシーに使用できます。1 つのポリシーで使用できるプロファイルは 1 つだけです。

アクセスプロファイルは、ICA ポリシーとは独立して作成できます。ポリシーを作成するときに、ポリシーにアタッチするアクセスプロファイルを選択できます。アクセスプロファイルは、ユーザーが使用できるリソースを指定します。 タブでは、次のコマンドを使用できます。

- 追加
- 編集
- 削除

GUI を使用したアクセスプロファイルの作成

1. ［**NetScaler Gateway**］>［**ポリシー** ］に移動し、［ **ICA**］をクリックします。
2. 詳細ウィンドウで、 タブをクリックし、 をクリックします。
3. プロファイルの設定を行い、 をクリックし、 をクリックします。プロファイルを作成したら、そのプロファイルをICAポリシーに含めることができます。

GUI を使用してアクセスプロファイルをポリシーに追加する

1. ［**NetScaler Gateway**］>［**ポリシー** ］に移動し、［ **ICA**］をクリックします。
2. 「 ポリシー 」タブで、次のいずれかを実行します。
   - をクリックして ICA ポリシーを作成します。
   - ポリシーを選択し、 をクリックします。
3. メニューで、リストからアクセスプロファイルを選択します。
4. ICAポリシーの構成を完了し、次のいずれかを実行します。

   a. をクリックし、 をクリックしてポリシーを作成します。

   1\. ［ **OK**］ をクリックし、［ **閉じる** ］をクリックしてポリシーを変更します。

追加

1. ［**NetScaler Gateway**］>［**ポリシー** ］に移動し、［ **ICA**］をクリックします。

2. 詳細ペインの タブで、 をクリックします。****

© 1997–2026 Citrix Systems, Inc. All rights reserved.



3. に、アクセスプロファイルの名前を入力します。



4. 表示されたメニューから または を選択して、アクセスプロファイルを作成します。
5. ［**Create**］ をクリックします。

編集

1. 編集するアクセスプロファイルを選択します。
2. 詳細ペインの タブで、 をクリックします。



アクセスプロファイルの設定

1. が修正する名前であることを確認します。



2. メニューから または を選択し、必要に応じて設定します。
3. ［**OK**］ をクリックします。

削除

1. 「**Citrix Gateway**」>「**アクション**」に移動し、「**ICA**」をクリックします。
2. リストから目的の ICA アクションを選択します。
3. 詳細ペインの タブで、 をクリックします。



4. をクリックして、削除するアクセスプロファイルを確認します。

共通プロセス

アクションを作成する

1. アクションの名前を入力します。
2. 次のいずれかを選択して、アクセスプロファイルを指定します。

    - をクリックして、既存のアクセスプロファイルを選択します。詳細については、(#common-processes) の を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- をクリックして、アクセスプロファイルを作成します。詳細については、 アクセスプロファイルの作成を参照してください。
- **鉛筆アイコンは無効です** 。

3. ［**Create**］ をクリックします。



アクションを選択

1. アクションの左側にあるラジオボタンをクリックして、アクションを選択します。関連付けられたアクセスプロファイルは、許可されるユーザ機能を指定します。
2. ** ボタンをクリックします。



アクセスプロファイルの作成

1. アクセスプロファイルに名前を付けます。



2. アクセスプロファイルは、このメニューから設定できます。
3. ［**Create**］ をクリックします。

既存のアクセスプロファイルを選択する

1. アクセスプロファイルをクリックして選択します。



2. ［編集］をクリックします。
3. アクセスプロファイルを設定します。詳細については、 アクセスプロファイルの設定を参照してください。

式

1. 既存の定義式を作成または改訂するには、「 **クリア」(Clear**) を選択します。

   式は典型的なICA式です。HTTP 式の場合は、名前を「」で入力し、() を削除します。

ICA.SERVER.PORT	この式は、指定されたポートが、ユーザーが接続しようとしているCitrix Virtual Apps and

© 1997–2026 Citrix Systems, Inc. All rights reserved.

	Desktops のポート番号と一致することをチェックします。
ICA.SERVER.IP	この式は、指定されたIPが、ユーザーが接続しようとしているCitrix Virtual Apps and Desktops のIPアドレスと一致することをチェックします。
`AAA.USER.IS_MEMBER_OF(“”)`.NOT	この式は、現在の接続が、指定されたグループ名のメンバーではないユーザーによってアクセスされているかどうかをチェックします。
AAA.USER.IS_MEMBER_OF(“`group name`”)	この式は、現在の接続にアクセスしているユーザーが指定されたグループのメンバーであることをチェックします。
AAA.USER.NAME.CONTAINS(“”).NOT	この式は、現在の接続にアクセスしているユーザーが指定されたグループのメンバーではないことをチェックします。
AAA.USER.NAME.CONTAINS (“enter `user name`”) ユーザー名のリソースを指定します。	この式は、現在の接続が指定された名前でアクセスされているかどうかをチェックします。
CLIENT.IP.DST.EQ (ここにIPアドレスを入力してください)。	この式は、現在のトラフィックの宛先 IP が指定された IP アドレスと等しくないことをチェックします。
CLIENT.IP.DST.EQ（ここにIPアドレスを入力してください）	この式は、現在のトラフィックの宛先 IP が指定された IP アドレスと等しいことをチェックします。
CLIENT.TCP.DSTPORT.EQ (ポート番号を入力)。ない	この式は、宛先ポートが指定されたポート番号と等しくないことをチェックします。
CLIENT.TCP.DSTPORT.EQ (ポート番号を入力)	この式は、宛先ポートが指定されたポート番号と等しいことをチェックします。

2. 同時に、 と バーを選択します。次に、オプションが表示されます。



© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. 期間を入力します。選択して、 **スペースバーを押します** 。
4. 前の表の式の各ピリオドに、ピリオドを入力します。選択して、 スペースバーを押します 。
5. **［OK］** をクリックします。



グループ識別

事前認証関数またはセッション関数は、グループ名変数を使用して式を定義します。

事前認証

1. 設定ペインで を選択します。



1. 事前認証ポリシーから名前を選択します。
2. タブから を選択します。



3. 「アクションのリクエスト」 **ダイアログ・ボックスの横にある鉛筆アイコンまたは** 「 **+** 」を選択します。



4. ダイアログボックスで (「<`groupname`>」) を定義します。



セッション

1. 設定ペインで を選択します。



ログアクションの作成

1. 画面で、 ダイアログボックスの横にある アイコンを選択します。



監査メッセージの作成アクション

1. ** 画面が表示されます。監査メッセージに名前を付けます。監査メッセージには、数字、文字、またはアンダースコア文字のみを使用できます。
2. メニューから を指定します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

緊急	サーバー上の緊急の危機を示すイベント。
アラート	アクションが必要になる可能性のあるイベント。
重大	差し迫ったサーバー危機を示すイベント。
エラー	何らかのエラーを示すイベント。
警告	すぐに行動が必要なイベント。
お知らせ	管理者が知っておく必要があるイベント。
情報	低レベルのイベントを除くすべて。
デバッグ	すべてのイベント、非常に詳細に。

1. を入力します。式は、ログの形式と内容を定義します。
2. チェックボックス。
   - ログイン`newnslog`をチェックして、メッセージを新しい ns ログに送信します。
   - **安全性チェックをバイパスするには、 を選択します。これにより、安全でない式が許可されます。
3. ［**Create**］ をクリックします。



ログアクションの改訂

1. 画面で、 ダイアログボックスの横にあるアイコンをクリックします。



監査メッセージアクションの設定

編集可能なフィールドは次のとおりです。

1. メニューから を指定します。
2. を入力します。式は、ログの形式と内容を定義します。
3. 次のチェックボックスがあります。
   - ログイン `newnslog` をチェックして、メッセージを新しい ns ログに送信します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **安全性チェックをバイパスするには、 を選択します。これにより、安全でない式が許可されます。

4. ［OK］ をクリックします。



既存のポリシーを選択する

1. アイコンをクリックして、既存のポリシーを選択します。



2. 目的のポリシーのラジオボタンを選択します。



ポリシーを作成する

1. ** に、ポリシーの名前を入力します。
2. をクリックしてポリシーを作成します。



3. アクションを作成します。詳細については、「**新しいアクションを作成する**」を参照してください。
4. アクセスプロファイルに名前を付けます。



5. このメニューからアクセスプロファイルを設定します。
6. ［Create］ をクリックします。
7. ［Bind］ をクリックします。



事前認証および認証後のエンドポイント分析の設定

このセクションでは、認証後および事前認証エンドポイント分析（EPA）を設定する方法について説明します。

SmartControl で認証後 EPA を設定するには、VPNセッションアクションの`Smartgroup`パラメータを使用します。EPA 式は VPN セッションポリシーで設定されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

スマートグループパラメータにはグループ名を指定できます。このグループ名は任意の文字列にすることができます。グループ名は、Active Directory 上の既存のグループである必要はありません。

HTTP.REQ.IS_MEMBER_OFという式 ("`groupname`") を使用して、ICAポリシーを構成します。スマートグループに対して以前に指定したグループ名を使用します。

SmartControl で事前認証 EPA を構成するには、事前認証プロファイルの パラメーターを使用します。EPA 式は、事前認証ポリシーで設定されます。

デフォルト EPA グループパラメータにグループ名を指定できます。このグループ名は任意の文字列にすることができます。グループ名は、Active Directory 上の既存のグループである必要はありません。

式の HTTP.REQ.IS_MEMBER_Of ("`groupname`") を使用してICAポリシーを構成し、デフォルトのEPAグループに対して以前に指定されたグループ名を使用します。

認証後の設定

次の手順を使用して、認証後の構成用にスマートグループを設定します。

1. **NetScaler Gateway > ポリシー > セッションに移動します。**

   ▢

2. > **に移動します。

   ▢

NetScaler Gateway セッションプロファイルの作成

1. **［セキュリティ］** タブを選択します。
2. NetScaler Gateway **プロファイルの名前** （アクション）を入力します。
3. メニューの右側にあるボックスを選択し、目的の「**デフォルト承認アクション**」を選択します。

   ユーザーが内部ネットワークにログオンするときにアクセスできるネットワークリソースを指定します。承認のデフォルト設定では、すべてのネットワークリソースへのアクセスを拒否します。デフォルトのグローバル設定を使用し、承認ポリシーを作成して、ユーザーがアクセスできるネットワークリソースを定義することをお勧めします。デフォルトの承認ポリシーを DENY に設定した場合は、ネットワークリソースへのアクセスを明示的に許可する必要があります。これにより、セキュリティが向上します。

4. メニューの右側にあるボックスを選択し、 **目的のSecure Browse を選択します。**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix Workspaceアプリを使用して、ユーザーがNetScaler Gateway 経由でiOSおよびAndroid モバイルデバイスからネットワークリソースに接続できるようにします。ユーザは、セキュアネットワーク内のリソースにアクセスするために完全な VPN トンネルを確立する必要はありません。

5. メニューの右側にあるボックスを選択し、**`Smartgroup`**名を入力します。

   これは、このセッションアクションに関連付けられたセッションポリシーが成功したときにユーザーが配置されるグループです。VPN セッションポリシーは、認証後 EPA チェックを行い、チェックが成功すると、スマートグループで指定されたグループにユーザを配置します。is_member_of (aaa.user.is_member_of) 式をポリシーとともに使用して、このスマートグループに属するユーザーに EPA が渡されたかどうかを確認できます。

6. ［**Create**］ をクリックします。
7. **NetScaler Gateway > ポリシー > セッションに移動します**。
8. > **に移動します。
9. ユーザーがNetScaler Gateway **にログオンした後に適用される新しいセッションポリシーの名前を入力します** 。
10. メニューを使用して アクションを選択します。

    規則の条件が満たされた場合に新しいセッションポリシーによって適用されるアクション。

    注: 目的のプロファイルを作成する必要がある場合は、 を選択します。詳しくは、「NetScaler Gateway セッションプロファイルの作成」を参照してください。

11. このフィールドに「 **式** 」と入力します。

    このフィールドは、ポリシーに一致するトラフィックを指定する名前付き式を定義します。式は、デフォルト構文またはクラシック構文で記述できます。式のリテラル文字列の最大長は 255 文字です。長い文字列はそれぞれ最大 255 文字の小さな文字列に分割でき、小さい文字列は+演算子で連結されます。たとえば、500 文字の文字列を次のように作成できます。""""" + """"

    次の要件は、NetScaler ADC CLIにのみ適用されます。

    - 式に 1 つ以上のスペースが含まれる場合は、式全体を二重引用符で囲みます。
    - 式自体に二重引用符が含まれている場合は、文字を使用して引用符をエスケープします。* または、一重引用符を使用してルールを囲むこともできます。この場合、二重引用符をエスケープする必要はありません。

12. ［**Create**］ をクリックします。
13. に移動します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

14. **セッションポリシーの名前を選択します** 。
15. 「 **アクション** 」メニューから「 **グローバルバインド** 」を選択します。
16. を選択します。
17. **** を選択して、既存のポリシーを選択します。

    注: ポリシーを作成するには、「+」を選択します。詳しくは、「NetScaler Gateway セッションプロファイルの作成」セクションを参照してください。
18. リストから名前を選択し、 ボタンを押します。
19. **優先度を入力し** 、 をクリックします。
20. 「 **完了**」をクリックします
21. このチェックは、選択内容が であることを示します。

事前認証の設定

次の手順を使用して、事前認証構成を設定します。

1. **NetScaler Gateway > ポリシー > 事前認証に移動します**。

   
2. タブを選択し、 を選択します。

   
3. 事前認証アクションの を入力します。

   名前は英字、数字、またはアンダースコア文字 (_) で始まり、文字、数字、ハイフン (-)、ピリオド (.)、ポンド (#)、スペース ()、アットマーク (@)、等号 (=)、コロン (:)、およびアンダースコア文字のみで構成する必要があります。事前認証アクションが作成された後は変更できません。

   注： 次の要件は、NetScaler ADC CLIにのみ適用されます。 名前に 1 つ以上のスペースが含まれる場合は、名前を二重引用符または一重引用符で囲みます。
4. **接続がポリシーに一致したときにポリシーが呼び出すリクエストアクションを選択します** 。

   注: 事前認証プロファイルを作成または作成する場合は、 を選択します。詳細については、 事前認証プロファイルの作成を参照してください。
5. Citrix **ADCの名前付きルールの名前である式** 、またはポリシーと一致する接続を定義するデフォルトの構文式を入力します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

6. ［**Create**］ をクリックします。
7. タブに移動し、目的のポリシーを選択します。
8. 「 **アクション** 」メニューから「 **グローバルバインド** 」を選択します。
9. を選択します。
10. を選択して、既存のポリシーを選択します。 を選択してポリシーを作成します。詳しくは、「NetScaler Gateway セッションプロファイルの作成」を参照してください。
11. **「ポリシー」を選択します** 。
12. **優先度を入力し** 、 をクリックします。
13. ［**完了**］ をクリックします。
14. このチェックは、 **事前認証ポリシーがグローバルにバインドされていることを示しています** 。

事前認証プロファイルの作成

1. **事前認証アクションの名前を入力します** 。

   名前は英字、数字、またはアンダースコア文字 (_) で始まり、文字、数字、ハイフン (-)、ピリオド (.)、ポンド (#)、スペース ()、アットマーク (@)、等号 (=)、コロン (:)、およびアンダースコア文字のみで構成する必要があります。事前認証アクションが作成された後は変更できません。

   注: 名前にスペースが 1 つ以上含まれている場合は、名前を二重引用符または一重引用符で囲んでください。これは、NetScaler ADC CLIにのみ適用されます。
2. メニューから を入力します。

   このオプションは、エンドポイント分析 (EPA) の結果後にログオンを許可または拒否します。
3. **キャンセルされるプロセス**

   このオプションは、エンドポイント分析 (EPA) ツールが終了する必要がある一連のプロセスを識別します。
4. **削除するファイル**

   このオプションは、エンドポイント分析 (EPA) ツールで削除する必要があるファイルのパスと名前を指定する文字列を指定します。
5. **デフォルトの EPA グループ**

   デフォルトの EPA グループは、EPA チェックが成功したときに選択されるグループです。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

6. ［**Create**］ をクリックします。

Web インターフェイスへのシングルサインオンの設定

Webベース認証を使用する内部ネットワーク内のサーバーにシングルサインオンを提供するようにNetScaler Gateway を構成できます。シングルサインオンを使用すると、ユーザーを SharePoint サイトなどのカスタムホームページや Web Interface にリダイレクトできます。また、Access Interfaceで構成されたブックマークまたはユーザーがWebブラウザーに入力するWebアドレスから、NetScaler Gateway プラグインを使用してリソースへのシングルサインオンを構成することもできます。

Access インターフェイスを SharePoint サイトまたは Web インターフェイスにリダイレクトする場合は、サイトの Web アドレスを指定します。ユーザーがNetScaler Gateway または外部認証サーバーによって認証されると、ユーザーは指定されたホームページにリダイレクトされ、自動的にログオンされます。ユーザクレデンシャルは Web サーバに透過的に渡されます。Web サーバーが資格情報を受け入れると、ユーザーは自動的にログオンします。Web サーバがクレデンシャルを拒否すると、ユーザはユーザ名とパスワードの入力を求める認証プロンプトを受け取ります。

Web アプリケーションへのシングルサインオンは、グローバルに構成することも、セッションポリシーを使用して構成することもできます。

スマートカードを使用して Web Interface へのシングルサインオンを構成することもできます。詳細については、「 スマートカードを使用した Web インターフェイスへのシングルサインオンの構成」を参照してください。

NetScaler Gateway は、次のバージョンのWeb Interfaceと互換性があります。

- Web Interface 4.5
- Web Interface 5.0
- Web Interface 5.1
- Web Interface 5.2
- Web Interface 5.3
- Web Interface 5.4

シングルサインオンを構成する前に、Web Interfaceが構成済みであり、NetScaler Gateway で動作していることを確認してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Web アプリケーションへのシングルサインオンをグローバルに構成するには

シングルサインオンをグローバルに適用すると、Webサービスは、NetScaler Gateway でそれらのセッションを認証するのではなく、すべてのWebアプリケーションセッションを認証できます。

1. 構成ユーティリティの［ **構成** ］タブのナビゲーションペインで、［ **Citrix Gateway** ］を展開し、［ **グローバル設定**］をクリックします。
2. 詳細ペインの で、 をクリックします。
3. ［ **グローバルNetScaler Gateway 設定** ］ダイアログボックスの［ **クライアントエクスペリエンス** ］タブで、［ **Webアプリケーションへのシングルサインオン** ］をクリックし、［ **OK］**をクリックします。

セッションポリシーを使用して Web アプリケーションへのシングルサインオンを構成するには

1. 構成ユーティリティの［ **構成** ］タブのナビゲーションペインで、［ **Citrix Gateway** ］>［ **ポリシー** ］を展開し、［ **セッション**］をクリックします。
2. 詳細ペインの タブで、ポリシーを選択し、 をクリックします。
3. 「 **セッションポリシー**の構成 」ダイアログ・ボックスの「 **リクエスト・プロファイル**」の横にある「 **変更**」をクリックします。
4. ［ **セッションプロファイルの構成** ］ダイアログボックスの［ **クライアントエクスペリエンス** ］タブで、［Webアプリケーションへのシングルサインオン］の横にある［ **グローバルオーバーライド**］、［ **Webアプリケーションへのシングルサインオン** ］、［ **OK］**の順にクリックします。

Web アプリケーションへのシングルサインオン用の HTTP ポートを定義するには

シングルサインオンは、宛先ポートが HTTP ポートと見なされるネットワークトラフィックに対してのみ試行されます。HTTPトラフィックにポート80以外のポートを使用するアプリケーションへのシングルサインオンを許可するには、NetScaler Gateway で1つ以上のポート番号を追加します。複数のポートを有効にできます。ポートはグローバルに設定します。

1. 構成ユーティリティの［ **構成** ］タブのナビゲーションペインで、［ **Citrix Gateway** ］を展開し、［ **グローバル設定**］をクリックします。
2. 詳細ペインの で、 をクリックします。
3. タブで、 をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. ［HTTP ポート］にポート番号を入力し、［ **追加** ］、［ **OK］**の順にクリックします。

   注:内部ネットワークの Web アプリケーションが別のポート番号を使用している場合は、ポート番号を入力し、 をクリックします。Web Interface を含む Web アプリケーションへのシングルサインオンを許可するには、HTTP ポート番号を定義する必要があります。

その他の設定ガイドライン

Web Interface をシングルサインオン用に設定する場合は、次のガイドラインに従ってください。

- 認証サービスの URL は https で始まる必要があります。
- Web Interfaceを実行するサーバーは、NetScaler Gateway 証明書を信頼し、証明書の完全修飾ドメイン名（FQDN）を仮想サーバーのIPアドレスに解決できる必要があります。
- Web Interfaceは、NetScaler Gateway 仮想サーバーへの接続を開くことができる必要があります。この目的には、任意のNetScaler Gateway 仮想サーバーを使用できます。これは、ユーザーがログオンする仮想サーバーである必要はありません。
- Web InterfaceとNetScaler Gateway の間にファイアウォールがある場合、ファイアウォールルールによってユーザーアクセスが妨げられ、Web Interfaceへのシングルサインオンが無効になります。この問題を回避するには、ファイアウォールルールを緩和するか、Web Interfaceが接続できる別の仮想サーバーをNetScaler Gateway 上に作成します。仮想サーバーには、内部ネットワーク内の IP アドレスが必要です。Web Interface に接続するときは、セキュアポート 443 を宛先ポートとして使用します。
- 仮想サーバーのプライベート認証局 (CA) からの証明書を使用している場合は、Microsoft 管理コンソール (MMC) で証明書スナップインを使用して、Web Interface を実行しているサーバーのローカルコンピューター証明書ストアに CA ルート証明書をインストールします。
- ユーザーがログオンし、アクセス拒否のエラーメッセージが表示された場合は、Web Interface イベントビューアで詳細を確認してください。
- 公開アプリケーションまたはデスクトップに正常にユーザー接続するには、NetScaler Gateway で構成したSecure Ticket Authority（STA）が、Web Interfaceで構成したSTAと一致する必要があります。

Web Interface へのシングルサインオン接続をテストするには

Web Interface のシングルサインオンを構成したら、クライアントデバイスから Web ブラウザを開き、正常な接続をテストします。

1. Webブラウザで、`https://NetScalerGatewayFQDN`と入力します。ここで、netscalerGatewayFQDNは、仮想サーバーにバインドされた証明書の完全修飾ドメイン名 (FQDN) です。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Active Directory のドメインユーザーアカウントにログオンします。ログオンすると、Web インターフェイスにリダイレクトされます。

アプリケーションは自動的に表示され、追加の認証は行われません。ユーザーが公開アプリケーションを起動すると、Citrix Workspace アプリはNetScaler Gateway アプライアンスを介してファーム内のサーバーにトラフィックを転送します。

スマートカードを使用した Web インターフェイスへのシングルサインオンの構成

ユーザーログオンにスマートカードを使用する場合は、Web Interface へのシングルサインオンを構成できます。NetScaler Gateway の設定を構成し、スマートカードを使用したシングルサインオンを受け入れるようにWeb Interfaceを構成します。シングルサインオンは、パススルー認証とも呼ばれます。

Web Interface バージョン 5.3 および 5.4 では、スマートカードを使用した Web Interface へのシングルサインオンがサポートされています。NetScalerバージョン10で利用可能なNetScaler ADC機能でWeb Interfaceを有効にすると、スマートカードでシングルサインオンを使用することもできます。この機能の構成について詳しくは、「NetScaler Gateway を介したWeb Interfaceでのスマートカード認証の使用」を参照してください。

証明書アクションでのユーザー名の抽出が subjectAltName: PrincipalName である限り、ユーザーは Active Directory の複数の CN グループに属してシングルサインオンを機能させることができます。Subject: CN パラメータを使用する場合、ユーザは複数の CN グループに属することはできません。

スマートカードを使用してWeb InterfaceへのシングルサインオンをNetScaler Gatewayを構成するには、次の操作を行う必要があります。

- 認証局 (CA) からの署名付きサーバー証明書をインストールします。詳細については、「NetScaler Gateway への署名付き証明書のインストール」を参照してください。
- NetScaler Gateway とユーザーデバイスにルート証明書をインストールします。
- Web Interface のログオンポイントとして仮想サーバーを作成します。仮想サーバーを構成するときは、クライアント証明書の SSL パラメーターを に設定する必要があります。仮想サーバーの構成の詳細については、「仮想サーバーの作成」を参照してください。
- SSL パラメータでクライアント認証が無効になっているセカンダリ仮想サーバを作成します。この設定により、ユーザは個人識別番号 (PIN) のセカンダリ要求を受信できなくなります。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- クライアント証明書認証ポリシーを作成します。 フィールドで、パラメーター subjectAltName: PrincipalName を使用して、複数のグループからユーザーを抽出します。 フィールドは空白のままにします。
- NetScaler Gateway でセッションポリシーとプロファイルを作成します。セッションプロファイル内で、ICAプロキシを有効にし、シングルサインオンに使用するWeb Interfaceとドメインを指定します。

次の手順に従って、スマートカードを使用したシングルサインオン用のセッションプロファイルを作成できます。

スマートカードを使用してシングルサインオン用のセッションプロファイルを作成するには

1. 構成ユーティリティの［構成］タブのナビゲーションペインで、［**Citrix Gateway ポリシー**］を展開し、［**セッション**］をクリックします。
2. 詳細ペインで、 タブをクリックし、** をクリックします。
3. タブで、 の横にある をクリックし、** をオフにします。
4. の横にある をクリックし、** をクリックします。
5. ［**Published Applications**］ タブをクリックします。
6. **ICAプロキシ**の横にある「**グローバル上書き」をクリックし、** 「オン」を選択します。
7. で、 をクリックし、完全修飾ドメイン名 (FQDN) または Web インターフェイスを入力します。
8. で、 をクリックし、**ドメイン名を入力します。

注

.domain.com の形式ではなく、フォーマットドメインを使用してください。

1. ［**Create**］ をクリックしてから、［**Close**］ をクリックします。

セッションプロファイルを完了したら、セッションポリシーを設定し、そのプロファイルをポリシーの一部として使用します。その後、セッションポリシーを仮想サーバーにバインドできます。

スマートカードを使用してシングルサインオン用にクライアント証明書を構成するには

スマートカードを使用して Web Interface へのシングルサインオンを構成する場合は、 ダイアログボックスの で を選択し、クライアント証明書を として構成する必要があります。 を選択すると、Web インターフェイスへのシングルサインオンが失敗します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. 構成ユーティリティの［構成］タブのナビゲーションペインで、［ NetScaler Gateway ］を展開し、［ 仮想サーバー］をクリックします。
2. 詳細ペインで仮想サーバーをクリックし、 をクリックします。
3. ［NetScaler Gateway 仮想サーバーの構成］ダイアログボックスの［証明書］タブで、［SSL パラメーター］をクリックします。
4. ダイアログボックスの で、 をクリックします。
5. 「クライアント証明書」で、「オプション」を選択し、「OK」を 2 回クリックします。

Citrix Virtual Apps およびファイル共有のシングルサインオンを構成するには

ユーザーがCitrix Virtual Apps を実行しているサーバーに接続し、SmartAccess を使用している場合は、サーバーファームに接続するユーザーのシングルサインオンを構成できます。セッションポリシーとプロファイルを使用して公開アプリケーションへのアクセスを構成する場合は、サーバーファームのドメイン名を使用します。

また、ネットワーク内のファイル共有へのシングルサインオンを構成することもできます。

1. 構成ユーティリティの［ **構成** ］タブのナビゲーションペインで、［ **Citrix Gateway** ］>［ **ポリシー** ］を展開し、［ **セッション**］をクリックします。
2. 詳細ペインの タブで、セッションポリシーを選択し、 をクリックします。
3. 「 **セッションポリシーの構成** 」ダイアログ・ボックスの「 **リクエスト・プロファイル** 」の横にある「 **変更**」をクリックします。
4. **「セッションプロファイルの設定」ダイアログボックスの「公開アプリケーション」タブの「シングルサインオンドメイン」で、「Override Global」をクリックし、ドメイン名を入力して「OK」を 2 回クリックします。**

ファイルタイプの関連付けを許可する

ファイルタイプの関連付けにより、ユーザーはCitrix Virtual Apps またはDesktops 7を介して公開されたアプリケーションでドキュメントを開くことができます。このアクセス許可を使用して、ユーザーが信頼できる環境にあるサーバー上のドキュメントを開いたり編集したりすることを許可し、ドキュメントをユーザーデバイスに送信しないようにすることができます。ファイルタイプの関連付けは、公開アプリケーションに関連付けられているドキュメントタイプに対してのみ使用でき、NetScaler Gateway で仮想サーバーのプロパティを正しく構成した場合にのみ使用できます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

リソースドキュメントを編集するための唯一の手段としてファイルタイプの関連付けを提供すると、ユーザーデバイスではなくサーバー上で編集を行う必要があるため、セキュリティを強化できます。たとえば、従業員が進行中のプロジェクトミーティングのレポートを投稿するファイル共有のファイルタイプの関連付けを許可し、ダウンロードまたはアップロードできないようにすることができます。

ファイルタイプの関連付けを提供するには、次のことが必要です：

- ユーザーは、ユーザーデバイス上でCitrix Workspace アプリを実行します。
- ユーザーは、トラフィックポリシーがバインドされ、Citrix Virtual Appsのポリシーを構成した仮想サーバーを介して接続します。
- ユーザーは、Citrix Virtual Apps and Desktops 7で目的のアプリケーションに割り当てられます。
- 管理者は、NetScaler Gateway と互換性があるようにCitrix仮想アプリを構成します。

ファイルタイプの関連付けを作成する手順は次のとおりです：

- Web インターフェイスサイトの作成。
- NetScaler Gateway のトラフィックポリシーを使用してファイルタイプの関連付けを構成する。
- Citrix Virtual Apps and Desktops でのファイル名拡張子の定義 7.

Web インターフェイスサイトの作成

ファイルの種類の関連付けをサポートするように Web Interface を構成するには、まず Web Interface サイトを作成します。Web Interface サイトは、ダイレクトアクセスコントロールまたはアドバンスアクセスコントロールに設定できます。次のディレクトリを Web Interface サイトにコピーします。

- app_data
- `auth`
- サイト

これらのディレクトリを Web Interface サイトにコピーすると、既存のディレクトリが上書きされます。

Web インターフェイス 4.6 または 5.0 を使用している場合は、Web インターフェイスサイトディレクトリにある web.config ファイルを開き、次のコードを追加します。このコードは、Citrix サ

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ポートサイト（`<http://support.citrix.com/article/ctx116253>`）からダウンロードできます。

```
<location path="site/contentLaunch.ica">

<system.web>

<httpHandlers>

<add verb="*" path="*.ica" type="System.Web.UI.PageHandlerFactory"/>

</httpHandlers>

</system.web>

</location>

<location path="site/contentLaunch.rad">

<system.web>

<httpHandlers>

<add verb="*" path="*.rad" type="System.Web.UI.PageHandlerFactory"/>

</httpHandlers>

</system.web>

</location>
```

このコードは、web.config ファイルの次のセクションの後に追加する必要があります。

```
<location path="site/launch.rad">

        <system.web>

            <httpHandlers>

                <add verb="*" path="*.rad"
type="System.Web.UI.PageHandlerFactory"/>
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
            </httpHandlers>

        </system.web>

    </location>
```

NetScaler Gateway でファイルタイプの関連付けを構成する

NetScaler Gateway でファイルタイプの関連付けを構成する前に、ファイルタイプの関連付けをサポートするようにWeb Interfaceサイトを構成します。Web Interfaceを作成して構成したら、NetScaler Gateway で設定を作成する必要があります。手順は次のとおりです。

- 新しい仮想サーバーを作成するか、既存の仮想サーバーを使用します。仮想サーバーの作成の詳細については、「仮想サーバーの作成」を参照してください。
- Web Interface が設定されたセッションポリシーとプロファイルを作成する。
- セッションポリシーを仮想サーバーにバインドします。
- トラフィックポリシーの作成。

セッションポリシーを作成して仮想サーバにバインドしたら、トラフィックポリシーを作成し、仮想サーバにもバインドします。

ファイルタイプの関連付けのトラフィックポリシーを設定する場合は、ファイル名拡張子を定義する式を作成します。たとえば、Microsoft Word と Excel のファイルタイプの関連付けを有効にするとします。エクスプレッションの例は次のとおりです。

R`EQ.HTTP.URL == /*.doc || REQ.HTTP.URL == /*.xls`

ファイルタイプの関連付けのセッションポリシーとプロファイルを作成するには

1. **構成ユーティリティで［構成］タブをクリックし、ナビゲーションペインで［NetScaler Gateway］>［ポリシー］の順に展開し、［セッション］をクリックします。**
2. 詳細ペインの タブで、 をクリックします。
3. に、ポリシーの名前を入力します。
4. 「リクエストプロファイル」の横にある「**新規**」をクリックします。
5. に、プロファイルの名前を入力します。
6. タブで、次の設定を構成します。
    a. の横にある をクリックし、Web インターフェイスの Web アドレスを入力します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

b. の横にある をクリックし、 または を選択します。

c. の横にある をクリックし、ユーザーアカウントが存在するドメインの名前を入力して、 をクリックします。

7. ダイアログボックスで、 の横にある を選択し、、、** の順にクリックします。

ファイルタイプの関連付けのトラフィックプロファイルを作成するには

1. 構成ユーティリティの［ 構成 ］タブの**ナビゲーションペイン**で、［NetScaler Gateway ポリシー］を展開し、［トラフィック］をクリックします。
2. 詳細ウィンドウで、 タブをクリックし、 をクリックします。
3. に、プロファイルの名前を入力します。
4. で、 を選択し、、 の順にクリックします。

トラフィックポリシーでファイルタイプの関連付けを設定するには

1. 構成ユーティリティの［ 構成 ］タブのナビゲーションペインで、［NetScaler Gateway ポリシー］を展開し、［トラフィック］をクリックします。
2. 詳細ペインの タブで、 をクリックします。
3. に、ポリシーの名前を入力します。
4. 「プロファイルの要求」で、プロファイルを選択します。
5. ダイアログボックスの で、 を選択し、 をクリックします。
6. ダイアログボックスで、次の操作を行います：

   a. で、 をクリックします。

   b. 「 フロータイプ」で、「 REQ」を選択します。

   c. ［Protocol］ で、［HTTP］ を選択します。

   d. 「修飾子」で「URL」を選択します。

   e. 「演算子」で「= =」を選択します。

   f. 「値」に「/*.FileExtensionType」と入力します。ここで、ファイル拡張子タイプは、.doc や.xls などのファイルの種類で、 **「OK」**をクリックします。

7. ダイアログボックスの で、 の横にある をクリックします。
8. 含めるファイル名拡張子ごとに手順 4、5、6 を繰り返し、、 の順にクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

__index__

一般的な展開

組織の内部ネットワーク（またはイントラネット）の境界にCitrix Gateway を展開して、内部ネットワークに存在するサーバー、アプリケーション、およびその他のネットワークリソースへの安全な単一アクセスポイントを提供できます。すべてのリモートユーザーは、内部ネットワーク上のリソースにアクセスする前に、Citrix Gateway に接続する必要があります。

Citrix Gateway は、通常、ネットワーク内の次の場所にインストールされます。

- ネットワークDMZで
- DMZ< を持たないセキュアなネットワークの場合

また、Citrix Virtual Apps、Citrix Virtual Desktops、StoreFront、およびCitrix Endpoint Management を使用してCitrix Gatewayを展開して、ユーザーがWindows、Web、モバイル、SaaSアプリケーションにアクセスできるようにすることもできます。展開環境にCitrix Virtual Apps、StoreFront、デスクトップ7が含まれている場合は、シングルホップまたはダブルホップのDMZ構成でCitrix Gateway を展開できます。ダブルホップ展開は、以前のバージョンのCitrix Virtual Desktops またはCitrix Endpoint Management ではサポートされません。

これらのCitrixソリューションおよびサポートされているその他のCitrixソリューションを使用してCitrix Gatewayインストールを拡張する方法の詳細については、Citrix 製品との統合トピックを参照してください。

Citrix Endpoint Management 環境の設定の構成

Citrix Endpoint Management 用Citrix ADCウィザードの指示に従って、Citrix Endpoint Management 展開用のCitrix ADC機能の構成を行います。このウィザードを使用すると、次の操作を実行できます。

- **マイクロ VPN を設定します。**このシナリオでは、リモートユーザーは内部ネットワークのアプリやデスクトップにアクセスできます。
    - Citrix Endpoint Management MAM専用モードでは、認証にCitrix Gateway を使用する必要があります。
    - MDMの展開では、モバイルデバイスVPNとしてCitrix Gatewayをお勧めします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

    - ENT展開では、ユーザーがMDM登録をオプトアウトすると、デバイスは従来のMAMモードで動作し、Citrix Gateway のFQDNを使用して登録されます。

- **証明書ベースの認証を構成します。 Citrix Endpoint Management デフォルト構成は、ユーザー名とパスワード認証です。**Citrix Endpoint Management 環境への登録とアクセスのセキュリティをさらに強化するには、証明書ベースの認証の使用を検討してください。
- **Citrix Endpoint Management サーバーの負荷を分散します。**Citrix ADCの負荷分散は、複数のCitrix Endpoint Management サーバーがある場合、またはCitrix Endpoint Management がDMZまたは内部ネットワーク内にある場合（したがって、デバイスからCitrix ADCにトラフィックが流れる）、すべてのCitrix Endpoint Management デバイスモードに必要です。このシナリオでは、Citrix ADCアプライアンスはユーザーデバイスとCitrix Endpoint Managementサーバー間のDMZに存在し、モバイルデバイスからCitrix Endpoint Management サーバーに暗号化された送信データを負荷分散します。
- **メールフィルタリング機能を備えたMicrosoft Exchangeサーバの負荷を分散します。**このシナリオでは、Citrix ADCアプライアンスは、ユーザーデバイスとCitrix Endpoint Management Citrix ADCコネクタ（XNC）との間、およびユーザーデバイスとMicrosoft Exchange CASサーバーの間にあります。ユーザーデバイスからの要求はすべてCitrix Gateway アプライアンスに送信され、XNCと通信してデバイスに関する情報を取得します。XNCからの応答に応じて、Citrix ADCアプライアンスはホワイトリストに登録されたデバイスから内部ネットワークのサーバーに要求を転送するか、ブラックリストに登録されたデバイスからの接続を切断します。
- **要求されたコンテンツの種類に基づいて、ShareFileストレージゾーン・コネクタのロード・バランシングを行います。**このシナリオでは、StorageZones Controller 環境に関する基本情報の入力を求められ、次の処理を行う構成が生成されます。

    - ストレージ・ゾーン・コントローラ間でトラフィックのロード・バランシングを行います。
    - ストレージ・ゾーン・コネクタのユーザー認証を提供します。
    - ShareFileアップロードとダウンロードのURI署名を検証します。
    - Citrix ADCアプライアンスでSSL接続を終了します。

ShareFileの構成について詳しくは、「StorageZones Controller 用のCitrix ADC 構成」を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

重要

Citrix Endpoint Management ウィザードを使用する前に、以下のCitrix Endpoint Managementの展開に関する記事を参照して、設計と展開に関する情報と推奨事項を確認してください。

Citrix Endpoint Management 統合
Citrix GatewayおよびCitrix ADCとの統合
MDXアプリのSSOとプロキシの考慮事項
認証

Citrix Endpoint Management 用Citrix ADCウィザードは、1回だけ使用できます。テスト環境、開発環境、実稼働環境など、複数のCitrix Endpoint Management インスタンスが必要な場合は、追加の環境用にCitrix ADCを手動で構成する必要があります。以下のサポート記事では、ウィザードで実行されるコマンドの一覧と、それらのコマンドを実行して新しいCitrix ADCインスタンスを作成する方法を説明します。

Citrix ADC-SSLブリッジでCitrix Endpoint Management ウィザードによって生成されるコマンド
Citrix ADC-SSLオフロードでCitrix Endpoint Management ウィザードによって生成されるコマンド

Citrix ADC機能のライセンス要件

以下のCitrix ADC機能を有効にするには、ライセンスをインストールする必要があります。

- Citrix Endpoint Management MDM負荷分散には、Citrix ADC標準ライセンスが必要です。
- ストレージゾーンを使用したShareFile負荷分散には、Citrix ADC標準ライセンスが必要です。
- Exchangeの負荷分散には、Citrix ADCライセンスまたは統合キャッシュライセンスを追加したAdvancedライセンスが必要です。

Citrix Endpoint Management ウィザード用Citrix ADCウィザード

このセクションでは、Citrix ADC for Citrix Endpoint Management ウィザードを使用して以下の操作を行う例を示します。

- 内部ネットワーク内のCitrix Endpoint Managementで管理されるリソースへのリモートユーザー接続用のマイクロVPNアクセスをセットアップする
- 証明書ベースの認証を構成します。パブリックSSL証明書の取得とインストールについては、「証明書のインストールと管理」を参照してください。
- Citrix Endpoint Management サーバーの負荷分散を構成します。

ウィザードを使用するには、次の手順に従います。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. 構成ユーティリティで、［ **構成** ］タブをクリックし、 **［Citrix Endpoint Management］** をクリックします。

2. Citrix Endpoint Management のバージョンを選択し、［ **開始**］をクリックします。
3. 設定する機能のチェックボックスをオンにします。このウィザードは 1 回だけ使用できるため、以降の構成を手動で実行する必要があります。これらの手順は、次の設定を選択することを前提としています。 **Citrix Gateway 経由のアクセス** （ENTモードまたはMAMモードで実行されているCitrix Endpoint Management 用） **負荷分散Citrix Endpoint Management サーバー**

4. **Citrix Gateway 設定** ページで、外部の**Citrix GatewayのIPアドレス** 、 **ポート** 、 **仮想サーバー名** の値を入力します。

5. **Citrix Gateway のサーバー証明書** ］ページの［ **証明書ファイル** ］ドロップダウンメニューから、［ **ローカル** ］または［ **アプライアンス** ］から証明書ファイルを選択します。証明書がローカルマシン上にある場合:

   証明書がアプライアンス上にある場合：

6. \[**認証設定**\] ページの \[**プライマリ認証方法**\] フィールドで、\[**クライアント証明書**\] を選択します。

   これによって、次の2つのフィールドで自動的に **［Use existing certificate policy］** および **［Cert Auth］** を選択します。次の手順では、証明書ポリシーがすでにあることを前提しています。

   証明書を作成する必要がある場合、 **［Create certificate policy］** をクリックして、設定を完了します。［ **Citrix Endpoint Management 証明書** ］画面で、既存のサーバー証明書を選択するか、新しい証明書をインストールします。複数のCitrix Endpoint Management サーバーを実行している場合は、それぞれに証明書を追加します。\[**サーバーログオン名の属性\]**で、要件に応じて、 **ユーザープリンシパル**名または **samAccountName**を指定します。

   - a.\[**ここをクリックして CA 証明書を変更してください**\] を選択し、\[**参照\]** ボックスの一覧で目的の CA 証明書に移動します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- b. プライマリ認証タイプとしてクライアント証明書を使用する場合、セカンダリ認証タイプとして LDPA（または RADIUS）を設定できます。

  クライアント証明書認証のみを使用するには、\[**2 番目の認証方法** \] を \[**なし** \] のままにして、\[**続行** \] をクリックします。

  クライアント証明書+ドメイン (LDAP) 認証を使用するには、\[**2 番目の認証方法** \] を \[**LDAP** \] に変更し、認証サーバーの設定を構成します。
- c. ［ **デバイス証明書** ］画面で、証明書がまだインストールされていない場合は、Citrix Endpoint Management コンソールからこの証明書をエクスポートする必要があります。コンソールで、右上隅にある歯車アイコンをクリックして **［設定］** 画面を開きます。
- d. \[**証明書** \] をクリックし、一覧から CA 証明書を選択します。
- e. **［エクスポート］** をクリックします。
- f. Citrix ADCウィザードに戻り、エクスポートした（ダウンロードした）証明書を選択してインストールします。
- g. **［続行］** をクリックします。

設定したCitrix Endpoint Management IPアドレスが表示されます。

7. **Citrix Endpoint Management アプリケーションの管理設定**を構成します。

   - **Citrix Endpoint Management の FQDN**を入力します。これは MAM のロードバランシング FQDN です。
   - Citrix Endpoint Management サーバーの **負荷分散を行う仮想サーバーの、MAM専用内部負荷分散IPアドレスを** 入力します。Citrix Gateway は、このMAM負荷分散仮想IPを介して Citrix Endpoint Management と通信します。
   - これはSSLオフロード展開であるため、 **［Citrix Endpoint Management サーバーとの通信 ］**で ［ **HTTP** ］を選択します。
   - **MicroVPN フィールドのスプリット DNS モード** は自動的に **両方** に設定されます。

   展開で分割トンネリングが必要な場合は、\[**分割トンネリングを有効にする**\] を選択します。次に、分割トンネリングを有効にする場合は、イントラネットアプリケーションバインディングを設定する必要があります。

   デフォルトでは、Secure Webアクセスは内部ネットワークにトンネリングされます。つまり、Secure Webはすべてのネットワークアクセスに対してアプリケーションごとのVPNトン

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ネルを内部ネットワークに戻し、Citrix ADCアプライアンスは分割トンネル設定を使用します。

8. Citrix Gateway でユーザー接続の傍受ルールを構成するには、 **イントラネットアプリケーションのバインド**を構成する必要があります。バインドを追加するには、\[**+** \] をクリックします。
9. ネットワークアクセスを許可するためのパラメータを入力し、\[**Create**\] をクリックします。
10. Citrix Endpoint Management 証明書を追加します。これは、MAM 負荷分散仮想サーバーに使用されます。
11. ［ **Citrix Endpoint Management サーバー**］で［ **サーバーの追加**］をクリックして、負荷分散仮想 **IPにバインドするCitrix Endpoint Management**IPアドレスを追加します。
12. Citrix ADC ダッシュボードで、Citrix Gateway とCitrix Endpoint Management 負荷分散が次のように構成されていることを確認します。

ユーザープリンシパル名 (UPN) の代わりとしてユーザー証明書で sAMAccount 属性を使用する場合は、の説明に従って証明書プロファイルを構成クライアント証明書認証のためのCitrix Gateway の手動構成します。

Citrix モバイル生産性アプリを使用したモバイルデバイスからのアクセスの許可

Citrix ADC for XenMobile ウィザードでは、サポートされているデバイスからCitrix Gateway 経由で内部ネットワークのモバイルアプリやリソースに接続するために必要な設定を構成します。ユーザーは、Secure Hub（以前はWorx Home）を使用して接続し、Micro VPNトンネルを確立します。ユーザーが接続すると、VPNトンネルがCitrix Gateway に開き、内部ネットワークの XenMobile に渡されます。ユーザーは、XenMobile からWeb、モバイル、およびSaaSアプリケーションにアクセスできます。

複数のデバイスでCitrix Gateway に同時に接続するときに、ユーザーが単一のユニバーサルライセンスを使用できるようにするには、仮想サーバーでセッション転送を有効にします。詳しくは、「仮想サーバでの接続タイプの設定」を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix ADC for XenMobile ウィザードを使用した後に構成を変更する必要がある場合は、この記事のセクションを参照してください。設定を変更する前に、変更の影響を理解しておいてください。詳細については、XenMobileの展開記事を参照してください。

Citrix Gateway でのSecure Browse 構成

Secure Browse は、グローバル設定の一部として、またはセッションプロファイルの一部として変更できます。セッション・ポリシーは、ユーザー、グループ、または仮想サーバーにバインドできます。Secure Browse を設定する場合は、クライアントレスアクセスも有効にする必要があります。ただし、クライアントレスアクセスでは、Secure Browse を有効にする必要はありません。クライアントレスアクセスを設定する場合は、**\[クライアントレスアクセス URL エンコーディング**\] を \[クリア\]** に設定します。

Secure Browse をグローバルに構成するには：

1. 構成ユーティリティの ［**構成** ］タブのナビゲーションペインで **Citrix Gateway** を展開し、［**グローバル設定** ］をクリックします。
2. 詳細ウィンドウで、\[**設定**\] の \[**グローバル設定の変更**\] をクリックします。
3. ［ **グローバルCitrix Gateway 設定** ］ダイアログボックスの［ **セキュリティ］タブで、［セキュリティ** で **Secure Browse** をクリックし、［ **OK**］ をクリックします。

セッション・ポリシーおよびプロファイルでSecure Browse を構成するには：

1. 構成ユーティリティーの **構成** タブのナビゲーションペインで、［ **Citrix Gateway**］**>**［**ポリシー** ］の順に展開し、［ **セッション** ］をクリックします。
2. 詳細ウィンドウで、次のいずれかの操作を行います。
   - 新しいセッションポリシーを作成する場合は、\[**Add**\] をクリックします。
   - 既存のポリシーを変更する場合は、ポリシーを選択して \[**開く**\] をクリックします。
3. ポリシーで、新しいプロファイルを作成するか、既存のプロファイルを変更します。これを行うには、次のいずれかの操作を行います。
   - \[**プロファイルの要求**\] の横にある \[**新規**\] をクリックします。
   - \[**プロファイルの要求**\] の横にある \[**変更**\] をクリックします。
4. \[**セキュリティ** \] タブの \[セキュリティで **Secure Browse** \] の横にある \[**グローバルに上書き** \] をクリックし、\[**セキュリティで保護された参照** \] を選択します。
5. 次のいずれかを行います：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 新しいプロファイルを作成する場合は、\[**Create**\] をクリックし、ポリシーダイアログボックスで式を設定し、\[**Create**\] をクリックして、\[**Close**\] をクリックします。
- 既存のプロファイルを修正する場合は、選択後に \[**OK** \] を 2 回クリックします。

セキュアSecure Browse モードで Secure Web のトラフィックポリシーを設定するには：

次の手順に従って、Secure Web トラフィックをセキュアSecure Browse モードでプロキシサーバー経由でルーティングするトラフィックポリシーを設定します。

1. 構成ユーティリティの \[**構成** \] タブで、\[**Citrix Gateway\] > \[ポリシー** \] を展開し、\[**トラフィック** \] をクリックします。
2. 右ペインで、\[**Traffic Profiles** \] タブをクリックし、\[**Add** \] をクリックします。
3. \[**名前**\] にプロファイルの名前を入力し、\[**プロトコル**\] として \[**TCP**\] を選択し、残りの設定はそのままにします。
4. **［作成］** をクリックします。
5. \[**トラフィックプロファイル** \] タブをクリックし、\[**追加** \] をクリックします。
6. \[**名前\]**にプロファイルの名前を入力し、\[**プロトコル**\] として \[**HTTP**\] を選択します。 このトラフィックプロファイルは、HTTP と SSL の両方用です。CVPN トラフィックは、宛先ポートまたはサービスタイプに関係なく、設計上 HTTP トラフィックです。したがって、トラフィックプロファイルで SSL トラフィックと HTTP トラフィックの両方を **HTTP** として指定します。
7. 「 **プロキシ**」に、プロキシ・サーバーのIPアドレスを入力します。「 **ポート**」に、プロキシ・サーバーのポート番号を入力します。
8. **［作成］** をクリックします。
9. \[**トラフィックプロファイル** \] タブをクリックし、\[**追加** \] をクリックします。
10. トラフィックポリシーの **名前** を入力し、\[**Request Profile** \] で、ステップ 3 で作成したトラフィックプロファイルを選択します。次の **式** を入力し、\[**作成** \] をクリックします。

    REQ.HTTP.HEADER HOSTにActiveSyncServerが含まれています || REQ.HTTP.HEADER User-Agent CONTAINS WorxMail || REQ.HTTP.HEADER User-Agent CONTAINS com.zenprise || REQ.HTTP.HEADER User-Agent CONTAINS WorxHome || REQ.HTTP.URL CONTAINS AGServices || REQ.HTTP.URL CONTAINS StoreWeb

    このルールは、ホストヘッダーに基づいてチェックを実行します。プロキシからのアクティブ同期トラフィックをバイパスするには、 **ActiveSyncServerを適切なActiveSync c** サーバー名に置き換えます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

11. \[**トラフィックプロファイル** \] タブをクリックし、\[**追加** \] をクリックします。トラフィックポリシーの **名前** を入力し、\[**Request Profile** \] で、ステップ 6 で作成したトラフィックプロファイルを選択します。次の **式** を入力し、\[**作成** \] をクリックします。

    (REQ.HTTP.HEADER User-Agent CONTAINS Mozilla || REQ.HTTP.HEADER User-Agent CONTAINS com.citrix.browser || REQ.HTTP.HEADER User-Agent CONTAINS WorxWeb) && REQ.TCP.DESTPORT == 80

12. \[**トラフィックプロファイル** \] タブをクリックし、\[**追加** \] をクリックします。トラフィックポリシーの **名前** を入力し、\[**Request Profile** \] で、ステップ 6 で作成したトラフィックプロファイルを選択します。次の **式** を入力し、\[**作成** \] をクリックします。

    (REQ.HTTP.HEADER User-Agent CONTAINS Mozilla || REQ.HTTP.HEADER User-Agent CONTAINS com.citrix.browser || REQ.HTTP.HEADER User-Agent CONTAINS WorxWeb) && REQ.TCP.DESTPORT == 443

13. **［Citrix Gateway］>［仮想サーバー］**に移動し、右側のペインで仮想サーバーを選択し、［ **編集**］をクリックします。
14. \[**ポリシー** \] 行で、\[**+** \] をクリックします。
15. \[**ポリシーの選択** \] メニューから、\[**トラフィック** \] を選択します。
16. **［続行］** をクリックします。
17. \[**ポリシーのバインド**\] の \[**ポリシーの選択**\] で、\[**>**\] をクリックします。
18. 手順 10 で作成したポリシーを選択し、\[**OK**\] をクリックします。
19. **［バインド］** をクリックします。
20. \[**ポリシー**\] で、\[**トラフィックポリシー**\] をクリックします。
21. \[**VPN 仮想サーバートラフィックポリシーバインディング**\] で、\[**バインドの追加**\] をクリックします。
22. \[**ポリシーのバインド**\] で、\[**ポリシーの選択**\] メニューの横にある \[**>**\] をクリックしてポリシーのリストを表示します。
23. 手順 17 で作成したポリシーを選択し、\[**OK**\] をクリックします。
24. **［バインド］** をクリックします。
25. \[**ポリシー**\] で、\[**トラフィックポリシー**\] をクリックします。
26. \[**VPN 仮想サーバートラフィックポリシーバインディング**\] で、\[**バインドの追加**\] をクリックします。
27. \[**ポリシーのバインド**\] で、\[**ポリシーの選択**\] メニューの横にある \[**>**\] をクリックしてポリシーのリストを表示します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

28. 手順 18 で作成したポリシーを選択し、\[**OK**\] をクリックします。
29. **［バインド］** をクリックします。
30. **［閉じる］** をクリックします。
31. **［完了］** をクリックします。

XenMobile コンソールでSecure Web（WorxWeb）アプリを構成してください。\[**設定\] > \[アプリ**\] に移動し、\[Secure Web アプリ\] を選択し、\[**編集**\] をクリックして、次の変更を行います。

- \[**アプリの情報** \] ページで、\[**初期 VPN モード\]** を **\[Secure Browse** に変更します。
- \[**iOS** \] ページで、\[**初期VPNモード\]** を \[**Secure Browse\]** に変更します。
- \[**Android** \] ページで、\[**優先VPNモード\]** を \[**Secure Browse\]** に変更します。

アプリケーションおよびMDXトークンのタイムアウトの構成

ユーザーが iOS または Android デバイスからログオンすると、アプリケーショントークンまたは MDX トークンが発行されます。トークンは、Secure Ticket Authority（STA）に似ています。

トークンがアクティブになる秒数または分数を設定できます。トークンの有効期限が切れた場合、ユーザーはアプリケーションや Web ページなどの要求されたリソースにアクセスできません。

トークンのタイムアウトはグローバル設定です。この設定を構成すると、Citrix Gateway にログオンするすべてのユーザーに適用されます。

1. 構成ユーティリティの **［構成** ］タブのナビゲーションペインで **Citrix Gateway** を展開し、［ **グローバル設定** ］をクリックします。
2. 詳細ウィンドウで、\[**設定**\] の \[**グローバル設定の変更**\] をクリックします。
3. ［ **グローバルCitrix Gateway 設定** ］ダイアログボックスの［ **クライアントエクスペリエンス］** タブで、［ **詳細設定］** をクリックします。
4. \[**全般** \] タブの \[**アプリケーショントークンのタイムアウト (秒)** \] に、トークンの有効期限が切れるまでの秒数を入力します。デフォルトは **100** 秒です。
5. \[**MDXトークンのタイムアウト (分)**\] に、トークンの有効期限が切れるまでの分数を入力し、\[**OK**\] をクリックします。デフォルトは **10** 分です。

モバイルデバイスのエンドポイント分析の無効化

エンドポイント分析を設定する場合は、エンドポイント分析スキャンが Android または iOS モバイルデバイスで実行されないように、ポリシー式を設定する必要があります。エンドポイント分析スキャンは、モバイルデバイスではサポートされていません。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

エンドポイント分析ポリシーを仮想サーバーにバインドする場合は、モバイルデバイス用のセカンダリ仮想サーバーを作成する必要があります。事前認証または認証後のポリシーは、モバイルデバイスの仮想サーバーにバインドしないでください。

事前認証ポリシーでポリシー式を設定する場合は、ユーザーエージェント文字列を追加して Android または iOS を除外します。ユーザーがこれらのデバイスのいずれかからログオンし、デバイスタイプを除外すると、エンドポイント分析は実行されません。

たとえば、ユーザーエージェントに Android が含まれているかどうか、アプリケーション virus.exe が存在しない場合、および事前認証プロファイルを使用して実行されている場合 keylogger.exe プロセスを終了するには、次のポリシー式を作成します。ポリシー表現は次のようになります。

REQ.HTTP.HEADER User-Agent NOTCONTAINS Android &&
CLIENT.APPLICATION.PROCESS(keylogger.exe) に含まれる ||
CLIENT.APPLICATION.PROCESS (virus.exe) に含まれる

事前認証ポリシーとプロファイルを作成したら、ポリシーを仮想サーバーにバインドします。ユーザーが Android または iOS デバイスからログオンすると、スキャンは実行されません。ユーザーが Windows ベースのデバイスからログオンすると、スキャンが実行されます。

事前認証ポリシーの構成について詳しくは、「エンドポイントポリシーの設定」を参照してください。

AndroidデバイスでDNSサフィックスを使用したDNSクエリのサポート

ユーザーがAndroidデバイスからMicro VPN接続を確立すると、Citrix Gateway はスプリットDNS設定をユーザーデバイスに送信します。Citrix Gateway では、構成したスプリットDNS設定に基づいて、スプリットDNSクエリがサポートされます。Citrix Gateway では、アプライアンス上で構成したDNSサフィックスに基づいたスプリットDNSクエリもサポートできます。ユーザーがAndroidデバイスから接続する場合は、Citrix Gateway でDNS設定を構成する必要があります。

スプリット DNS は次のように動作します。

- スプリット DNS を **\[ローカル\]**に設定すると、Android デバイスはすべての DNS 要求をローカル DNS サーバーに送信します。
- スプリットDNSを **リモート**に設定すると、すべてのDNS要求がCitrix Gateway（リモートDNSサーバー）で構成されたDNSサーバーに送信され、解決されます。
- スプリット DNS を \[**両方**\] に設定すると、Android デバイスは DNS 要求の種類をチェックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- DNS 要求の種類が「A」でない場合は、DNS 要求パケットをローカルおよびリモートの DNS サーバーに送信します。
- DNSリクエストタイプが「A」の場合、Androidプラグインはクエリ FQDNを抽出し、その FQDNをCitrix ADCで設定されたDNSサフィックスリストと照合します。DNS 要求の FQDN が一致すると、DNS 要求がリモート DNS サーバーに送信されます。FQDN が一致しない場合、DNS 要求はローカル DNS サーバーに送信されます。

次の表は、タイプ A のレコードとサフィックス一覧に基づく分割 DNS の動作をまとめたものです。

スプリット DNS 設定	それはタイプAレコードですか?	接尾辞リストに載っていますか?	DNS 要求が送信される場所
Local	[はい] または [いいえ] の両方	[はい] または [いいえ] の両方	Local
Remote	[はい] または [いいえ] の両方	[はい] または [いいえ] の両方	Remote
Both	いいえ	-	Both
Both	はい	はい	Remote
Both	はい	いいえ	Local

DNS サフィックスを構成するには、次の手順を実行します。

1. 構成ユーティリティーの **構成** タブのナビゲーションペインで、［**Citrix Gateway**］>［**ポリシー**］の順に展開し、［**セッション**］をクリックします。
2. 詳細ペインの \[**ポリシー** \] タブでセッションポリシーを選択し、\[**開く** \] をクリックします。
3. \[**プロファイルの要求**\] の横にある \[**変更**\] をクリックします。
4. \[**ネットワーク構成** \] タブで、\[**詳細設定** \] をクリックします。
5. \[**イントラネット IP DNS サフィックス**\] の横の \[**グローバル上書き**\] をクリックし、DNS サフィックスを入力して \[**OK**\] を 3 回クリックします。

Citrix Gateway でスプリットDNSをグローバルに設定するには：

1. 構成ユーティリティの ［**構成**］タブのナビゲーションペインで **Citrix Gateway** を展開し、［**グローバル設定**］をクリックします。
2. 詳細ウィンドウで、\[**設定**\] の \[**グローバル設定の変更**\] をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. \[**クライアントエクスペリエンス** \] タブで、\[**詳細設定** \] をクリックします。
4. \[**全般** \] タブの \[**スプリット DNS** \] で、\[**両方** \]、\[**リモート** \]、または \[**ローカル** \] を選択し、\[**OK** \] をクリックします。

Citrix Gateway のセッションポリシーでスプリットDNSを構成するには：

1. 構成ユーティリティーの **構成** タブのナビゲーションペインで、［**Citrix Gateway**］>［**ポリシー**］の順に展開し、［**セッション**］をクリックします。
2. 詳細ウィンドウの \[**ポリシー** \] タブで、\[**追加** \] をクリックします。
3. \[**名前\]**に、ポリシーの名前を入力します。
4. \[**プロファイルの要求**\] の横にある \[**新規**\] をクリックします。
5. \[**名前\]**に、プロファイルの名前を入力します。
6. \[**クライアントエクスペリエンス** \] タブで、\[**詳細設定** \] をクリックします。
7. \[**全般** \] タブの \[**スプリット DNS** \] の横にある \[**グローバル上書き** \] をクリックし、\[**両方** \]、\[**リモート** \]、または \[**ローカル** \] を選択して、\[**OK** \] をクリックします。
8. \[**セッションポリシーの作成**\] ダイアログボックスで、\[**名前付き式**\] の横にある \[**全般**\]、\[**True**\]、\[**式の追加**\]、\[**作成** \]、\[**閉じる** \] の順にクリックします。

Citrix Endpoint Management、Citrix Virtual Apps、およびデスクトップを使用した展開

ユーザーは、Windows、Web、SaaS、およびモバイルアプリケーション、およびネットワークでホストされている仮想デスクトップに接続できます。Citrix Gateway、Citrix Endpoint Management、およびCitrix Virtual Apps and Desktops を使用して、リモートユーザーおよび内部ユーザーにアプリケーションおよびデスクトップへのアクセスを提供できます。Citrix Gateway は、ユーザーを認証し、Citrix Workspace アプリまたはSecure Hub を使用してアプリケーションへのアクセスを許可します。

ユーザーは、Citrix WorkspaceアプリとStoreFront を使用して、Citrix Virtual Appsで公開されたWindowsベースのアプリとCitrix Virtual Desktops で公開された仮想デスクトップに接続します。

Citrix Endpoint Management には、ユーザーがWeb、SaaS、およびMDXアプリケーションに接続できるようにするCitrix Endpoint Management が含まれています。Endpoint Management では、ShareFileドキュメントとともに、シングルサインオン（SSO）用のウェブ、SaaS、MDXアプリケーションを管理できます。Endpoint Management は、内部ネットワークにインストールします。リモートユーザーは、Citrix Gateway を介してEndpoint Management に接続し、アプリケーションおよびShareFileデータにアクセスします。リモートユーザーは、Citrix Gatewayプラグイ

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ン、Citrix Workspace アプリ、またはSecure Hub のいずれかを使用して接続し、アプリケーションおよびShareFileにアクセスできます。内部ネットワークにいるユーザーは、Citrix Workspace アプリを使用してEndpoint Management に直接接続できます。 次の図は、Endpoint ManagementとStoreFront を使用して展開されたCitrix Gateway を示しています。

展開環境で、Endpoint Management からMDXアプリケーションにアクセスでき、StoreFront からWindowsベースのアプリケーションにアクセスできる場合は、次の図に示すように、StoreFrontの前にEndpoint Management を展開します。

図1：StoreFront の前でEndpoint Management を使用したCitrix Gateway の展開



展開環境でMDXアプリケーションへのアクセスが提供されていない場合、StoreFront は、次の図に示すように、Endpoint Management の前に存在します。

図2：Endpoint Management の前でStoreFront を使用したCitrix Gateway の展開



展開するたびに、StoreFront とEndpoint Management が内部ネットワークに存在し、Citrix Gateway がDMZに存在する必要があります。Endpoint Managementの展開について詳しくは、「Endpoint Management インストール」を参照してください。 StoreFrontの展開について詳しくは、「StoreFront」を参照してください。

ダブルホップDMZでの展開

内部ネットワークを保護するために、3つのファイアウォールを使用する場合があります。3つのファイアウォールは、DMZを2つの段階にわけて、内部ネットワークにさらなるセキュリティを提供します。このネットワーク構成を、ダブルホップDMZと呼びます。

図1：ダブルホップDMZにデプロイされたCitrix Gateway アプライアンス



注

：説明のため、前述の例では、StoreFront、Web InterfaceおよびCitrix Virtual Apps で3つのファイアウォールを使用したダブルホップ構成について説明していますが、DMZ内に1つのアプライアンス、安全なネットワーク内に1つのアプライアンスを含むダブルホップDMZを使用することもできます。DMZ 内の 1 つのアプライアンスとセキュアネットワーク内の 1 つのアプライアンスでダブルホップ構成を構成する場合、3 番目のファイアウォールでポートを開く手順は無視できます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ダブルホップDMZは、Citrix StoreFront またはCitrixCitrix Gateway プロキシと並行してインストールされたWeb Interfaceと連携するように構成できます。ユーザーは、Citrix Workspace アプリを使用して接続します。

注

・StoreFront を使用してダブルホップDMZにCitrix Gateway を展開すると、Citrix Workspace アプリの電子メールベースの自動検出が機能しません。

ダブルホップDMZでのCitrix Gateway の展開

内部ネットワークを保護するために、3つのファイアウォールを使用する場合があります。3つのファイアウォールは、DMZを2つの段階にわけて、内部ネットワークにさらなるセキュリティを提供します。このネットワーク構成を、ダブルホップDMZと呼びます。Citrix Virtual Apps および StoreFront を使用して、ダブルホップDMZにCitrix Gatewayを展開できます。

図1：ダブルホップDMZにデプロイされたCitrix Gateway アプライアンス



注：説明のため、前述の例では、3 つのファイアウォールと Web Interface を使用したダブルホップ構成について説明していますが、DMZ 内の 1 つのアプライアンスとセキュアネットワーク内の 1 つのアプライアンスを持つダブルホップ DMZ を使用することもできます。DMZ 内の 1 つのアプライアンスとセキュアネットワーク内の 1 つのアプライアンスでダブルホップ構成を構成する場合、3 番目のファイアウォールでポートを開く手順は無視できます。

ダブルホップDMZは、Citrix StoreFront またはWeb Interfaceで動作するように構成できます。ユーザーは、Citrix Workspace アプリを使用して接続します。

注

StoreFront を使用してダブルホップDMZにCitrix Gateway を展開すると、Citrix Workspace アプリの電子メールベースの自動検出が機能しません。

ファイアウォールで適切なポートを開く

ダブルホップ DMZ 展開に関連するさまざまなコンポーネント間で発生するさまざまな接続をサポートするために、ファイアウォールで適切なポートが開いていることを確認する必要があります。接続処理の詳細については、「ダブルホップDMZ配置における通信フロー」を参照してください。

次の図は、ダブルホップ DMZ 配置で使用できる一般的なポートを示しています。



© 1997–2026 Citrix Systems, Inc. All rights reserved.

次の表に、最初のファイアウォールを介して発生する接続と、接続をサポートするために開く必要があるポートを示します。

最初のファイアウォールを介した接続	使用するポート
インターネットからのWebブラウザは、最初のDMZでCitrix Gateway に接続します。**注：** Citrix Gateway には、ポート80で行われた接続をセキュアなポートにリダイレクトするオプションがあります。Citrix Gateway でこのオプションを有効にすると、最初のファイアウォールからポート80を開くことができます。ユーザーがポート80でCitrix Gateway に暗号化されていない接続を行うと、Citrix Gatewayは自動的に安全なポートにリダイレクトされます。	最初のファイアウォールを介して TCP ポート 443 を開きます。
インターネットからのCitrix Workspace アプリは、最初のDMZでCitrix Gateway に接続します.	最初のファイアウォールを介して TCP ポート 443 を開きます。

次の表に、2 番目のファイアウォールを介して発生する接続と、接続をサポートするために開く必要があるポートを示します。

2 番目のファイアウォールを介した接続	使用するポート
最初のDMZのCitrix Gateway は、2番目のDMZのWeb Interfaceに接続します.	セキュリティで保護されていない接続の場合は TCP ポート 80、2 番目のファイアウォールを経由してセキュリティで保護された接続の場合は TCP ポート 443 のいずれかを開きます。
最初のDMZのCitrix Gateway は、2番目のDMZのCitrix Gateway に接続します.	TCP ポート 443 を開いて、2 番目のファイアウォールを介したセキュアな SOCKS 接続を確立します。
最初のDMZでCitrix Gateway で認証を有効にした場合、このアプライアンスは内部ネットワークの認証サーバーに接続する必要があります。	認証サーバが接続をリッスンする TCP ポートを開きます。たとえば、RADIUS 用のポート 1812、LDAP 用のポート 389 などがあります。

次の表に、3 番目のファイアウォールを介して発生する接続と、接続をサポートするために開く必要があるポートを示します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3 番目のファイアウォールを介した接続	使用するポート
StoreFront または2番目のDMZのWeb Interfaceは、内部ネットワークのサーバーでホストされているXMLサービスに接続します。	セキュリティで保護されていない接続の場合はポート 80、3 番目のファイアウォールを介した安全な接続の場合はポート 443 のいずれかを開きます。
StoreFront または2番目のDMZのWeb Interfaceは、内部ネットワークのサーバーでホストされているSecure Ticket Authority（STA）に接続します。	セキュリティで保護されていない接続の場合はポート 80、3 番目のファイアウォールを介した安全な接続の場合はポート 443 のいずれかを開きます。
2つ目のDMZのCitrix Gateway は、安全なネットワーク内に存在するSTAに接続します。	セキュリティで保護されていない接続の場合はポート 80、3 番目のファイアウォールを介した安全な接続の場合はポート 443 のいずれかを開きます。
2番目のDMZのCitrix Gateway は、内部ネットワーク上のサーバー上の公開アプリケーションまたは仮想デスクトップにICA接続を行います。	TCPポート1494を開き、3番目のファイアウォールを介したICA接続をサポートします。Citrix Virtual Apps セッション画面の保持を有効にした場合は、1494ではなくTCPポート2598を開きます。
最初のDMZでCitrix Gateway で認証を有効にした場合、このアプライアンスは内部ネットワークの認証サーバーに接続する必要があります。	認証サーバが接続をリッスンする TCP ポートを開きます。たとえば、RADIUS 用のポート 1812、LDAP 用のポート 389 などがあります。

システムのインストール

Citrix Gateway アプライアンスを受け取ったら、アプライアンスを開梱し、サイトとラックを準備します。アプライアンスを設置する場所が環境基準を満たしており、指示に従ってサーバラックが設置されていることを確認したら、ハードウェアを取り付けます。アプライアンスをマウントしたら、ネットワーク、電源、および初期設定に使用するコンソール端末に接続します。アプライアンスの電源を入れたら、初期構成を実行し、管理およびネットワーク IP アドレスを割り当てます。インストール手順に記載されている注意事項と警告を必ず守ってください。

Citrix ADC VPX仮想アプライアンスをインストールする場合は、まず仮想アプライアンスのイメージを取得し、Hypervisor または他の仮想マシンモニターにインストールする必要があります。

Citrix Gatewayアプライアンスを構成する前に、設定を書き留めておくことができるように、Citrix Gateway のインストール前のチェックリストトピックを使用することをお勧めします。この

© 1997–2026 Citrix Systems, Inc. All rights reserved.

チェックリストには、Citrix Gateway とアプライアンスのインストールに関する情報が含まれています。

証明書のインストールと管理

Citrix Gateway では、証明書を使用して安全な接続を作成し、ユーザーを認証します。

セキュアな接続を確立するには、接続の一方の端にサーバー証明書が必要です。サーバー証明書を発行した認証局 (CA) のルート証明書は、接続のもう一方の端に必要です。

- サーバー証明書。サーバー証明書は、サーバーの ID を証明します。Citrix Gateway では、この種類のデジタル証明書が必要です。
- ルート証明書。ルート証明書は、サーバー証明書に署名した CA を識別します。ルート証明書は CA に属します。ユーザーデバイスでは、サーバー証明書を検証するために、このタイプのデジタル証明書が必要です。

ユーザーデバイス上のWebブラウザとの安全な接続を確立すると、サーバーはその証明書をデバイスに送信します。

ユーザーデバイスがサーバー証明書を受信すると、Internet ExplorerなどのWebブラウザは、証明書を発行したCAと、そのCAがユーザーデバイスによって信頼されているかどうかを確認します。CA が信頼されていない場合、またはテスト証明書の場合、Web ブラウザは、証明書を受け入れるか拒否するかをユーザに求めます（サイトへのアクセスを効果的に許可または拒否します）。

Citrix Gateway では、次の3種類の証明書がサポートされています。

- 仮想サーバーにバインドされ、サーバーファームへの接続にも使用できるテスト証明書。Citrix Gateway には、テスト証明書がプリインストールされています。
- CA によって署名され、秘密キーとペアになっている PEM または DER 形式の証明書。
- 証明書と秘密キーを格納または転送するために使用される PKCS #12 形式の証明書。PKCS #12 証明書は通常、既存のWindows証明書からPFXファイルとしてエクスポートされ、Citrix Gateway にインストールされます。

ThawteやVeriSignなど、信頼されたCAによって署名された証明書を使用することをお勧めします。

証明書署名要求の作成

SSLまたはTLSを使用してセキュアな通信を提供するには、Citrix Gateway でサーバー証明書が必要です。証明書をCitrix Gateway にアップロードする前に、証明書署名リクエスト（CSR）と秘密キーを生成する必要があります。Citrix Gateway ウィザードまたは構成ユーティリティに含まれて

© 1997–2026 Citrix Systems, Inc. All rights reserved.

いる証明書要求の作成を使用して、CSRを作成します。証明書要求の作成は、署名のために認証局（CA）に電子メールで送信される.csr ファイルと、アプライアンスに残る秘密キーを作成します。CA は証明書に署名し、指定した電子メールアドレスで返却します。署名付き証明書を受け取ったら、Citrix Gateway にインストールできます。CA から証明書を受け取ったら、証明書を秘密キーとペアにします。

重要：Citrix Gateway ウィザードを使用してCSRを作成する場合は、ウィザードを終了し、署名付き証明書がCAから送信されるまで待つ必要があります。証明書を受け取ったら、Citrix Gateway ウィザードを再度実行して設定を作成し、証明書をインストールできます。Citrix Gatewayウィザードの詳細については、「Citrix Gateway ウィザードを使用した設定の構成」を参照してください。

Citrix Gateway ウィザードを使用してCSRを作成するには

1. 構成ユーティリティで、\[構成\] タブをクリックし、ナビゲーションペインで \[Citrix ADC Gateway\] をクリックします。
2. 詳細ペインの \[はじめに\] で、\[Citrix ADC Gatewayウィザード\] をクリックします。
3. \[サーバー証明書の指定\] ページが表示されるまで、ウィザードの指示に従います。
4. \[証明書署名要求の作成\] をクリックし、フィールドに入力します。 注：完全修飾ドメイン名（FQDN）は、Citrix Gateway のホスト名と同じである必要はありません。FQDN は、ユーザーログオンに使用されます。
5. \[作成\] をクリックして証明書をコンピュータに保存し、\[閉じる\] をクリックします。
6. 設定を保存せずにCitrix Gateway ウィザードを終了します。

Citrix ADC GUIを使用してCSRを作成するには

CitrixCitrix Gateway ウィザードを実行せずに、Citrix ADC GUIを使用してCSRを作成することもできます。

1. \[**トラフィック 管理** \] > \[**SSL\] > \[SSL ファイル** \] に移動し、\[**証明書署名要求 (CSR) の作成** \] を選択します。
2. 証明書の設定を完了し、\[**作成**\] をクリックします。

証明書と秘密キーを作成したら、Thawte や VeriSign などの証明書を CA に電子メールで送信します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

既存の証明書のインポートとインストール

既存の証明書は、インターネットインフォメーションサービス（IIS）を実行しているWindows ベースのコンピュータから、またはSecure Gateway を実行しているコンピュータからインポートできます。

証明書をエクスポートするときは、秘密キーもエクスポートしてください。場合によっては、秘密キーをエクスポートできないため、Citrix Gateway に証明書をインストールできないことがあります。このような場合は、証明書署名要求 (CSR) を使用して新しい証明書を作成します。詳しくは、「証明書署名要求の作成」を参照してください。

証明書と秘密キーを Windows からエクスポートすると、コンピューターによって個人情報交換 (.pfx) ファイルが作成されます。このファイルは、PKCS #12 証明書としてCitrix Gateway にインストールされます。

Secure GatewayをCitrix Gateway Gatewayに置き換える場合は、証明書と秘密鍵をSecure Gatewayからエクスポートできます。Secure GatewayからCitrix Gateway Gatewayへのインプレース移行を行う場合は、アプリケーションとアプライアンスの完全修飾ドメイン名（FQDN）が同じである必要があります。Secure Gatewayから証明書をエクスポートすると、すぐにSecure Gatewayを破棄し、Citrix Gateway に証明書をインストールしてから、構成をテストします。FQDNが同じであれば、ネットワーク上でSecure GatewayとCitrix Gatewayを同時に実行することはできません。

Windows Server 2003 または Windows Server 2008 を使用している場合は、Microsoft Management Consoleを使用して証明書をエクスポートできます。詳細については、Windows オンラインヘルプを参照してください。

他のすべてのオプションのデフォルト値をそのまま使用し、パスワードを定義して、.pfx ファイルをコンピューターに保存します。証明書をエクスポートしたら、Citrix Gateway にインストールします。

証明書と秘密キーをCitrix Gateway にインストールするには

1. 構成ユーティリティで、［構成］タブをクリックし、ナビゲーションペインで［Citrix Gateway］をクリックします。
2. 詳細ペインの \[はじめに\] で、\[Citrix Gateway ウィザード\] をクリックします。
3. \[次へ\] をクリックし、既存の仮想サーバーを選択して、\[次へ\] をクリックします。
4. \[証明書オプション\] で、\[PKCS #12 (.pfx) ファイルをインストールする\] を選択します。
5. \[PKCS #12 ファイル名\] で、\[参照\] をクリックし、証明書に移動し、\[選択\] をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

6. \[パスワード\] に、秘密キーのパスワードを入力します。

   これは、証明書を PEM 形式に変換するときに使用したパスワードです。

7. ［次へ］をクリックして、他の設定を変更せずにCitrix Gateway ウィザードを終了します。

証明書がCitrix Gateway にインストールされると、証明書は構成ユーティリティの［SSL］>［証明書］ノードに表示されます。

秘密キーを作成するには

1. 構成ユーティリティの \[構成\] タブのナビゲーションウィンドウで、\[SSL\] をクリックします。
2. 詳細ペインの \[SSL キー\] で、\[RSA キーの作成\] をクリックします。
3. \[Key Filename\] にプライベートキーの名前を入力するか、\[Browse\] をクリックして既存のファイルに移動します。
4. \[キーサイズ (ビット)\] に、秘密キーのサイズを入力します。
5. \[公衆指数\] で、\[F4\] または \[3\] を選択します。

   RSA キーの公開指数値。これは暗号アルゴリズムの一部であり、RSA キーの作成に必要です。値は F4 (16 進数:0x10001) または 3 (16 進数:0x3) です。デフォルトは F4 です。

6. \[キー形式\] で、\[PEM\] または \[DER\] を選択します。証明書にはPEM形式をお勧めします。
7. \[PEM エンコーディングアルゴリズム\] で、\[DES\] または \[DES3\] を選択します。
8. \[PEM パスフレーズ\] および \[パスフレーズの検証\] にパスワードを入力し、\[作成\]、\[閉じる\] の順にクリックします。

   注:パスフレーズを割り当てるには、\[Key Format\] が PEM である必要があり、エンコードアルゴリズムを選択する必要があります。

構成ユーティリティで DSA 秘密キーを作成するには、\[DSA キーの作成\] をクリックします。上記の同じ手順に従って DSA 秘密キーを作成します。

Citrix Gateway への署名付き証明書のインストール

認証局（CA）から署名付き証明書を受け取ったら、アプライアンスの秘密キーとペアリングし、Citrix Gateway に証明書をインストールします。

署名付き証明書と秘密キーをペアリングするには

1. WinSCPなどのセキュアシェル（SSH）プログラムを使用して、証明書をCitrix Gateway のフォルダnsconfig/sslにコピーします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. 構成ユーティリティの \[構成\] タブのナビゲーションウィンドウで、\[SSL\] を展開し、\[証明書\] をクリックします。
3. 詳細ペインで、［Install］をクリックします。
4. \[証明書とキーのペア名\] に、証明書の名前を入力します。
5. 「証明書ファイル名」で、「参照」のドロップダウン・ボックスを選択し、「アプライアンス」をクリックします。
6. 証明書に移動し、\[選択\]、\[開く\] の順にクリックします。
7. 「秘密鍵ファイル名」で、「参照」のドロップダウン・ボックスを選択し、「アプライアンス」をクリックします。秘密キーの名前は、証明書署名要求 (CSR) と同じ名前です。秘密鍵は、Citrix Gateway の\ nsconfig\ ssl ディレクトリにあります。
8. 秘密キーを選択し、\[開く\] をクリックします。
9. 証明書が PEM 形式の場合は、\[パスワード\] に秘密キーのパスワードを入力します。
10. 証明書の有効期限が切れたときの通知を構成する場合は、\[有効期限が切れたときに通知\] を選択します。
11. \[通知期間\] に日数を入力し、\[作成\]、\[閉じる\] の順にクリックします。

証明書と秘密キーを仮想サーバーにバインドするには

証明書と秘密キーのペアを作成してリンクしたら、仮想サーバーにバインドします。

1. 構成ユーティリティの \[構成\] タブのナビゲーションペインで、\[Citrix Gateway\] を展開し、\[仮想サーバー\] をクリックします。
2. 詳細ウィンドウで、仮想サーバーをクリックし、\[開く\] をクリックします。
3. \[証明書\] タブの \[使用可能\] で証明書を選択し、\[追加\] をクリックし、\[OK\] をクリックします。

仮想サーバーからテスト証明書をバインド解除するには

署名付き証明書をインストールした後、仮想サーバーにバインドされているテスト証明書のバインドを解除します。構成ユーティリティーを使用して、テスト証明書のバインドを解除できます。

1. 構成ユーティリティの \[構成\] タブのナビゲーションペインで、\[Citrix Gateway\] を展開し、\[仮想サーバー\] をクリックします。
2. 詳細ウィンドウで、仮想サーバーをクリックし、\[開く\] をクリックします。
3. \[証明書\] タブの \[構成済み\] で、テスト証明書を選択し、\[削除\] をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

認証にデバイス証明書を使用する

Citrix Gateway では、デバイスIDを証明書の秘密キーにバインドできるデバイス証明書チェックがサポートされています。デバイス証明書チェックは、従来の EPA ポリシーまたは高度な EPA ポリシーの一部として設定できます。従来の EPA ポリシーでは、デバイス証明書は事前認証 EPA に対してだけ設定できます。

Citrix Gatewayに2つ以上のデバイス証明書をインストールする場合、ユーザーがCitrix Gatewayへのログオンを開始するとき、またはエンドポイント分析スキャンを実行する前に、正しい証明書を選択する必要があります。

デバイス証明書を作成するときは、X.509 証明書である必要があります。

重要:

Windows では、デフォルトで、デバイス証明書にアクセスするための管理者権限が義務されています。管理者以外のユーザのデバイス証明書チェックを追加するには、VPN プラグインをインストールする必要があります。VPN プラグインのバージョンは、デバイス上の EPA プラグインと同じバージョンである必要があります。

デバイス証明書の作成の詳細については、以下を参照してください。

- Active Directory 証明書サービス (AD CS) のネットワークデバイス登録サービス (NDES)を参照してください。
- Microsoft System Center web サイトの構成マネージャー用の PKI 証明書の展開手順の例:Windows Server 2008 証明機関を参照してください。
- DCE/RPC および Active Directory 証明書プロファイルペイロードを使用して、Microsoft Certificate Authorityから証明書を要求する方法をアップルのサポートウェブサイトでご確認ください。
- iPad/iPhoneの証明書発行「ディレクトリサービスチームに問い合わせる Microsoft サポートブログ」を参照してください。
- ネットワークデバイス登録サービスの設定を参照してください。

従来のEPAポリシーの仮想サーバーでデバイス証明書を有効にしてバインドするには

デバイス証明書を作成したら、Citrix Gateway への既存の証明書のインポートとインストールの手順に従ってCitrix Gateway に証明書をインストールします。証明書をインストールした後、証明書を仮想サーバーにバインドします。

1. 構成ユーティリティで、 **［Citrix Gateway］** > **［仮想サーバー］** に移動します。
2. 詳細ウィンドウで、仮想サーバーをクリックし、\[**編集\] をクリックします。**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. 仮想サーバーの詳細ウィンドウで、鉛筆アイコンをクリックし、\[詳細\] を展開します。
4. \[**デバイス証明書を有効にする\]**を選択します。
5. 表示される選択ダイアログで、\[**Add** \] を選択し、有効にするデバイス証明書をクリックします。選択したデバイス証明書の隣にあるプラス記号のアイコンをクリックし、\[**OK**\] をクリックします。

注： 高度なEPAポリシーの仮想サーバー上でデバイス証明書を有効化およびバインドする方法については、EPA コンポーネントとしての nFactor でのデバイス証明書を参照してください 。

DNS 仮想サーバの構成

DNS 仮想サーバーを構成するには、名前と IP アドレスを指定します。Citrix Gateway 仮想サーバーと同様に、DNS仮想サーバーにIPアドレスを割り当てる必要があります。ただし、ユーザデバイスがすべての内部アドレスを解決できるように、この IP アドレスはターゲットネットワークの内部側にある必要があります。DNS ポートも指定する必要があります。

注：アプライアンスにCitrix ADC負荷分散ライセンスをインストールすると、［仮想サーバーとサービス］ノードはナビゲーションペインに表示されません。この機能は、負荷分散仮想サーバーを使用して構成できます。詳しくは、Citrix eDocsの「Citrix ADC」のトピックを参照してください。

DNS 仮想サーバーを構成するには

1. 構成ユーティリティの \[構成\] タブのナビゲーションウィンドウで、\[仮想サーバーとサービス\] を展開し、\[仮想サーバー\] をクリックします。
2. 詳細ウィンドウで、\[追加\] をクリックします。
3. \[名前\] に、仮想サーバーの名前を入力します。
4. \[IP アドレス\] に、DNS サーバーの IP アドレスを入力します。
5. \[ポート\] に、DNS サーバーがリッスンするポートを入力します。
6. \[プロトコル\] で \[DNS\] を選択し、\[作成\] をクリックします。

最後に、展開環境のニーズに応じて、次の2つの方法のいずれかを使用して、DNS仮想サーバーをCitrix Gateway に関連付けます。

- サーバーをCitrix Gateway にグローバルにバインドします。
- DNS 仮想サーバーを仮想サーバーごとにバインドします。

DNS 仮想サーバをグローバルに展開すると、すべてのユーザがそれにアクセスできます。次に、DNS 仮想サーバーを仮想サーバーにバインドすることで、ユーザーを制限できます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ユーザ接続用の IPv6 の設定

インターネットプロトコルバージョン6（IPv6）を使用して、ユーザー接続をリッスンするように Citrix Gateway を構成できます。次のいずれかの設定を構成する場合は、\[IPv6\] チェックボックスをオンにして、ダイアログボックスに IPv6 アドレスを入力します。

- グローバル設定-公開アプリケーション-ICAプロキシ
- グローバル認証-Radius
- グローバル認証-LDAP
- グローバル認証-TACACS
- セッションプロファイル-公開アプリケーション-ICAプロキシ
- Citrix Gateway 仮想サーバー
- 認証サーバの作成-Radius
- 認証サーバーの作成-LDAP
- 認証サーバの作成-TACACS
- 監査サーバーの作成
- 高可用性のセットアップ
- 高可用性を実現するためのルートモニタのバインド/バインド解除
- 仮想サーバ（負荷分散）

IPv6アドレスでリッスンするようにCitrix Gateway 仮想サーバーを構成すると、ユーザーはCitrix Workspace アプリでのみ接続できます。 Citrix Gateway プラグインを使用したユーザー接続は、IPv6ではサポートされていません。

Citrix Gateway でIPv6を構成するには、次のガイドラインを使用できます。

- Citrix Virtual Apps Web Interface. ユーザー接続用にIPv6を構成し、IPv6を使用するマップされたIPアドレスがある場合、Citrix Virtual Apps およびWeb Interfaceサーバーでも IPv6を使用できます。Web Interfaceは、Citrix Gateway の背後にインストールする必要があります。ユーザーがCitrix Gateway 経由で接続すると、IPv6アドレスはIPv4に変換されます。接続が戻ると、IPv4 アドレスは IPv6 に変換されます。
- 仮想サーバ。Citrix Gateway ウィザードを実行するときに、仮想サーバーのIPv6を構成できます。Citrix Gateway ウィザードの［仮想サーバー］ページで［IPv6］をクリックし、IPアドレスを入力します。Citrix Gateway ウィザードでは、仮想サーバーのIPv6アドレスの構成のみを使用できます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- その他。ICAプロキシ、認証、監査、高可用性用にIPv6を構成するには、ダイアログボックスの「IPv6」チェックボックスを選択し、IPアドレスを入力します。

初回セットアップウィザードを使用したCitrix Gateway の構成

Citrix Gateway（物理アプライアンスまたはVPX仮想アプライアンス）を初めて構成するには、アプライアンスと同じネットワーク上に構成された管理コンピューターが必要です。

アプライアンスの管理IPアドレスとして、Citrix Gateway IP（NSIP）アドレスと、サーバーが接続できるサブネットIP（SNIP）アドレスを割り当てる必要があります。Citrix Gateway とSNIPアドレスの両方に適用されるサブネットマスクを割り当てます。タイムゾーンも設定する必要があります。ホスト名を割り当てる場合は、NSIPアドレスの代わりに名前を指定してアプライアンスにアクセスできます。

初回セットアップウィザードには、2 つのセクションがあります。最初のセクションでは、Citrix Gateway アプライアンスの基本的なシステム設定を構成します。

- NSIPアドレス、SNIPアドレス、サブネット・マスク
- アプライアンスのホスト名
- DNSサーバー
- タイムゾーン
- 管理者パスワード

2 番目のセクションでは、ライセンスをインストールします。DNS サーバーのアドレスを指定すると、ローカルコンピューターからアプライアンスにライセンスをアップロードする代わりに、ハードウェアシリアル番号 (HSN) またはライセンスアクティベーションコード (LAC) を使用してライセンスを割り当てることができます。

注：ライセンスをローカルコンピュータに保存することをお勧めします。

これらの設定の構成が完了すると、Citrix Gateway からアプライアンスの再起動を求めるメッセージが表示されます。アプライアンスに再度ログオンすると、他のウィザードと構成ユーティリティを使用して追加設定を構成できます。

Citrix Gateway ウィザードを使用した設定の構成

セットアップウィザードを実行した後、Citrix Gatewayウィザードを実行してCitrix Gatewayに追加の設定を構成できます。Citrix Gateway ウィザードは、構成ユーティリティから実行します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix Gateway には、テスト証明書が付属しています。認証局（CA）からの署名付き証明書がない場合は、Citrix Gateway ウィザードを使用してテスト証明書を使用できます。署名付き証明書を受け取ったら、テスト証明書を削除し、署名付き証明書をインストールできます。Citrix Gateway を公開する前に、署名付き証明書を取得することをお勧めします。

注：証明書署名リクエスト（CSR）は、Citrix Gateway ウィザードから作成できます。Citrix Gateway ウィザードを使用してCSRを作成する場合は、ウィザードを終了し、CAから署名付き証明書を受け取ったときにウィザードを再度開始する必要があります。証明書について詳しくは、「証明書のインストールと管理」を参照してください。

仮想サーバーを構成するときに、Citrix Gateway ウィザードでインターネットプロトコルバージョン6（IPv6）のユーザー接続を構成できます。ユーザー接続のIPv6の使用について詳しくは、ユーザ接続用の IPv6 の設定を参照してください。

Citrix Gateway ウィザードを起動するには

1. 構成ユーティリティで、［構成］タブをクリックし、ナビゲーションペインで［Citrix Gateway］をクリックします。
2. 詳細ペインの \[はじめに\] で、\[Citrix Gateway ウィザード\] をクリックします。
3. ［Next］をクリックして、ウィザードの指示に従います。

Configuring Settings with the Quick Configuration Wizard

Citrix Gateway で、クイック構成ウィザードを使用して、Citrix Endpoint Management、StoreFront、またはWeb Interfaceとの通信を有効にするための設定を構成できます。構成が完了すると、ウィザードによって、Citrix Gateway、Endpoint Management、StoreFront、またはWeb Interface間の通信に関する適切なポリシーが作成されます。これらのポリシーには、認証、セッション、およびクライアントレスアクセスポリシーが含まれます。ウィザードが完了すると、ポリシーが仮想サーバにバインドされます。

クイック構成ウィザードを完了すると、Citrix Gateway はEndpoint Management またはStoreFront と通信でき、ユーザーはWindowsベースのアプリケーション、仮想デスクトップ、Web、SaaS、およびモバイルアプリケーションにアクセスできます。ユーザーはEndpoint Management に直接接続できます。

ウィザードでは、次の設定を構成します。

- 仮想サーバ名、IP アドレス、およびポート
- 非セキュアポートからセキュアポートへのリダイレクション
- 証明書

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- LDAP サーバー
- RADIUSサーバー
- 認証用のクライアント証明書 (2 要素認証のみ)
- Endpoint Management、StoreFront、またはWeb Interface

クイック構成ウィザードは、LDAP、RADIUS、およびクライアント証明書の認証をサポートします。ウィザードで 2 要素認証を構成するには、次のガイドラインに従います。

- プライマリ認証タイプとして LDAP を選択した場合は、セカンダリ認証タイプとして RADIUS を設定できます。
- プライマリ認証タイプとして RADIUS を選択した場合は、セカンダリ認証タイプとして LDAP を設定できます。
- プライマリ認証タイプとしてクライアント証明書を選択した場合は、セカンダリ認証タイプとして LDAP または RADIUS を設定できます。

クイック構成ウィザードを使用して複数の LDAP 認証ポリシーを作成することはできません。たとえば、\[サーバーログオン名の属性\] フィールドで sAMAccountName を使用するポリシーと、\[サーバーログオン名の属性\] フィールドでユーザープリンシパル名 (UPN) を使用する LDAP ポリシーを構成するとします。これらの個別のポリシーを構成するには、Citrix Gateway 構成ユーティリティを使用して認証ポリシーを作成します。詳しくは、「LDAP認証の構成」を参照してください。

簡易構成ウィザードでは、以下の方法を使用して、Citrix Gateway の証明書を構成できます。

- アプライアンスにインストールされている証明書を選択します。
- 証明書と秘密キーをインストールします。
- テスト証明書を選択します。 注:テスト証明書を使用する場合は、証明書に含まれる完全修飾ドメイン名 (FQDN) を追加する必要があります。

クイック構成ウィザードは、次の 2 つの方法のいずれかで開くことができます。

- Citrix Gateway のログオンページで、［展開の種類］で［Citrix Gateway］を選択すると、［ホーム］タブが表示されます。\[展開の種類\] で他のオプションを選択すると、\[ホーム\] は表示されません。
- Citrix Gatewayの詳細ペインの［Citrix Gateway の作成/監視］リンクから選択します。Citrix ADC機能を有効にするライセンスをインストールすると、このリンクが表示されます。Citrix Gateway のみのアプライアンスのライセンスを取得した場合、リンクは表示されません。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ウィザードを最初に実行した後、ウィザードを再度実行して、追加の仮想サーバーと設定を作成できます。

重要：クイック構成ウィザードを使用して追加のCitrix Gateway 仮想サーバーを構成する場合は、一意のIPアドレスを使用する必要があります。既存の仮想サーバーで使用されている IP アドレスと同じ IP アドレスを使用することはできません。たとえば、IP アドレスが 192.168.10.5 で、ポート番号が 80 の仮想サーバーがあるとします。ポート番号 443 の IP アドレス 192.168.10.5 の 2 番目の仮想サーバーを作成するのには、クイック構成ウィザードを実行します。構成を保存しようとすると、エラーが発生します。

クイック構成ウィザードで設定を構成するには

1. 構成ユーティリティで、次のいずれかの操作を行います。
    a. アプライアンスにCitrix Gateway のみのライセンスが付与されている場合は、［ホーム］タブをクリックします。
    b. アプライアンスにCitrix ADC機能を含めるライセンスが付与されている場合は、［構成］タブのナビゲーションペインで［Citrix Gateway］をクリックし、詳細ペインの［はじめに］で［エンタープライズストア用のCitrix Gatewayの構成］をクリックします。
2. ダッシュボードで、［新しいCitrix Gateway の作成］をクリックします。
3. Citrix Gateway の設定で、以下を構成します。
    a. \[名前\] に、仮想サーバーの名前を入力します。
    b. \[IP アドレス\] に、仮想サーバーの IP アドレスを入力します。
    c. ［Port］ボックスにポート番号を入力します。デフォルトのポート番号は 443 です。
    d. ポート 80 からポート 443 へのユーザー接続を許可するには、\[ポート 80 からセキュアポートへ要求をリダイレクト\] を選択します。
4. ［続行］ をクリックします。
5. \[証明書\] ページで、次のいずれかの操作を行います。
    a. \[証明書の選択\] をクリックし、\[証明書\] で証明書を選択します。
    b. \[証明書のインストール\] をクリックし、\[証明書の選択\] で \[キーの選択\] の \[参照\] をクリックして、証明書と秘密キーに移動します。
    c. \[テスト証明書の使用\] をクリックし、\[証明書 FQDN\] に、テスト証明書に含まれる完全修飾ドメイン名 (FQDN) を入力します。
6. ［続行］ をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

7. \[認証設定\] で、次の操作を行います。

    a. \[プライマリ認証\] で、\[LDAP\]、\[RADIUS\]、または \[証明書\] を選択します。

    b. 認証サーバーを選択するか、前の手順で選択した認証タイプの設定を構成します。\[Cert\] を選択した場合は、クライアント証明書を選択するか、新しいクライアント証明書をインストールします。

    c. \[セカンダリ認証\] で、認証の種類を選択し、認証サーバーの設定を構成します。

8. ［続行］ をクリックします。

ネットワークと認証の設定が完了したら、Citrix Endpoint Management またはCitrix Virtual Apps and Desktops（StoreFront またはWeb Interface）の設定を構成できます。

エンタープライズストア設定の構成

Citrix Gateway では、Web、SaaS、モバイルアプリケーションおよびShareFileへのユーザーアクセスは、Endpoint Management 経由でのみサポートされます。StoreFront またはWeb Interfaceも展開すると、ユーザーはWindowsベースのアプリと仮想デスクトップにアクセスできます。次のオプションの設定を構成できます。

- Endpoint Management のみ
- StoreFront のみ
- Endpoint Management とStoreFront の併用
- Web Interfaceのみ

前の手順で \[続行\] をクリックすると、展開シナリオの設定を構成できます。次の手順は、Citrix の統合設定ページで開始します。

仮想サーバーを作成した後、クイック構成ウィザードで仮想サーバーを編集しても、Citrix Endpoint Management またはCitrix Virtual Apps and Desktopsの設定は変更できません。

たとえば、Citrix Enterprise Storeの設定を構成する前に仮想サーバーの構成をキャンセルすると、設定を行わずにWebインターフェイスが自動的に選択されます。この状況が発生した場合、Web Interfaceを構成するために仮想サーバーの詳細を編集することはできますが、Citrix Endpoint Management に切り替えることはできません。切り替えるには、新しい仮想サーバを作成する必要があります。構成中はウィザードをキャンセルしないでください。Web Interface 仮想サーバーが必要ない場合は、クイック構成ウィザードを使用して削除できます。

StoreFront のみの設定を構成するには

1. ［Citrix Virtual Apps and Desktops］をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. \[展開の種類\] で、\[StoreFront\] を選択します。
3. StoreFront サーバーの完全修飾ドメイン名（FQDN）に、StoreFront サーバーの完全修飾ドメイン名（FQDN）を入力します。
4. Receiver for Webパスで、デフォルトのパスをそのまま使用するか、独自のパスを入力します。
5. セキュアなユーザー接続の場合は、\[HTTPS\] を選択します。
6. 「シングルサインオンドメイン」で、StoreFront のドメインを入力します。
7. StoreFront を展開し、Citrix Virtual Apps またはCitrix Virtual Desktops から公開アプリケーションへのアクセスを許可する場合は、STA URLに、Secure Ticket Authority（STA）を実行しているサーバーの完全なIPアドレスまたはFQDNを入力します。
8. ［完了］ をクリックします。

ユーザーがCitrix Gateway 経由でStoreFront に接続すると、ユーザーはReceiver for Webまたは Receiverからアプリやデスクトップを起動できます。

Endpoint Management のみの設定を構成するには

1. ［Citrix Endpoint Management］をクリックします。
2. \[App Controller FQDN\] に、Endpoint Management の FQDN を入力します。
3. ［完了］ をクリックします。

Web Interface設定を構成するには

1. クイック構成ウィザードで、［Citrix Virtual Apps and Desktops］をクリックします。
2. \[展開の種類\] で \[Web Interface\] を選択し、次の構成を行います。
    a. ［Citrix Virtual Apps サイトのURL］に、Web Interfaceの完全なIPアドレスまたはFQDNを入力します。
    b. Citrix Virtual Apps サービスサイトのURLに、PNAgentパスを含むWeb Interfaceの完全なIPアドレスまたはFQDNを入力します。既定のパスを入力することも、独自のパスを入力することもできます。
    c. 「シングル・サインオン・ドメイン」で、使用するドメインを入力します。
    d. \[STA URL\] に、STA を実行しているサーバーの完全な IP アドレスまたは FQDN を入力します。
3. ［完了］ をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

仮想サーバーの作成

仮想サーバーは、ユーザーがログオンするアクセスポイントです。各仮想サーバには、独自の IP アドレス、証明書、およびポリシーセットがあります。仮想サーバは、着信トラフィックを受け入れるIPアドレス、ポート、およびプロトコルの組み合わせで構成されます。仮想サーバーには、ユーザーがアプライアンスにログオンするときの接続設定が含まれます。仮想サーバーでは、次の設定を構成できます。

- 証明書
- 認証
- ポリシー
- ブックマーク
- アドレスプール (IP プールまたはイントラネット IP とも呼ばれます)
- Citrix Gateway を使用したダブルホップDMZ展開
- Secure Ticket Authority
- SmartAccess ICAプロキシセッション転送

Citrix Gateway ウィザードを実行すると、ウィザード中に仮想サーバーを作成できます。追加の仮想サーバは、次の方法で構成できます。

- **仮想サーバノードから**。このノードは、構成ユーティリティのナビゲーション区画にあります。構成ユーティリティを使用して、仮想サーバーを追加、編集、および削除できます。
- **クイック構成ウィザードを使用します**。Citrix Endpoint Management、StoreFront またはWeb Interfaceを環境内に展開する場合は、クイック構成ウィザードを使用して、仮想サーバーと展開に必要なすべてのポリシーを作成できます。

ユーザーがログオンして RADIUS などの特定の認証タイプを使用できるようにするには、仮想サーバーを構成し、サーバーに一意の IP アドレスを割り当てます。ユーザーがログオンすると、仮想サーバーに送信され、RADIUS 資格情報の入力が求められます。

また、ユーザーがCitrix Gateway にログオンする方法を構成することもできます。セッションポリシーを使用して、ユーザーソフトウェアの種類、アクセス方法、およびログオン後にユーザーに表示されるホームページを構成できます。

仮想サーバでの接続タイプの設定

仮想サーバーを作成および構成するときに、次の接続オプションを構成できます。

- Citrix Workspace アプリとの接続は、SmartAccess、エンドポイント分析、またはネットワーク層トンネリング機能を使用しない、Citrix Virtual Apps and Desktops にのみ行えます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Citrix Gateway プラグインとSmartAccessとの接続。これにより、SmartAccess、エンドポイント分析、ネットワーク層トンネリング機能を使用できます。
- モバイルデバイスからCitrix Gateway へのマイクロVPN接続を確立するSecure Hub との接続。
- 複数のデバイスからユーザーがICAセッション・プロトコルを介して行われる並列接続。複数のユニバーサルライセンスを使用できないように、接続は単一のセッションに移行されます。

ユーザソフトウェアを使用せずにユーザがログオンできるようにするには、クライアントレスアクセスポリシーを設定して、それを仮想サーバにバインドします。

仮想サーバー上で基本接続または SmartAccess 接続を構成するには

1. 構成ユーティリティの \[構成\] タブのナビゲーションペインで、\[Citrix Gateway\] を展開し、\[仮想サーバー\] をクリックします。
2. 詳細ウィンドウで、\[追加\] をクリックします。
3. \[名前\] に、仮想サーバーの名前を入力します。
4. \[IP アドレス\] と \[ポート\] に、仮想サーバーのIPアドレスとポート番号を入力します。
5. 次のいずれかを行います：
   - ICA接続のみを許可するには、\[基本モード\] をクリックします。
   - Secure Hub、Citrix Gateway プラグイン、およびSmartAccessを使用したユーザーのログオンを許可するには、［SmartAccess モード］をクリックします。
   - SmartAccessが複数のユーザー接続のICAプロキシセッションを管理できるようにするには、［ICAプロキシセッションの移行］をクリックします。
6. 仮想サーバーのその他の設定を構成し、\[作成\]、\[閉じる\] の順にクリックします。

Web Interfaceを使用したCitrix Virtual Apps and Desktops のリソースへのアクセス

Citrix Virtual Apps and Desktopsを実行している1台以上のコンピューターでサーバーファームが作成されます。エンタープライズネットワークにサーバーファームが含まれている場合は、NetScaler Gateway を展開して、Web Interfaceを使用して公開アプリケーションまたは仮想デスクトップへの安全なインターネットアクセスを提供できます。

このような展開では、NetScaler Gateway はWeb InterfaceとSecure Ticket Authority（STA）をサポートし、Citrix Virtual Appsを実行しているコンピューターでホストされている公開アプリケー

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ションまたはCitrix Virtual Desktopsが提供する仮想デスクトップへの認証、承認、およびリダイレクトを提供します。

この機能は、NetScaler Gateway をWeb Interface、Citrix Virtual Apps and Desktopsと統合することによって実現されます。この統合により、Web Interface に対する高度な認証とアクセス制御オプションが提供されます。Web Interfaceの詳細については、Citrix ドキュメントライブラリのWeb Interfaceのドキュメントを参照してください。

サーバーファームへのリモート接続には、NetScaler Gateway プラグインは必要ありません。公開アプリケーションまたはデスクトップにアクセスするには、Citrix Workspace アプリを使用して接続します。

NetScaler Gateway とCitrix Virtual Apps and Desktops の統合

ユーザー接続用にNetScaler Gateway を構成するときは、Citrix Virtual Apps、Citrix Virtual Desktops、またはその両方へのネットワークトラフィックの設定を含めることができます。これを行うには、NetScaler Gateway とWeb Interfaceを相互に通信するように構成します。

これらの製品を統合するためのタスクは次のとおりです。

- Citrix Virtual Apps and Desktops ファームにWeb Interfaceサイトを作成する。
- Web Interface内の設定を構成して、NetScaler Gateway 経由でユーザー接続をルーティングします。
- Web InterfaceおよびSecure Ticket Authority（STA）と通信するようにNetScaler Gateway を構成する。

また、NetScaler Gateway をダブルホップDMZに展開して、Citrix Virtual Apps サーバーファームと通信するようにNetScaler Gateway を構成することもできます。詳細については、「ダブルホップDMZでのNetScaler Gateway の展開」を参照してください。

NetScaler Gateway とWeb Interfaceは、STAおよびCitrix XMLサービスを使用してユーザー接続を確立します。STAおよびXMLサービスは、Citrix Virtual Apps and Desktops サーバー上で実行されます。

サーバーファームへのセキュアな接続を確立する

次の例は、DMZに展開されたNetScaler Gateway がWeb Interfaceをサポートし、セキュアなエンタープライズネットワークで利用可能な公開リソースへのセキュアな単一アクセスポイントを提供する方法を示しています。

この例では、次の条件が存在します：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- インターネットからのユーザーデバイスは、Citrix Workspaceアプリを使用してNetScaler Gateway に接続します。
- Web Interfaceは、セキュリティで保護されたネットワーク内のNetScaler Gateway の背後に存在します。ユーザーデバイスはNetScaler Gateway への最初の接続を行い、接続がWeb Interfaceに渡されます。
- セキュアネットワークには、サーバファームが含まれています。このサーバーファーム内の1つのサーバーは、セキュリティで保護されたチケット機関（STA）とCitrix XMLサービスを実行します。STAおよびXMLサービスは、Citrix Virtual Apps and Desktops のいずれかで実行できます。

プロセスの概要:サーバーファーム内の公開リソースへのユーザーアクセス

1. リモートユーザーは、NetScaler Gateway のアドレス（Webブラウザーのアドレスフィールドなど）を入力します。 `https://www.ag.wxyco.com` ユーザーデバイスはこの SSL 接続をポート 443 で試みます。接続を成功させるには、ファイアウォールを介してポートを開く必要があります。
2. NetScaler Gateway は接続要求を受信し、ユーザーは資格情報を要求されます。資格情報は NetScaler Gateway を介して返され、ユーザーは認証され、接続がWeb Interfaceに渡されます。
3. Web Interfaceは、サーバーファームで実行されているCitrix XMLサービスにユーザーの資格情報を送信します。
4. XML サービスは、ユーザーの資格情報を認証し、ユーザーがアクセスを許可されている公開アプリケーションまたはデスクトップの一覧を Web Interface に送信します。
5. Web Interfaceは、ユーザーがアクセスを許可されている公開リソース（アプリケーションまたはデスクトップ）のリストをWebページに入力し、このWebページをユーザーデバイスに送信します。
6. ユーザーが公開アプリケーションまたはデスクトップのリンクをクリックします。HTTP 要求が Web Interface に送信され、ユーザーがクリックした公開リソースが示されます。
7. Web Interface は XML サービスと対話し、公開リソースが実行されているサーバーを示すチケットを受け取ります。
8. Web インターフェイスは STA にセッションチケット要求を送信します。この要求は、公開リソースが実行されているサーバーの IP アドレスを指定します。STAがこのIPアドレスを保存し、要求されたセッションチケットをWeb Interfaceに送信します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

9. Web Interfaceは、STAによって発行されたチケットを含むICAファイルを生成し、それをユーザーデバイス上のWebブラウザに送信します。Web Interfaceによって生成されたICAファイルには、NetScaler Gateway の完全修飾ドメイン名（FQDN）またはドメインネームシステム（DNS）名が含まれています。要求されたリソースを実行しているサーバーの IP アドレスは、ユーザーに公開されることはありません。
10. ICAファイルには、Citrix Workspace アプリを起動するようにWebブラウザーに指示するデータが含まれています。ユーザーデバイスは、ICAファイル内のNetScaler Gateway FQDNまたはDNS名を使用してNetScaler Gateway に接続します。最初のSSL/TLSハンドシェークは、NetScaler Gateway のアイデンティティを確立するために発生します。
11. ユーザーデバイスはセッションチケットをNetScaler Gateway に送信し、NetScaler Gatewayはチケット検証のためにSTAに接続します。
12. STAは、要求されたアプリケーションが存在するサーバーのIPアドレスをNetScaler Gatewayに返します。
13. NetScaler Gateway は、サーバーへのTCP接続を確立します。
14. NetScaler Gateway は、ユーザーデバイスとの接続ハンドシェイクを完了し、サーバーとの接続が確立されたことをユーザーデバイスに通知します。ユーザーデバイスとサーバー間のそれ以降のすべてのトラフィックは、NetScaler Gateway を介してプロキシされます。ユーザーデバイスとNetScaler Gateway 間のトラフィックは暗号化されます。NetScaler Gateway とサーバー間のトラフィックは個別に暗号化できますが、デフォルトでは暗号化されません。

Citrix Gateway とCitrix Virtual Apps and Desktops の統合

公開リソースおよびデータへのアクセスを管理するには、StoreFrontサーバーを展開および構成します。リモートアクセスの場合は、Citrix GatewayをStoreFrontの前に追加することをお勧めします。

注

Citrix Virtual Apps and DesktopsをCitrix Gatewayと統合する構成手順については、StoreFrontのドキュメントを参照してください。

次の図は、Citrix Gatewayを含むCitrixの簡易展開の例を示しています。Citrix GatewayはStoreFrontと通信して、Citrix Virtual Apps and Desktopsが配信するアプリやデータを保護します。ユーザーデバイスはCitrix Workspaceアプリを実行してセキュリティで保護された接続を構築し、アプリ、デスクトップ、ファイルにアクセスします。



© 1997–2026 Citrix Systems, Inc. All rights reserved.

ユーザーは、Citrix Gatewayを使用してログオンおよび認証を行います。Citrix Gatewayは、DMZで展開およびセキュリティ保護されます。2要素認証が構成されます。ユーザーの資格情報に基づいて、ユーザーに該当のリソースおよびアプリケーションが提供されます。アプリケーションとデータは適切なサーバー上に存在します（図には表示されていません）。セキュリティ上機微なアプリケーションとデータについては、別のサーバーが使用されます。

ライセンス

Citrix Gateway を展開してユーザー接続をサポートするには、アプライアンスのライセンスを適切に取得する必要があります。

重要：

受け取ったすべてのライセンスファイルのコピーをローカルに保存しておくことをお勧めします。構成ファイルのバックアップコピーを保存すると、アップロードしたすべてのライセンスファイルもバックアップに含まれます。Citrix Gateway アプライアンスソフトウェアを再インストールする必要があり、構成のバックアップがない場合は、元のライセンスファイルが必要になります。

Citrix Gateway にライセンスをインストールする前に、アプライアンスのホスト名を設定してから、Citrix Gatewayを再起動してください。セットアップウィザードを使用して、ホスト名を構成します。Citrix Gateway のユニバーサルライセンスを生成すると、ホスト名がそのライセンスで使用されます。

Citrix Gateway にライセンスをインストールするには

ライセンスファイルをコンピューターに正常にダウンロードしたら、Citrix Gateway にライセンスをインストールできます。ライセンスは /nsconfig/license ディレクトリにインストールされます。

セットアップウィザードを使用してCitrix Gateway の初期設定を構成した場合、ウィザードの実行時にライセンスファイルがインストールされます。ライセンスの一部を割り当てた後、後で追加番号を割り当てる場合は、セットアップウィザードを使用せずにライセンスをインストールできます。

1. 構成ユーティリティの \[構成\] タブのナビゲーションペインで、\[システム\] を展開し、\[ライセンス\] をクリックします。
2. 詳細ウィンドウで、\[ライセンスの管理\] をクリックします。
3. \[新しいライセンスの追加\] をクリックし、\[参照\] をクリックしてライセンスファイルに移動し、\[OK\] をクリックします。

   構成ユーティリティに、Citrix Gateway を再起動する必要があるというメッセージが表示されます。\[再起動\] をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

最大ユーザー数を設定するには

アプライアンスにライセンスをインストールしたら、アプライアンスに接続できるユーザーの最大数を設定する必要があります。グローバル認証ポリシーの最大ユーザー数を設定します。

1. 構成ユーティリティの［構成］タブのナビゲーションペインで Citrix Gateway を展開し、［グローバル設定］をクリックします。
2. 詳細ペインの \[設定\] で、\[認証 AAA 設定の変更\] をクリックします。
3. \[最大ユーザー数\] に、ユーザーの合計数を入力し、\[OK\] をクリックします。

   このフィールドの数字は、ライセンスファイルに含まれるライセンスの数に対応します。この数は、アプライアンスにインストールされているライセンスの合計数以下である必要があります。たとえば、100 のユーザライセンスを含む 1 つのライセンスと 400 のユーザライセンスを含む 2 番目のライセンスをインストールするとします。ライセンスの合計数は 500 です。ログオンできるユーザーの最大数は 500 以下です。500 人のユーザーがログオンしている場合、その数を超えてログオンしようとするユーザーは、ユーザーがログオフするか、セッションを終了するまでアクセスが拒否されます。

Citrix Gateway のライセンスの種類

Citrix Gateway にはプラットフォームライセンスが必要です。プラットフォームライセンスでは、ICAプロキシを使用してCitrix Virtual Apps、Citrix Virtual Desktops、またはStoreFront への無制限の接続が可能です。Citrix Gateway プラグイン、SmartAccessログオンポイント、またはSecure Hub、WorxWeb、またはSecure Mail からのVPN接続を許可するには、ユニバーサルライセンスも追加する必要があります。Citrix Gateway VPXには、プラットフォームライセンスが付属しています。

プラットフォームライセンスは、以下のCitrix Gateway バージョンでサポートされています。

- Citrix Gateway 13.0
- Citrix Gateway 12.1
- NetScaler Gateway 12.0
- NetScaler Gateway 11.1
- NetScaler Gateway 11.0
- NetScaler Gateway 10.5
- NetScaler Gateway 10.1
- Access Gateway 10
- Citrix ADC VPX

© 1997–2026 Citrix Systems, Inc. All rights reserved.

重要：受け取ったすべてのライセンスファイルのコピーをローカルに保存しておくことをお勧めします。構成ファイルのバックアップコピーを保存すると、アップロードされたすべてのライセンスファイルがバックアップに含まれます。Citrix Gateway アプライアンスソフトウェアを再インストールする必要があり、構成のバックアップがない場合は、元のライセンスファイルが必要です。

プラットフォームライセンス

プラットフォームライセンスでは、Citrix Virtual Apps上の公開アプリケーションまたはCitrix Virtual Desktopsからの仮想デスクトップへの無制限のユーザー接続が可能です。Citrix Workspace アプリを使用した接続では、Citrix Gateway ユニバーサルライセンスは使用されません。これらの接続に必要なのは、プラットフォームライセンスのみです。プラットフォームライセンスは、物理ライセンスと仮想ライセンスにかかわらず、新しいCitrix Gateway のすべての注文とともに電子的に提供されます。保証契約または保守契約の対象となるアプライアンスをすでに所有している場合は、シトリックスWebサイトからプラットフォームライセンスを取得できます。

重要：

プラットフォームライセンスに基づき、次の数のユニバーサルライセンスが含まれています。

- スタンダードエディション — 500
- アドバンスドエディション — 1000
- プレミアム — 無制限

ユニバーサルライセンス

ユニバーサルライセンスでは、同時ユーザーセッションの数は、購入したライセンス数に制限されます。

ユニバーサルライセンスでは、次の機能がサポートされています。

- 完全 VPN トンネル
- マイクロVPN
- エンドポイント解析
- ポリシーベースのSmartAccess
- Web サイトやファイル共有へのクライアントレスアクセス

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Standard エディションのライセンスを購入すると、いつでも 500 の同時セッションを持つことができます。ユーザーがセッションを終了すると、そのライセンスは次のユーザーのために解放されます。複数のコンピューターからCitrix Gateway にログオンするユーザーは、セッションごとにライセンスを占有します。

すべてのライセンスが使用されている場合、ユーザーがセッションを終了するか、セッションを終了するまで、追加の接続を開くことはできません。接続が閉じられると、ライセンスが解放され、新しいユーザーが使用できるようになります。

Citrix Gateway アプライアンスを受け取ると、ライセンスは次の順序で行われます。

- ライセンス認証コード (LAC) が電子メールで送信されます。
- セットアップウィザードを使用して、ホスト名でCitrix Gateway を構成します。
- CitrixのウェブサイトからCitrix Gatewayのライセンスを割り当てます。ホスト名を使用して、割り当てプロセス中にライセンスをアプライアンスにバインドします。
- ライセンスファイルは、Citrix Gateway にインストールします。

ユニバーサルライセンスの詳細については、Citrix Gateway ユニバーサルライセンスを参照してください。

認証のネイティブ OTP サポート

Citrix Gateway では、サードパーティのサーバーを使用せずに、ワンタイムパスワード（OTP）をサポートしています。ワンタイムパスワードは、生成される番号またはパスコードがランダムであるため、セキュリティで保護されたサーバに対して認証を行うための非常に安全なオプションです。以前は、ランダムな数字を生成する特定のデバイスを備えた RSA などの専門企業によってOTP が提供されていました。このシステムは、サーバーが期待する数値を生成するために、クライアントと常に通信する必要があります。

この機能は、設備コストと運用コストの削減に加えて、Citrix ADCアプライアンスの構成全体を維持することで、管理者の管理を強化します。

注

サードパーティ製サーバーが不要になったため、Citrix ADC管理者は、ユーザーデバイスを管理および検証するためのインターフェイスを構成する必要があります。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ユーザーがOTPソリューションを使用するには、Citrix Gateway 仮想サーバーに登録されている必要があります。登録は、一意のデバイスごとに 1 回だけ必要で、特定の環境に制限できます。登録ユーザーの設定と検証は、追加の認証ポリシーの設定に似ています。

ネイティブ OTP サポートの利点

- Active Directory に加えて認証サーバに追加のインフラストラクチャを使用する必要がなくなるため、運用コストが削減されます。
- 構成をCitrix ADCアプライアンスにのみ統合し、管理者に優れた制御を提供します。
- クライアントが期待する数値を生成するために、追加の認証サーバーへのクライアントの依存を排除します。

ネイティブ OTP ワークフロー

ネイティブOTPソリューションは2つ折りプロセスであり、ワークフローは次のように分類されます。

- デバイス登録
- エンドユーザーログイン

重要

サードパーティ製のソリューションを使用している場合や、Citrix ADCアプライアンス以外のデバイスを管理している場合は、登録プロセスをスキップできます。追加する最後の文字列は、Citrix ADC で指定された形式である必要があります。

次の図は、OTP を受信する新しいデバイスを登録するためのデバイス登録フローを示しています。



注

デバイスの登録は、任意の数の要因を使用して行うことができます。デバイス登録プロセスを説明する例として、1 つのファクタ（前の図を参照）を使用します。

次の図は、登録されたデバイスを介した OTP の検証を示しています。



© 1997–2026 Citrix Systems, Inc. All rights reserved.

前提条件

ネイティブ OTP 機能を使用するには、次の前提条件が満たされていることを確認します。

- Citrix ADC 機能のリリースバージョンは 12.0 ビルド 51.24 以降です。
- 高度なエディションまたはプレミアムエディションのライセンスがCitrix Gateway にインストールされている。
- Citrix Gateway には管理IPが設定されており、管理コンソールにはブラウザーとコマンドラインの両方を使用してアクセスできます。
- Citrix ADCは、ユーザーを認証するための認証、承認、監査仮想サーバーで構成されています。
- Citrix ADCアプライアンスはUnified Gateway で構成され、認証、承認、監査プロファイルがGateway仮想サーバーに割り当てられます。
- ネイティブOTPソリューションは、nFactor認証フローに制限されています。ソリューションを構成するには、高度なポリシーが必要です。詳細については、記事CTX222713を参照してください。

また、Active Directory については、次の点を確認してください。

- 256文字の属性の最小長。
- 属性タイプは、ユーザーパラメータなどの 'ディレクトリ文字列' である必要があります。これらの属性は文字列値を保持できます。
- デバイス名が英語以外の文字である場合、属性文字列タイプは Unicode である必要があります。
- Citrix ADC LDAP管理者は、選択したAD属性への書き込みアクセス権を持っている必要があります。
- Citrix ADCアプライアンスとクライアントマシンは、共通のネットワークタイムサーバーに同期する必要があります。

GUI を使用したネイティブ OTP の設定

ネイティブ OTP 登録は、単要素認証ではありません。次のセクションでは、シングルファクタ認証と 2 番目のファクタ認証の設定について説明します。

最初の要素のログインスキーマの作成

1. \[**セキュリティ AAA\] > \[アプリケーショントラフィック\] > \[ログインスキーマ\]** に移動します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. \[**プロファイル** \] に移動し、\[**追加** \] をクリックします。
3. 「 **認証ログイン・スキーマの作成** 」ページで、「 *名前* 」フィールドに **lschema_first_factor** と入力し、「 **noschema** 」の横にある **「編集」** をクリックします。
4. \[**LoginSchema** \] フォルダをクリックします。
5. 下にスクロールして **SingleAuth.xml** を選択し、\[**選択** \] をクリックします。
6. **［作成］** をクリックします。
7. \[**ポリシー** \] をクリックし、\[**追加** \] をクリックします。
8. \[**認証ログインスキーマポリシーの作成** \] 画面で、次の値を入力します。

   名前: lschema_first_factor **プロファイル:** リストから lschema_first_factor を選択します。 **ルール:** HTTP.要求.クッキー.値 (「NSC_TASS」) .EQ (「管理」)

認証、承認、監査仮想サーバーの構成

1. \[**セキュリティ\] > \[AAA\] > \[アプリケーショントラフィック\] > \[認証仮想サーバ\]** に移動します。既存の仮想サーバーを編集する場合にクリックします。
2. 右側のペインの \[**詳細設定\]** の \[**ログインスキーマ** \] の横にある \[**+** \] アイコンをクリックします。
3. 「 **ログインスキーマなし**」を選択します。
4. 矢印をクリックして、 **lschema_first_factor** ポリシーを選択します。
5. **lschema_first_factor** ポリシーを選択し、\[**選択** \] をクリックします。
6. \[**バインド**\] をクリックします。
7. 上にスクロールし、\[**高度な認証ポリシー**\] の下の \[**認証ポリシー**\] を 1つ選択します。
8. **nFactor ポリシーを** 右クリックし、\[**バインディングの編集\]** を選択します。
9. \[**次の係数の選択**\] の下にある \[**+** \] アイコンをクリックし、\[**次の係数**\] を作成して \[**バインド** \] をクリックします。
10. 「 **認証ポリシーラベルの作成** 」画面で次のように入力し、「 **続行** 」をクリックします。

    名前: OTP 管理ファクター

    ログインスキーマ: Lschema_Int
11. 「 **認証ポリシーラベル」** 画面で、「 **+** 」アイコンをクリックしてポリシーを作成します。
12. \[**認証ポリシーの作成** \] 画面で、次のように入力します。

    名前. otp_manage_ldap

© 1997–2026 Citrix Systems, Inc. All rights reserved.

13. \[アクションタイプ\] リストを使用して、 **アクションタイプ** を選択します。
14. 「 **アクション」** フィールドで、「 **+** 」アイコンをクリックしてアクションを作成します。
15. 「 **認証 LDAP サーバーの作成** 」ページで、「 **サーバー IP** 」ラジオ・ボタンを選択し、「 **認証** 」の横にあるチェック・ボックスの選択を解除し、次の値を入力して「 **接続のテスト** 」を選択します。

    名前: LDAP_no_auth

    IPアドレス：192.168.10.11

    ベース DN: DC = トレーニング、DC = ラボ

    管理者: Administrator@training.lab

    パスワード: xxxxx
16. \[**その他の設定\]** セクションまで下にスクロールします。ドロップダウンメニューを使用して、次のオプションを選択します。

    「サーバー・ログオン名」属性 として「 **新規** 」と入力し、「 **ユーザープリンシパル名** 」と入力します。
17. ドロップダウンメニューを使用して、「 **新規** 」として「 **SSO 名属性」** を選択し、「 **userprincipalname** 」と入力します。
18. 「 **OTP シークレット** 」フィールドに「ユーザーパラメータ」と入力し、「 **詳細** 」をクリックします。
19. 次の属性を入力します。

    属性 1 = メール **属性 2** = オブジェクト GUID **属性 3** = 変更不可能 ID
20. **［OK］** をクリックします。
21. \[**認証ポリシーの作成** \] ページで、\[式\] を **true** に設定し、\[**作成** \] をクリックします。
22. 「 **認証ポリシーの作成」ラベル** ページで、「 **バインド** 」をクリックし、**「完了」をクリックします。**
23. \[**ポリシーのバインド** \] ページで、\[**バインド** \] をクリックします。
24. \[**認証ポリシー** \] ページで、\[**閉じる** \] をクリックし、\[**完了** \] をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注

認証仮想サーバーは RFWebUI ポータルテーマにバインドする必要があります。サーバー証明書をサーバーにバインドします。サーバー IP '1.2.3.5' には、後で使用するために otpauth.server.com という対応する FQDN が必要です。

第 2 要素 OTP のログインスキーマの作成

1. \[**セキュリティ\] > \[AAA アプリケーショントラフィック\] > \[仮想サーバ**\] に移動します。編集する仮想サーバを選択します。
2. 下にスクロールして、\[**ログインスキーマ\] を 1**つ選択します。
3. \[**バインドを追加\]**をクリックします。
4. \[**ポリシーのバインド** \] セクションで、\[**+** \] アイコンをクリックしてポリシーを追加します。
5. \[**認証ログインスキーマポリシーの作成** \] ページで、「名前」に OTP と入力し、\[**+** \] アイコンをクリックしてプロファイルを作成します。
6. 「 **認証ログイン・スキーマの作成** 」ページで、「名前」に「OTP」と入力し、「noschema」の横のアイコンをクリックします。
7. \[**LoginSchema** \] フォルダーをクリックし、\[**DualAuth.xml** \] を選択し、\[**選択** \] をクリックします。
8. **［作成］** をクリックします。
9. \[**ルール** \] セクションで、 **True** と入力します。 **［作成］** をクリックします。
10. **［バインド］** をクリックします。
11. 認証の 2 つの要素に注目してください。\[**閉じる** \] をクリックし、\[**完了** \] をクリックします。

OTP を管理するためのコンテンツスイッチングポリシーを構成する

Unified Gateway を使用する場合は、次の設定が必要です。

1. \[**トラフィック管理\] > \[コンテンツの切り替え\] > \[ポリシー\]**に移動します。コンテンツスイッチングポリシーを選択し、右クリックして \[**編集**\] を選択します。
2. 式を編集して次の OR ステートメントを評価し、\[**OK**\] をクリックします。

is_vpn_url||HTTP.REQ.URL.CONTAINS(“manageotp”)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CLI を使用したネイティブ OTP の設定

OTP デバイス管理ページを設定するには、次の情報が必要です。

- 認証仮想サーバに割り当てられた IP
- 割り当てられた IP に対応する FQDN
- 認証用サーバー証明書仮想サーバー

注

ネイティブOTPは、Webベースのソリューションのみです。

OTP デバイスの登録および管理ページを構成するには

認証仮想サーバーの作成

```
> add authentication vserver authvs SSL 1.2.3.5 443

> bind authentication vserver authvs -portaltheme RFWebUI

> bind ssl vserver authvs -certkeyname otpauthcert
```

注

認証仮想サーバーは RFWebUI ポータルテーマにバインドする必要があります。サーバー証明書をサーバーにバインドする必要があります。サーバー IP '1.2.3.5' には、後で使用するために otpauth.server.com という対応する FQDN が必要です。

LDAP ログオンアクションを作成するには

`add authentication ldapAction <LDAP ACTION NAME> -serverIP <SERVER IP> -serverPort <SERVER PORT> -ldapBase <BASE> -ldapBindDn <AD USER> -ldapBindDnPassword <PASSWO> -ldapLoginName <USER FORMAT>`

例:

```
add authentication ldapAction ldap_logon_action -serverIP 1.2.3.4
-serverPort 636 -ldapBase "OU=Users,DC=server,DC=com" -ldapBindDn
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
administrator@ctxnsdev.com -ldapBindDnPassword PASSWORD -ldapLoginName
userprincipalname
```

LDAP ログオンの認証ポリシーを追加するには

```
add authentication Policy auth_pol_ldap_logon -rule true -action
ldap_logon_action
```

ログインスキーマを使用して UI を表示するには

ログオン時にユーザー名のフィールドとパスワードフィールドをユーザーに表示する

```
add authentication loginSchema lschema_single_auth_manage_otp
-authenticationSchema "/nsconfig/loginschema/LoginSchema/
SingleAuthManageOTP.xml"
```

デバイスの登録と管理ページを表示する

デバイスの登録と管理画面を表示するには、URLまたはホスト名の2つの方法があります。

- **URL を使用する**

  URLに'/manageotp'が含まれている場合

  - `add authentication loginSchemaPolicy lpol_single_auth_manage_otp_by_url -rule "http.req.cookie.value("NSC_TASS").contains("manageotp")" -action lschema_single_auth_manage_otp`
  - `bind authentication vserver authvs -policy lpol_single_auth_manage_otp_by_url -priority 10 -gotoPriorityExpression END`

- **ホスト名の使用**

  ホスト名が「alt.server.com」の場合。

  - `add authentication loginSchemaPolicy lpol_single_auth_manage_otp_by_host -rule "http.req.header("host").eq("alt.server.com")" -action lschema_single_auth_manage_otp`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- `bind authentication vserver authvs -policy lpol_single_auth_manage_otp_by_host -priority 20 -gotoPriorityExpression END`

CLI を使用してユーザログインページを設定するには

\[ユーザーログオン\] ページを構成するには、次の情報が必要です。

- 負荷分散仮想サーバのIP
- 負荷分散仮想サーバーの対応する FQDN
- 負荷分散仮想サーバーのサーバー証明書

注

2 要素認証に既存の認証仮想サーバー (authvs) を再利用します。

負荷分散仮想サーバーを作成するには

```
> add lb vserver lbvs_https SSL 1.2.3.162 443 -persistenceType NONE
-cltTimeout 180 -  AuthenticationHost otpauth.server.com -Authentication
ON -authnVsName authvs

> bind ssl vserver lbvs_https -certkeyname lbvs_server_cert
```

ロードバランシングにおけるバックエンドサービスは、次のように表されます。

```
> add service iis_backendsso_server_com 1.2.3.210 HTTP 80

> bind lb vserver lbvs_https iis_backendsso_server_com
```

OTP パスコード検証アクションを作成するには

`add authentication ldapAction <LDAP ACTION NAME> -serverIP <SERVER IP> -serverPort <SERVER PORT> -ldapBase <BASE> -ldapBindDn <AD USER> -ldapBindDnPassword <PASSWORD> -ldapLoginName <USER FORMAT> -authentication DISABLED -OTPSecret <LDAP ATTRIBUTE>`

例：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
add authentication ldapAction ldap_otp_action -serverIP 1.2.3.4
-serverPort 636 -ldapBase "OU=Users,DC=server,DC=com" -ldapBindDn
administrator@ctxnsdev.com -ldapBindDnPassword PASSWORD -ldapLoginName
userprincipalname -authentication DISABLED -OTPSecret userParameters
```

重要

LDAP ログオンと OTP アクションの違いは、認証を無効にし、新しいパラメータ「OTPSecret」を導入する必要があることです。AD 属性値を使用しないでください。

OTP パスコード検証の認証ポリシーを追加するには

```
> add authentication Policy auth_pol_otp_validation -rule true -action
ldap_otp_action
```

LoginSchema を使用して 2 要素認証を表示するには

2 要素認証用の UI を追加します。

```
> add authentication loginSchema lscheme_dual_factor -authenticationSchema
"/nsconfig/loginschema/LoginSchema/DualAuth.xml"



> add authentication loginSchemaPolicy lpol_dual_factor -rule true -action
lscheme_dual_factor
```

ポリシーラベルを使用してパスコード検証係数を作成するには

次の要素の管理 OTP フローポリシーラベルを作成する（最初の要素は LDAP ログオン）

```
> add authentication loginSchema lschema_noschema -authenticationSchema
noschema



> add authentication policylabel manage_otp_flow_label -loginSchema
lschema_noschema`
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

OTPポリシーをポリシー・ラベルにバインドするには

```
bind authentication policylabel manage_otp_flow_label -policyName
 auth_pol_otp_validation -priority 10 -gotoPriorityExpression NEXT
```

UI フローをバインドするには

LDAPログオンに続いてOTP検証を認証仮想サーバーとバインドします。

```
> bind authentication vserver authvs -policy auth_pol_ldap_logon -priority
10 -nextFactor  manage_otp_flow_label -gotoPriorityExpression NEXT



> bind authentication vserver authvs -policy lpol_dual_factor -priority 30
-gotoPriorityExpression END
```

Citrix ADCでデバイスを登録する

1. /manageotpというサフィックスが付いた、Citrix ADC FQDN（最初のパブリックIPアドレス）に移動します。たとえば、ユーザーの資格情報で `<https://otpauth.server.com/manageotp>` にログインします。
2. \[**+** \] アイコンをクリックして、デバイスを追加します。

   
3. デバイス名を入力し、 **Go**キーを押します。バーコードが画面に表示されます。
4. \[**セットアップの開始** \] をクリックし、\[**バーコードのスキャン** \] をクリックします。
5. デバイスのカメラを QR コードの上に置きます。必要に応じて、16 桁のコードを入力できます。

   注：

   表示されているQRコードは3分間有効です。
6. スキャンに成功すると、ログインに使用できる6桁の時間依存コードが表示されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

7. テストするには、QR画面で \[**完了** \] をクリックし、右側の緑色のチェックマークをクリックします。
8. プルダウンメニューから端末を選択し、Google Authenticator からコード（赤ではなく青でなければならない）を入力し、\[**Go**\] をクリックします。
9. ページの右上隅にあるドロップダウンメニューを使用してログアウトしてください。

OTPを使用してCitrix ADCにログインします

1. 最初の公開URLに移動し、Google Authenticator からOTPを入力してログオンします。
2. Citrix ADCスプラッシュページへの認証を行います。



インストール前のチェックリスト

チェックリストは、Citrix Gateway をインストールする前に完了する必要があるタスクと計画情報の一覧で構成されています。

タスクを完了してメモを作成するときに、各タスクをチェックオフできるようにスペースが用意されています。インストールプロセス中およびCitrix Gatewayの構成中に入力する必要がある構成値をメモしておくことをお勧めします。

Citrix Gatewayのインストールと構成の手順については、Citrix Gateway のインストールを参照してください。

ユーザーデバイス

- ユーザーデバイスが、Citrix Gateway プラグインのシステム要件で説明されているインストールの前提条件を満たしていることを確認します。
- ユーザーが接続するモバイルデバイスを識別します。**注意**: ユーザーが iOS デバイスに接続する場合は、セッションプロファイルで「Secure Browse」を有効にする必要があります。

Citrix Gateway の基本的なネットワーク接続

アプライアンスの構成を開始する前に、ライセンスと署名付きサーバー証明書を取得することをお勧めします。

- Citrix Gateway のホスト名を特定して書き留めます。**注**: これは完全修飾ドメイン名 (FQDN) ではありません。FQDN は、仮想サーバーにバインドされている署名付きサーバー証明書に含まれています。
- ユニバーサルライセンスをCitrixから取得します

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 証明書署名要求（CSR）を生成し、認証局（CA）に送信します。CSR を CA に送信する日付を入力します。
- システム IP アドレスとサブネットマスクを書き留めます。
- サブネット IP アドレスとサブネットマスクを書き留めます。
- 管理者パスワードを書き留めます。Citrix Gateway に付属するデフォルトのパスワードは nsrootです。
- ポート番号を書き留めます。これは、Citrix Gateway がセキュアなユーザー接続をリッスンするポートです。デフォルトは TCP ポート 443 です。このポートは、セキュリティで保護されていないネットワーク（インターネット）と DMZ の間のファイアウォール上で開かれている必要があります。
- デフォルト Gateway の IP アドレスを書き留めます。
- DNS サーバの IP アドレスとポート番号を書き留めます。デフォルトのポート番号は 53 です。さらに、DNS サーバーを直接追加する場合は、アプライアンスで ICMP (ping) も構成する必要があります。
- 最初の仮想サーバの IP アドレスとホスト名を書き留めます。
- 2 番目の仮想サーバの IP アドレスとホスト名 (該当する場合) を書き留めます。
- WINS サーバの IP アドレスを書き留めます (該当する場合)。

Citrix Gateway を介してアクセス可能な内部ネットワーク

- ユーザーがCitrix Gateway 経由でアクセスできる内部ネットワークを書き留めます。例：10.10.0.0/24
- ユーザーがCitrix Gatewayプラグインを使用してCitrix Gateway 経由で接続するときにアクセスする必要があるすべての内部ネットワークとネットワークセグメントを入力します。

高可用性

Citrix Gateway アプライアンスが2つある場合は、1つのCitrix Gatewayが接続を受け入れて管理する高可用性構成でそれらを展開し、2つ目のCitrix Gatewayが最初のアプライアンスを監視します。最初のCitrix Gateway が何らかの理由で接続の受け入れを停止すると、2番目のCitrix Gatewayが引き継ぎ、アクティブな接続の受け入れを開始します。

- Citrix Gateway ソフトウェアのバージョン番号をメモします。
- バージョン番号は、両方のCitrix Gateway アプライアンスで同じである必要があります。
- 管理者パスワード（nsroot）を書き留めます。パスワードは、両方のアプライアンスで同じである必要があります。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- プライマリCitrix Gateway のIPアドレスとIDを書き留めます。最大 ID 番号は 64 です。
- セカンダリCitrix Gateway のIPアドレスとIDを書き留めます。
- ユニバーサルライセンスを取得し、両方のアプライアンスにインストールします。
- 両方のアプライアンスに同じユニバーサルライセンスをインストールする必要があります。
- RPC ノードのパスワードを書き留めます。

認証と承認

Citrix Gateway では、さまざまな種類の認証と承認がサポートされており、さまざまな組み合わせで使用できます。認証と認可の詳細については、認証と承認を参照してください。

LDAP 認証

環境に LDAP サーバーが含まれている場合は、LDAP を使用して認証できます。

- LDAP サーバの IP アドレスとポートを書き留めます。

  LDAP サーバへのセキュアでない接続を許可する場合、デフォルトはポート 389 です。SSL を使用して LDAP サーバーへの接続を暗号化する場合、デフォルトはポート 636 です。
- セキュリティの種類を書き留めます。

  セキュリティは、暗号化の有無にかかわらず設定できます。
- 管理者のバインド DN を書き留めます。

  LDAPサーバーで認証が必要な場合は、LDAPディレクトリへのクエリを実行するときにCitrix Gateway が認証に使用する管理者DNを入力します。たとえば、cn = 管理者、cn = ユーザー、dc = エース、dc = com などです。
- 管理者パスワードを書き留めます。

  これは、管理者のバインド DN に関連付けられたパスワードです。
- ベース DN を書き留めます。

  ユーザーを検索するDN（またはディレクトリレベル）です。たとえば、ou=users,dc=ace,dc=comです。
- サーバーのログオン名属性を書き留めます。

  ユーザーのログオン名を指定する LDAP ディレクトリの人物オブジェクト属性を入力します。既定値は sAMAccountName です。Active Directory を使用していない場合、この設定に共通する値は cn または uid です。 LDAP ディレクトリ設定の詳細については、「LDAP認証の構成」を参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- グループ属性を書き留めます。 ユーザーが属するグループを指定する LDAP ディレクトリ個人オブジェクト属性を入力します。デフォルトは memberOf です。この属性により、Citrix Gateway は、ユーザーが属するディレクトリグループを識別できます。
- サブアトリビュート名を書き留めます。

RADIUS 認証および認可

環境に RADIUS サーバが含まれている場合は、認証に RADIUS を使用できます。 RADIUS認証には、RSA SecurID、セーフワード、およびゲマルトプロティバ製品が含まれます。

- プライマリ RADIUS サーバの IP アドレスとポートを書き留めます。デフォルトのポートは 1812 です。
- プライマリ RADIUS サーバシークレット（共有シークレット）を書き留めます。
- セカンダリ RADIUS サーバの IP アドレスとポートを書き留めます。デフォルトのポートは 1812 です。
- セカンダリ RADIUS サーバシークレット（共有シークレット）を書き留めます。
- パスワードエンコードのタイプ（PAP、CHAP、MS-CHAP v1、MSCHAP v2）を書き留めます。

SAML 認証

セキュリティーアサーションマークアップ言語 (SAML) は、ID プロバイダー (IdP) とサービスプロバイダーの間で認証と承認を交換するための XML ベースの標準です。

- セキュアなIdP証明書を取得してCitrix Gateway にインストールします。
- リダイレクト URL を書き留めます。
- ユーザフィールドを書き留めます。
- 署名証明書の名前を書き留めます。
- SAML 発行者名を書き留めます。
- デフォルトの認証グループを書き留めます。

ファイアウォールを介したポートのオープン（シングルホップ DMZ）

組織が単一のDMZで内部ネットワークを保護し、DMZにCitrix Gateway を展開する場合は、ファイアウォールを介して次のポートを開きます。ダブルホップDMZ展開に2つのCitrix Gatewayアプライアンスをインストールする場合は、ファイアウォールで適切なポートを開くを参照してください。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

セキュリティで保護されていないネットワークと DMZ 間のファイアウォール

- インターネットとCitrix Gateway の間のファイアウォールでTCP/SSLポート（デフォルト443）を開きます。ユーザーデバイスはこのポートでCitrix Gateway に接続します。

セキュリティで保護されたネットワーク間のファイアウォール

- DMZ とセキュリティで保護されたネットワーク間のファイアウォールで 1 つ以上の適切なポートを開きます。Citrix Gateway は、1つ以上の認証サーバー、またはこれらのポート上の保護されたネットワーク内のCitrix Virtual Apps and Desktops を実行しているコンピューターに接続します。
- 認証ポートを書き留めます。

  Citrix Gateway 構成に適したポートのみを開きます。

  - LDAP 接続の場合、デフォルトは TCP ポート 389 です。
  - RADIUS 接続の場合、デフォルトは UDP ポート 1812 です。Citrix Virtual Apps and Desktops のポートをメモします。
- Citrix Virtual Apps and Desktops でCitrix Gatewayを使用している場合は、TCPポート1494を開きます。セッション画面の保持を有効にする場合は、1494 ではなく TCP ポート 2598 を開きます。これらのポートは両方とも開いたままにしておくことをお勧めします。

Citrix Virtual Desktops、Citrix Virtual Apps、Web Interface、または StoreFront

Citrix Gateway を展開して、Web InterfaceまたはStoreFront 経由でCitrix Virtual Apps and Desktops にアクセスできるようにする場合は、以下のタスクを実行します。この展開では、Citrix Gateway プラグインは必要ありません。ユーザーは、WebブラウザーとCitrix Receiverのみを使用して、Citrix Gateway 経由で公開アプリケーションおよびデスクトップにアクセスします。

- Web InterfaceまたはStoreFront を実行しているサーバーのFQDNまたはIPアドレスを書き留めます。
- Secure Ticket Authority（STA）を実行しているサーバのFQDNまたはIPアドレスを書き留めます（Web Interfaceの場合のみ）。

Citrix Endpoint Management

内部ネットワークにCitrix Endpoint Management を展開する場合は、以下のタスクを実行します。ユーザーがインターネットなどの外部ネットワークからEndpoint Management に接続する場合、

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ユーザーはモバイル、Web、SaaSアプリケーションにアクセスする前にCitrix Gateway に接続する必要があります。

- Endpoint Management の FQDN または IP アドレスを書き留めます。
- ユーザーがアクセスできるウェブ、SaaS、モバイル iOS または Android アプリケーションを特定します。

Citrix Virtual Apps を使用したダブルホップDMZ展開

ダブルホップDMZ構成で2つのCitrix Gateway アプライアンスを展開して、Citrix Virtual Apps を実行しているサーバーへのアクセスをサポートする場合は、以下のタスクを実行します。

最初のDMZでのCitrix Gateway

最初の DMZ は、内部ネットワークの最も外側のエッジ (インターネットまたは安全でないネットワークに最も近い) にある DMZ です。クライアントは、DMZとインターネットを分離するファイアウォールを介して最初のDMZのCitrix Gateway に接続します。最初のDMZにCitrix Gateway をインストールする前に、この情報を収集してください。

- このCitrix Gatewayのチェックリストの「Citrix Gatewayの基本的なネットワーク接続」セクションの項目に入力します。

  これらの項目を完了すると、インターフェイス0はこのCitrix Gateway をインターネットに接続し、インターフェイス1はこのCitrix Gatewayを2番目のDMZのCitrix Gatewayに接続します。
- プライマリアプライアンスで 2 番目の DMZ アプライアンス情報を設定します。

  ダブルホップDMZの最初のホップとしてCitrix Gateway を構成するには、最初のDMZのアプライアンス上の2番目のDMZでCitrix Gatewayのホスト名またはIPアドレスを指定する必要があります。最初のホップでアプライアンス上でCitrix Gateway プロキシーをいつ構成するかを指定したら、Citrix Gatewayにグローバルにバインドするか、仮想サーバーにバインドします。
- アプライアンス間の接続プロトコルとポートをメモします。

  二重DMZの最初のホップとしてCitrix Gateway を構成するには、接続プロトコルと2番目のDMZのCitrix Gatewayが接続をリッスンするポートを指定する必要があります。接続プロトコルとポートは SSL を使用する SOCKS (デフォルトのポート 443) です。プロトコルとポートは、最初の DMZ と 2 番目の DMZ を分離するファイアウォールを介して開かれている必要があります。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2番目のDMZのCitrix Gateway

2 番目の DMZ は、内部のセキュアなネットワークに最も近い DMZ です。2番目のDMZに展開されたCitrix Gateway は、ICAトラフィックのプロキシとして機能し、外部ユーザーデバイスと内部ネットワーク上のサーバー間で2番目のDMZを通過します。

- このCitrix Gateway のチェックリストの「Citrix Gatewayの基本的なネットワーク接続」セクションのタスクを完了します。

  これらの項目を完了すると、インターフェイス0がこのCitrix Gateway を最初のDMZのCitrix Gatewayに接続することに注意してください。インターフェイス1は、このCitrix Gateway をセキュリティ保護されたネットワークに接続します。

Citrix Endpoint Management またはStoreFront との統合

このセクションでは、リモートユーザーからNetScaler Gateway を介して、Endpoint ManagementおよびStoreFront 展開環境への接続を構成する方法について説明します。

Endpoint Management とStoreFront をサポートするようにNetScaler Gateway を構成できます。Endpoint ManagementまたはStoreFront をサポートするようにNetScaler Gateway を構成する場合は、クイック構成ウィザードを使用して設定を構成することをお勧めします。クイック構成ウィザードでは、仮想サーバーと、セッション、クライアントレスアクセス、および認証ポリシーの設定を構成します。また、StoreFront およびEndpoint Managementへの接続用にDNSサーバーを構成することもできます。

NetScaler Gateway とEndpoint Management 統合

ネットワークにEndpoint Managementを展開する場合は、NetScaler Gateway とEndpoint Managementを統合することで、リモートユーザーからのユーザー接続を許可できます。この展開により、ユーザーはEndpoint Managementに接続して、Web、サービスとしてのソフトウェア（SaaS）、Android、iOSモバイルアプリ、およびShareFileからドキュメントを取得できます。ユーザーは、Secure Hub、Citrix Workspace アプリ、またはNetScaler Gateway プラグインを使用して接続します。

このEndpoint Management展開では、NetScaler Gateway はDMZに存在し、Endpoint Managementは内部ネットワークに存在します。

リモートユーザーからEndpoint Managementへの接続を許可するには、NetScaler Gateway のクイック構成ウィザードを使用して、Endpoint Management、StoreFront、またはWeb InterfaceのWebアドレスを構成することをお勧めします。このウィザードでは、認証、セッション、クライアントレスアクセスポリシーなど、ユーザーがEndpoint Managementに接続するために必要なすべ

© 1997–2026 Citrix Systems, Inc. All rights reserved.

てのポリシーを構成します。ウィザードの詳細については、「クイック構成ウィザードを使用した設定の構成」を参照してください。

また、構成ユーティリティを使用して次のようなポリシーを作成して、Endpoint Managementへの接続を構成することもできます：

- 1つのセッションポリシーで、Citrix Workspace Secure Hub とStoreFront への接続を管理します。このセッションポリシーは、Windows向けCitrix Workspace アプリ、Mac向けCitrix Workspace アプリ、Android向けCitrix Workspace アプリ、iOS向けCitrix Workspace アプリをサポートしています。ユーザーがiOSデバイス上のSecure Hub、Secure Mail、またはWorxWebで接続する場合は、クライアントレスアクセスとSecure Browse を有効にして、NetScaler Gateway を介した接続を許可する必要があります。iOS デバイスのみにSecure Browse を設定します。iOS デバイスと Android デバイスの両方が、内部ネットワークへのVPN トンネルを確立するマイクロ VPN を使用します。
- 1つのセッションポリシーで、Web向けCitrix Workspace アプリへのブラウザー接続を管理します。ユーザは、クライアントレスアクセスを使用して接続します。
- クライアントレスアクセスも可能にする SmartAccess モードが有効になっている 1 つの仮想サーバー。この展開には、ユニバーサルライセンスが必要です。
- カスタムのクライアントレスアクセスポリシー。これらのポリシーは、XMLおよびHTMLトラフィックの書き換えポリシーと、NetScaler Gateway によるCookieの処理方法を定義します。

NetScaler Gateway とStoreFront の統合

ユーザーは、StoreFront を使用して次のいずれかの方法で接続できます：

- クライアントレスアクセスとWeb向けCitrix Workspace アプリ
- NetScaler Gateway プラグイン
- Android向けCitrix Workspaceアプリ
- iOS向けCitrix Workspaceアプリ
- Mac向けCitrix Workspaceアプリ
- Windows向けCitrix Workspaceアプリ
- Secure Hub

重要：

StoreFrontの完全修飾ドメイン名（FQDN）は、NetScaler Gateway仮想サーバーのFQDNとは異なる一意である必要があります。StoreFrontとNetScaler Gateway 仮想サーバーに同じFQDNを使用することはできません。Citrix Workspace アプリでは、StoreFront FQDNが、内部ネットワーク

© 1997–2026 Citrix Systems, Inc. All rights reserved.

に接続されているユーザーデバイスからのみ解決される一意のアドレスである必要があります。そうでない場合、Windows向けCitrix Workspace アプリユーザーは電子メールベースのアカウント検出を使用できません。

ユーザーが接続すると、使用可能なアプリケーション、デスクトップ、およびドキュメントの一覧がCitrix Workspace アプリウィンドウに表示されます。ユーザーは、ストアからアプリケーションをサブスクライブすることもできます。ストアは、Citrix Virtual Desktopsサイト、Citrix VirCitrix Virtual Apps ファーム、およびEndpoint Managementのデスクトップとアプリケーションを列挙して集約し、これらのリソースをユーザーが利用できるようにします。

注：

ユーザーがMDXモバイルアプリにアクセスできるようにするには、StoreFront の前にEndpoint Managementを展開する必要があります。MDXモバイルアプリへのアクセスを提供していない場合、StoreFront はEndpoint Managementの前に配置されます。

StoreFront に接続するようにNetScaler Gateway を構成するときは、次の項目を構成します：

- Secure HubおよびCitrix Workspace アプリのStoreFront への接続を管理する1つのセッションポリシー。このセッションポリシーは、Windows向けCitrix Workspace アプリ、Mac向けCitrix Workspace アプリ、Android向けCitrix Workspace アプリ、iOS向けCitrix Workspace アプリをサポートしています。ユーザーがAndroid向けCitrix Workspace アプリまたはiOS向けCitrix Workspace アプリで接続する場合は、クライアントレスアクセスとSecure Browse を有効にして、NetScaler Gateway を介した接続を許可する必要があります。
- Web向けCitrix Workspace アプリへのブラウザー接続を管理する1つのセッションポリシー。ユーザは、クライアントレスアクセスを使用して接続します。
- Secure Browse を有効にしていない場合に、Android向けCitrix Workspace アプリ、iOS向けCitrix Workspace アプリ、その他のモバイルデバイスを介して行われるPNAサービス接続を管理するための1つのセッションポリシー。PNAサービスのセッションポリシーを構成する場合、Windows向けCitrix Workspace アプリはサポートされません。
- クライアントレスアクセスも可能にする SmartAccess モードが有効になっている 1 つの仮想サーバー。この展開には、ユニバーサルライセンスが必要です。
- カスタムのクライアントレスアクセスポリシー。これらのポリシーは、XMLおよびHTMLトラフィックの書き換えポリシーと、NetScaler Gateway によるCookieの処理方法を定義します。

Endpoint Management とStoreFront のポリシーの構成

Endpoint ManagementとStoreFront を展開し、クイック構成ウィザードを使用して設定を構成しない場合は、次のポリシーを構成する必要があります。これらのポリシーは、NetScaler Gateway

© 1997–2026 Citrix Systems, Inc. All rights reserved.

とEndpoint Managementのみ、NetScaler Gateway とStoreFront のみ、またはNetScaler Gateway、Endpoint Management、およびStoreFront を含む展開環境に対して構成できます。

- Endpoint ManagementまたはStoreFront へのCitrix Workspace アプリの接続を管理する1つのセッションポリシー。このセッションポリシーは、Windows向けCitrix Workspace アプリ、Mac向けCitrix Workspace アプリ、Android向けCitrix Workspace アプリ、iOS向けCitrix Workspace アプリをサポートしています。ユーザーがAndroid向けCitrix Workspace アプリまたはiOS向けCitrix Workspace アプリで接続する場合は、クライアントレスアクセスを有効にする必要があります。iOS向けCitrix Workspace アプリからの接続の場合、［Secure Browse］を有効にして、NetScaler Gateway を介した接続を許可する必要があります。
- Web向けCitrix Workspace アプリへのブラウザー接続を管理する1つのセッションポリシー。ユーザは、クライアントレスアクセスを使用して接続します。
- クライアントレスアクセスも可能にする SmartAccess モードが有効になっている 1 つの仮想サーバー。この展開には、ユニバーサルライセンスが必要です。
- カスタムのクライアントレスアクセスポリシー。これらのポリシーは、XMLおよびHTMLトラフィックの書き換えポリシーと、NetScaler Gateway によるCookieの処理方法を定義します。

StoreFront を展開し、ユーザーが従来のバージョンのCitrix Workspace アプリで接続する場合、［Secure Browse］を有効にしていない場合、Android向けCitrix Workspace アプリ、iOS向けCitrix Workspace アプリ、その他のモバイルデバイスを介して行われるPNAサービス接続を管理するためのセッションポリシーを1つ作成します。PNAサービスのセッションポリシーを構成する場合、Windows向けCitrix Workspace アプリはサポートされません。

注：NetScaler Gateway（`https://<SFLite-FQDN>/Citrix/StoreWeb`など）でStoreFront URLを設定する場合、StoreWebというテキストでは大文字と小文字が区別されます。

Citrix Gateway プラグインのシステム要件

Citrix Gateway プラグインは、クライアントマシンからCitrix Gateway アプライアンスへの安全な接続を確立します。

このプラグインは、Microsoft Windows、macOS X、および Linux オペレーティングシステム用のデスクトップアプリとして配布されます。WebブラウザでCitrix Gateway アプライアンスのセキュアなURLを認証すると、プラグインがダウンロードされ、マシンに自動的にインストールされます。

プラグインは、Android および iOS デバイス用のモバイルアプリとしてプロビジョニングされます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注： プラグインをインストールするには、オペレーティングシステムでadmin権限またはroot権限が必要です。

デスクトップアプリケーションとしてのCitrix Gateway プラグインは、以下のオペレーティングシステムとWebブラウザーでサポートされています。

オペレーティングシステム	サポートされているブラウザー
macOS X (10.9 以降)	Safari 7.1以降、Google Chrome Release 30以降、Mozilla Firefox Release 30以降
Windows 10 (x86およびx64)	Internet Explorer 11、Google Chrome Release 30以降、Mozilla Firefox Release 24以降、Edge Chromium
Windows 8.1	Internet Explorer 11、Google Chrome Release 30以降、Mozilla Firefox Release 24以降、Edge Chromium
Windows 8	Internet Explorer 9および10、Google Chrome Release 30以降、Mozilla Firefox Release 24以降、Edge Chromium
Windows 7	Internet Explorer 9、10、11、Google Chrome Release 30以降、Mozilla Firefox Release 24以降、Edge Chromium
Linux、Ubuntu 18.04 LTS、16.04 LTS、14.04 LTS、12.04 LTS. 32ビットおよび64ビットOSがサポートされています。	Mozilla Firefox Release 44以降、Google Chrome 50以降

重要：

Ubuntu 16.04 LTS のバグ（1573408）により、VPN プラグインのインストールが失敗します。同じ場合の回避策は、次のようにリストされます。

コマンドラインインターフェイスを使用して次のコマンドを入力します。

```
sudo dpkg -i nsgclient*.deb
```

必要な依存関係パッケージが見つからない場合、コマンドはそれらを一覧表示し、プラグインのインストールは失敗します。これらの依存関係パッケージは手動でインストールする必要があり

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ます。管理者は、コマンドラインインターフェイスを使用して次のコマンドを入力して、不足しているパッケージをインストールできます。

```
apt-get install <dependency package>
```

モバイルアプリとしてのCitrix Gateway プラグインは、以下のオペレーティングシステムでサポートされています。

VPN アプリ	サポートされるオペレーティングシステム
Android	Android 4.1 以降
iOS	iOS 8以降

クライアントインターセプションの設定

イントラネットアプリケーションを使用して、Citrix Gateway 上のユーザー接続の傍受ルールを構成します。デフォルトでは、アプライアンスでシステム IP アドレス、マッピング IP アドレス、またはサブネット IP アドレスを設定すると、これらの IP アドレスに基づいてサブネットルートが作成されます。イントラネットアプリケーションは、これらのルートに基づいて自動的に作成され、仮想サーバーにバインドできます。分割トンネリングを有効にする場合は、クライアントインターセプションが発生するようにイントラネットアプリケーションを定義する必要があります。

構成ユーティリティを使用して、イントラネットアプリケーションを構成できます。イントラネットアプリケーションをユーザー、グループ、または仮想サーバーにバインドできます。

分割トンネリングを有効にし、ユーザーが WorxWeb または WorxMail を使用して接続する場合、クライアント傍受を構成するときに、Citrix Endpoint Management と Exchange サーバーの IP アドレスを追加する必要があります。分割トンネリングを有効にしない場合は、イントラネットアプリケーションでEndpoint Management と Exchange の IP アドレスを構成する必要はありません。

Citrix Gateway プラグイン用のイントラネットアプリケーションの構成

リソースへのユーザーアクセス用のイントラネットアプリケーションを作成するには、次の項目を定義します。

- 1 つの IP アドレス
- IP アドレスの範囲

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- ホスト名

Citrix Gateway atewayでイントラネットアプリケーションを定義すると、Windows用のCitrix Gatewayプラグインは、リソース宛てのユーザーのトラフィックをインターセプトし、Citrix Gateway経由でトラフィックを送信します。

イントラネットアプリケーションを構成する場合は、次の点を考慮してください。

- 次の条件が満たされている場合、イントラネットアプリケーションを定義する必要はありません。
  - インターセプションモードが透過モードに設定されている
  - ユーザーがWindows用のCitrix Gateway プラグインを使用してCitrix Gatewayに接続している
  - 分割トンネリングは無効です。
- ユーザーがJava用Citrix Gateway プラグインを使用してCitrix Gatewayに接続する場合は、イントラネットアプリケーションを定義する必要があります。Citrix Gateway プラグインは、イントラネットアプリケーションで定義されたネットワークリソースへのトラフィックのみをインターセプトします。ユーザーがこのプラグインで接続する場合は、インターセプションモードをプロキシに設定します。

イントラネットアプリケーションを構成するときは、接続に使用するプラグインソフトウェアのタイプに対応する傍受モードを選択する必要があります。

注意:イントラネットアプリケーションは、プロキシインターセプションと透過インターセプションの両方に対して構成できません。Windows用のCitrix GatewayプラグインとJava用のCitrix Gateway プラグインの両方で使用されるネットワークリソースを構成するには、2つのイントラネットアプリケーションポリシーを構成し、そのポリシーをユーザー、グループ、仮想サーバー、またはCitrix Gatewayグローバルにバインドします。

1 つの IP アドレスに対してイントラネットアプリケーションを作成するには

1. 構成ユーティリティの［構成］タブのナビゲーションペインで **［Citrix Gatewayリソース］** を展開し、［ **イントラネットアプリケーション**］をクリックします。
2. 詳細ウィンドウで、\[**追加\] をクリックします。**
3. \[名前\] に、プロファイルの名前を入力します。
4. \[**イントラネットアプリケーションの作成** \] ダイアログボックスで、\[**透明**\] を選択します。
5. \[**宛先の種類**\] で、\[**IP アドレス**\] と \[**ネットマスク**\] を選択します。
6. \[プロトコル\] で、ネットワークリソースに適用するプロトコルを選択します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

7. \[**IP アドレス**\] に IP アドレスを入力します。
8. \[**ネットマスク**\] に「サブネットマスク」と入力し、\[**作成**\]、\[**閉じる**\] の順にクリックします。

IP アドレス範囲を構成するには

Web、電子メール、ファイル共有など、ネットワークに複数のサーバーがある場合は、ネットワークリソースの IP 範囲を含むネットワークリソースを構成できます。この設定により、ユーザーは IP アドレス範囲に含まれるネットワークリソースにアクセスできます。

1. 構成ユーティリティの ［**構成** ］タブのナビゲーションペインで ［**Citrix Gatewayリソース**］を展開し、［ **イントラネットアプリケーション**］**をクリックします。**
2. 詳細ウィンドウで、\[**追加**\] をクリックします。
3. \[**名前**\] に、プロファイルの名前を入力します。
4. \[プロトコル\] で、ネットワークリソースに適用するプロトコルを選択します。
5. \[イントラネットアプリケーションの作成\] ダイアログボックスで、\[透明\] を選択します。
6. 「 **宛先の種類**」で、「 **IPアドレスの範囲**」を選択します。
7. \[**IP 開始**\] に開始 IP アドレスを入力し、\[IP 終了\] に終了 IP アドレスを入力し、\[**作成**\]、\[**閉じる**\] の順にクリックします。

ホスト名のイントラネットアプリケーションを作成するには

1. 構成ユーティリティの［構成］タブのナビゲーションペインで ［**Citrix Gatewayリソース**］を展開し、［ **イントラネットアプリケーション**］をクリックします。
2. 詳細ウィンドウで、\[**追加**\] をクリックします。
3. \[名前\] に、プロファイルの名前を入力します。
4. \[**イントラネットアプリケーションの作成** \] ダイアログボックスで、\[**透明**\] を選択します。
5. 「 **デスティネーション・タイプ**」で、 **ホスト名**を選択します。
6. \[プロトコル\] で、\[**ANY**\] を選択し、\[**作成**\] をクリックして \[**閉じる**\] をクリックします。

注意点

1. ワイルドカードホスト名がサポートされています。ホスト名「*.example.com」のイントラネットアプリケーションが構成されている場合、a1.example.com、b2.example.com などはトンネリングされます。
2. ホスト名ベースのイントラネットアプリケーションは、分割トンネリングが **ON**に設定されている場合にのみ機能します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. ホスト名ベースのイントラネットアプリケーションは、Windows VPN プラグインでのみサポートされます。

ユーザ接続のプロキシサポートの有効化

ユーザーデバイスは、内部ネットワークにアクセスするためにプロキシサーバーを介して接続できます。Citrix Gateway は、HTTP、SSL、FTP、およびSOCKSプロトコルをサポートしています。ユーザー接続のプロキシサポートを有効にするには、Citrix Gateway で設定を指定します。Citrix Gateway のプロキシサーバーが使用するIPアドレスとポートを指定できます。プロキシサーバーは、内部ネットワークへのすべてのそれ以降の接続のためのフォワードプロキシとして使用されます。

ユーザー接続のプロキシサポートを構成するには

1. 構成ユーティリティの ［**構成** ］タブのナビゲーションペインで **Citrix Gateway** を展開し、［**グローバル設定**］をクリックします。
2. 詳細ウィンドウで、\[**設定**\] の \[グローバル設定の変更\] をクリックします。
3. \[クライアントエクスペリエンス\] タブで、\[詳細設定\] をクリックします。
4. \[**プロキシ**\] タブの \[**プロキシ設定**\] で、\[**オン**\] を選択します。
5. プロトコルの場合は、IP アドレスとポート番号を入力し、\[**OK**\] をクリックします。

注意：

Applianceを選択した場合は、セキュアおよびセキュアでないHTTP接続のみをサポートするプロキシ・サーバーを構成できます。

Citrix Gateway でプロキシサポートを有効にした後、プロトコルに対応するプロキシサーバーの構成の詳細をユーザーデバイス上で指定します。

プロキシサポートを有効にすると、Citrix Gateway によってプロキシサーバーの詳細がクライアントのWebブラウザーに送信され、ブラウザーでプロキシ構成が変更されます。ユーザーデバイスがCitrix Gateway に接続すると、ユーザーデバイスはプロキシサーバーと直接通信し、ユーザーのネットワークに接続できます。

Citrix Gateway のすべてのプロトコルを使用するように1つのプロキシサーバーを構成するには

Citrix Gateway で使用されるすべてのプロトコルをサポートするように、1つのプロキシサーバーを構成できます。この設定では、すべてのプロトコルに対して 1 つの IP アドレスとポートの組み合わせを提供します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. 構成ユーティリティの ［**構成** ］タブのナビゲーションペインで **Citrix Gateway** を展開し、［**グローバル設定** ］をクリックします。
2. 詳細ウィンドウで、\[**設定**\] の \[グローバル設定の変更\] をクリックします。
3. \[**クライアントエクスペリエンス** \] タブで、\[**詳細設定\] をクリックします。**
4. \[**プロキシ** \] タブの \[**プロキシ設定** \] で、 **\[オン\] を選択します。**
5. プロトコルの場合は、IP アドレスとポート番号を入力します。
6. \[すべてのプロトコルに同じプロキシサーバーを使用する\] をクリックし、\[**OK\] をクリックします。**

分割トンネリングを無効にし、すべてのプロキシ設定を On に設定すると、プロキシ設定がユーザデバイスに伝播されます。プロキシ設定がApplianceに設定されている場合、設定はユーザー・デバイスには反映されません。

Citrix Gateway は、ユーザーデバイスの代わりにプロキシサーバーに接続します。プロキシ設定はユーザーのブラウザには反映されないため、ユーザーデバイスとプロキシサーバー間の直接通信はできません。

Citrix Gateway をプロキシサーバーとして構成するには

Citrix Gateway をプロキシサーバーとして構成する場合、サポートされるプロトコルは安全でない安全なHTTPだけです。

1. 構成ユーティリティの ［**構成** ］タブのナビゲーションペインで **Citrix Gateway** を展開し、［**グローバル設定］をクリックします。**
2. 詳細ウィンドウで、\[**設定**\] の \[グローバル設定の変更\] をクリックします。
3. \[**クライアントエクスペリエンス** \] タブで、\[**詳細設定\] をクリックします。**
4. \[**プロキシ** \] タブの \[**プロキシ設定\] で、\[** アプライアンス\] を選択します。
5. プロトコルの場合は、IP アドレスとポート番号を入力し、\[**OK\] をクリックします。**

アドレスプールの設定

設定ユーティリティを使用して、ポリシーをバインドするレベルでアドレスプールを設定します。たとえば、仮想サーバーのアドレスプールを作成する場合は、そのノードでイントラネット IP アドレスを構成します。アドレスプールを設定すると、ポリシーが設定されているエンティティにバインドされます。アドレスプールを作成し、Citrix Gateway でグローバルにバインドすることもできます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ユーザー、グループ、または仮想サーバーのアドレスプールを構成するには

1. 構成ユーティリティのナビゲーションペインで **［Citrix Gateway］**を展開し、次のいずれかの操作を行います。
   - Citrix Gateway ユーザーの管理］を展開し、［ **AAAユーザー**］をクリックします。
   - **Citrix Gateway** >［ **ユーザー管理］の順に展開し、［**AAAグループ** ］をクリックします。
   - **Citrix Gateway** を展開し、［ **仮想サーバー** ］をクリックします。
2. 詳細ウィンドウで、ユーザー、グループ、または仮想サーバーをクリックし、\[**開く**\] をクリックします。
3. \[**イントラネット IP** \] タブの \[IP アドレスとネットマスク\] に IP アドレスとサブネットマスクを入力し、\[**追加** \] をクリックします。
4. プールに追加する IP アドレスごとにステップ 3 を繰り返し、\[**OK**\] をクリックします。

アドレスプールをグローバルに設定するには

1. 構成ユーティリティの ［**構成** ］タブのナビゲーションペインで **Citrix Gateway** を展開し、［ **グローバル設定** ］をクリックします。
2. 詳細ペインの \[**イントラネット**IP\] で、すべてのクライアントCitrix Gateway セッションで使用する一意の静的IPアドレスまたはIPアドレスのプールを割り当てるには、\[イントラネット IP\] を構成します。
3. \[**イントラネット IP のバインド** \] ダイアログボックスで、\[**操作** \] をクリックし、\[**挿入** \] をクリックします。
4. \[IP アドレス\] と \[ネットマスク\] に IP アドレスとサブネットマスクを入力し、\[**追加**\] をクリックします。
5. プールに追加する各 IP アドレスに対してステップ 3 と 4 を繰り返し、\[**OK**\] をクリックします。

SmartAccess 設定

SmartAccessをCitrix Virtual Apps and Desktopsとともに使用すると、公開アプリケーションと仮想デスクトップをインテリジェントにユーザーに配信できます。

SmartAccessを使用すると、NetScaler Gateway セッションポリシーを使用して、サーバー上の公開アプリケーションおよびデスクトップへのアクセスを制御できます。公開リソースにアクセスす

© 1997–2026 Citrix Systems, Inc. All rights reserved.

るための条件として、事前認証および認証後のチェックを他の条件とともに使用します。その他の条件には、Citrix Virtual Apps and Desktopsポリシーで制御できるすべての条件（プリンターの帯域幅制限、ユーザーデバイスドライブのマッピング、クリップボード、オーディオ、プリンターマッピングなど）が含まれます。ユーザーがNetScaler Gateway チェックに合格するかどうかに基づいて、Citrix Virtual Apps and Desktopsポリシーを適用できます。

NetScaler Gateway は、Web Interface、ICAプロキシアクセス、クライアントレスアクセス、およびNetScaler Gateway アクセスで使用できるのと同じオプションを使用して、Citrix 仮想デスクトップを配信できます。

この機能は、NetScaler GatewayコンポーネントをWeb InterfaceおよびCitrix Virtual Apps and Desktopsと統合することによって実現されます。この統合により、Web Interface に対する高度な認証とアクセス制御オプションが提供されます。詳しくは、Citrix 製品ドキュメントの［テクノロジー］ノードにあるWeb Interfaceのドキュメントを参照してください。

サーバーファームへのリモート接続には、NetScaler Gateway プラグインは必要ありません。ユーザーはCitrix Workspace アプリに接続できます。ユーザーは、NetScaler Gateway プラグインを使用してログオンし、NetScaler Gateway のデフォルトのホームページであるAccess Interfaceを介して公開アプリケーションと仮想デスクトップを受信できます。

複合クライアントセキュリティ式の設定

クライアントセキュリティ文字列を組み合わせて、複合クライアントセキュリティ式を作成できます。

Citrix Gateway でサポートされているブール演算子は次のとおりです。

- And (&&)
- Or (\|\|)
- Not (!)

精度を高めるために、括弧を使用して文字列をグループ化することができます。

注:

コマンドラインを使用して式を設定する場合は、複合式を作成するときに、カッコを使用してセキュリティ式をグループ化します。カッコを使用すると、クライアント式の理解とデバッグが向上します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

AND (&&) 演算子を使用したポリシーの構成

AND (&&) 演算子は、2 つのクライアントセキュリティ文字列を組み合わせて機能し、両方のチェックが true の場合にのみ複合チェックに合格するようにします。式は左から右に評価され、最初のチェックが失敗した場合、2 番目のチェックは実行されません。

AND（&&）演算子は、キーワード「AND」または記号'&&&' を使用して構成できます。

例：

以下は、ユーザーデバイスにバージョン 7.0 の Sophos AntiVirus がインストールされ、実行されているかどうかを判断するクライアントセキュリティチェックです。また、同じコンピュータ上で netlogon サービスが実行されているかどうかも確認します。

CLIENT.APPLICATION.AV(sophos).version==7.0 AND CLIENT.SVC(netlogon) EXISTS

この文字列は、次のように設定することもできます。

CLIENT.APPLICATION.AV(sophos).version==7.0 && CLIENT.SVC(netlogon) EXISTS

OR (\|\|) 演算子を使用したポリシーの構成

OR (||）演算子は、2つのセキュリティ文字列を組み合わせることによって機能します。いずれかのチェックが true の場合、複合チェックは合格します。式は左から右に評価され、最初のチェックが合格した場合、2 番目のチェックは実行されません。最初のチェックが合格しない場合は、2 番目のチェックが実行されます。

次を構成できます。OR（||) 演算子。次を使用：‘OR’ または記号'||'.

例：

以下は、ユーザーデバイスにファイル c:\file.txt があるか、putty.exe プロセスが実行されているかを判断するクライアントのセキュリティチェックです。

client.file(c:\\\\\\\file.txt) EXISTS) OR (client.proc(putty.exe) EXISTS

この文字列は、次のように構成できます。

client.file(c:\\\\\\\file.txt) EXISTS) || (client.proc(putty.exe) EXISTS

NOT (!) 演算子を使用したポリシーの構成

NOT (!) または否定演算子は、クライアントのセキュリティ文字列を否定します。

例：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ファイル c:\sophos_virus_defs.dat ファイルが 2 日以内に経過している場合、次のクライアントセキュリティチェックはパスします。

!(client.file(c:\\\\\\\\sophos_virus_defs.dat).timestamp==2dy)

認証後ポリシーの設定

認証後のポリシーは、セッションをアクティブに保つためにユーザーデバイスが満たす必要のある汎用規則のセットです。ポリシーが失敗すると、Citrix Gateway への接続は終了します。認証後のポリシーを構成する場合、条件付きにできるユーザー接続の設定を構成できます。

注：

この機能は、Citrix Gateway プラグインでのみ機能します。ユーザーがCitrix Workspace アプリでログオンした場合、エンドポイント分析スキャンはログオン時にのみ実行されます。

セッションポリシーを使用して、認証後のポリシーを設定します。まず、ポリシーを適用するユーザーを作成します。次に、ユーザーをグループに追加します。次に、セッション、トラフィックポリシー、およびイントラネットアプリケーションをグループにバインドします。

承認グループとしてグループを指定することもできます。このタイプのグループでは、セッションポリシー内のクライアントセキュリティ表現に基づいて、ユーザーをグループに割り当てることができます。

また、ユーザーデバイスがポリシーの要件を満たしていない場合に、ユーザーを隔離グループに入れるように認証後のポリシーを設定することもできます。単純なポリシーには、クライアントセキュリティ式とクライアントセキュリティメッセージが含まれます。ユーザーが検疫グループに属している場合、ユーザーはCitrix Gateway にログオンできますが、ネットワークリソースへのアクセスは制限されます。

同じセッションプロファイルとポリシーを使用して、承認グループと検疫グループを作成することはできません。認証後のポリシーを作成する手順は同じです。セッションポリシーを作成するときは、承認グループまたは検疫グループを選択します。2 つのセッションポリシーを作成し、各ポリシーをグループにバインドできます。

認証後のポリシーは、SmartAccess でも使用されます。SmartAccessについて詳しくは、「Citrix Gateway でのSmartAccess 構成」を参照してください。

トラフィックポリシーの作成

トラフィックポリシーを設定するには、プロファイルを作成し、次のパラメータを設定します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- プロトコル (HTTP または TCP)
- アプリケーションのタイムアウト
- Webアプリケーションへのシングル・サインオン
- フォームのシングルサインオン
- ファイルタイプの関連付け
- リピータプラグイン
- Kerberos 制約付き委任 (KCD) アカウント

トラフィックポリシーを作成したら、ポリシーを仮想サーバ、ユーザ、グループ、またはグローバルにバインドできます。

たとえば、Web アプリケーション PeopleSoft 人事管理が内部ネットワークのサーバーにインストールされているとします。このアプリケーションのトラフィックポリシーを作成して、宛先 IP アドレスと宛先ポートを定義し、ユーザーがアプリケーションにログオンしたままにできる時間（15 分など）を設定できます。

アプリケーションへの HTTP 圧縮などの他の機能を設定する場合は、トラフィックポリシーを使用して設定を構成できます。ポリシーを作成するときは、アクションの HTTP パラメータを使用します。式で、アプリケーションを実行しているサーバーの宛先アドレスを作成します。

トラフィックポリシーを設定するには

1. 構成ユーティリティーの構成タブのナビゲーションペインで、［Citrix Gateway］>［ポリシー］の順に展開し、［トラフィック］をクリックします。
2. 詳細ウィンドウの \[ポリシー\] タブで、\[追加\] をクリックします。
3. \[トラフィックポリシーの作成\] ダイアログボックスの \[名前\] に、ポリシーの名前を入力します。
4. \[プロファイルの要求\] の横にある \[新規\] をクリックします。
5. \[名前\] に、プロファイルの名前を入力します。
6. \[プロトコル\] で、\[HTTP\] または \[TCP\] を選択します。

   注:
   プロトコルとして \[TCP\] を選択した場合、シングルサインオンは構成できず、\[プロファイル\] ダイアログボックスで設定が無効になります。

7. \[AppTimeout (分)\] に、分数を入力します。この設定により、ユーザーが Web アプリケーションにログオンしたままにできる時間が制限されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

8. Webアプリケーションへのシングル・サインオンを有効にするには、「シングル・サインオン」で「ON」を選択します。

   注：フォームベースのシングルサインオンを使用する場合は、トラフィックプロファイル内で設定を構成できます。詳しくは、「 フォームベースのシングル・サインオンの設定」を参照してください。

9. ファイル・タイプの関連付けを指定するには、「ファイル・タイプの関連付け」で「ON」を選択します。
10. リピータプラグインを使用してネットワークトラフィックを最適化するには、\[ブランチリピータ\] で \[ON\] を選択し、\[作成\] をクリックして \[閉じる\] をクリックします。
11. アプライアンスで KCD を構成する場合は、\[KCD アカウント\] でアカウントを選択します。

    アプライアンスでの KCD の設定の詳細については、「NetScaler アプライアンスでのKerberos制約付き委任の構成」を参照してください。

12. \[Create Traffic Policy\] ダイアログボックスで、式を作成または追加し、\[Create\] をクリックし、\[Close\] をクリックします。

フォームベースのシングル・サインオンの設定

フォームベースのシングルサインオンにより、ユーザーはネットワーク内のすべての保護されたアプリケーションに一度ログオンできます。Citrix Gateway でフォームベースのシングルサインオンを構成すると、ユーザーはパスワードを再入力しなくても、HTMLフォームベースのログオンを必要とするWebアプリケーションにアクセスできます。シングルサインオンを使用しない場合、ユーザーは各アプリケーションにアクセスするために個別にログオンする必要があります。

フォームのシングルサインオンプロファイルを作成したら、フォームシングルサインオンプロファイルを含むトラフィックプロファイルとポリシーを作成します。詳しくは、「トラフィックポリシーの作成」を参照してください。

フォームベースのシングルサインオンを構成するには

1. 構成ユーティリティーの構成タブのナビゲーションペインで、［Citrix Gateway］>［ポリシー］の順に展開し、［トラフィック］をクリックします。
2. 詳細ウィンドウで、\[フォーム SSO プロファイル\] タブをクリックし、\[追加\] をクリックします。
3. \[名前\] に、プロファイルの名前を入力します。
4. \[アクション URL\] に、完成したフォームの送信先の URL を入力します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

注：

URLは、ルート相対URLです。

5. \[ユーザー名フィールド\] に、ユーザー名フィールドの属性の名前を入力します。
6. 「パスワード・フィールド」に、パスワード・フィールドの属性の名前を入力します。
7. \[SSO 成功規則\] で、ポリシーによって呼び出されたときにこのプロファイルが実行するアクションを記述する式を作成します。このフィールドの下にある \[接頭辞\]、\[追加\]、および \[演算子\] ボタンを使用して式を作成することもできます。

   このルールは、シングルサインオンが成功したかどうかをチェックします。
8. \[名前値のペア\] に、ユーザー名フィールドの値を入力し、続けてアンパサンド (&)、パスワードフィールドの値を入力します。

   値の名前は、アンパサンド (&) で区切ります。たとえば、名前 1 = 値 1、名前 2 = 値 2 です。
9. \[レスポンスサイズ\] に、レスポンスサイズ全体を許可するバイト数を入力します。フォームを抽出するために解析する応答のバイト数を入力します。
10. 「抽出」で、名前と値のペアが静的か動的かを選択します。既定の設定は \[動的\] です。
11. \[送信方法\] で、ログオン資格情報をログオンサーバーに送信するためにシングルサインオンフォームで使用する HTTP 方法を選択します。デフォルトは Get です。
12. ［Create］ をクリックしてから、［Close］ をクリックします。

Active Directory からのCitrix Gateway プラグインの展開

ユーザーデバイスにCitrix Gateway プラグインをインストールするための管理者権限がない場合は、Active Directory からユーザー用にプラグインを展開できます。

この方法を使用してCitrix Gateway プラグインを展開する場合、インストールプログラムを抽出し、グループポリシーを使用してプログラムを展開できます。このタイプの展開の一般的な手順は次のとおりです。

- MSI パッケージを抽出しています。
- グループポリシーを使用してプラグインを配布する。
- 配布ポイントを作成する。
- グループポリシーオブジェクトを使用してCitrix Gateway プラグインパッケージを割り当てます。 注：Active Directory からのCitrix Gateway プラグインの配布は、Windows XP、Windows Vista、Windows 7およびWindows 8でのみサポートされています。

MSIパッケージは、構成ユーティリティまたはCitrix のWebサイトからダウンロードできます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

構成ユーティリティからCitrix Gateway プラグインのMSIパッケージをダウンロードするには

1. 構成ユーティリティで、\[ダウンロード\] をクリックします。
2. ［Citrix Gateway プラグイン］で［Windows用Citrix Gatewayプラグインのダウンロード］をクリックし、nsvpnc_setup.exeファイルをWindowsサーバーに保存します。

   注：\[ファイルのダウンロード\] ダイアログボックスが表示されない場合は、Ctrl キーを押しながら \[Citrix Gateway Plugin for Windows をダウンロード\] リンクをクリックします。
3. コマンドプロンプトで、nsvpnc_setup.exe を保存したフォルダに移動し、次のように入力します。

   setup /c

   これにより、agee.msi ファイルが抽出されます。
4. 解凍したファイルを Windows サーバ上のフォルダに保存します。

ファイルを抽出した後、Windows Server のグループポリシーを使用してファイルを配布します。

配布を開始する前に、グループポリシー管理コンソールを Windows Server 2003、Windows Server 2008、または Windows Server 2012 にインストールします。詳細については、Windows のオンラインヘルプを参照してください。

注：グループポリシーを使用してCitrix Gateway プラグインを公開する場合は、パッケージをユーザーデバイスに割り当てることをお勧めします。MSI パッケージは、デバイスごとにインストールされるように設計されています。

ソフトウェアを配布する前に、Microsoft インターネットセキュリティとアクセラレータ (ISA) サーバーなどの公開サーバー上のネットワーク共有に配布ポイントを作成します。

配布ポイントを作成するには

1. 管理者として公開サーバーにログオンします。
2. フォルダーを作成し、配布パッケージにアクセスする必要があるすべてのアカウントの読み取りアクセス許可を持つネットワーク上で共有します。
3. コマンドプロンプトで、解凍したファイルを保存するフォルダに移動し、「msiexec-a agee.msi」と入力します。
4. ［ネットワークの場所］画面で［変更］をクリックし、Citrix Gateway プラグインの管理インストールを作成する共有フォルダーに移動します。
5. \[OK\] をクリックし、\[インストール\] をクリックします。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

展開したパッケージをネットワーク共有に配置した後、Windows のグループポリシーオブジェクトにパッケージを割り当てます。

Citrix Gateway プラグインを管理ソフトウェアパッケージとして正常に構成すると、ユーザーデバイスの次回起動時にプラグインが自動的にインストールされます。

注：

インストールパッケージがコンピュータに割り当てられている場合、ユーザーはコンピュータを再起動する必要があります。

インストールが開始されると、Citrix Gateway プラグインがインストール中であることを示すメッセージが表示されます。

Java用Citrix Gateway プラグインを使用した接続

Java用のCitrix Gateway プラグインは、Javaをサポートする任意のユーザーデバイスで使用できます。

注：

Javaランタイム環境（JRE）バージョン1.4.2から最新バージョンのJREまで、次のオペレーティング・システムおよびWebブラウザが必要です。

- Mac OS X
- Linux
- Windows XP（すべてのバージョン）、Windows Vista、Windows 7、Windows 8
- Internet Explorer
- Firefox
- ウェブブラウザの最新バージョンにSafari 1.2まで

Java用のCitrix Gateway プラグインは、ほとんどのTCPベースのアプリケーションをサポートしますが、Windows用のCitrix Gateway プラグインまたはMac OS X用のCitrix Gatewayプラグインの一部の機能のみを提供します。

Java用Citrix Gateway プラグインを使用するために、ユーザーデバイスに対する管理者権限は必要ありません。セキュリティ上の理由から、使用するユーザーデバイスに関係なく、特定の仮想サーバー、グループ、またはユーザーに対してこのプラグインバージョンを使用する必要がある場合があります。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ユーザーデバイスにCitrix Gateway wayプラグインをインストールするようにCitrix Gatewayを構成するには、セッションポリシーを構成し、仮想サーバー、グループ、またはユーザーにバインドします。

ユーザーが Windows 7 を実行しているコンピューターからログオンした場合、Internet Explorer でプロキシサーバーの情報は自動的には設定されません。ユーザーは、Windows 7 を実行しているコンピューターでプロキシサーバーを手動で構成する必要があります。

Java用にCitrix Gateway プラグインを構成するには

1. 構成ユーティリティーの構成タブのナビゲーションペインで、［Citrix Gateway］>［ポリシー］の順に展開し、［セッション］をクリックします。
2. 詳細ウィンドウで、\[プロファイル\] タブをクリックします。
3. セッションプロファイルを選択し、\[開く\] をクリックします。
4. \[クライアントエクスペリエンス\] タブで、\[プラグインの種類\] の横にある \[グローバル上書き\] をクリックし、\[Java\] を選択して \[OK\] をクリックします。

インターセプションモードを設定するには

セッションポリシーを作成したら、イントラネットアプリケーションを作成して、Citrix Gateway プラグインfor Javaでログオンするユーザーの傍受モードを定義します。

1. 構成ユーティリティーの構成タブのナビゲーションペインで、［Citrix Gateway］>［リソース］の順に展開し、［イントラネットアプリケーション］をクリックします。
2. 詳細ウィンドウで、\[追加\] をクリックします。
3. \[名前\] ボックスに名前を入力します。
4. \[プロキシ\] をクリックします。
5. \[宛先 IP アドレス\] に IP アドレスを入力します。
6. \[宛先ポート\] に、ポート番号を入力します。
7. \[送信元 IP アドレス\] に IP アドレスを入力します。
8. \[ソースポート\] にポート番号を入力し、\[作成\]、\[閉じる\] の順にクリックします。

送信元IPアドレスとポート番号を指定しない場合、Citrix Gateway ではIPアドレスに127.0.0.1、ポートに0が自動的に使用されます。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Windows ベースのコンピュータでの HOSTS ファイルの更新

ユーザーがWindows Vista、Windows 7、またはWindows 8を実行しているコンピューターでJava用のCitrix Gateway プラグインを使用してログオンすると、TCPイントラネットアプリケーションのネットワークトラフィックはトンネリングされません。HOSTS ファイルは、Vista および Windows 7 を実行しているコンピューターでは自動的に更新されません。イントラネットアプリケーションを HOSTS ファイルに手動で追加する必要があります。

Windows ベースのコンピュータでは、メモ帳などのテキストエディタで HOSTS ファイルを編集できます。HOSTS ファイルをメモ帳で編集する場合は、管理者としてメモ帳を実行する必要があります。Java用Citrix Gateway プラグイン用のイントラネットアプリケーションのマッピングエントリを追加し、ファイルを保存します。

Citrix 製品との統合

Citrix Gatewayのインストールと構成を担当するシステム管理者は、Citrix Endpoint Management、StoreFront、およびWeb Interfaceで動作するようにアプライアンスを構成できます。

ユーザーは、内部ネットワークまたはリモートの場所から直接 Endpoint Management に接続できます。ユーザーが接続すると、Web、SaaS、およびモバイルアプリにアクセスできます。また、ShareFileにあるドキュメントをどのデバイスからでも操作できます。

Citrix Gateway を介したサーバーファームへのユーザー接続を許可するには、StoreFront または Web Interface、およびCitrix Gatewayで設定を構成します。ユーザーが接続すると、公開アプリケーションおよび仮想デスクトップにアクセスできます。

Citrix Gateway をEndpoint Management、StoreFront およびWeb Interfaceと統合するための構成手順は、次のことを前提としています。

- Citrix Gateway はDMZ内に存在し、既存のネットワークに接続されています。
- Citrix Gateway はスタンドアロンアプライアンスとして展開され、リモートユーザーはCitrix Gateway に直接接続します。
- StoreFront、Endpoint Management、Citrix Virtual Apps、Citrix Virtual Desktops、およびWeb Interfaceは、安全なネットワークに存在します。
- ShareFile は、Endpoint Management で設定されます。ShareFileの詳細については、ShareFileトピックとユーザーアクセス用のShareFile 構成トピックを参照してください。

StoreFront とEndpoint Management 展開方法は、モバイルデバイスに提供するアプリによって異なります。MDX Toolkitでラップされ MDXアプリにユーザーがアクセスできる場合、Endpoint

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Management はセキュアネットワークのStoreFront の前に存在します。MDXアプリケーションへのアクセスを提供しない場合、StoreFront はセキュアネットワークのEndpoint Management の前に存在します。

© 1997–2026 Citrix Systems, Inc. All rights reserved.