Citrix Gateway 12.1

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

Contents

NetScaler Gatewayリリースノート 39
NetScaler Gatewayについて 40
NetScaler Gatewayアーキテクチャ 41
ユーザー接続の仕組み 43
NetScaler Gateway プラグインとの接続 43
Citrix Receiver との接続 45
iOS デバイスと Android デバイスとの接続 45
一般的な展開 46
非武装地帯での展開 46
DMZ でのNetScaler Gateway接続 47
安全なネットワークへの展開 47
クライアントソフトウェア要件 49
NetScaler Gatewayプラグインのシステム要件 49
エンドポイント分析要件 51
Citrix製品との互換性 54
Citrix 製品とサポート対象バージョン 54
Citrix Workspaceアプリ、Citrix 業務用モバイルアプリ、プラグイン 54
Windows ゲートウェイプラグインでサポートされている NetScaler Gateway 機能 55
ライセンス 57
NetScaler Gatewayライセンスの種類 57
プラットフォームライセンス 58
ユニバーサル・ライセンス 58
ユニバーサルライセンスの取得 59
ユニバーサルライセンスのインストール 60
ユニバーサルライセンスのインストールの確認 60
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の取得 60

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

NetScaler Gateway にライセンスをインストールするには 61
最大ユーザー数を設定するには 61
ユニバーサルライセンスのインストールの確認 62
構成ユーティリティ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 62
コマンドライン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 62
ライセンスに関するよくある質問 63
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 63
ライセンスをインストールするには 63
Gateway ライセンスにはどのような種類がありますか 63
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 63
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? 63
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 64
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 64
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? 64
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? 64
開始する前に 65
セキュリティ計画 66
安全な証明書管理の設定 66
認証サポート 67
前提条件 67
インストール前のチェックリスト 68
ユーザーデバイス 68
NetScaler Gatewayの基本的なネットワーク接続 68
NetScaler Gateway 経由でアクセス可能な内部ネットワーク 69
高可用性 69
認証と承認 70
LDAP 認証 70

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

RADIUS 認証および承認 71
SAML認証 71
ファイアウォール (シングルホップ DMZ) 経由でポートを開く 71
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について 72
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について 72
Citrix Virtual Desktops、Citrix Virtual Apps、Web Interface、またはStoreFront 72
Citrix Endpoint Management 72
Citrix Virtual Appsによるダブルホップ DMZ 展開 73
最初のDMZのNetScaler Gateway 73
第二DMZのNetScaler Gateway 74
アップグレードしています 75
ソフトウェアアップデートを確認するには 75
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には 76
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には 76
システムをインストールする 77
NetScaler Gatewayの構成 77
構成ユーティリティの使用 78
構成ユーティリティにログオンするには 78
NetScaler Gateway のポリシーとプロファイル 79
ポリシーの仕組み 79
ポリシーの優先順位の設定 80
条件付きポリシーの設定 80
NetScaler Gatewayでのポリシーの作成 81
システム式の設定 81
クライアントセキュリティ式の設定 82
単純式と複合式の作成 82
カスタムエクスプレッションの追加 83
ポリシー表現での演算子とオペランドの使用 83

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

NetScaler Gateway構成設定の表示 92
NetScaler Gateway構成の保存 92
NetScaler Gateway で構成を保存するには 93
NetScaler Gateway で構成ファイルを表示して保存するには 93
現在の実行構成を表示するには 93
保存済み構成と実行構成を比較するには 93
NetScaler Gateway構成のクリア 94
NetScaler Gateway の構成設定をクリアするには 94
ウィザードを使用した NetScaler Gatewayの構成 94
初回セットアップウィザードの仕組み 95
セットアップウィザードの仕組み 95
統合Citrix Endpoint Management 構成の仕組み 96
クイック構成ウィザードの仕組み 96
NetScaler Gatewayウィザードの仕組み 97
公開アプリケーションウィザードの仕組み 97
初回セットアップウィザードによるNetScaler Gateway の構成 98
Configuring Settings with the Quick Configuration Wizard 99
クイック構成ウィザードで設定を構成するには 100
NetScaler Gateway ウィザードを使用して設定を構成する 103
NetScaler Gateway ウィザードを起動するには 103
NetScaler Gateway でのホスト名と FQDN の設定 104
証明書の FQDN を表示するには 104
証明書のインストールと管理 104
証明書署名リクエストの作成 105
NetScaler Gateway ウィザードを使用してCSRを作成するには 105
Citrix ADC GUI を使用して CSR を作成するには 106
NetScaler Gateway への署名付き証明書のインストール 106
署名付き証明書と秘密キーをペアリングするには 106

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

証明書と秘密キーを仮想サーバーにバインドするには 107
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 107
中間証明書の構成 107
中間証明書をインストールするには 108
中間証明書をサーバー証明書にリンクするには 108
認証にデバイス証明書を使用する 109
デバイス証明書を構成する手順 110
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 110
Windows マシンでのデバイス証明書の検証 111
既存の証明書のインポートとインストール 111
NetScaler Gateway に証明書と秘密キーをインストールするには 112
PFX 形式から PEM 形式への証明書の変換 113
`OpenSSL Utility` 115
証明書失効リスト 116
CRL を追加するには 116
構成ユーティリティで LDAP または HTTP を使用して CRL 自動更新を構成するには 117
OCSP による証明書ステータスの監視 120
OCSP 証明書ステータスの設定 121
NetScaler Gateway構成のテスト 122
構成ユーティリティを使用して新しいユーザーアカウントを作成する 122
仮想サーバーの作成 123
仮想サーバーを作成するには 124
GUI を使用して仮想サーバーを作成するには 124
CLI を使用して仮想サーバーを作成するには 125
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 125
仮想サーバーでの接続タイプの設定 125
仮想サーバーで基本接続または SmartAccess 接続を構成するには 126
ワイルドカード仮想サーバーのリッスンポリシーの設定 126

© 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 127
NetScaler Gatewayの IP アドレスの設定 128
NetScaler Gatewayが IP アドレスを使用する方法 128
マップされた IP アドレスの変更または削除 129
新しいマッピング IP アドレスを作成するには 129
マップされた IP アドレスを削除するには 129
サブネットIPアドレスの構成 129
サブネット IP アドレスを追加するには 130
ユーザー接続用の IPv6 の設定 130
安全なネットワークにある DNS サーバーの解決 131
DNS サービスと DNS モニターを構成するには 131
DNS サービスを DNS 仮想サーバーにバインドするには 132
DNS 仮想サーバーの設定 132
DNS 仮想サーバーを構成するには 132
ネームサービスプロバイダの設定 133
NetScaler Gateway にDNSサーバーを追加するには 133
WINSサーバーをNetScaler Gateway に追加するには 133
名前ルックアップの優先度を指定するには 134
サーバー起動接続の設定 134
NetScaler Gatewayでのルーティングの設定 135
スタティックルートの設定 136
スタティックルートを設定するには 136
スタティックルートをテストするには 136
オートネゴシエーションの設定 137
オートネゴシエーションを有効または無効にするには 137
認証と承認 138
デフォルトのグローバル認証タイプの設定 139
認証をグローバルに設定するには 139

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

認可なしの認証の設定 140
認可の設定 140
承認ポリシーの構成 140
GUI を使用して認可ポリシーを設定するには 142
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 142
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 143
デフォルトのグローバル認証の設定 143
認証の無効化 143
認証を無効にするには 144
特定の時刻の認証の設定 144
時刻、日付、または曜日の認証を設定するには 144
認証ポリシーの仕組み 145
認証プロファイルの設定 146
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 146
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 146
認証ポリシーを削除するには 146
認証ポリシーのバインド 147
認証ポリシーの優先度の設定 147
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 148
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 148
ローカルユーザの設定 148
ローカルユーザーを作成するには 148
ユーザーパスワードを変更するには 149
ユーザーの認証方法を変更するには 149
ユーザーを削除するには 149
グループの設定 149
グループを作成するには 150
グループを削除するには 150

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

グループへのユーザーの追加 150
グループを使用したポリシーの設定 151
LDAP認証の構成 152
構成ユーティリティを使用して LDAP 認証を構成するには 154
LDAP ディレクトリ内の属性を決定する 156
LDAP グループ抽出の設定 156
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 157
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 157
LDAP 認可グループ属性フィールド 157
LDAP 認証を設定するには 158
LDAP ネストされたグループ抽出の設定 158
複数ドメインの LDAP グループ抽出の設定 159
グループ抽出のためのセッションポリシーの作成 160
複数ドメインの LDAP 認証ポリシーの作成 161
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 162
クライアント証明書認証の構成 162
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 163
クライアント証明書からのユーザー名の抽出 163
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 163
2 要素クライアント証明書認証の設定 165
スマートカード認証の構成 165
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 167
RADIUS認証の構成 168
ジェムアルトプロティバの設定 168
セーフワードを構成する 169
RADIUS認証を構成するには 169
RADIUS 認証プロトコルの選択 169

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

IP アドレス抽出の設定 170
RADIUS グループ抽出の設定 171
Windows Server 2003 での RADIUS の設定 171
Windows Server 2008 での認証用の RADIUS の設定 172
RADIUS 認可を設定するには 174
RADIUS ユーザアカウンティングの設定 174
RADIUS ポリシーを作成するには 176
セッションポリシーを作成するには 176
セッションポリシーをグローバルにバインドするには 177
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 177
SAML認証の構成 177
Active Directory フェデレーションサービス 2.0 の構成 179
SAML 二要素認証の設定 181
SAML 認証を設定するには 181
SAML認証を使用してNetScaler Gateway にログインする 182
サポートされているプラットフォームとアプリ 182
高度な SAML ポリシーを使用した SAML 認証の設定 183
SAML 認証の認証機能の強化 183
解決策 184
プラットフォーム 184
構成 184
TACACS+ 認証の設定 185
基本設定をクリアしても TACACS 設定はクリアされない 186
概要 186
新しいコマンド 186
CLI 構成 187
多要素認証の設定 187
カスケード認証の設定 188

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

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 188
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 188
2 要素認証の設定 189
2 要素認証を構成するには 189
シングルサインオンの認証タイプの選択 189
クライアント証明書と LDAP の 2 要素認証の設定 190
シングルサインオンの設定 193
Windows でのシングルサインオンの構成 193
Windows でシングルサインオンをグローバルに構成するには 193
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 193
Web アプリケーションへのシングルサインオンの構成 194
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 194
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 195
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 195
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 195
ドメインへのシングルサインオンの設定 196
ドメインへのシングルサインオンを構成するには 196
ワンタイムパスワードの使用の設定 197
RSA SecurID 認証の設定 197
RADIUS を使用したパスワードリターンの設定 199
Configuring SafeWord Authentication 200
Gemalto プロティバ認証の設定 201
ゲートウェイ認証用の nFactor 201
使用例 202
認証レスポンスの処理 202
クライアントサポート 203
コマンドライン設定 203

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

相互運用に関する課題 204
エンドポイント分析 (EPA) 204
設定ミスの考慮事項 204
Citrix クライアントの定義 204
ゲートウェイの nFactor を制限する 205
ログインスキーマ 205
LoginSchemaと nFactor の知識が必要 205
loginSchema を使用しないデュアルファクタ認証の設定 206
ユーザー名パスワード表現 206
nFactor 構成のハイレベルな手順 206
GUI 構成 206
仮想サーバーを作成する 207
認証仮想サーバーの作成 211
認証 CERT プロファイルの作成 212
認証ポリシーの作成 212
LDAP 認証サーバの追加 213
LDAP 認証ポリシーの追加 213
RADIUS 認証サーバの追加 214
RADIUS 認証ポリシーの追加 215
認証ログインスキーマの作成 216
ポリシーラベルの作成 216
Unified Gateway ビジュアライザー 218
概要 218
Unified Gateway の設定 218
GUI 構成 220
VPN 仮想サーバーの詳細 221
`The Pre Auth Block` 221

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

`The Auth Block` 221
StoreFront の追加 222
SaaS を追加する 223
ウェブアプリの追加 223
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 224
1つのActive Directory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 227
LDAP検索フィルター方式 227
概要 227
前提条件 227
1つのActive Directoryグループのメンバーに対するLDAP検索フィルターを構成する手順 228
NetScaler Gateway セッションポリシー方式 230
SameSite Cookie属性の構成サポート 232
SameSite Cookie 属性を設定する 232
CLI を使用して SameSite 属性を設定する 233
CLI を使用してクッキーをパッチセットにバインドする 233
GUI を使用して sameSite 属性を設定する 233
NetScaler Gateway VPN 分割トンネルのOffice365用に最適化 235
GUI を使用した設定 235
GUI を使用して分割トンネリングを設定するには 235
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 236
CLI を使用した設定 236
Office 365 サービス (EXO、SPO、およびTeams) の IP アドレスの一覧 237
IPv4 アドレス範囲 237
IPv6 アドレス範囲 237
VPN ユーザーエクスペリエンスの設定 239
NetScaler Gateway プラグインによるユーザー接続の仕組み 240
安全なトンネルの確立 241

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

安全な接続を介したプライベートネットワークトラフィックのトンネリング 241
ファイアウォールを介した操作 242
NetScaler Gateway プラグインのアップグレードコントロール 242
プラグインの動作 242
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 243
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 243
VPN 構成 243
EPA 構成 244
要件 244
NetScaler Gateway で完全な VPN セットアップを構成する 245
前提条件 245
NetScaler Gateway アプライアンスで完全な VPN セットアップを構成する 246
その他のパラメーター 248
分割トンネリングを設定するには 249
ネームサービス解決を構成する 251
ユーザーアクセス方法の選択 252
ユーザーアクセス用のNetScaler Gateway プラグインの展開 253
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 254
一元化された展開ツールを使用する利点 254
展開するソフトウェアプラグインの決定 254
ユーザー向けNetScaler Gateway プラグインの選択 254
プラグインをグローバルに設定するには 255
セッションプロファイルで Windows または Mac OS X のプラグインタイプを設定するには 255
Windows向けNetScaler Gateway プラグインのインターセプトモードを設定するには 256
Windows向けNetScaler Gatewayプラグインのインストール 256
Windows向けNetScaler Gateway プラグインをインストールするには 257
Windows向け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には 258

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

Active Directory から NetScaler Gateway プラグインをデプロイする 258
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 258
配布ポイントを作成するには 260
Active Directory を使用した NetScaler Gateway プラグインのアップグレードと削除 260
Active Directory を使用したNetScaler Gateway プラグインのインストールのトラブルシューティング 261
Java向けNetScaler Gateway プラグインとの接続 261
Java 向けNetScaler Gateway プラグインを構成するには 262
インターセプトモードを設定するには 262
Windows ベースのコンピューターでの HOSTS ファイルの更新 263
NetScaler Gateway プラグインと Citrix Receiver の統合 263
Citrix Receiveでのユーザー接続の仕組み 264
Citrix Workspaceアプリアイコンのデカップリング 264
CLI を使用してアイコン統合を設定する 265
GUI を使用してアイコン統合を設定する 265
ICA 接続用の IPv6 の設定 265
IPv6 を ICA プロキシ用に構成するには 266
NetScaler Gateway でのReceiverホームページの構成 267
Receiverのホームページをグローバルに設定するには 267
セッションプロファイルでReceiverホームページを構成するには 267
Receiverテーマのログオンページへの適用 268
ログオンページのカスタムテーマの作成 268
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 269
ユーザーポータルのカスタマイズ 269
ポータル・テーマの適用 270
キャクストン・テーマ 270
グリーンバブルテーマ 270

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

X1のテーマ 270
VPN 仮想サーバーへのポータル・テーマのバインド 270
コマンドラインを使用してポータル・テーマを既存の VPN 仮想サーバーにバインドする 270
構成ユーティリティを使用してポータル・テーマを既存の VPN 仮想サーバーにバインドする 270
ポータル・テーマを VPN Global にバインドする 271
コマンドラインを使用してポータル・テーマを VPN グローバル・スコープにバインドする 271
構成ユーティリティを使用してポータル・テーマを VPN グローバル・スコープにバインドする 271
ポータル・テーマの作成 272
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 272
コマンドラインを使用してポータル・テーマを作成する 272
構成ユーティリティを使用してポータル・テーマを作成する 272
ポータルテーマのカスタマイズ 273
ポータル・テーマ・インターフェースについて 273
ポータル・テーマ・インターフェース 273
カスタマイズ可能なページ属性のタイプ 274
古いポータルのカスタマイズに関する注意事項 275
カスタムポータル構成の手動作成 275
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 276
エンドユーザー使用許諾契約書の作成 277
コマンドラインを使用して EULA エンティティを作成する 277
構成ユーティリティを使用して EULA エンティティを作成する 278
コマンドラインを使用して EULA を VPN Global にバインドする 278
構成ユーティリティを使用してグローバル EULA VPN バインディングを作成する 278
コマンドラインを使用して EULA を VPN 仮想サーバーにバインドする 278
構成ユーティリティを使用して EULA を VPN 仮想サーバーにバインドする 279

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

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 279

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 279

クライアントレスアクセスの設定 280

クライアントレスアクセスの有効化 281

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 281

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 281

Web アドレスのエンコーディング 282

クライアントレスアクセスポリシーの仕組み 283

新しいクライアントレスアクセスポリシーの作成 284

NetScaler Gateway を使用した高度なクライアントレス VPN アクセス 286

ユーザーのドメインアクセスの設定 288

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 289

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 289

SharePoint 2003、SharePoint 2007、および SharePoint 2013 のクライアントレスアクセスの設定 289

Citrix 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には 290

SharePoint サイトをホームページとして設定する 290

SharePoint 2007 サーバーの名前解決を有効にする 291

クライアントレスアクセスパーシステント Cookie の有効化 292

SharePoint のクライアントレスアクセス用のパーシステントクッキーの設定 292

Web インターフェイスによるクライアントレスアクセス用のユーザ設定の保存 293

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 293

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 294

モバイルデバイス用のCitrix SSO VPNクライアント 294

参照ドキュメント 294

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

クライアント選択ページの設定 294
ログオン時にクライアント選択ページを表示する 296
クライアント選択オプションをグローバルに有効にするには 296
セッションポリシーの一部としてクライアント選択を有効にするには 296
クライアント選択オプションの設定 297
承認グループを作成するには 297
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には 297
STA サーバーをグローバルに設定するには 299
STA を仮想サーバーにバインドするには 299
アクセスシナリオフォールバックの設定 299
アクセスシナリオフォールバックのポリシーの作成 300
検疫グループを作成するには 301
ユーザー接続を検疫するための設定を構成するには 301
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には 302
セッションポリシーを検疫グループにバインドするには 302
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には 303
NetScaler Gateway プラグインの接続の設定 303
ユーザーセッション数の設定 303
グローバルユーザー制限を設定するには 304
仮想サーバーあたりのユーザー制限を設定するには 304
タイムアウト設定 304
強制タイムアウトの設定 305
セッションまたはアイドルタイムアウトの設定 306
内部ネットワークリソースへの接続 307
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 308
分割トンネリングの構成 308
分割トンネリングを設定するには 309
分割トンネリングおよび認可の設定 309

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

クライアントインターセプトの設定 310
NetScaler 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 310
Java向けNetScaler 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 312
ネームサービス解決の設定 313
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 313
ユーザー接続のプロキシサポートの有効化 313
プロキシ設定 314
ユーザー接続のプロキシサポートを構成するには 314
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 315
NetScaler Gateway をプロキシサーバーとして構成するには 316
アドレスプールの設定 316
イントラネット IP DNS 登録 318
アドレスプールの設定 319
アドレスプールオプションの定義 320
VoIP 電話のサポート 322
Java向けNetScaler Gateway プラグインのアプリケーションアクセスの構成 323
HOSTS ファイル変更方法を使用したアプリケーションへのアクセス 323
SourceIP および SourcePort メソッドを使用したアプリケーションへのアクセス 324
アクセスインターフェースの設定 324
アクセスインターフェースのカスタムホームページへの置き換え 325
アクセスインターフェースの変更 326
Web リンクとファイル共有リンクの作成と適用 326
ブックマークのユーザー名トークンの設定 329
Web リンクの作成と適用 329
エンタープライズブックマークの作成 330
個人用ブックマークの作成 333
ブックマークでユーザー名トークンを構成する 333

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

トラフィックポリシーの仕組み 333
トラフィックポリシーの作成 334
トラフィックポリシーを設定するには 334
フォームベースのシングルサインオンの設定 335
SAML シングルサインオンの設定 336
トラフィックポリシーのバインド 337
トラフィックポリシーの削除 337
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解除するには 337
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するには 338
セッションポリシーの設定 338
セッションポリシーを作成するには 339
セッションプロファイルの作成 339
セッションプロファイルでのユーザー接続のネットワーク設定 339
セッションプロファイルでの接続設定 340
セッションプロファイルのセキュリティ設定 341
セッションプロファイルでのCitrix Virtual Apps and Desktops の設定 341
構成ユーティリティを使用してセッションプロファイルを作成するには 341
構成ユーティリティ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 342
バインディングセッションポリシー 342
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には 342
GUIを使用してセッションポリシーをCitrix ADC AAAグループにバインドするには 342
GUIを使用してセッションポリシーをCitrix ADC AAAユーザーにバインドするには 343
StoreFront のNetScaler Gateway セッションポリシーを構成する 343
最小要件 343
StoreFront でNetScaler Gateway を構成する 344
StoreFront の認証を構成する 347
エンドポイントポリシーの設定 347
エンドポイントポリシーの仕組み 347

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

ユーザーログオンオプションの評価 349
事前認証ポリシーの優先順位の設定 350
事前認証ポリシーの優先順位を変更するには 350
事前認証ポリシーとプロファイルの設定 351
構成ユーティリティを使用して事前認証プロファイルをグローバルに構成するには 352
構成ユーティリティを使用して事前認証プロファイルを構成するには 352
エンドポイント分析式の設定 353
カスタムエクスプレッションの設定 354
複合式の設定 355
バインディング事前認証ポリシー 355
事前認証ポリシーのバインド解除と削除 356
認証後ポリシーの設定 357
認証後ポリシーの設定 357
認証後スキャンの頻度の設定 358
検疫グループと承認グループの設定 358
ユーザーデバイスのセキュリティ事前認証式の設定 361
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、またはスパム対策表現の設定 362
サービスポリシーの設定 363
プロセスポリシーの設定 364
オペレーティングシステムポリシーの設定 365
レジストリポリシーの設定 367
複合クライアントセキュリティ式の設定 369
AND (&&) 演算子によるポリシーの設定 369
OR (\|\|) 演算子によるポリシーの設定 370
NOT (!) 演算子 を使ったポリシーの設定 370
Advanced Endpoint Analysisスキャン 370
高度なエンドポイント分析スキャンの設定 371

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

OPSWAT スキャンの設定 371
システムスキャンの設定 373
EPA ライブラリをアップグレードする 374
高度なエンドポイント分析ポリシー式リファレンス 377
エクスプレッションフォーマット 377
エクスプレッション文字列 377
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 385
ユーザーセッションの管理 385
GUI を使用したユーザーセッションの管理 385
ユーザーセッションを表示するには 385
セッションリストを更新するには 386
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 386
CLI を使用してユーザセッションを管理する 386
常時オン 387
Always On をいつ使用するのか 387
Always On フレームワークを理解する 387
トンネルの自動再確立 388
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 388
Always On の設定要件 389
常時オン機能を有効にする際の考慮事項 389
常時オンの設定 390
IIP に関する注意事項 391
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 391
Windows ログオン前に常時接続 VPN (旧式は常時接続サービス) 393
NetScaler Gatewayの構成 394
NetScaler Gateway搭載Citrix ADC: 1 URL 394
NetScaler Gateway構成ウィザード 395

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

追加の構成管理 396
コンテンツスイッチング仮想サーバー 396
VPN 仮想サーバー 397
Unified Gateway に関するよくある質問 397
セットアップ 399
認証 400
AAA トラフィック管理 402
ポータルのカスタマイズ 403
RDPプロキシ 405
ライセンスの変更 405
コマンドを有効にする 405
RDP プロキシのその他の変更 405
他のCitrix ソフトウェアとの統合 406
HDX Insight はUnified Gateway と互換性がありますか 406
既存のHDX Insight構成を移行するにはどうすればよいですか 406
ダブルホップ DMZ への展開 408
ダブルホップDMZでのNetScaler Gateway の展開 408
ダブルホップ導入の仕組み 409
ダブルホップ DMZ 展開での通信フロー 410
接続プロセス 411
ダブルホップ DMZ 導入の準備 414
導入を開始するために必要なコンポーネント 414
ダブルホップDMZへのNetScaler Gatewayのインストールと構成 414
最初のDMZへのNetScaler Gatewayのインストール 415
最初の DMZ でのNetScaler Gatewayの設定 415
2 つ目の DMZ へのNetScaler Gatewayのインストール 415
NetScaler Gateway プロキシ上の仮想サーバーの設定の構成 416

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

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 416
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 416
アプライアンスプロキシと通信するためのアプライアンスの設定 416
NetScaler Gateway プロキシと通信するようにNetScaler Gateway を構成するには 417
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 417
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 417
STAおよびICAトラフィックを処理するためのNetScaler Gatewayの構成 418
ファイアウォールの適切なポートを開く 419
ダブルホップ DMZ 展開での SSL 証明書の管理 421
高可用性の使用 424
高可用性の仕組み 425
高可用性の設定に関するガイドライン 425
高可用性の設定の構成 426
高可用性ノードを追加するには 427
セカンダリノードを有効または無効にするには 427
高可用性の設定を構成するには 428
RPC ノードのパスワードを変更する 428
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 428
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 429
通信間隔の設定 429
セカンダリNetScaler Gateway の通信間隔を構成するには 429
NetScaler Gateway アプライアンスの同期 430
高可用性同期を有効または無効にするには 430
アプライアンス間で同期を強制するには 430
高可用性セットアップの設定ファイルの同期 431
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 431
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 431

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

コマンド伝播の設定 432
プライマリノードで伝播を有効または無効にするには 432
コマンド伝播のトラブルシューティング 432
フェイルセーフモードを構成する 433
フェールセーフモードを構成するには 435
仮想 MAC アドレスの設定 435
IPv4 仮想 MAC アドレスの設定 436
IPv4 仮想 MAC アドレスの作成または変更 436
IPv6 仮想 MAC アドレスの設定 437
IPv6 用の仮想 MAC アドレスの作成または変更 438
異なるサブネットでの高可用性ペアの設定 439
独立したネットワーク構成の仕組み 439
リモートノードの追加 440
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 441
リモートノードを削除するには 441
ルートモニタの設定 441
ルートモニタの追加または削除 443
ルートモニタを追加するには 443
ルートモニタを削除するには 443
リンク冗長性の設定 444
リンク冗長性を設定するには 444
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 444
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 444
フェイルオーバーの原因を理解する 445
ノードからのフェイルオーバーの強制 446
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 446
プライマリノードまたはセカンダリノードでフェイルオーバーを強制するには 447
プライマリノードを強制的にプライマリのままにする 447

© 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 447
セカンダリノードを強制的にセカンダリに維持する 447
セカンダリノードを強制的にセカンダリに保つには 448
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 448
クラスタリングの使用 449
クラスタリングの構成 449
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 450
NetScaler Gateway クラスターへのノードの追加 451
クラスタノードグループの作成 451
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 452
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 452
システムのメンテナンスとモニタリング 454
委任管理者の構成 454
委任管理者のコマンドポリシーの設定 455
NetScaler Gateway で管理ユーザーを作成するには 456
管理グループの作成 456
委任管理者用のカスタムコマンドポリシーの設定 456
簡単なカスタムコマンドポリシーを作成するには 457
高度なカスタムコマンドポリシーを作成するには 457
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 458
NetScaler Gateway での監査の構成 458
NetScaler Gateway でのログの構成 459
監査ポリシーを作成するには 459
監査ポリシーをグローバルにバインドするには 460
監査ポリシーを変更するには 460
監査ポリシーを削除するには 461
ACL ロギングの設定 461
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 462

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

NetScaler Gateway でACLまたはTCPのログを有効にするには 462
NetScaler Gateway プラグインログの有効化 462
ロギングを有効にするには 464
ICA 接続を監視するには 464
Citrix 製品との統合 465
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 466
Citrix Endpoint Management、Citrix Virtual Apps and Desktopsを使用した展開 468
WebインターフェイスによるCitrix Virtual Apps and Desktops リソースへのアクセス 470
NetScaler GatewayとCitrix Virtual Apps and Desktops との統合 470
サーバーファームへの安全な接続の確立 471
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 471
Web インターフェイスによるデプロイ 473
セキュアネットワークへのウェブインターフェースの展開 474
DMZ内のNetScaler Gatewayと並行してWebインターフェイスを展開する 474
DMZ内のNetScaler Gatewayの背後にWebインターフェイスを展開する 475
Web Interfaceの機能 475
Web Interfaceのサイトのセットアップ 476
Web インターフェイス 5.4 サイトの作成 477
設定ファイルの使用 477
Citrix Web Interface管理コンソールを使用したサイトの構成 478
Web InterfaceでのNetScaler Gateway 設定の構成 5.4 479
Web InterfaceでNetScaler Gateway 設定を構成するには 479
Web インターフェイス 5.3 サイトの作成 481
Web Interface 5.3のサイトを作成するには 481
Web Interface 5.3でのNetScaler Gateway 設定の構成 482
NetScaler Gateway のWeb Interface5.3設定を構成するには 483
単一サイトへのCitrix Virtual Apps and Desktops の追加 483

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

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 484

NetScaler Gateway を介したユーザー接続のルーティング 484

Citrix Virtual Apps 6.5サーバーのプロパティを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構成するには 484

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 485

Web インターフェイスとの通信の設定 485

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 485

NetScaler Gateway でWeb Interfaceをグローバルに構成するには 486

Web Interface のセッションポリシーを構成するには 486

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 487

公開アプリケーションウィザードで設定を構成する 487

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 487

NetScaler Gateway でのSecure Ticket Authority 構成 488

STA をグローバルにバインドするには 488

STA を仮想サーバーにバインドするには 488

参照ドキュメント 489

NetScaler Gateway での追加のWeb Interface設定の構成 489

Web インターフェイスフェールオーバーの設定 489

Web インターフェイスフェールオーバーを設定するには 490

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 490

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 491

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 492

イントラネットアプリケーションを構成するには 492

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 493

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 493

SmartAccess 設定 493

© 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 494
Citrix Virtual Apps ポリシーとフィルターの構成 495
SmartAccess のセッションポリシーを構成するには 496
Citrix Virtual Apps でのユーザーデバイスマッピングの構成 496
Citrix Virtual Apps 6.5で制限ポリシーを構成するには 497
Citrix Virtual Apps 6.5で非制限ポリシーを構成するには 498
検疫アクセス方法としてのCitrix Virtual Apps 有効化 498
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 499
SmartAccess 向けの Citrix Virtual Desktops の構成 499
Citrix Virtual Desktops で SmartAccess のセッションポリシーを構成するには 500
Citrix Virtual Desktops でポリシーとフィルターを構成するには 5 501
Desktop Delivery Controller を STA として追加するには 501
SmartControl の設定 502
ポリシー 503
追加 503
編集 504
削除 505
バインディングを表示 505
ポリシーマネージャ 505
バインディングを追加 506
ポリシーバインディング 506
ポリシーのバインド解除 506
バインドNOPOLICY 506
編集 506
バインディングを編集 507
ポリシーの編集 507
アクションを編集 508
アクション 508

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

アクション 508

追加 509

編集 509

アクションの設定 509

削除 510

アクション 510

アクセスプロファイル 510

GUI を使用したアクセスプロファイルの作成 511

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 511

追加 511

編集 511

アクセスプロファイルの設定 512

削除 512

共通プロセス 512

アクションを作成する 512

アクションを選択 512

アクセスプロファイルの作成 513

既存のアクセスプロファイルを選択する 513

式 513

グループ識別 514

事前認証 514

セッション 515

ログアクションの作成 515

監査メッセージの作成アクション 515

ログアクションの改訂 516

監査メッセージアクションの設定 516

既存のポリシーを選択する 516

ポリシーを作成する 516

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

事前認証および認証後のエンドポイント分析の設定 517
認証後の設定 517
NetScaler Gateway セッションプロファイルの作成 518
事前認証の設定 519
事前認証プロファイルの作成 520
Web インターフェイスへのシングルサインオンの設定 521
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 522
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 522
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 523
その他の設定ガイドライン 523
Web Interface へのシングルサインオン接続をテストするには 524
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 524
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 525
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 526
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 526
ファイルタイプの関連付けを許可する 527
Web インターフェイスサイトの作成 528
NetScaler Gateway でファイルタイプの関連付けを構成する 529
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 530
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 530
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 530
NetScaler Gateway をCitrix Virtual Apps and Desktops 統合する 532
NetScaler Gateway とStoreFront の統合 533
StoreFront で使用するようにNetScaler Gatewayを構成する方法 533
前提条件 533
Citrix Endpoint Management 環境の設定を構成する 536

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

NetScaler ADC 機能のライセンス要件 537
Citrix Endpoint Management用のNetScaler ADCウィザード 538
Citrix Endpoint Management または Citrix Endpoint Management 用の負荷分散サーバーの構成 541
Citrix ADC VIP で SSL ブリッジモードを使用するには 541
NetScaler ADC VIPでSSLオフロードモードを使用するには 541
電子メールセキュリティフィルタリングを使用した Microsoft Exchange の負荷分散サーバの構成 542
Citrix Endpoint Management Citrix ADC Connector (XNC) ActiveSync フィルタリングの設定 543
Citrix 業務用モバイル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 543
NetScaler GatewayでのSecure Browseの設定 544
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 547
モバイルデバイスのエンドポイント分析を無効にする 547
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 548
Citrix Endpoint Managementのドメインおよびセキュリティトークン認証の構成 550
前提条件 550
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 551
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の設定 553
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 553
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 554
Citrix ADC証明書失効一覧（CRL） 555
CloudBridge によるネットワークトラフィックの最適化 557
トラフィックポリシーを作成するには 558
ゲートウェイ UX 構成での RfWebUI ペルソナ 559
RfWebUI ペルソナを使用する時は 559
RfWebUI ペルソナによって提供される機能 559
GO 560
アプリケーションの集約 560
ユーザ設定の RDP プロキシリンク 560

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

お気に入りのアプリケーション 560
RfWebUI ペルソナを有効にする際の考慮事項 561
RfWebUI ペルソナの設定 561
RfWebUI 設定パラメーター 561
NetScaler Gateway ポータルのカスタマイズ 563
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 563
設定例 564
ログインスキーマの作成とカスタマイズ 566
ログインスキーマプロファイルの作成 566
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 567
管理 UI からのポータルのカスタマイズ 567
共通属性 568
文字列のカスタマイズ 568
RDPプロキシ 570
クライアントレス VPN を介した導入 571
ICA プロキシを介した展開 571
強制の詳細 571
強制用にサポートされている RDP パラメータ 572
接続フロー 572
ステートレス (デュアル) ゲートウェイの互換性 572
シングルゲートウェイの互換性 573
シングルリスナーのサポート 574
RDP プロキシのライセンス要件 574
ブックマーク 574
ブックマークを作成する 575
RDP プロキシで有効にする機能とモード 575
RDP プロキシの概要設定手順 575
クライアントプロファイルを構成する 576

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

サーバープロファイルを構成する 577
CLI を使用した RDP プロキシの設定 577
GUI を使用した RDP プロキシの設定 578
SSO を無効にするオプション 581
ステートレス RDP プロキシ 582
前提条件 582
構成 582
接続カウンター 584
接続フロー 584
シングル・ゲートウェイの互換性 585
アップグレードノート 585
RDP サーバープロファイルの作成 586
RDP クライアントプロファイルの設定 586
仮想サーバーのセットアップ 586
RDP 接続リダイレクト 586
前提条件 587
接続ブローカの存在下で RDP プロキシを展開する 587
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 588
NetScaler ADC GUIを使用してRDP接続リダイレクトを構成する 588
LDAP 属性に基づいて RDP URL を設定 588
CLI を使用して LDAP 属性に基づいて RDP URL を入力するには 588
LDAP サーバ設定 589
GUI を使用して LDAP 属性に基づいて RDP URL を入力するには 590
RDP プロキシで RDP ファイル名をランダム化する 590
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 590
NetScaler Gateway 対応の PCoIP プロキシサポート（VMware Horizon View） 592
VMware Horizon View 用の NetScaler Gateway 有効な PCoIP プロキシの構成 592
前提条件 592

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

USB リダイレクトを有効にする手順 596
Unified Gateway のコンテンツスイッチング式の更新 596
PCoIP ゲートウェイを使う 597
VMware Horizon View 接続サーバの構成 597
HDX Enlightened Data Transport サポート 598
Enlightened Data Transport サポートを使用する場合 598
EDTおよびHDX InsightをサポートするようにNetScaler Gatewayを構成 599
Enlightened Data Transport をサポートするようにNetScaler Gateway を構成する 600
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 600
CLIを使用してEDTサポート用にNetScaler Gateway を構成するには 601
HDX InsightをサポートするようにNetScaler Gatewayを構成する 601
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 601
CLIを使用してNetScaler Gateway for HDX Insight サポートを構成するには、次のコマンドを入力します 603
L7 遅延しきい値処理 603
L7 レイテンシは L4 レイテンシとどう違うのですか 604
ICA RTT と L7 のレイテンシー計算の違い 604
CLI を使用した L7 遅延しきい値の設定 604
引数 605
GUI を使用した L7 遅延しきい値の設定 606
NetScaler ADMでL7レイテンシーパラメーターを表示する 607
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 607
CLI を使用してレイテンシー頻度を設定するには 607
CLI を使用してレイテンシー頻度を設定するには 608
L7 レイテンシー測定モデル 608
L7 遅延しきい値レポートモデル 608
Microsoft Intune グレーション 609
統合 Intune MDM ソリューションを使用する場合 609

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

NetScaler Gatewayと Intune MDM の統合について 610

単一要素認証展開用の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の構成 610

ライセンス 611

システム要件 611

前提条件 612

参照ドキュメント 612

ゲートウェイ展開用nFactorを搭載したNetScaler Gateway仮想サーバーを追加するには 612

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 615

トラブルシューティング 616

一般的な問題 616

NetScaler Gatewayの問題 616

NetScaler Gateway OAuthのステータスとエラー状態 617

Intune 構成チェック 618

Azure Portalでの NetScaler Gateway アプリケーションの構成 618

前提条件 618

Azure でNetScaler Gatewayアプリを作成するには 618

Azure ADAL トークン認証について 621

Microsoft ADALトークン認証用のNetScaler Gateway 仮想サーバーの構成 622

UDP トラフィックのサービスタイプサポート 624

NetScaler Gateway の送信プロキシサポートのプロキシ自動構成 625

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 625

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 625

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 626

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

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 626
送信ICAプロキシのサポート 627
アウトバウンドICAプロキシのサポートについて 627
アウトバウンドICAプロキシの構成 627
NetScaler Gateway をCitrix Virtual Apps and Desktops 統合する 630
認証のためのネイティブOTPサポート 631
ネイティブ OTP をサポートすることの利点 631
ネイティブ OTP ワークフロー 631
前提条件 632
GUI を使用したネイティブ OTP の設定 633
第 1 ファクタのログインスキーマの作成 633
認証、承認、および監査仮想サーバーの構成 633
第 2 要素 OTP のログインスキーマの作成 635
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 635
CLI を使用したネイティブ OTP の設定 635
OTP デバイスの登録および管理ページを設定するには 636
LDAP ログオンアクションを作成するには 636
LDAP ログオンの認証ポリシーを追加するには 636
Loginschemaを使用して UI を表示するには 637
デバイスの登録と管理ページを表示する 637
CLI を使用してユーザログインページを設定するには 637
OTP パスコード検証アクションを作成するには 638
OTP パスコード検証の認証ポリシーを追加するには 638
LoginSchema を介して 2 要素認証を提示するには 638
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 639
OTPポリシーをポリシー・ラベルにバインドするには 639
UI フローをバインドするには 639

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

NetScalerでデバイスを登録する 639
OTPを使用してNetScalerにログインします 640
サーバー名表示拡張機能の設定 641
SSL ハンドシェイク中のサーバ証明書の検証 642
アドバンスポリシーを使用した VPN ポリシーの作成 644
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 644
高度な EPA を使用した事前認証 EPA 645
アドバンスド EPA を使用した事後認証 EPA 645
高度なポリシーを使用した事前認証および認証後 EPA 645
nFactor 認証の要素としての定期的な EPA スキャン 646
テンプレートを使用した簡略化された SaaS アプリ設定 648
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 648
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 650
EPA コンポーネントとしての nFactor のデバイス証明書 657
nFactor のデバイス証明書を EPA コンポーネントとして設定する 657
__index__ 660
Citrix Endpoint Management またはStoreFront との統合 660
NetScaler Gateway とEndpoint Management 統合 660
NetScaler Gateway とStoreFront の統合 661
Endpoint Management とStoreFront のポリシーの構成 662

© 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 12.1の拡張機能、既知の問題、およびバグ修正について詳しくは、 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	NetScaler Gateway をネットワーク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より多くのアプライアンスに展開する方法について説明します。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、認可、アカウンティング。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。アカウンティングサーバーは、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。アカウンティングの詳細については、「 NetScaler Gateway での監査の構成」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

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

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 Receiverをインストールしている場合、ユーザーはReceiverからNetScaler Gatewayプラグインを使用してログオンします。Receiver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ると、Receiver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。
- macOS X、Linux、およびオプションでWindowsユーザーがWebブラウザーを使用してログオンできるようにするJava向けNetScaler Gateway プラグイン。
- Web InterfaceまたはCitrix StoreFront を使用して、ユーザーが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に接続できるようにするReceiverです。
- Receiver、Secure Hub、WorxMail、WorxWebにより、ユーザーは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Citrix Endpoint Management でホストされている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。

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

- 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。
- 仮想アダプタ。NetScaler Gateway 仮想アダプタは、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 Receiver
- WorxMailとWorxWeb
- Android と iOS のモバイルデバイス

NetScaler Gateway プラグインとの接続

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：

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

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した場合、ユーザーがWindowsベースのコンピューターまたはMac OS 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て、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に合格すると、ログオンページが表示され、ユーザーは自分の資格情報を入力できます。NetScaler Gateway 10.1、Build 120.1316.eをインストールすると、Mac OS 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Mac OS 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。Java用のNetwork Gatewayプラグインを使用している場合は、ユーザーデバイスも事前構成済みのリソースIPアドレスとポート番号のリストで初期化されます。
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。

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

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。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を介して、またはCitrix Receiver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 Receiver との接続

ユーザーはReceiverに接続して、Windowsベースのアプリケーションや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。Receiver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Receiver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Receiver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 デバイスと Android デバイスとの接続

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を使用してメールにアクセスし、WorxWebを使用して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、接続には自動的にマイクロ VPN が使用されます。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。

非武装地帯での展開

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。NetScaler GatewayをDMZに展開すると、ユーザーはNetScaler GatewayプラグインまたはCitrix Receiverを使用して接続します。

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。

安全なネットワークへの展開

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。ただし、この構成にはファイアウォールが 1 つしかないため、遠隔地から接続するユーザーにとっては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

このセクションでは、NetScaler Gateway クライアントソフトウェアのシステム要件について説明します。

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したネットワークリソースに接続して操作できます。

NetScaler Gateway でエンドポイントポリシーを構成する場合、ユーザーがログオンすると、NetScaler Gateway はエンドポイント分析プラグイン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
Windows 8.1	Internet Explorer 11、Google Chrome リリース 30 以降、Mozilla Firefox リリース 24 以降、Edge Chromium
Windows 8	Internet Explorer 9 と 10、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、16.04 LTS、14.04 LTS、12.04 LTS。32ビットと64ビットのOSに対応している。	Mozilla Firefox リリース 44 以降。Google Chrome 50 以降

重要：

- Ubuntu 16.04 LTS のバグ (1573408) が原因で、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とおりです。
- SモードのWindows 10およびWindows 11は、NetScaler Gatewayプラグインをサポートしていません。
- 現在、Ubuntu向けCitrix Secure Access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。

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。

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

```
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要件

NetScaler Gateway は、エンドポイント分析プラグインをユーザーデバイスにインストールします。エンドポイント分析プラグインは、NetScaler Gateway で構成したエンドポイントの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。

Windowsユーザーが初めてブラウザーを使用してNetScaler Gateway に接続すると、ポータルはエンドポイント分析プラグインのインストールを要求します。その後のログオン試行では、プラグインはアップグレード制御構成をチェックして、クライアントエンドポイント分析プラグイン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、新しい Endpoint Analysis 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るプロンプトが表示されます。Windows 用のエンドポイント分析プラグインは、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。インストールまたは使用に特別な権限は必要ありません。

macOS の場合、ユーザーはエンドポイント分析プラグインをインストールする必要があります。macOS 用プラグインは 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。インストールに特別な権限は必要ありません。以降のログオン試行で、プラグインのバージョンが一致しない場合、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。

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

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
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
Windows 8.1	Internet Explorer 11、Google Chrome リリース 30 以降、Mozilla Firefox リリース 24 以降、Edge Chromium
Windows 8	Internet Explorer 9 と 10、Google Chrome リリース 30 以降、Mozilla Firefox リリース 24 以降、Edge Chromium
Windows 7	Internet Explorer 9 と 10、11、Google Chrome リリース 30 以降、Mozilla Firefox リリース 24 以降、Edge Chromium

© 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 Vista	Internet Explorer 9; Mozilla Firefox リリース 9 と 10
Linux; Ubuntu 12.04 LTS、14.04 LTS、16.04 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 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バージョンの場合、エンドポイント分析はプラグイン対応でなければならず、最低限必要なバージョンは3.0です。
- 現在、Ubuntu向け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.

Citrix製品との互換性

次の表に、NetScaler Gateway 12.1と互換性があるCitrix製品とバージョンを示します。

注:NetScaler Gateway 機能は Citrix ADC VPX で使用できます。

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
XenMobile	10.5, 10.6, 10.7, 10.8, 10.9, 10.10, 10.11, 10.12

注：

- Citrix Virtual Apps and Desktops バージョン7.6は、バージョン12.1ビルド52.xxでサポートされています。

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

Windows ゲートウェイプラグインでサポートされている NetScaler Gateway 機能

機能	サポートされているプラグインの最小バージョン
デバイスガードのサポート	12.1 ビルド 48.x 以降、12.0 ビルド 58.x 以降

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

機能	サポートされているプラグインの最小バージョン
nFactor サポート	12.1 ビルド 48.x およびそれ以降
Opswat v4サポート	12.1 ビルド 48.x 以降、12.0 ビルド 57.x 以降
SAML サポート	nFactor の一部としてサポートされ、スタンドアロンではサポートされません
常時稼働	12.1ビルド51.x およびそれ以降

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の詳細については、「NetScaler Gateway VPNクライアントとサポートされている機能」を参照してください。

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

ライセンス

NetScaler Gateway を展開してユーザー接続をサポートする前に、アプライアンスに適切なライセンスを取得する必要があります。

重要：Citrix では、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になります。

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、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

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

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。

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

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

- 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。

- 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。

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

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。
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。

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の取得

NetScaler Gateway をインストールすると、プラットフォームライセンスファイルまたはユニバーサルライセンスファイルをCitrix から入手する準備が整います。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

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

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。

重要：NetScaler Gateway には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。

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。

NetScaler 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、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、後から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. 「新規ライセンスを追加」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。

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. 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、［Citrix Gateway］を展開し、［Global Settings］をクリックします。
2. 詳細ペインの［Settings］で、［Change authentication AAA settings］をクリックします。

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

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にする必要があります。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の確認

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。

構成ユーティリティ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。

コマンドライン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、「show license」と入力します。SSL VPN パラメーターが Yes で、最大ユーザー数パラメーター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。

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

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**

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

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。

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て情報を収集し、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、セキュリティへの影響を考慮し、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 製品で動作します：

- Citrix Endpoint Management
- Citrix Virtual Apps
- Citrix Virtual Desktops
- StoreFront
- Web Interface
- CloudBridge

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。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、リスク分析で定義したデータなど、アクセスを提供したい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アクセスを提供できます。ユーザーは、Citrix ReceiverまたはSecure Hub を使用してログオンするか、クライアントレスアクセスを使用してログオンする必要があります。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

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

らのアクセスシナリオは、ユーザーが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。

セキュリティ計画

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しておく必要があります。

安全な証明書管理の設定

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。

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

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 を導入する前に、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ディレクトリと認証サーバーを用意する必要があります：

- 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

環境が前述の認証タイプのいずれもサポートしていない場合、またはリモートユーザーが少ない場合は、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。

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。

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

- 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。
- 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。

インストール前のチェックリスト

チェックリストには、NetScaler Gatewayをインストールする前に完了する必要のあるタスクと計画情報のリストが含まれています。

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、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 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。

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

- 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。NetScaler Gateway に付属してい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、NetScaler Gateway が安全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 経由で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 (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。
- 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。
- セカンダリNetScaler Gateway IPアドレスとIDを書き留めます。

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

- 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

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 サーバーへの安全でない接続を許可する場合、デフォルトはポート 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サーバーに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。

  これは管理者バインド DN に関連付けられているパスワードです。
- 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。

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

- 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 認証および承認

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。

ファイアウォール (シングルホップ DMZ) 経由でポートを開く

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。

© 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 の間のファイアウォールについて

- 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について

- 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。

- 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、

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

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によるダブルホップ 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したら、インターフェイス0がこのNetScaler Gatewayをインターネットに接続し、インターフェイス1がこのNetScaler Gatewayを2番目のDMZのNetScaler Gatewayに接続することに注意してください。
- 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を二重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が接続を受信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。

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

第二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したら、インターフェイス0がこのNetScaler Gatewayを最初のDMZのNetScaler Gatewayに接続していることに注意してください。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.

アップグレードしています

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を確認するには

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、「 ダウンロード」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には

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 ディレクトリに変更するには、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. ソフトウェアを解凍するには、tar —xvzf Build_X_XX.tgz と入力します

   ここで Build_X_XX.TGZ はアップグレードしたいビルドの名前です。
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.

システムをインストールする

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。

NetScaler Gatewayの構成

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 では複数の仮想サーバーを構成できるため、実装する必要の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ても、セカンダリアプライアンスがユーザーセッションに影響を与えずに処理を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するには

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「nsroot」と入力します
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

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、指定された一連の条件が満たされたときに有効になる構成設定を規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。

NetScaler Gateway のポリシーについて詳しくは、以下のトピックを参照してください：

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、ポリシーを適用すべき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状態を維持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と連携するように構成する場合、Citrix Virtual Appsで次の設定を行います：

- 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。

Citrix Endpoint Managementと連携するようにNetScaler Gatewayを構成する方法について詳しくは 、「Citrix Endpoint Management 環境の設定の構成」を参照してください。

NetScaler GatewayをCitrix Virtual Apps and Desktopsと連携するように構成する方法について詳しくは、「 Web Interface を使用してCitrix Virtual AppsおよびCitrix Virtual Desktopsリソースにア

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

クセスする」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。

ポリシーの優先順位の設定

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。

条件付きポリシーの設定

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。

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

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から、またはモバイルデバイスからMicro VPNを使用して内部ネットワークの外部からNetScaler Gateway Plug-inを使用して接続するユーザーにはLDAPによる認証を要求し、WAN経由で接続するユーザーはRADIUSを使用して認証を受け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。

NetScaler Gatewayでのポリシーの作成

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
- 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式
- 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

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。

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

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

単純式と複合式の作成

単純な式は 1 つの条件をチェックします。簡単な式の例は次のとおりです：

REQ.HTTP.URL == `HTTP://www.mycompany.com`

複合式は複数の条件をチェックします。複合式を作成するには、論理演算子 && と 1 つまたは複数の式名に接続します ||. シンボルを使用して、評価順に式をグループ化できます。

複合式は次のように分類できます：

- 名前付き表現。名前付き式は独立したエンティティであるため、他のポリシーで再利用でき、ポリシーの一部となります。名前付き式は、構成ユーティリティのシステムレベルで設定します。ポリシーでは定義済みの名前付き式を使用することも、独自の式を作成することもできます。
- インライン表現。インライン式は、ポリシー内で作成するポリシー固有の式です。

名前付きエクスプレッションを作成するには

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、［Add］ をクリックします。
3. ダイアログボックスの に、式の名前を入力します。
4. エクスプレッションを作成するには、「追加」をクリックします。
5. 次のいずれかを行います：

    a. 「よく使う式」で、リストから式を選択し、「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。

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

b. 「式の構築」で、式文字列のパラメータを選択し、「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。

カスタムエクスプレッションの追加

ポリシーを作成する場合は、ポリシーの設定時にカスタム式を作成できます。たとえば、ユーザーがNetScaler Gateway Plug-inを使用してログオンできるようにするセッションプロファイルを作成し、セッションの時間制限を設定し、Windowsでのシングルサインオンを許可します。セッションプロファイルを作成したら、Create Session Policy ダイアログボックスで式を作成できます。次の例は、プロセスとウイルス対策アプリケーションを確認する式を示しています：

CLIENT.APPLICATION.PROCESS(ccapp.exe)EXISTS -frequent 5 &&
CLIENT.APPLICATION.AV(Symantec).VERSION==14.20.0.29 -freshness 5 && ns_true

ポリシー表現での演算子とオペランドの使用

演算子は、1 つ以上のオブジェクトまたはオペランドを操作する操作 (数学演算、ブール演算、リレーショナル演算など) を識別する記号です。このトピックの最初のセクションでは、使用できる演算子を定義し、定義を示します。2 番目のセクションでは、メソッド、URL、クエリなどの特定の修飾子で使用できる演算子の一覧を示します。

演算子と定義

このセクションでは、ポリシー式を作成するときに使用できる演算子を定義し、その演算子について説明します。

=, !=, EQ, NEQ

> これらの演算子は、完全に一致するかどうかをテストします。大文字と小文字は区別されます（「cmd.exe」は「cMd.exe」と同じではありません)。これらの演算子は、厳密な構文を満たす特定の文字列を許可するが、他の文字列は除外する権限を作成する場合に便利です。

GT

> この演算子は数値比較に使用されます。URL とクエリ文字列の長さに使用されます。

CONTAINS, NOTCONTAINS

> これらの演算子は、指定された修飾子と照合して、指定された文字列が修飾子に含まれているかどうかを判断します。これらの演算子は大文字と小文字を区別しません。

EXISTS, NOTEXISTS

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

これらの演算子は、特定の修飾子の存在を確認します。たとえば、これらの演算子を HTTP ヘッダーに適用して、特定の HTTP ヘッダーが存在するかどうか、または URL クエリが存在するかどうかを判断できます。

目次

この演算子は、修飾子が存在するかどうか、内容があるかどうか（つまり、値が何であれ、ヘッダーが存在し、それに関連する値があるかどうか）をチェックします。

修飾子、演算子、オペランド、アクション、例

このセクションでは、演算子とオペランドに使用できるパラメーターを示します。各項目は修飾子で始まり、関連する演算子とオペランドを一覧表示し、式が実行するアクションを説明し、例を示します。

方法

演算子:EQ、NEQ

オペランド:必須：

- 標準 HTTP メソッド
- サポート対象メソッド
- GET、HEAD、POST、PUT、DELETE OPTIONS、TRACE、CONNECT

アクション:受信したリクエストメソッドを設定されたメソッドに検証します。

例: Method EQ GET

URL

演算子:EQ、NEQ

オペランド:必須:URL（フォーマット:/\[プレフィックス\] \[*\] \[.suffix\])

アクション:受信した URL を設定された URL で検証します。

例:

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

```
URL EQ /foo&ast;.asp

URL EQ /foo&ast;

URL EQ /&ast;.asp

URL EQ /foo.asp
```

```
演算子:CONTAINS, NOTCONTAINS

オペランド:必須:任意の文字列 (引用符で囲まれた)

アクション:受信URLに設定されたパターンが存在することを確認します。(URL と URL クエリを含みます。)

例:URL に「ZZZ」が含まれています
```

URL LEN

```
演算子:GT

オペランド:必須:長さ (整数値として)

アクション:受信URLの長さを設定された長さと比較します。(URL と URL クエリを含みます。)

例:ルーレン GT 60
```

URL QUERY

```
演算子:含む、含まない

オペランド:必須:任意の文字列 (引用符で囲む)。

オプション:長さとオフセット

のアクション:

受信したURLクエリに、構成されたパターンが存在するかどうかを確認します。

コンテンツと同様に使用されます。
```

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

オプションが指定されていない場合は、パターンの後の URL クエリ全体が使用されます。

オプションが存在する場合、パターンの後のクエリの長さのみが使用されます。

オフセットは、パターンの検索をどこから開始するかを示すために使用されます。

例:URL クエリには「ZZZ」が含まれています

URL QUERY LEN

演算子:GT

オペランド:必須:長さ (整数値として)

アクション:受信 URL クエリの長さを設定された長さと比較します。

例: URLQUERYLN GT 60

URL TOKENS

演算子:EQ、NEQ

オペランド:必須:URL トークン (サポートされている URL トークン =, +,%,!、&、?)。

アクション:受信URLと設定されたトークンの有無を比較します。疑問符の前にバックスラッシュ (\\) を入力する必要があります。

例:URLTOKENS EQ '%, +, &,\\? '

VERSION

演算子:EQ、NEQ

オペランド:必須:標準 HTTP バージョン。有効な HTTP バージョン文字列 HTTP/1.0、HTTP/1.1

アクション:受信リクエストの HTTP バージョンと、設定された HTTP バージョンを比較します。

例:バージョン EQ HTTP/1.1

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

Header

演算子:EXISTS、NOTEXISTS

オペランド:なし

アクション:受信リクエストに HTTP ヘッダが存在するかどうかを調べます。

例:ヘッダークッキーが存在する

演算子:含む、含まない

オペランド:必須:任意の文字列 (引用符で囲む)。

オプション:長さとオフセット

のアクション:受信リクエストの特定のヘッダーに設定されたパターンが存在するかどうかを確認します。コンテンツと同様に使用されます。オプションが指定されていない場合は、パターンの後の HTTP ヘッダー値全体が使用されます。オプションがある場合は、パターンの後のヘッダーの長さのみが使用されます。オフセットは、パターンの検索をどこから開始するかを示すために使用されます。

例:ヘッダークッキーには「&sid」が含まれています

演算子:内容

オペランド:オプション:長さとオフセット

アクション:HTTP ヘッダーの内容を使用します。オプションが指定されていない場合は、HTTP ヘッダ値全体が使用されます。オプションが存在する場合、オフセットから始まるヘッダーの長さのみが使用されます。

例：Header User-Agent CONTENTS

SOURCEIP

演算子:EQ、NEQ

オペランド:必須:IPアドレス

オプション:サブネットマスクアクション:受信リクエスト

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

の送信元 IP アドレスを、設定された IP アドレスと照合して検証します。オプションのサブネットマスクを指定すると、受信リクエストは設定された IP アドレスとサブネットマスクに照らして検証されます。

例：Sourceip EQ 192.168.100.0 -netmask 255.255.255.0

DESTIP

オペレータ:EQ、NEQ

オペランド:必須:IPアドレスオプション:サブネットマスクアクション:受信リクエスト

の宛先

IP アドレスを、設定された IP アドレスと照合して検証します。オプションのサブネットマスクを指定すると、受信リクエストは設定された IP アドレスとサブネットマスクに照らして検証されます。

例：Sourceip EQ 192.168.100.0 -netmask 255.255.255.0

SOURCEPORT

演算子:EQ、NEQ

オペランド:必須:ポート番号

オプション:ポート範囲

アクション:受信リクエストの送信元ポート番号を設定されたポート番号と照合します。

例：SOURCEPORT EQ 10-20

DESTPORT

演算子:EQ、NEQ

オペランド:必須:ポート番号

オプション:ポート範囲

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

アクション:受信要求の宛先ポート番号を設定されたポート番号と照合します。

例：DESTPORT NEQ 80

CLIENT.SSL.VERSION

演算子:EQ、NEQ

オペランド:必須:SSLバージョン

アクション:セキュア接続で使用されている SSL または TLS バージョンのバージョンを確認します。

例：CLIENT.SSL.VERSION EQ SSLV3

CLIENT.CIPHER.TYPE

演算子:EQ、NEQ

オペランド:必須:クライアント暗号タイプ

アクション:使用されている暗号のタイプ（エクスポートまたは非エクスポート）を確認します。

例：CLIENT.CIPHER.TYPE EQ EXPORT

CLIENT.CIPHER.BITS

演算子:EQ、NEQ、GE、LE、GT、LT

オペランド:必須:クライアント暗号ビット

アクション:使用されている暗号のキー強度を確認します。

例：CLIENT.CIPHER.BITS GE 40

CLIENT.CERT

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

演算子:EXISTS、NOTEXISTS

オペランド:なしアクション:SSL

ハンドシェイク中にクライアントが有効な証明書を送信したかどうかを確認します。

例：CLIENT.CERT EXISTS

CLIENT.CERT.VERSION

演算子:EQ、NEQ、GE、LE、GT、LT

オペランド:クライアント証明書バージョン

アクション:クライアント証明書のバージョンを確認します。

例：CLIENT.CERT.VERSION EQ 2

CLIENT.CERT.SERIALNUMBER

演算子:EQ、NEQ

オペランド:必須:クライアント証明書のシリアル番号

アクション:クライアント証明書のシリアル番号を確認します。シリアル番号は文字列として扱われます。

例：CLIENT.CERT.SER IALNUMBER EQ 2343323

CLIENT.CERT.SIGALGO

演算子:EQ、NEQ

オペランド:必須:クライアント証明書署名アルゴリズム。

アクション:クライアント証明書で使用されている署名アルゴリズムを確認します。

例：CLIENT.CERT.SIGALGO EQ md5WithRSAEncryption

CLIENT.CERT.SUBJECT

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

演算子:CONTAINS、NOTCONTAINS

オペランド:必須:クライアント証明書の件名

オプション:長さ、オフセット

アクション:クライアント証明書の件名フィールドを確認します。

例：CLIENT.CERT.SUBJECT CONTAINS CN= Access_Gateway

- CLIENT.CERT.ISSUER

演算子:CONTAINS、NOTCONTAINS

オペランド:必須:クライアント証明書

発行者オプション:長さ、オフセット

アクション:クライアント証明書の発行者フィールドを確認します。

例：CLIENT.CERT.ISSUER CONTAINS O=Verisign

- CLIENT.CERT.VALIDFROM

演算子:EQ、NEQ、GE、LE、GT、LT

オペランド:必須:日付

アクション:クライアント証明書の有効日を確認します。

有効な日付形式は次

のとおりです。1994年11月5日火曜日 08:12:31 GMT

グリニッジ標準時 94年11月5日火曜日 08:12:31

GMT1994

年11月14日火曜日 08:12:31 例:CLIENT.CERT.VALIDFROM GE '1994年11月14日火曜日 08:12:31 '

-

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

CLIENT.CERT.VALIDTO

```
演算子:EQ、NEQ、GE、LE、GT、LT

オペランド:必須:日付

アクション:クライアント証明書が有効になるまでの日付を確認します。

有効な日付形式は次

のとおりです。1994年11月5日火曜日 08:12:31 GMT

グリニッジ標準時 94年11月5日火曜日 08:12:31

GMT1994

年11月14日火曜日 08:12:31 例:CLIENT.CERT.VALIDTO GE '1994年11月14日火曜日
 08:12:31 '
```

NetScaler Gateway構成設定の表示

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構成の保存

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。

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

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。

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。

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

NetScaler Gateway構成のクリア

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。

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。

ウィザードを使用した NetScaler Gatewayの構成

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：

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

- 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。
- 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。
- 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。
- 公開アプリケーションウィザードでは、Citrix Receiver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の仕組み

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。

セットアップウィザードの仕組み

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

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

統合Citrix Endpoint Management 構成の仕組み

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

クイック構成ウィザードの仕組み

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

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

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

NetScaler Gatewayウィザードの仕組み

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

公開アプリケーションウィザードの仕組み

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。

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

- 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。

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。

初回セットアップウィザードによるNetScaler Gateway の構成

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、タイムゾーンも構成します。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、およびサブネットマスク
- 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.

Configuring Settings with the Quick Configuration Wizard

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設定の構成

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 の追加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。

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、CAから署名付き証明書を受け取ったらウィザードを再起動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。

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

3. ［Next］をクリックして、ウィザードの指示に従います。

NetScaler Gateway でのホスト名と FQDN の設定

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. 詳細ペインで証明書を選択し、 をクリックし、 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。証明書の FQDN がリストに表示されます。

証明書のインストールと管理

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 CA のものです。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。

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

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。
- 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。

証明書署名リクエストの作成

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 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。

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

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。

Citrix ADC GUI を使用して CSR を作成するには

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 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、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。

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ウィンドウで、 を展開し、 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. に、証明書の名前を入力します。
5. 「証明書ファイル名」で、「ブラウズ」のメニューボックスを選択し、「アプライアンス」をクリックします。
6. 証明書に移動し、、 の順にクリックします。
7. 「プライベート・キー・ファイル名」で、「ブラウズ」のメニュー・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。秘密キーは、NetScaler Gateway の\n sconfig\ ssl ディレクトリにあります。

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

8. 秘密キーを選択し、 をクリックします。
9. 証明書が PEM 形式の場合は、 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るときの通知を設定する場合は、「期限切れ時に通知する」を選択します。
11. に日数を入力し、、 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、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 ］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. ［証明書］タブの［ 使用可能］で証明書を選択し、［ 追加］、［ OK］の順にクリックします。

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 ］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. 「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。

中間証明書の構成

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 は独自の証明書に署名する (つまり、自己署名する) ことも、別の CA が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、CA による自己署名証明書です。ルート CA の直下にある CA

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

には、ルート CA 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

サーバー証明書が CA によって自己署名証明書で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 CA という 2 つの証明書だけで構成されます。ユーザー証明書またはサーバー証明書が中間 CA 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 CA の証明書をこの順序で示しています。中間 CA の証明書の後には、その CA 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 CA 用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、［Install］をクリックします。
3. に、証明書の名前を入力します。
4. 「詳細」の「証明書ファイル名」で、「参照（アプライアンス）」をクリックし、メニューボックスで「ローカル」または「アプライアンス」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.

- Configuration Managerの PKI 証明書の展開のステップバイステップの例:Windows Server 2008 証明機関 をMicrosoft System Centerの Web サイトから入手してください。
- 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 。

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。場合によっては、秘密キーをエクスポートできないため、証明書をNetScaler Gateway にインストールできません。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てください。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. で、 を選択します。
5. 「PKCS #12 ファイル名」で、「参照」をクリックし、証明書に移動して「選択」をクリックします。
6. 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NetScaler 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、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 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 エンコードアルゴリズムで、DES または DES3 を選択します。
8. と にパスワードを入力し、 をクリックして をクリックします。

   注: パスフレーズを割り当てるには 、Key Format が PEM で、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 鍵の作成」をクリックします。上記と同じ手順に従って DSA 秘密キーを作成します。

PFX 形式から PEM 形式への証明書の変換

SSL証明書は、SSL負荷分散仮想サーバーおよびNetScaler Gateway 仮想サーバーに使用されます。PEM 証明書は Base64 でエンコードされた ASCII ファイルです。PEM 証明書はテキストエディタ/メモ帳で開くことができ、「—BEGIN CERTIFICATE—」および「—END CERTIFICATE—」ステートメントが含まれていることがわかります。

安全で信頼できるアクセスを行うには、NetScaler Gateway サーバーにSSLサーバー証明書をインストールする必要があります。アップロードされた証明書ファイルには、次の特性が必要です。

- エンドユーザーによって信頼される証明機関 (CA) は、サーバー証明書を発行する必要があります。最良の結果を得るには、ベリサイン、Thawte、GeoTrust などの商用 CA を使用してください。
- 証明書は、プライバシー拡張メール (PEM) 形式である必要があります。PEM は、バイナリ識別符号化規則 (DER) 形式の Base64 エンコーディングであるテキストベースの形式です。

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

- 証明書ファイルには秘密キーが含まれている必要があり、秘密キーは暗号化してはいけません。PEM ファイルを使用するためにパスワードは必要ありません。
- 必要な中間証明書は、PEM ファイルの最後に追加する必要があります。

NetScaler Gateway ウィザードを使用してPFX証明書をPEM形式に変換するには、次の手順を実行します。

1. に移動し、 ノードを選択します。
2. リンクをクリックします。

3. フィールドに、PEM 証明書のファイル名を指定します** 。
4. をクリックし、PEM 形式に変換する PFX 証明書を選択します。一部のユーザーは、証明書を /ncsonfig/SSL ディレクトリにアップロードし、そこからそれを使用することを好みます。PFX証明書がNetScaler Gateway に保存されている場合は 、 **［アプライアンス］**オプションを選択し、ワークステーションに保存されている場合はローカルを使用します。

5. インポートパスワードを指定します。
6. ファイルがエンコードされている場合は、エンコード形式として DES または 3DES を選択します。
7. **［OK］** をクリックします。
8. PEM パスフレーズと PEM パスフレーズの検証を指定します。
9. // リンクをクリックして** 、変換された PEM 証明書ファイルを表示します。

10. アップロードされた PFX ファイルは、変換された PEM ファイルとともに表示できます。

11. **SSL** ノードを展開します。
12. ノードを選択します。
13. **［Install］**をクリックします。
14. **証明書のインストールウィザードで、証明書とキーのペア名を指定します** 。
15. と の両方の PEM ファイルを参照します。
16. パスワードを指定します。
17. **［Install］**をクリックします。

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

`OpenSSL Utility`

インターネットインフォメーションサービス (IIS) 証明書ウィザードを使用して Windows サーバーに証明書を要求してインストールした場合は、その証明書とその秘密キーを個人情報交換 (PFX) ファイルにエクスポートできます。この証明書をNetScaler Gateway にインポートするには、PFXファイルを暗号化されていないPEM形式に変換する必要があります。

オープンソースユーティリティ`OpenSSL`を使用して、PFX から PEM への変換を実行できます。Win32`OpenSSL`から`OpenSSL`のWin32ディストリビューションをダウンロードします。

また、`OpenSSL`を使用したい場合は C++ の再配布可能ファイルが必要になる場合があります。Microsoft Visual C++ 2008 再頒布可能パッケージ (x86) からダウンロードしてください。

PFX ファイルを PEM ファイルに変換するには、Windows マシンで次の手順を実行します。

1. Win32`OpenSSL`からWin32`OpenSSL`パッケージをダウンロードしてインストールします。
2. フォルダ c:\certs を作成し、ファイル yourcert.pfx を c:\certs フォルダにコピーします。
3. コマンドプロンプトを開き、`OpenSSL`\ bin ディレクトリに移動します。`cd %homedrive%\OpenSSL\bin`
4. 次のコマンドを実行して、PFX ファイルを暗号化されていない PEM ファイルに変換します（すべて一行で）。`OpenSSL` pkcs12-in c:\certs\yourcert.pfx-out c:\certs\cag.pem —nodes

5. インポートパスワードの入力を求められたら、証明書を PFX ファイルにエクスポートするときに使用したパスワードを入力します。MAC 検証済み OK というメッセージを受信する必要があります。

6. ブラウザーでNetScaler Gateway 管理ポータルまたはHTTPSポート9001: `https://netscaler-gateway-server:9001`を参照します。
7. root としてログオンします。デフォルトのパスワードは`rootadmin`です。
8. ページの上部にある リンクをクリックします。
9. 「**秘密キー+証明書のアップロード (.pem)**」フィールドの横にある「**参照**」ボタンをクリックします。c:\certs\cag.pem ファイルを参照し、 をクリックします。
10. NetScaler Gateway を再起動して、新しいSSL証明書を適用します。

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

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

CRL を追加するには

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日

1. 構成ユーティリティの「構成」タブで、「SSL」を展開し、「CRL」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

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

- 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、先ほど設定した 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。

構成ユーティリティで LDAP または HTTP を使用して CRL 自動更新を構成するには

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公開されます。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 更新パラメータ

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。

-

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

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

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 サーバーが 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

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バインド DN 属性。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

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

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。これは、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に必要です。

間隔

CRL 更新を実行する間隔。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 更新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

CRL 更新を実行する必要がある正確な時間（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

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

- 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。CRL ペインで、先ほど設定した 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 による証明書ステータスの監視

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。

NetScaler Gatewayの OCSP の実装

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処理

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、

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

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 レスポンスキャッシュ

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

Online Certificate Status Protocol(OCSP) を設定するには、OCSP レスポンダを追加し、OCSP レスポンダを認証局 (CA) 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する必要があります。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. Proceds At Time Skew 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。

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

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. 一度だけ使用した番号 (ノンス) の拡張を有効にするには、「ナンス」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。

NetScaler Gateway構成のテスト

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。

構成ユーティリティを使用して新しいユーザーアカウントを作成する

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］を展開し、［AAAユーザー］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、ユーザー名を入力します。

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

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。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。

仮想サーバーの作成

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

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

- 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。次の方法で追加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、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。

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。

GUI を使用して仮想サーバーを作成するには

1. 「構成」タブで、「 **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。

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

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。
- 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。

仮想サーバー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 Receiverによる接続は、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のないCitrix Virtual Apps and Desktopsにのみ接続します。
- NetScaler 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、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。

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

- 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. 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、［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、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 で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、 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、 をクリックし、 をクリックします。

ワイルドカード仮想サーバーのリッスンポリシーの設定

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。

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

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

パラメーター	説明
	(#)、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。

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. 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、［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. 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。

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

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］ダイアログボックスで、［追加］をクリックし、式を構成して［OK］をクリックします。
10. ［Create］ をクリックしてから、［Close］ をクリックします。

NetScaler Gatewayの IP アドレスの設定

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。

- **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ーと通信します。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。

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

    - 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。

マップされた IP アドレスの変更または削除

NetScaler Gatewayは1つのマップされたIPアドレスをサポートします。アプライアンスにマップされた IP アドレスを 1 つ設定した場合、そのアドレスを変更または削除することはできません。マップされた IP アドレスを変更する必要がある場合は、まず新しいマッピング IP アドレスを作成し、次に元のマッピング IP アドレスを削除します。

セットアップウィザードまたは構成ユーティリティのネットワークノードを使用して、マップされた追加の IP アドレスを設定できます。

新しいマッピング IP アドレスを作成するには

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、［Add］ 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、 をクリックします。

マップされた IP アドレスを削除するには

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. 詳細ウィンドウで、マップされたアドレスをクリックし、 をクリックします。

サブネットIPアドレスの構成

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。

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

システムIPアドレスやマップされた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必要はありません。

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. 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、 をクリックして をクリックします。

ユーザー接続用の 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 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)

NetScaler Gateway 仮想サーバーをIPv6アドレスでリッスンするように構成すると、ユーザーは Citrix Receiverとのみ接続できます。NetScaler 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。

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

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。
- 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。

安全なネットワークにある DNS サーバーの解決

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。

注記：

- 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。

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

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、 をクリックし、 をクリックします。

次に、DNS 仮想サーバーを作成します。詳細については、「 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」を参照してください。

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 仮想サーバーの設定

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。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、Citrix 製品ドキュメントの「Citrix ADC 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。

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

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。

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、追加の 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。

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

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。

サーバー起動接続の設定

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は次のとおりです。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アドレスとポートを事前に認識して接続します。NetScaler Gateway はこの接続を傍受します。

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

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。

  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り、ユーザーデバイスがクリーンログオフを実行できなかったりしても、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でのルーティングの設定

内部ネットワークリソースへのアクセスを提供するには、NetScaler Gateway が内部の安全なネットワークにデータをルーティングできる必要があります。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。

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

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の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場合、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る場合があります。

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. 詳細ウィンドウの タブで、 をクリックします。
3. ルートの設定を行い、 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ペインで、 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、Ping ダイアログボックスで「停止」をクリックし、「閉じる」をクリックします。

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

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。

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ペインで、 > を展開し、 をクリックします。
2. 詳細ペインでインターフェイスを選択し、 をクリックします。
3. ダイアログボックスで、次のいずれかの操作を行います：

    - 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。

© 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、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加えて、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にも対応でき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。

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。
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。

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

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。

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。

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

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。
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。

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

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。
- 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。

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

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。
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。

© 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。どちら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することもできます。

構成ユーティリティ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、次の手順に従います：

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. 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。

構成ユーティリティ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、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. 「 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」タブの「ポリシー名」でポリシーを選択し、「ポリシーのバインド解除」をクリックして「OK」をクリックします。

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。

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

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。

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。

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

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. 詳細ペイン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. 詳細ペイン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。
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

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

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「**NetScaler 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「**NetScaler 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。

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. 「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。

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

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。

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

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

- 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認証では、Active Directory、LDAPサーバー、およびNetScaler Gatewayに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。

- 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

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

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
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

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

LDAP サーバ	バインド DN
Lotus Domino	cn=Notes 管理者、O=Citrix、C=米国
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**/承認 >**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。

    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 は通常、ユーザー名を削除し、ユーザーがいるグループを指定することによってバインド DN から生成されます。基本識別名の構文の例を次に示します：

    ```
    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
    ```

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

```
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、グループ名は必須ではないか、必要な場合は ou=groupname として指定されます。

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. 追加の LDAP 設定を自動的に取得するには、「**属性を取得**」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。これを行いたくない場合は、ステップ 12 と 13 に進んでください。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属性］に、NetScaler Gateway が構成しているLDAPサーバーのユーザーログオン名を検索する属性を入力します。デフォルトは `samAccountName` です。

12. **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。

13. で、セキュリティの種類を選択し、 をクリックします。

14. 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。

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

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。
- 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。

NetScaler Gateway 認証で機能するかどうかにかかわらず、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

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

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 認証と連携します。

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グループ抽出と連携します。

たとえば、IBM Directory Serverでは、静的、動的、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す。Sun ONE では、マネージド、フィルタ、ネストを含むすべてのロールが 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の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 認証では動作しません。

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 グループ抽出では機能しません。このタイプの LDAP サーバーでは、グループのメンバーリストでユーザーを検索してグループメンバーシップを検索します。

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

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

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。
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。

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

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。
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。

NetScaler Gateway を複数のドメインのグループ抽出用に構成するには、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。

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

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、［ 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. 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. の横にある をクリックし、 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. 「シングル・サインオン・ドメイン」の横で、最初のWindowsドメインの名前を消去し、2つ目のドメインの名前を入力して、「作成」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、［ 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. 「 要求プロファイル」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。

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

7. 「リクエストプロファイル」で、2 番目のドメインのプロファイルを選択し、「作成」をクリックし、「閉じる」をクリックします。

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を抽出するため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。
2. ナビゲーションペインで ［LADP］ をクリックします。
3. 詳細ウィンドウで、 タブをクリックし、 をクリックします。
4. 名前に、Sampaなど、最初のドメインの名前を入力します。
5. LDAP サーバーの設定を行い、 をクリックします。
6. 手順 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用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、［NetScaler Gateway］>［ポリシー］>［認証］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、 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. 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. 「サーバー」で、2 番目のドメインの認証プロファイルを選択し、「作成」をクリックし、「閉じる」をクリックします。

© 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

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、［**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。
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。グループ名も大文字と小文字が区別され、大文字と小文字は Active Directory に入力した大文字と小文字が一致する必要があります。
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、［**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。

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。

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

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。

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。

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

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. と 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設定した場合は、ポリシーに使用したのと同じ名前を使用してください。デフォルトの認証タイプで「ユーザー名フィールド」と「グループ名フィールド」を入力した場合は、プロファイルにも同じ値を使用してください。

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。

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

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。

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 と連携するようにスマートカードを構成するには、以下を実行する必要があります：

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

- 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用のルート証明書を仮想サーバーに追加する場合、次の図に示すように、「 **CA 証明書の選択**」 ドロップダウンボックスから証明書を選択する必要があります。
  図1：スマートカード認証用のルート証明書の追加

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 ではなく mydomain.com として設定した場合。
- タブでドメイン名を設定せず、wi-sso-split-upn コマンドを実行した場合は、値を 1 に設定します。この例では、ユーザープリンシパル名には「mydomain.com」というドメイン名が含まれています。

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、公開キーの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。

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

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て安全なICA接続を確立したユーザーは、ログオン時と公開リソースを起動しようとしたときの2つの異なるタイミングで、個人識別番号（PIN）の入力を求めるメッセージが表示されることがあります。この状況は、WebブラウザーとCitrix Receiver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 Receiverは、プロセスまたはSSL（Secure Sockets Layer）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。

- 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。

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

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、これらはそれぞれ RADIUS サーバを使用して設定されます。

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。
- 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。NetScaler Gateway と連携するようにGemalto Protivaを設定するには、以下のガイドラインを使用してください：

- 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。

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

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。これは、RADIUSサーバ・クライアント構成で設定したIPアドレスと同じ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。
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)

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

- 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。

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たフレーム付き IP アドレス（アクセス要求では RADIUS 属性 8 フレーム IP アドレスとも呼ばれる）を返します。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。

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

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。

RADIUS サーバからの IP アドレス抽出を設定するには：

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、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。

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。

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

- 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。
- 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

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

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。

- 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。

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

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。
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は、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 イベントの一覧です。

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	Citrix ADC セッション ID。	X	X

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

属性	意味	RAD_START	RAD_STOP
Acct-Session-Time	セッション継続時間 (秒)。	X	
Acct-Terminate-Cause	アカウント停止の理由 (次の表を参照)。	X	

表2. RADIUS 終了の原因

CITRIX ADC 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
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。

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

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。
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てプロンプトに従って 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. アクションメニューで、+ アイコンをクリックして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。

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

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。
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。

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

- 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。
- 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、`SAMLRequest`および`SAMLResponse`と呼ばれる 2 つの非表示フィールドが含まれている必要があります。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。

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

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。NetScaler Gateway と連携するようにAD FSサーバーを構成する場合は、Windows Server 2008またはWindows Server 2012の依存パーティ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:

- 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。

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

- 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。テスト展開を設定する場合は、中継側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

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。次のことを行う必要があります：

- 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。

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

- 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ようになります：

```
=> 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。

- 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、［**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、［Add］ 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、サーバープロファイルの名前を入力します。
7. 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。

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

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。

8. 「リダイレクト URL」に、認証アイデンティティプロバイダー (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。

9. に、抽出するユーザー名を入力します。
10. で、手順 9 で選択した証明書の秘密キーを選択します。

    これは、Citrix ADC AAA 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. SAML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. デフォルト認証グループに、グループ名を入力します。
13. 二要素認証を有効にするには、二段階認証でクリックします。
14. を無効にします。この設定は、SAML または IdP サーバーが SAML レスポンスに署名している場合にのみ有効にしてください。
15. ［Create］ をクリックしてから、［Close］ をクリックします。
16. 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。

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Workspace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 認証によるみ 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 (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

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

PRODUCT	バージョン
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 認証の認証機能の強化

この機能はSAMLの知識があるユーザー向けであり、この情報を使用するには基本的な認証能力が必要です。この情報を使用するには、読者がFIPSを理解している必要があります。

以下のCitrix ADC機能は、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/サーバーで使用できます：

- 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)

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 と IdP の現在の実装は、パケットエンジンで署名計算を行います。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。

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

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 サブ機能の詳細については、docs.citrix.com 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。

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`

  SAML IdP モジュールの samlIdpProfile でこれを使用してください

- `set samlidpprofile fipstest –samlIdpCertName fips-cert`

FIPS キーは初めて使用できません。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。

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

- `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。
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
```

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

```
( 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。

基本設定をクリアしても TACACS 設定はクリアされない

概要

この拡張機能では、clear config コマンドの実行時に RBA (ロールベースアクセス) 関連の設定がすべてクリアされないことに重点が置かれています。

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

選択したレベルに基づいて、NetScaler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。

使用するコマンドは次のとおりです：

```
clear ns config \[-force\] \&lt;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

Clear RBAconfig設定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。

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

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/ポリシーを追加)。
   - システムグローバルをバインドする

   注：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、またはクリアされている場合、TACACS関連の設定（アクション/ポリシー）は保持されます

CLI 構成

使用したコマンド

```
clear config [–force] &lt;level> [-RBAconfig]
```

デフォルトでは YES に設定され、指定されたレベルに基づいて設定がクリアされます。

—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。

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

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、［**NetScaler Gateway**］>［**ポリシー**］>［**認証**］**の順に展開します。**
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」に数値を入力し、「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。

© 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選択し、 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. 認証ポリシーの横の「優先度」に数値を入力し、「OK」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。

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

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

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 ］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、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、 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. タブで、 の横にある をクリックし、 または を選択します。
4. 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。
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。

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

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。
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してください。

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、メニューで「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。

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

重要:スマートカード認証用にルート証明書を仮想サーバーに追加する場合、次の図に示すように、**「CA 証明書の選択」メニューから証明**書を選択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、メニューの「追加」の横にある「CA として登録」をクリックして、「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。
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。

ユーザーとグループがドメインルートレベルにない場合、NetScaler Gateway 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 CN=Users と記載されているとします。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。

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

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。

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NetScaler Gateway に渡されて認証されます。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. 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、「Windows と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、［ NetScaler Gateway］> ［ポリシー ］を展開し、［セッション］をクリックします。
2. 詳細ペインで、［Add］ 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. 「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」をクリックし、「Windowsで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。
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 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。

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

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。

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

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

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。
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、ユーザーのログオン形式を入力し、「 **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。

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

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。

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。

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。

Citrix Receiverを使用するように接続が構成されていて、ユーザーがRADIUSまたはLDAPを使用してWeb Interfaceに接続している場合も、再認証が試みられ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。

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

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。

- 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。

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

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、ログオン時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。

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

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

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、［ **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。
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。

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行うのに役立ちます。ユーザーがパスコードを入力すると、そのパスコードは直ちに SafeWord によって無効になり、再び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。

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

- 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。
- Citrix Web インターフェイスと連携するには、SafeWord Web インターフェイスエージェントをインストールします。認証はAccess Gatewayで構成する必要はなく、Citrix Web Interfaceで処理できます。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。

Gemalto ProtivaがNetScaler Gatewayと連携するように構成するには、次のガイドラインを使用してください：

- 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、まったく新しい認証の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（Citrix ADC AAA）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

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

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。

注:

nFactor は Citrix ADC スタンダードエディションではサポートされていません。Citrix ADC エンタープライズエディションと Citrix ADC プラチナエディションでサポートされています。

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。ユーザーが直感的に理解できるような単純なフローである場合もあります。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. **ユーザー名とパスワードの動的な選択。**従来、Citrixクライアント（ブラウザとReceiverを含む）は、最初のパスワードフィールドとしてActive Directory（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、使用されているデバイスに基づいて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。したがって、独立した一連のポリシーが独自のフローになり、効率が向上し、複雑さが軽減されます。

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。

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

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：

- NetScaler Gateway プラグインは、12.1 ビルド 49.37 以降の nFactor 認証をサポートしています。
- 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。このモデルに必要な構成はこれだけです。

```
add authnProfile <name-of-profile> -authnVsName <name-of-auth-vserver>
```

authnVsNameは、認証仮想サーバーの名前です。この仮想サーバーは高度な認証ポリシーを使用して構成する必要があり、nFactor 認証に使用されます。

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

```
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。

相互運用に関する課題

ほとんどのレガシーゲートウェイクライアントと rfWebクライアントは、Gateway から送信される応答をモデルにしています。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。また、これらのクライアントは 、`pwcount`、「NSC_CERT」などのさまざまなGateway Cookie に依存しています

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。

設定ミスの考慮事項

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、（設定に従って）設定された要素で再利用されます。ワンタイムパスワード (OTP) を複数回再利用してはならないよう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

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断するのに役立つように提供されています。

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。

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

同様に、ユーザーエージェントに「Citrix Receiver」が含まれているすべてのCitrixクライアントを無視するには、「Citrix Receiver」文字列を上記`patset`にバインドします。

ゲートウェイの nFactor を制限する

ゲートウェイ認証の nFactor は、次の条件に当てはまる場合は実行されません。

1. authnProfileは、NetScaler Gateway では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ーにバインドされておらず、同じ認証仮想サーバーがauthnProfileに記載されています。
3. HTTPリクエストのユーザーエージェント文字列は、`patset ns_vpn_client_useragents`で設定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（すべてのブラウザがユーザーエージェント文字列に「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 の共通フォームプロトコル仕様に準拠しています。

LoginSchema は、製品の「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。これには、フォーム自体のラベルも含まれます。顧客は、特定の時点で提示されたフォームを説明する成功メッセージまたは失敗メッセージを提供できます。

LoginSchema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。

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。

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

管理者は、Citrix ADCが要因を発見できるようにする他の構成オプションについて、Citrix 製品の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 を使用しないデュアルファクタ認証の設定

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、「パススルー」として設定された「NextFactor」が存在する可能性があります。「パススルー」とは、Citrix ADCアプライアンス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」要素を使用することで、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。`<https://docs.citrix.com/en-us/netscaler/12-1/aaa-tm/multi-factor-nfactor-authentication.html>`を参照してください。

ユーザー名パスワード表現

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。これらは高度なポリシー式であり、ユーザー入力をオーバーライドするためにも使用できます。

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

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

- 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

仮想サーバーを作成する

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. 次の情報を入力します。

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。

© 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。このエンティティを使用して、多要素（nFactor）認証用の認証をCitrix ADC AAA仮想サーバーにオフロードできます
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。
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開始してください。	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	ONに設定すると、ユーザーが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になります。 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。-OFFに設定すると、ユーザーがCitrix

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

パラメーター名	パラメータの説明
	Workspaceアプリ、ブラウザー、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 モードになります。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。
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。

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

パラメーター名	パラメータの説明
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。
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。

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

認証仮想サーバーの作成

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。

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。

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

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」のいずれかに設定する必要があります（両方の二重引用符のセットを含む）。
   - **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」のいずれかに設定する必要があります（両方の二重引用符のセットを含む）。
   - **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。

認証ポリシーの作成

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) **名前** — 事前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。

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

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 認証サーバの追加

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** 。

LDAP 認証ポリシーの追加

1. -> — -> -> -> -> 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** -事前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。

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

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 認証サーバの追加

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た**サーバ名**またはサーバIP**アドレスを入力します。

c) RADIUSサーバが**接続**を受信するポート番号を入力します 。

d) タイムアウト値を**数**秒で入力します 。これは、Citrix ADCアプライアンスがRADIUSサーバーからの応答を待つ値です。

e) RADIUSサーバーとCitrix ADCアプライアンス間で共有されるシークレットキーを入力し**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) **シークレットキーを確認**します。

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

4. **［作成］** をクリックします

RADIUS 認証ポリシーの追加

1. -> — -> -> -> -> 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) **名前** -事前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. **［OK］**をクリックします

5. 認証ポリシーがリストされていることを確認します。

© 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 — これは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ためのファイルの名前です。ログインフォームをレンダリングするには、このファイルにCitrix Forms認証プロトコルに基づく要素のxml定義が含まれている必要があります。管理者がユーザーに他の認証情報の入力を求めずに、以前に取得した認証情報をそのまま使用したい場合は、引数として`noschema`を指定できます。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) **ユーザー表現**を入力 -ログイン時にユーザー名を抽出するための式

   d) **パスワード表現**を入力 -これはログイン時にパスワード抽出するための式です

   e) **ユーザー認証情報インデックス**の入力 -これは、ユーザーが入力したユーザー名をセッションに保存する必要があるインデックスです。

   f) **パスワード認証情報インデックス**の入力 -これは、ユーザーが入力したパスワードをセッションに保存する必要があるインデックスです。

   g) **認証強度**の入力 -これは現在の認証の重みです。

4. **［作成］** をクリックします

   a. ログインスキーマプロファイルがリストされていることを確認します。

ポリシーラベルの作成

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

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

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. -> — -> -> -> -> に移動します。**

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名前を入力します** 。

   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) 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優先度を入力します** 。

   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。

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

Unified Gateway ビジュアライザー

概要

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** 。

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

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。
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。

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

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
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。

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

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。

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。

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

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。

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. 以下のフィールドに入力してStoreFront を構成します：

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。
シングル・サインオン・ドメイン*	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\| \|セキュアチケットオーソリティサーバー*\|Secure Ticket Authority のURLを入力してください。通常はDelivery Controllerにあります。 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. **［Continue］** をクリックします

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

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
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
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。

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

フィールド	説明
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。

- （+）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/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。

Citrix Receiverでモバイル/タブレットデバイスで使用する二要素認証を構成する場合、RSA SecureID（RADIUS認証）をプライマリ認証として追加する必要があります。ただし、Receiverでユーザー名、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ら、最初にLDAPを、2番目の資格情報としてRADIUSを入力することになります。管理者の観点からは、モバイル以外の構成とは構成が異なります。

- 次の手順を実行して、モバイル/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します。

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

1. 構成ユーティリティで、［NetScaler Gateway］>［ポリシー］ ［認証］の順に選択し、モバイルデバイスおよび非モバイルデバイス用の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ような論理条件を回避するために必要です。

2. LDAP の タブの 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。

   認証サーバーの構成方法の詳細については、「NetScalerでLDAP認証を構成する方法」の「認証サーバーの作成」を参照してください

3. 必要な LDAP サーバーを選択して、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：

   ```
   `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。

   (a)「NetScaler Gateway」>「ポリシー」>「認証」>「RADIUS」から「RADIUS」オプションに移動します。 タブの をクリックします。

   (b) 必要な詳細情報を追加します。RADIUS 認証のデフォルトポートは 1812 です。

   (c) 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：

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

```
`REQ.HTTP.HEADER User-Agent NOTCONTAINS CitrixReceiver`
```

8. NetScaler 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ポリシーを最優先度として追加し、続いてRSA_NonMobileポリシーをセカンダリ優先順位として追加します：

   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 の に設定する必要があります。

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。

(a) 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なります。 セッションポリシーを作成するには、必要な仮想サーバーに移動し、「編集」をクリックし、「 **ポリシー** 」セクションに移動して、「+」記号をクリックします：

(b) ドロップダウンから 「セッション」オプションを選択します。

(c) 目的のセッションポリシー名を入力し、 をクリックして新しい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 の に設定する必要があります。

(d) モバイルデバイス以外の場合も、同じ手順に従ってください。 > の を の に設定する必要があります。

式は次のように変更する必要があります：

```
`REQ.HTTP.HEADER User-Agent NOTCONTAINS CitrixReceiver`
```

(e) モバイルユーザー以外のユーザー用に新しいプロファイルを作成するには、「+ sign」をクリックします。

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

1. 必要な仮想サーバーの下にあるポリシーとプロファイルは、次のスクリーンショットのようになります：

2. さらに、StoreFront では、NetScaler Gateway構成で「ログオンタイプ」=「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。

- **LDAP検索フィルター:** LDAP検索フィルターに一致するユーザー名（例：Active Directoryグループメンバーシップ）のみにNetScaler Gatewayへのログオンアクセスを制限します。
- **NetScaler Gatewayセッションポリシー:** セッションポリシーまたはプロファイルに含まれるグループのユーザーのみにNetScaler Gatewayへのログオンアクセスを制限します。この方法は複数のActive Directoryグループをサポートします。

LDAP検索フィルター方式

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ポリシーまたはサーバーでLDAP検索フィルターが定義されていない場合、アプライアンスはすべてのActive Directoryユーザー名から一致するものを検索します。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) を取得し、そのユーザーのDNとパスワードを使用してActive Directoryに対して認証を行います。

LDAP検索フィルターが定義されている場合、LDAP検索フィルターに一致するユーザー名のみがユーザー名の一致を検索されます。例えば、LDAP検索フィルターがActive Directoryグループのメンバーのみを検索するように構築されている場合、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。

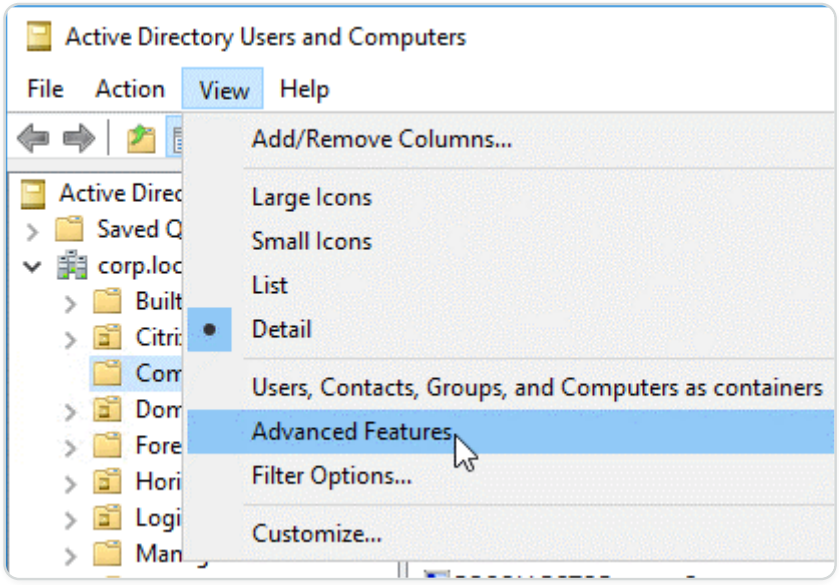
© 1997–2026 Citrix Systems, Inc. All rights reserved.

1つのActive Directoryグループのメンバーに対するLDAP検索フィルターを構成する手順

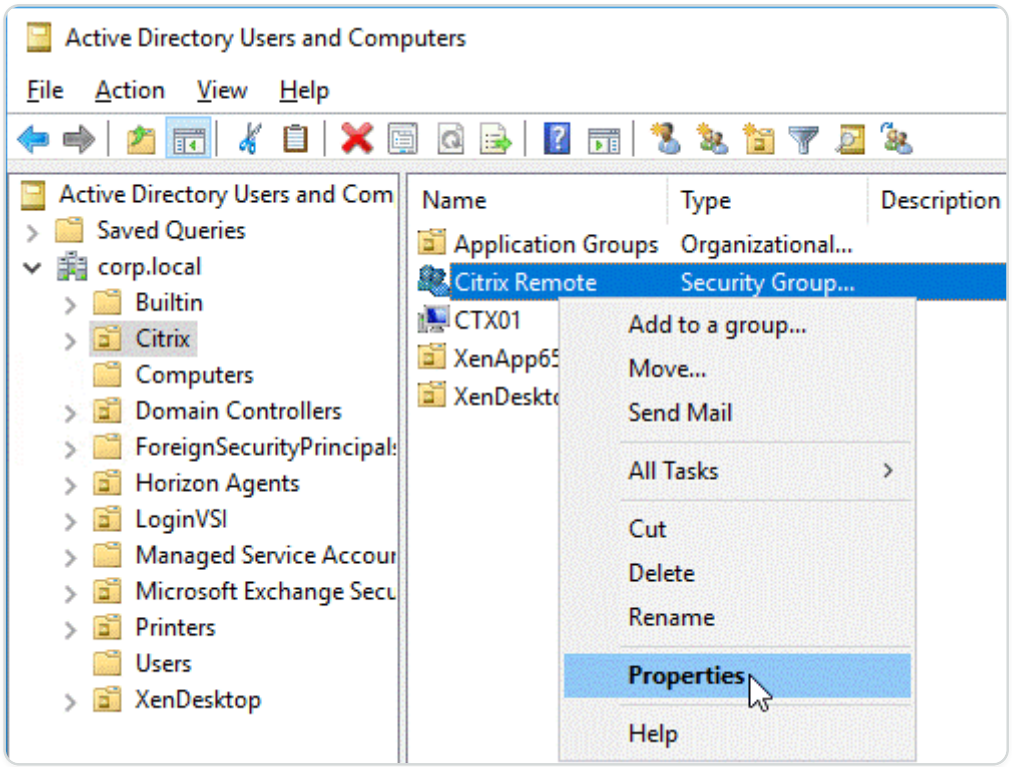
1. アクセス許可を持つActive Directoryグループを特定し、その完全な識別名を取得します。

   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ーを使用することです。

2. Active Directoryユーザーとコンピューターで、**表示**メニューから**高度な機能**を有効にします。

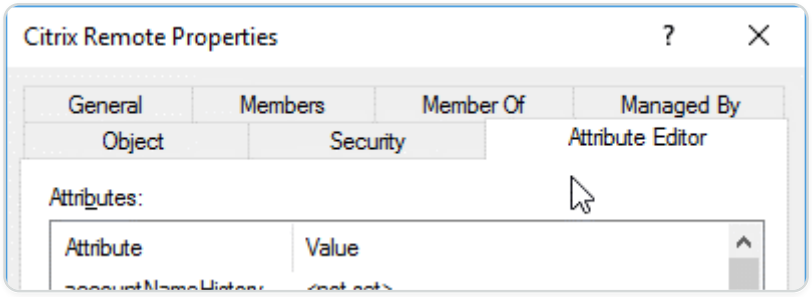


3. ツリーを参照してグループオブジェクトに移動し、右クリックして、**プロパティ**をクリックします。 **注: 検索**は使用できません。代わりに、ツリーをたどってオブジェクトを見つける必要があります。



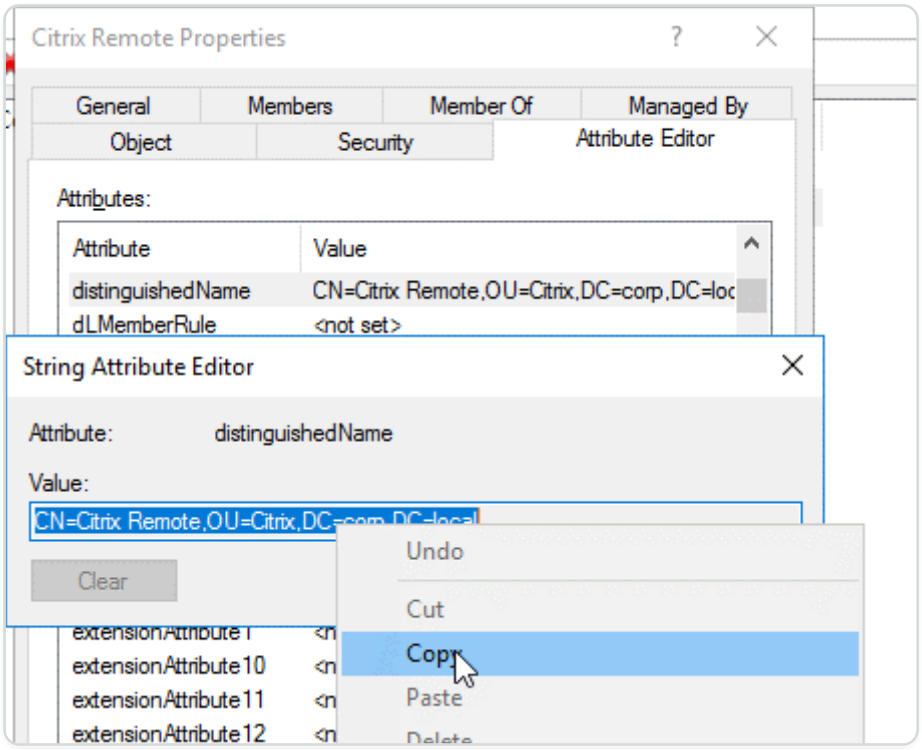
© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. 右側で、**属性エディター**タブに切り替えます。



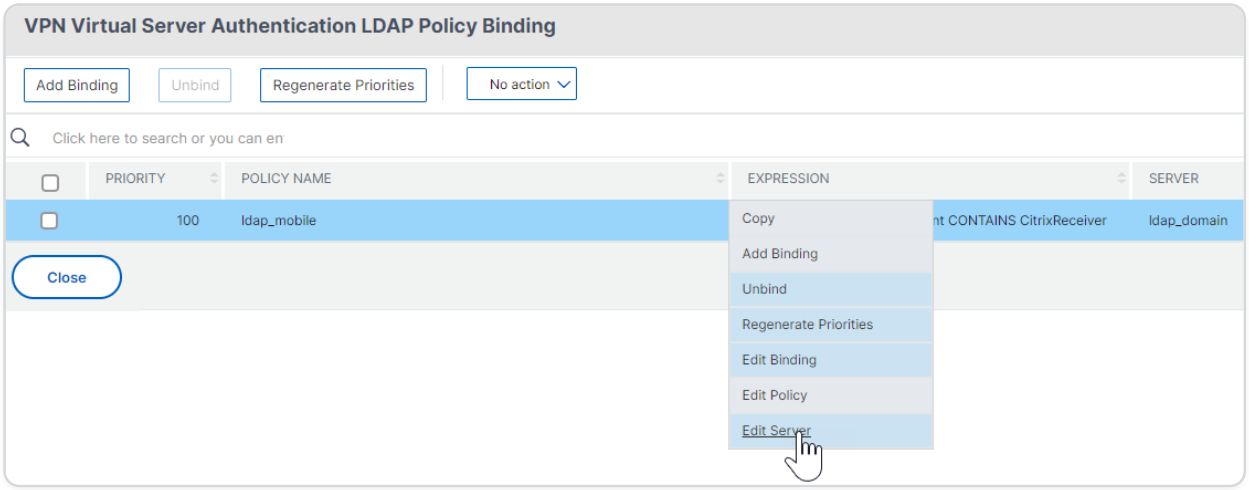
このタブは、**高度な機能**が有効になっており、**検索**機能を使用していない場合にのみ表示されます。

5. **distinguishedName**までスクロールし、ダブルクリックしてクリップボードにコピーします。

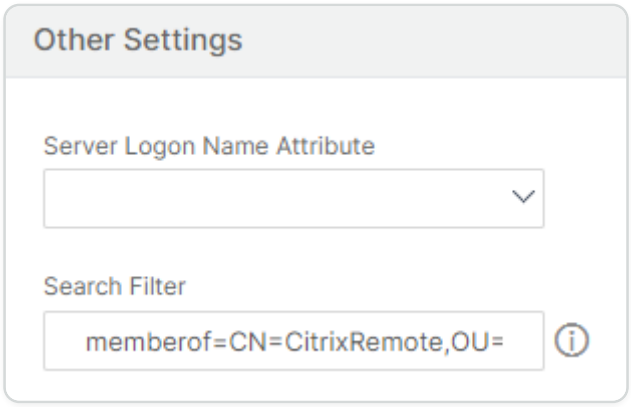


6. NetScaler Gateway GUIで、**NetScaler Gateway > 仮想サーバー**に移動します。
7. 既存のNetScaler Gateway仮想サーバーを選択し、**編集**をクリックします。
8. 「基本認証」セクションで、**LDAPポリシー**をクリックします。
9. 既存のLDAPポリシーを右クリックし、**サーバーの編集**をクリックします。

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



10. **その他の設定**セクションの**検索フィルター**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® Remote,OU=Citrix,DC=corp,DC=local **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検索フィルターに追加します。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。

NetScaler Gateway セッションポリシー方式

NetScaler Gateway では、管理者はセッションポリシーまたはプロファイルを通じてログオンを許可される Active Directory グループのユーザーを指定できます。Active Directory グループの作成とユーザーの追加については、「NetScaler Gateway でグループを作成するには」を参照してください。

CLI の使用:

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

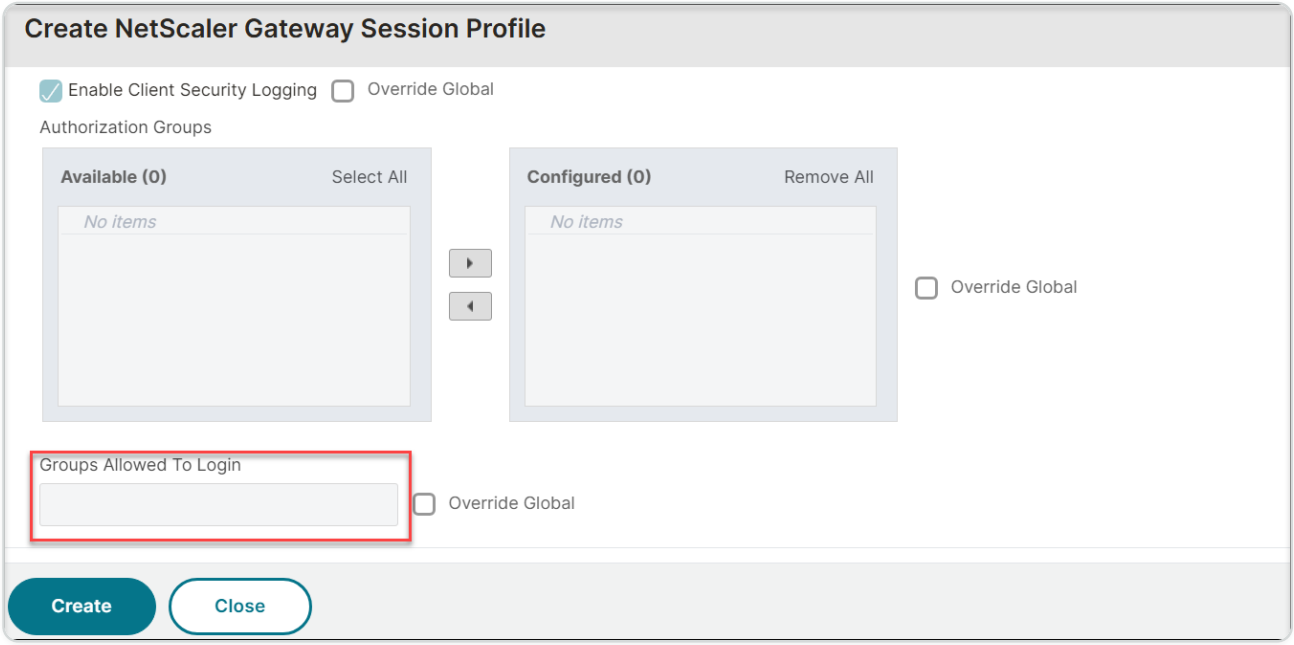
特定のグループのユーザーに対して NetScaler Gateway へのアクセスを制限するには、次のコマンドを実行します。

```
set vpn sessionAction sessionActionName -allowedLoginGroups groupName
```

GUI の使用:

1. **NetScaler Gateway** > **ポリシー** > **セッション**に移動します。
2. 詳細ペインで、「**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**の横にある「**追加**」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. **セキュリティ**タブをクリックし、「**詳細設定**」を選択します。
7. **ログインを許可するグループ**の横にある「**グローバルを上書き**」を選択し、NetScaler Gateway へのログインを許可する **Active Directory** グループを入力します。
8. 「**作成**」をクリックします。

セッションプロファイルを作成して閉じた後、「**NetScaler Gatewayセッションポリシーの作成**」ダイアログボックスでセッションポリシーの式を作成します。



© 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できるか、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。また、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 接続経由で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属性を設定しなくても、NetScaler GatewayとCitrix ADC AAAの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 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 None に設定されている場合があります。

- **なし**:ブラウザがセキュアな接続でのみクロスサイトコンテキストで Cookie を使用するように指示します。
- **Lax**: 同じサイトコンテキストのリクエストに Cookie を使用するようにブラウザに指示します。クロスサイトコンテキストでは、GETリクエストのような安全な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。

Cookie に SameSite 属性がない場合、Google Chrome は SameSite = Lax の機能を想定しています。 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Cookie 属性がVPNおよびCitrix ADC AAA仮想サーバーに追加されます。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、以下を実行する必要があります：

1. 仮想サーバーの SameSite 属性を設定する

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

2. クッキーをパッチセットにバインドする (ブラウザがドロップした場合、クロスサイトクッキーはブラウザによってドロップされる)

CLI を使用して SameSite 属性を設定する

仮想サーバーレベルで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。Citrix では、仮想サーバーレベルでSameSiteCookie 属性を設定することをお勧めします。

CLI を使用してクッキーをパッチセットにバインドする

ブラウザがクロスサイトクッキーをドロップした場合、そのCookie 文字列を既存の NS_cookies_SameSite パッチセットにバインドして、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

仮想サーバーレベルで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:

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.

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。

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。最高のパフォーマンスを発揮し、VPN 容量を最も効率的に使用するには、Office 365 Exchange Online、SharePoint Online、および Microsoft Teams に関連するこの専用 IP アドレス範囲 (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) へのトラフィックは、VPN トンネルの外部で直接ルーティングする必要があります。 この推奨事項の詳細については、 `<https://docs.microsoft.com/en-us/Office365/Enterprise/office-365-vpn-split-tunnel>` *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。

この設定には、 **GUI または CLI** コマンドを使用して手動で実行できる次のものが含まれます。

- リバース設定用の分割トンネルの設定
- 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する

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。
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。

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

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、［**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、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、 **［CIose］** 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。

- 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
```

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

Office 365 サービス (EXO、SPO、およびTeams) の IP アドレスの一覧

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|

IPv6 アドレス範囲

2603:1006::/40

2603:1016::/36 2603:1026::/36

2603:1036::/36 2603:1046::/36

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

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.

VPN ユーザーエクスペリエンスの設定

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 Receiver。
- Receiver for Webにより、ユーザーは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に接続できます。
- 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用の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（Feature Pack とFeature Pack 2を含む）、Citrix Virtual Desktops 7.0以降からReceiverをインストールすると、Receiverは自動的にNetScaler 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ReceiverからNetScaler Gateway プラグインを使用して接続できます。

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

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 Worx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への接続を可能にするSecure Browse が含まれています。Secure Hub に接続するAndroidデバイスでは、Micro VPNトンネルが自動的に確立され、内部ネットワークのリソースへの安全なWebおよびモバイルアプリケーションレベルのアクセスが可能になります。ユーザーがAndroidデバイスからWorxアプリを使用して接続する場合、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」トピックを参照してください 。

NetScaler Gateway プラグインによるユーザー接続の仕組み

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.

安全なトンネルの確立

ユーザーがNetScaler Gateway プラグイン、Secure Hub、またはCitrix Receiverを使用して接続すると、クライアントソフトウェアはポート443（またはNetScaler Gatewayで構成された任意のポート）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Receiverに、セキュリティで保護するネットワークを説明する構成情報を送信し、アドレスプールを有効にした場合はIPアドレスを含みます。

安全な接続を介したプライベートネットワークトラフィックのトンネリング

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。Receiverは、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ために、NetScaler Gateway プラグインをサポートしている必要があります。

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行うすべてのネットワーク接続をインターセプトし、Secure Sockets Layer（SSL）を介してNetScaler Gateway 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。

ファイアウォールを介した操作

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：

図1：2 つの内部ファイアウォールを介したユーザーデバイスからの接続

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コントロール

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

プラグインの動作

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)

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

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。

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 、次の手順に従います。

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。

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

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
   - 既定値は 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. サーバーを選択し、 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

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

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

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

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。

NetScaler Gateway で完全な VPN セットアップを構成する

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 Receiverを使用して接続すると、クライアントソフトウェアはポート443（またはNetScaler Gatewayで構成された任意のポート）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、保護するネットワークを説明する構成情報をNetScaler Gateway プラグイン、Secure Hub、またはReceiverに送信します。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。

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。

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

- 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な 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. 次のスクリーンショットに示すように、 リストから 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、必要な式または ns_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、 セッションポリシーのバインド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、「 NetScaler Gateway プラグイン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。

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

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。

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およびAndroid上のCitrix VPNの新しいポリシーを設定します。 `REQ.HTTP.HEADER("User-Agent").CONTAINS("CitrixVPN") && (REQ.HTTP.HEADER("User-Agent").CONTAINS("NSGiOSplugin") || REQ.HTTP.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

設定できるパラメータの一部を次に示します。

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トラフィックの監視と制御が目的の場合は、NetScalerを使用してこれらのリクエスト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、「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

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になっている場合、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（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。

分割トンネリングを設定するには

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。

© 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、［**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

   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、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。

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への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。

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

イントラネットIPアドレスを使用する場合、ユーザーはトラフィックをNetScaler Gateway VIPに送信し、そこからNetScalerはクライアントIPをプールから構成済みのイントラネットIPの1つにマップします。NetScaler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。Citrix ADCは、DHCPサーバーと同様に、着信VPN接続にイントラネットIPを割り当てます。NetScaler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作成します。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にルーティングする必要があります（NetScalerがイントラネットIPサブネットを所有していることを忘れないでください）。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。トラフィックが非対称にならないように、NetScalerから最初にパケットが送信されるルートを保持するSNIPにトラフィックを戻すことをお勧めします。

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、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。

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

- 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。

ユーザーアクセス方法の選択

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 Receiverを使用したユーザー接続。ReceiverはStoreFront またはWeb Interfaceと連携して、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します。Receiver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。ユーザーはユーザーデバイスにReceiver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Receiverをインストールすると、Receiver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組み込みます。NetScaler Gatewayは、Receiver for AndroidおよびReceiver for iOS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、およびイントラネット 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では、NetScaler Gateway Plug-inやReceiver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、必要な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。

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

- 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では、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かった場合に、Receiverを使用してNetScaler Gateway Plug-in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Receiver経由でNetScaler Gateway にログオンした場合、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。

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。
- Citrix 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します。

ユーザーアクセス用のNetScaler Gateway プラグインの展開

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プラグインについて詳しくは、「 Java向けNetScaler Gateway プラグインとの接続」を参照してください。

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

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。

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では、追加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の決定

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。

ユーザー向けNetScaler Gateway プラグインの選択

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
- Mac OS X 用NetScaler Gatewayプラグイン

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

- 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/Mac OS X または Java 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。プラグインタイプごとに個別のプロファイルを作成する必要があります。セッションプロファイルでは、Windows/Mac OS 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、［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。

セッションプロファイルで Windows または Mac OS X のプラグインタイプを設定するには

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. 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、詳細ウィンドウで、 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. 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. 「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、「Windows/Mac OS X」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、「作成」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、「作成」をクリックして「閉じる」をクリックします。
- 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 プラグインのインターセプトモードを設定するには

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」を展開して、「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、ポリシーの名前を入力します。
4. をクリックします。
5. で を選択します。
6. で と 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を入力し、 をクリックし、 をクリックします。

Windows向けNetScaler Gatewayプラグインのインストール

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。

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：

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

- ユーザーが自分のコンピューター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 アドレスへのトラフィックまたは着信トラフィックがファイアウォールによってブロックされないように、ファイアウォール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 接続を介してトラフィックをFTPに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、自分のコンピューターで XManager などの X サーバー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。

ユーザーはあたかも組織のネットワークのローカルにいるかのようにファイルやアプリケーションを操作するため、ユーザーを再トレーニングしたり、アプリケーションを設定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。

Windows向けNetScaler Gateway プラグインをインストールするには

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NetScaler Gateway プラグインを使用して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NetScaler

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

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が表示されるようにプラグインを構成できます。

Windows向け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には

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。

Active Directory から NetScaler Gateway プラグインをデプロイする

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 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 Webサイトからダウンロードできます。

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。

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

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。

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) Server 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。

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

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 を使用した NetScaler Gateway プラグインのアップグレードと削除

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。

そのためには、NetScaler Gateway プラグインの新しいディストリビューションポイントを作成します。新しいグループポリシーオブジェクトを作成し、そのオブジェクトに新しいバージョンのプラグインを割り当てます。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。

ユーザーデバイスからのNetScaler Gateway プラグインの削除

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。

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

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 を使用したNetScaler Gateway プラグインのインストールのトラブルシューティング

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 の高速ログオン最適化が原因で発生します。この最適化では、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ます。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 の高速ログオン最適化を無効にしてください。

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。

Java向けNetScaler Gateway プラグインとの接続

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と Web ブラウザには、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。

- Mac OS X
- Linux
- Windows XP（全バージョン）、Windows Vista、Windows 7、Windows 8
- Internet Explorer
- Firefox
- Safari 1.2 ウェブブラウザの最新バージョンまで

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

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ていますが、Windows用のNetScaler GatewayプラグインまたはMac OS X用のNetScaler Gatewayプラグインの一部の機能しか提供していません。

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 向けNetScaler Gateway プラグインを構成するには

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. 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、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。
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。

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

8. にポート番号を入力し、、 の順にクリックします。

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の HOSTS ファイルの更新

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 プラグインと Citrix Receiver の統合

NetScaler GatewayはReceiver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：

- Receiver for Windows 3.4以降
- Receiver for Mac
- Receiver for Android
- Receiver for iOS
- StoreFront 2.1 またはそれ以降
- AppController 2.8 以降またはCitrix Endpoint Management 10
- Citrix のWebサイトでホストされているCitrix アップデートサービス

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。

NetScaler Gateway は、ユーザーがアプライアンスにログオンしたときに、NetScaler Gateway プラグインによってWebブラウザーが開き、Receiverのホームページへのシングルサインオンが可能になるように構成できます。ユーザーはホームページからReceiverをダウンロードできます。

ユーザーがReceiverでログオンすると、ユーザー接続は次の方法でNetScaler Gatewayを経由できます：

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

- 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、AppController 2.0、AppController 2.5、AppController 2.6、App Controller 2.8、およびアプリケーションコントローラー 2.9 でのみサポートされています。ネットワークにAppController 1.1が展開されている場合、ユーザー接続はStoreFront を経由する必要があります。

Citrix Receiveでのユーザー接続の仕組み

ユーザーは、Citrix Receiver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Receiverのいずれかを使用してログオンできます：

- Receiver for Web
- Receiver for Windows
- Receiver for Mac
- Receiver for iOS
- Receiver for Android

ユーザーは、Webブラウザーまたはユーザーデバイスの Receiverアイコンを使用して、Receiver for Webにログオンできます。

ユーザーが任意のバージョンのReceiver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Receiverウィンドウに表示されます。

Citrix Workspaceアプリアイコンのデカップリング

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

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

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 を使用してアイコン統合を設定する

コマンドプロンプトで次を入力します：

```
set vpn parameter [-iconWithReceiver (ON/OFF)]
```

GUI を使用してアイコン統合を設定する

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。
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。**

重要:

この構成は、Windows VPN プラグインプロセスを再開した後に有効になります。

ICA 接続用の IPv6 の設定

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。

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

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。

IPv6 を ICA プロキシ用に構成するには

IPv6をICAプロキシ用に構成するには：

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。
2. コマンドプロンプトで、「ns機能の有効化 IPv6PT」と入力します。これにより IPv6 が有効になります。
3. コマンドプロンプトで、enable ns モード USNIP と入力します。これにより、サブネット IP アドレスを使用できるようになります。
4. コマンドプロンプトで、「 **set dns parameter –resolutionOrder AAAAThenAQuery AThenAAAAQuery OnlyAAAAQuery OnlyAQuery**」と入力します
5. コマンドプロンプトで、「**set vpn parameter -wihome** `http://XD_domain/Citrix/StoreWeb` 」と入力します。

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。

たとえば、**set vpn parameter -wihome** `http://storefront.domain.com/Citrix/StoreWeb` 。

または

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

VPN パラメータを設定-ウィホーム `http://[1000:2000::3000]/Citrix/StoreWeb`

IPv6 アドレスを使用してこのパラメータを設定する場合、IP アドレスを括弧で囲む必要があります。

NetScaler Gateway でのReceiverホームページの構成

Receiver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経由でStoreFront を認識しないReceiver for Webおよびそれ以前のバージョンのReceiverを構成する場合は、2つのセッションプロファイルを個別に作成する必要があります。Citrix Receiverのホームページフィールドには、ユーザーが正常にログオンできるように、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Receiverの場合、Receiver for WebとReceiverでプロファイルを共有できます。ただし、Citrix では、Receiver for Webにはセッションプロファイルを構成し、他のすべてのReceiverには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。

Receiverのホームページをグローバルに設定するには

Receiverのホームページ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. ［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 Receiverのホームページで、ReceiverのWebアドレスまたはReceiver for Webのホームページを入力し、「OK」をクリックします。

セッションプロファイルでReceiver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Receiver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。

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

4. Citrix Receiverのホームページで、ReceiverまたはReceiver for Web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。

Receiverテーマのログオンページへの適用

構成ユーティリティを使用して、NetScaler Gateway のログオンページにReceiverテーマを適用できます。Receiverテーマ、デフォルトテーマ、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。この機能は、以下のNetScaler Gateway バージョンで使用できます：

- NetScaler Gateway 10.1以降。
- Access Gateway 10、ビルド 71.6014.e
- Access Gateway 10、ビルド 73.5002.e

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、［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。

ログオンページのカスタムテーマの作成

構成ユーティリティを使用して、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をそのまま使用することも、Citrix Receiver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、構成ユーティリティ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
- Access Gateway 10、ビルド 73.5002.e (この機能を AppController バージョン 2.5、2.6、または 2.8 で使用するには、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)

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

- アクセスゲートウェイ 10、ビルド 71.6104.e

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

T0 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します：

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. 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。
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。

ユーザーポータルのカスタマイズ

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。

カスタムのエンドユーザー使用許諾契約 (EULA) を作成して、VPN ユーザーがサインインする前に提示することもできます。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

デフォルトでは、VPN ポータルは Caxton テーマを使用するように設定されています。Caxtonのテーマはデフォルトという名前です。

キャクストン・テーマ

NetScaler Gatewayには、ポータルに適用できるテーマが2つ追加されています。グリーンバブルとX1テーマです。

グリーンバブルテーマ

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。

VPN 仮想サーバーへのポータル・テーマのバインド

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。

コマンドラインを使用してポータル・テーマを既存の 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>
```

構成ユーティリティを使用してポータル・テーマを既存の 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. をクリックします。
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、VPN Virtual Server 編集ペインで手順 3 から上記の手順を実行して、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 Global にバインドする

コマンドラインを使用してポータル・テーマを VPN グローバル・スコープにバインドする

コマンドプロンプトで、「;」と入力します：

```
bind vpn global portaltheme <name>
```

構成ユーティリティを使用してポータル・テーマを VPN グローバル・スコープにバインドする

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。

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

12. 「完了」をクリックします。

ヒント

：一連の変更が完了したら、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Citrix 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。

コマンドラインを使用してポータル・テーマを作成する

コマンドプロンプトで次を入力します：

```
add portaltheme <name> basetheme <name>
```

構成ユーティリティを使用してポータル・テーマを作成する

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、テンプレートメニューからテンプレートを選択し、「**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。ただし、 ポータル・テーマの編集を続ける前に、インターフェースに関する次のポータル・テーマのカスタマイズ・セクションと 、インターフェース内のカスタマイズ可能なポータル属性のポップアップ説明をお読みください。

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

新しいテーマを作成したら、「ポータル・テーマを VPN [仮想サーバにバインドする」または「ポータル・テーマを VPN Global にバインドする 」で説明されているように、そのテーマをバインド](#binding-a-portal-theme-to-a-vpn-virtual-server)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。

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、このインターフェースを使用する前にこのインターフェースのさまざまな要素を理解しておく必要があります。

ポータル・テーマ・インターフェースについて

NetScaler 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**［**NetScaler 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。

ポータル・テーマ・インターフェース

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。

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

言語ペインでは 、 詳細設定ペインから編集するページを選択したときに**読み込まれる**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やサポート言語に加えて、ポータルのレイアウトのすべてのグラフィック要素は、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。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、該当する色属性のカラーピッカーにアクセスできます。

カラーピッカー

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、リストメニューには、ポータルの設計によって決定された各属性に使用できるサイズが表示されます。

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**

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

で言語を選択し、［**OK］**をクリックします。これで、 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になります。

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に関する注意事項

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の手動作成

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。*

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

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

   - グリーンバブルテーマをカスタマイズしたい場合は、**cp-r Greenbubble Custom** と入力 してグリーンバブルテーマのコピーを作成してください 。
   - デフォルトテーマ (Caxton) をカスタマイズする場合は、「 **cp-rデフォルトカスタム」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

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。

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

```
set vpn parameter UITHEME CUSTOM
```

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. 画面の一番下までスクロールし、 **UI テーマ**リストから 「 **カスタム** 」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。

エンドユーザー使用許諾契約書の作成

VPN ポータルシステムには、ポータル構成にエンドユーザーライセンス契約 (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。

コマンドラインを使用して 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：

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

```
add vpn eula <name>
```

構成ユーティリティを使用して 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。

コマンドラインを使用して EULA を VPN Global 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>
```

構成ユーティリティを使用してグローバル EULA VPN バインディングを作成する

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。

コマンドラインを使用して 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>
```

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

構成ユーティリティを使用して 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。
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. をクリックします。
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Citrix ADC 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の最新バージョンへのアップグレードを促すことができます。

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、Citrix ADC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Citrix ADC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、Citrix ADC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のクライアントが接続しようとすると、アクセスは拒否されます。

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

- 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：
  - 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。

クライアントレスアクセスの設定

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。

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

クライアントレスアクセスの有効化

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。

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。

© 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**］**>［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 アドレスのエンコーディング

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。
- 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. 「クライアントエクスペリエンス」タブの「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、エンコーディングレベルを選択して「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。

クライアントレス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。

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

- 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。

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。

新しい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ら、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。

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

デフォルト設定を使用して新しいクライアントレスアクセス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］ >［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. 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、 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ポリシーを仮想サーバにバインドするには

新しいポリシーを作成したら、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 ］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. 「ポリシーを挿入」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表現の作成と評価

クライアントレスアクセス用の新しいポリシーを作成するときに、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、［ 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. 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。
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. 「式を追加」ダイアログで式を作成し、「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。

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

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なくなります：

- 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。

アドバンストクライアントレス VPN は、絶対 URL とホスト名を識別し、HTTP レスポンスや Web ページに存在する相対 URL を書き換えるのではなく、新しい独自の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、..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。

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

- **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 アドレスの「*」の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
```

Citrix ADC GUI 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：

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。
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。

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

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の設定

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、ユーザがアクセスでき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。

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。

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

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。

SharePoint 2003、SharePoint 2007、および SharePoint 2013 のクライアントレスアクセスの設定

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。

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

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。

Webサイトを追加したり、NetScaler Gateway ウィザードの実行後に初めて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 OWA13 までのバージョンをサポートしています。高度なクライアントレスアクセスは、それ以降のバージョンをサポートします。

Citrix 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には

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. 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」タブの「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、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。

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

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、［Add］ 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、 をクリックし、 をクリックします。

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。

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、［Add］ 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。

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

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。

クライアントレスアクセスパーシステント Cookie の有効化

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アクセス用のパーシステントクッキーの設定

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。

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。

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

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. タブの 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 インターフェイスによるクライアントレスアクセス用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。構成ユーティリティまたはコマンドラインを使用してクッキーをクライアントクッキーのパターンセットにバインドし、セッション間でWeb Interfaceの設定を保存できます。

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。
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 を選択し、 をクリックします。
   - WINGDevice をクリックし、「追加」をクリックします。
   - WINGSession を選択し、「追加」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。

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

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。

   - ポリシーパッチセット ns_cvpn_default_client_cookies wiUser をバインドし、Enter キーを押します。
   - ポリシーパッチセット ns_cvpn_default_client_cookies WingDevice をバインドし、Enter キーを押します。
   - ポリシーパッチセット ns_cvpn_default_client_cookies WingSession をバインドして 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

クライアント選択ページの設定

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
- Mac OS X 用NetScaler Gatewayプラグイン

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

- 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や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 インターフェイスでは、ユーザーはファイル共有や 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用のNetScaler Gateway プラグインを選択すると 、プラグインが起動し、ユーザーがログオンします。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。

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

ログオン時にクライアント選択ページを表示する

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設定するときは、検疫グループを設定しないでください。エンドポイント分析スキャンに失敗したユーザーデバイスは隔離され、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ます。

クライアント選択オプションをグローバルに有効にするには

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、「 詳細設定」をクリックします。
4. 「一般」タブで、「クライアントの選択」をクリックし、「OK」をクリックします。

セッションポリシーの一部としてクライアント選択を有効にするには

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. 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。

© 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. タブで、 をクリックします。
7. 「一般」タブの「クライアントの選択」の横にある「グローバルを上書き」をクリックし、「クライアントの選択肢」をクリックして、「OK」をクリックし、「作成」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。

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］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。
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。
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. 「プラグインタイプ」の横にある「 **グローバルをオーバーライド** 」をクリックし、「Windows/Mac OS X」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. ICAプロキシの横にある「 **グローバル上書き** 」をクリックし、「 **オフ**」を選択します。
    b. ［Webインターフェイスアドレス］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（`<http://ipAddress/Citrix/>`など）を入力します。
    c. 「Web Interface Portal Mode」の横にある「 **グローバル上書き」をクリックし、** 「 **COMPACT**」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。

NetScaler 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。

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

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の選択肢は選択肢ページに表示されません。

STA サーバー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、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. ステップ 3 と 4 を繰り返して STA サーバを追加し、 OKをクリックします。

STA 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「 **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かった場合に、Citrix Receiverを使用して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。

アクセスシナリオフォールバックを有効にするには、ユーザーがNetScaler Gateway にログオンしたときに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

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

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：

- クライアント選択が有効になっている場合、ユーザーはReceiver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：

- 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ときは、次のガイドラインに従ってください：

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

- 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 Receiverのいずれかを使用して、引き続きWeb InterfaceまたはStoreFront にログオンできます。 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て隔離され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じように扱われます。
- 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、Receiver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、［Add］ 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。 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。

© 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［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. 詳細ペインで、［Add］ 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. 「公開アプリケーション」タブの「ICA Proxy」の横にある「グローバル上書き」をクリックし、「オン」を選択して「作成」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。

セッションポリシーを検疫グループ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］>［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. 「ポリシー」タブで「セッション」を選択し、「ポリシーの挿入」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。

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

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 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/12-1/install/ng-policies-profiles-wrapper-con/ng-config-system-expressions-con)」を参照してください
5. 「隔離グループ」で、グループ手順で設定したグループを選択し、「OK」を 2 回クリックします。

NetScaler Gateway プラグインの接続の設定

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。
- 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。

ユーザー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。

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

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。

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

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。

タイムアウトオプションには次の 3 つがあります。

- **強制タイムアウト。**この設定を有効にすると、NetScaler Gateway は、ユーザーが何をしているかにかかわらず、タイムアウト間隔が経過するとセッションを切断します。タイムアウト間隔が経過し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

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

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。

注：

- タイムアウト設定は常時接続 VPN には適用されません。
- 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。

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。

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。

強制タイムアウトの設定

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。

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

グローバル強制タイムアウトを設定するには

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］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。

セッションポリシー内で強制タイムアウトを設定するには

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。

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。

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

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。
   - 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への接続

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

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

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、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、［リソース］を展開して、［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. 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構成

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

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

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 Receiver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、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。

クライアントインターセプトの設定

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、クライアントインターセプト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。

NetScaler 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、以下を定義します：

- 1 つの IP アドレス
- IP アドレスの範囲

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用NetScaler Gateway プラグインは、リソース宛てのユーザートラフィックをインターセプトし、NetScaler Gateway を介して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ときは、次の点を考慮してください：

- 次の条件が満たされる場合、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：

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

- インターセプトモードはトランスペアレントに設定されています
- ユーザーは、Windows向けNetScaler Gateway プラグインを使用してNetScaler Gatewayに接続しています。
- 分割トンネリングは無効

- ユーザーがJava向けNetScaler Gateway プラグインを使用してNetScaler 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。Java向けNetScaler Gateway プラグインは、イントラネットアプリケーションによって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傍受します。ユーザーがこのプラグインで接続する場合は、インターセプト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インターセプトモードを選択する必要があります。

注:プロキシ代行受信と透過傍受の両方に対してイントラネットアプリケーションを構成することはできません。Windows向けNetScaler Gateway プラグインとJava向けNetScaler Gateway Plug-inの両方で使用するように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NetScaler Gateway グローバルにバインドします。

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. ダイアログボックスで、 を選択します。**
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。

© 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 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. ダイアログボックスで、 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。**

Java向けNetScaler 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

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、Java向けNetScaler Gateway Plug-in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のHOST名を設定して、HOSTファイルの変更を試みます。HOSTファイルを変更するには、ユーザーはユーザーデバイスの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**］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。**
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 アドレスに設定する必要があります。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。

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

ネームサービス解決の設定

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、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。

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。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。

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

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。

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。**

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

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［**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. 「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。

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

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
- 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。

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

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。リモートユーザは、内部ネットワーク上の IP アドレスでアドレス指定できます。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
  - 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。

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

- 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 トンネルが確立されると、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確認します。クライアントマシンがドメインに参加しているマシンの場合、VPN プラグインは DNS 登録プロセスを開始して、マシンのホスト名イントラネットを、割り当てられたイントラネット IP アドレスに関連付けます。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。

- **nsapimgr-ys enable_vpn_dns_override=1**: このフラグは、他の構成パラメーターとともに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リクエストをインターセプトすると、対応する「GET/DNS」HTTPリクエストがトンネル経由でNetScaler Gateway仮想サーバーに送信され、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

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

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、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、NetScaler Gatewayで上書きします。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。

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。

アドレスプールの設定

構成ユーティリティを使用して、ポリシーをバインドしたい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、そのノードにイントラネット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た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てNetScaler Gateway でグローバルにバインドすることもできます。

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、［**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。
   - 「**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 アドレスごとにステップ 3 を繰り返し、 **OK**をクリックします。

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

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. 「 **イントラネット IP のバインド** 」ダイアログボックスで、「 **アクション** 」をクリックし、「**挿入**」をクリックします。
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 アドレスごとにステップ 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NetScaler Gateway のグローバル設定を使用して、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 アドレスを使用してセッションを取得します。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の場合、 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。
- オフ -アドレスプールは設定されません。

注:マップされた IP アドレスが設定されていない場合は、SNIP が使用されます。

アドレスプールを設定するには

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、 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。

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

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「 **SPILLOVER** 」を選択した場合は、「Mapped IP」の横にある「 **Override Global** 」をクリックし、アプライアンスのホスト名を選択して「 **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、式を作成し、 をクリックし、 をクリックします。

転送ログインページの設定

ユーザーがイントラネットIPアドレスを持たず、NetScaler Gateway との別のセッションを確立しようとすると、［ログインの転送］ページが表示されます。［ログインの転送］ページでは、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。

ページは、ログオフ要求が失われた場合や、ユーザがクリーンログオフを実行しない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。ユーザが別のデバイスから 2 番目のセッションを確立しようとすると、ページが表示され、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。ユーザが 6 番目のセッションを確立しようとすると、 ページが表示され、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ができます。

注

.ユーザーに > 割り当てられた IP アドレスがなく、>Transfer Login ページを使用して新しい >session を確立できない場合、ユーザーには >エラーメッセージが表示されます。

ページは、アドレスプールを設定し、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 サフィックスの設定

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。

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

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

NetScaler 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NetScaler Gateway プラグインを使用して接続すると、NetScaler 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。

NetScaler Gateway は以下のVoIPソフトフォンをサポートしています。

- Cisco Softphone
- 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、NetScaler Gateway プラグインとサポートされているソフトフォンの1つ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 トラフィックがセキュアトンネルを介して送信される場合、次のソフトフォン機能がサポートされます。

- 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 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 アドレスを構成します。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。

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

Java向けNetScaler Gateway プラグインのアプリケーションアクセスの構成

アクセスレベルを設定し、セキュアネットワークでユーザがアクセスできるアプリケーションを設定できます。ユーザーがJava向けNetScaler Gateway プラグインを使用してログオンしている場合、［セキュアアクセスリモートセッション］ダイアログボックスで、［アプリケーション］をクリックできます。 ダイアログボックスが表示され、ユーザーがアクセスを許可されているすべてのアプリケーションが一覧表示されます。

ユーザーがJava向けNetScaler Gateway プラグインで接続している場合、ユーザーがアプリケーションにアクセスできるようにする2つの方法のいずれかを構成できます。

- HOSTS ファイルの変更方法
- sourceIP と sourcePort メソッド

HOSTS ファイル変更方法を使用したアプリケーションへのアクセス

HOSTSファイルの変更方法を使用すると、Java向けNetScaler Gateway プラグインは、HOSTS ファイルで構成したアプリケーションに対応するエントリを追加します。Windows ベースのデバイスでこのファイルを変更するには、管理者としてログオンするか、管理者権限を持っている必要があります。管理者権限でログオンしていない場合は、HOSTS ファイルを手動で編集し、適切なエントリを追加します。

注:Windows ベースのコンピューターでは、HOSTS ファイルは次のディレクトリパスにあります: %systemroot%\ system32\ drivers\ etc Macintosh または Linux コンピュータでは、HOSTS ファイルは /etc/hosts にあります。

たとえば、Telnet を使用して、セキュリティで保護されたネットワーク内のコンピューターに接続するとします。リモートコンピュータは、セキュリティで保護されたネットワーク内および自宅などのリモートでの作業の両方に使用します。IP アドレスは、ローカルホストの IP アドレス 127.0.0.1 である必要があります。HOSTS ファイルに、次のように IP アドレスとアプリケーション名を追加します：

127.0.0.1 telnet1

HOSTS ファイルを編集してユーザーデバイスに保存すると、接続をテストします。接続をテストするには、コマンドプロンプトを開き、Telnet を使用して接続します。ユーザーがセキュリティで保護されたネットワーク内にないユーザーデバイスを使用している場合は、Telnetを起動する前にNetScaler Gateway にログオンします。

セキュリティで保護されたネットワーク内のコンピュータに接続するには、次の操作を行います。

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

1. コンピュータで使用可能なソフトウェアを使用して Telnet セッションを開始します。
2. コマンドプロンプトから、次のように入力します。telnet を開く

   リモートコンピュータのログオンプロンプトが表示されます。

SourceIP および SourcePort メソッドを使用したアプリケーションへのアクセス

ユーザーがセキュリティで保護されたネットワーク内のアプリケーションにアクセスする必要があり、ユーザーデバイスに対する管理者権限がない場合は、 ダイアログボックスにある送信元 IP アドレスとポート番号を使用して、HOSTS ファイルを構成します。

ダイアログボックスを開いて IP アドレスとポート番号を見つけるには

1. ユーザーがプラグインを使用してログオンするときに、 ダイアログボックスで、 をクリックします。
2. リストでアプリケーションを見つけ、送信元 IP アドレスと送信元ポート番号を書き留めます。

IP アドレスとポート番号がわいたら、Telnet セッションを開始して、リモートネットワーク内のコンピュータに接続します。

アクセスインターフェースの設定

NetScaler Gateway には、ユーザーがログオンした後に表示されるWebページであ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。

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。

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

注:ユーザーがログオンしてAccess Interfaceからファイル共有を開こうとしても、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。

アクセスインターフェースのカスタムホームページへの置き換え

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. 「 クライアントエクスペリエンス 」タブの**「 ホームページ**」で、「 **ホームページの表示** 」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カスタムホームページを設定するには

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. 「 クライアントエクスペリエンス 」タブの**「**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。**

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

アクセスインターフェースの変更

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. ネットワーク内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**

Web リンクとファイル共有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、 と の ウィンドウと ウィンドウに表示されます。ユーザーが独自のリンクを追加すると、これらのリンクは と に表示されます。

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 Web アドレスを入力し、、 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。［**ブックマークの作成**］ダイアログボックスで、［**NetScaler Gateway をリバースプロキシとして使用する**］

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

チェックボックスをオンにします。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。

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。リンクは、Web サイトリンクまたはファイル共有リンクとして、タイプ別にページ上に整理されています。

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。**

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［ **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。**

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

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"
```

ファイル共有ブックマーク

```
add vpn url fileshare fileshare \fileshare.abc.com/shares
```

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

bind vpn global –urlName fileshare
```

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

個人用ブックマークの作成

VPN 仮想サーバーからのみ個人の Web サイトとファイル共有を作成できます。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、ブックマークまたはファイル共有を追加します。
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 サイトまたはファイル共有がそれぞれのタブに表示されます。

ブックマークのユーザー名トークンの設定

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。

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.

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サイトへのリクエストが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の仕組み

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：

- 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. 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。

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

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. Repeater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**］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。

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。

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

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. 「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. 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 、、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. ［Create］ をクリックしてから、［Close］ 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。

SAML シングルサインオンを設定するには

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。

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

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のバインド

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。

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。

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解除するには

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：
   - NetScaler Gateway を展開し、「 仮想サーバー」をクリックします。
   - **「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 」 >「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.

2. 詳細ウィンドウで、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。

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、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の設定

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。Windows用のNetScaler Gateway プラグインや Mac用のNetScaler Gateway プラグインなど、ユーザーのログオンに使用するソフトウェアを構成するための設定を定義できます。また、ユーザーにCitrix Receiver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。セッションポリシーは、ユーザーが認証された後に評価され、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、常に構成のグローバル設定を上書きします。
- 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。
- セッションポリシーまたは仮想サーバによって設定されていないその他の属性は、グローバル構成によって設定されます。

重要

.以下の手順は、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ことがありますが、その設定は、セッションプロファイルおよびポリシーに含まれる多くの設定の 1 つである場合があります。この手順では、セッションプロファイル内に設定を作成

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

し、そのプロファイルをセッションポリシーに適用するように指示します。新しいセッションポリシーを作成しなくても、プロファイルとポリシー内の設定を変更できます。さらに、すべての設定をグローバルレベルで作成し、セッションポリシーを作成してグローバル設定を上書きすることもできます。

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. 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、、 の順にクリックします。 注:式で を選択して、ポリシーがバインドされているレベルに常に適用されるようにします。

セッションプロファイルの作成

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式の条件を満たす場合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のユーザー接続のネットワーク設定

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

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

- 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の接続設定

セッションプロファイルの タブを使用して、次の接続設定を構成できます：

- 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)
- プラグインタイプ（Windows 用 NetScaler Gateway プラグイン、Mac OS X 用 NetScaler Gateway プラグイン、または Java 用 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。

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

セッションプロファイルのセキュリティ設定

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。

セッションプロファイルでのCitrix Virtual Apps and Desktops の設定

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 Receiver を使用するクライアント接続)
- 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
- Receiverホームページ
- アカウントサービスアドレス

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ための設定の構成について詳しくは、「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。

構成ユーティリティ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、 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。

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

構成ユーティリティ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、 > を展開し、 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、新しい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. 「 プロファイルの要求」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設定を完了し、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。
   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。

バインディングセッションポリシー

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には

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Citrix ADC AAAグループにバインドするには

1. **NetScaler Gateway > ユーザー管理 > AAA グループに移動します。**

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

2. 既存のNetScaler ADC AAAグループを選択し、 をクリックします。NetScaler ADC AAA 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. ［**ポリシーの選択**］で、このNetScaler ADC AAA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Citrix ADC AAAユーザーにバインドするには

1. **NetScaler Gateway > ユーザー管理 > AAAユーザーに移動します。**
2. 既存のNetScaler ADCユーザーを選択し、［ **編集**］をクリックします。また、NetScaler ADC AAA 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. ［**ポリシーの選択**］で、このNetScaler ADC AAA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。

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

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

- 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. セッションポリシーを作成するには、 **［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、Web_Browser_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** 。

   ☐

   すべてのタブの下にある **［グローバルを上書き］** チェックボックスをオンにすると、グローバルNetScaler Gateway パラメーターから継承された値を上書きできます。 設定例では、必須パラメーターに関する詳細のみが含まれています。
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：

   - **クライアントレスアクセス： ［オン］** に設定
   - **Web アプリケーションへのシングル・サインオン**:このチェックボックスを選択します
   - **プラグインの種類： ［Windows/Mac OS X］** に設定

   ☐

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

6. ［セキュリティ］ タブで、 ［デフォルトの承認アクション］ を有効にし、 ［許可］ に設定します。

7. ［公開アプリケーション］ 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の後に続くWeb用ストアへのパス
   - **シングルサインオンドメイン-ドメインの** NetBIOS 名

8. ［Create］ をクリックします。
9. クラシックポリシー式を使用している場合は、 フィールドに次の情報を追加し、 をクリックします。

```
REQ.HTTP.HEADER User-Agent NOTCONTAINS CitrixReceiver
```

10. 高度なポリシー式を使用する場合は、 フィールドに次の情報を追加し、 をクリックします。

```
HTTP.REQ.HEADER("User-Agent").CONTAINS("CitrixReceiver").NOT
```

このポリシーは、NetScaler 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 。**

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

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します。
   - **プラグインタイプ**: **Java**に設定

6. タブで、 を に設定します。

7. ［公開アプリケーション］ 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。
9. クラシックポリシー式を使用する場合は、 フィールドに次の情報を追加し、 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する場合は、 フィールドに次の情報を追加し、 をクリックします。

    ```
    HTTP.REQ.HEADER("User-Agent").CONTAINS("CitrixReceiver")
    ```

このポリシーは、NetScaler 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。

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

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。

エンドポイントポリシーの設定

エンドポイント分析は、ユーザーデバイスをスキャンし、オペレーティングシステム、ウイルス対策、ファイアウォール、ウェブブラウザ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。エンドポイント分析を使用すると、ネットワークへの接続を許可する前にユーザーデバイスが要件を満たしていることを確認したり、ユーザーがログオンした後も接続を維持したりできます。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監視して、デバイスが要件を満たしていることを確認できます。

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セキュリティ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

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

ル、レジストリエントリ、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すると、ユーザーはログオンできなくなります。

事前認証ポリシーで使用されていない追加のセキュリティ要件を設定する必要がある場合は、セッションポリシーを構成し、それをユーザーまたはグループにバインドします。このタイプのポリシーは、認証後ポリシーと呼ばれ、ユーザーセッション中に実行され、ウイルス対策ソフトウェアやプロセスなどの必須項目が引き続き有効であることを確認します。

事前認証ポリシーまたは認証後ポリシーを構成すると、NetScaler Gateway によってエンドポイント分析プラグインがダウンロードされ、スキャンが実行されます。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。

エンドポイントポリシーを設定するには、次の 3 種類のポリシーを使用します。

- 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セキュリティ式。ユーザーデバイスが Client Security 式の要件を満たさない場合、ユーザーを検疫グループに配置す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分類され、追加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、ユーザーのデバイスに基づいてさまざまなレベルのアクセスを許可できます。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。信頼できないコンピュータから接続するユーザーには、リモートサーバー上のドキュメントをダウンロードせずに編集できる、より制限されたアクセスレベルを提供できます。

エンドポイント分析は以下の基本ステップを実行します：

- 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。ユーザーが接続を試みると、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確認します。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:エンドポイント分析スキャンは、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。

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

- ユーザーデバイスで検出されたプロパティ値と、構成したスキャンでリストされている目的のプロパティ値を比較します。
- 目的のプロパティ値が見つかったかどうかを検証する出力を生成します。

注意: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ための特定の指示には、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、その設定は、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 つであってもかまいません。

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、エンドポイント分析スキャンをスキップすることを選択できます。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エンドポイント分析の失敗として処理します。ユーザがスキャンに失敗すると、Web Interface またはクライアントレスアクセスのみにアクセスできます。

たとえば、NetScaler Gateway プラグイン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エンドポイント分析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します。この時点で、ユーザーはネットワークレイヤーにアクセスでき、NetScaler Gateway プラグイン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：

- 指定したアプリケーションがユーザーデバイスで実行されていない場合は、ICAプロキシを有効にした状態でグローバル設定を行い、その他すべての必要な設定を行います。
- NetScaler Gateway プラグイン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内に式を作成し、次のようなアプリケーションを指定します。

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

(client.application.process (symantec.exe) が存在する)

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。エンドポイントの分析が失敗するか、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false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NetScaler Gateway プラグインを使用してフルアクセスできるようになります。

事前認証ポリシーの優先順位の設定

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、NetScaler ADC AAA Globalにバインドされた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。NetScaler ADC AAA グローバルでバインドされているポリシーが次に適用されます。

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優先順位を変更するには

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、 をクリックします。
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。

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

事前認証ポリシーとプロファイルの設定

警告：

認証、承認、および監査の事前認証ポリシーは、NetScaler 12.0ビルド56.20以降 では廃止されました。代わりに、Citrix ではnFactor認証を使用することを推奨しています。詳細については、「多要素 (nFactor) 認証] (/ja-jpo/netscaler/12/aaa-tm/multi-factor-nfactor-authentication.html)」トピックを参照してください。

ユーザーが認証される前にクライアント側のセキュリティをチェックするようにNetScaler Gateway を構成できます。この方法により、NetScaler Gateway とのセッションを確立するユーザーデバイスがセキュリティ要件に準拠することが保証されます。クライアント側のセキュリティー検査は、次の 2 つの手順で説明するように、仮想サーバーに固有の事前認証ポリシーを使用するか、グローバルに構成します。

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アクション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 がユーザーデバイスで実行されているとします。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場合はアクセスを許可または拒否できます。プロセスが実行されている場合にユーザーのログオンを許可しない場合は、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プロファイルを構成します。

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。作成された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 (&&) operators`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 (&&) operators`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。

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

- 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。
- 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ドロップダウンリストから、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。名前付き式を選択すると、NetScaler Gateway で構成されている詳細なクライアントセキュリティ文字列が表示されます。

構成ユーティリティを使用して事前認証プロファイル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が行われた後、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。

      これにより、エンドポイント分析プラグインによって停止するプロセスが指定されます。

   c. に、ファイル名を入力します。

      これにより、エンドポイント分析プラグインによって削除されるファイルが指定されます。

4. 「式」では、式ns_trueのままにするか、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、「OK」をクリックします。

構成ユーティリティを使用して事前認証プロファイルを構成するには

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］>［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、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
5. に、停止するプロセスの名前を入力します。

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

6. に、削除するファイルの名前 (c:\clientext.txt など) を入力し、 をクリックして をクリックします。

   注:

   > ファイルを削除したり、プロセスを停止したりすると、確認を求めるメッセージがユーザーに表示されます。ステップ 5 と 6 はオプションのパラメータです。

構成ユーティリティを使用して事前認証プロファイルを構成する場合は、 タブの をクリックして事前認証ポリシーを作成します 。「事前認証ポリシーの作成」ダイアログ・ボックスで、「リクエスト・プロファイル」ドロップダウン・リストからプロファイルを選択します。

エンドポイント分析式の設定

事前認証およびクライアントセキュリティセッションポリシーには、プロファイルと式が含まれます。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。ユーザーデバイスでアプリケーション、ファイル、プロセス、またはレジストリエントリをスキャンするには、ポリシー内に式または複合式を作成します。

エクスプレッションのタイプ

エクスプレッションは、エクスプレッションタイプとエクスプレッションのパラメータで構成されます。式のタイプは次のとおりです。

- 一般
- クライアントセキュリティ
- ネットワークベース

事前認証ポリシーへの事前設定済みの式の追加

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 Symantec AntiVirus 10 のウイルス定義が更新されているかどうかを確認したいとします。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。

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

事前認証ポリシーに名前付き式を追加するには

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］>［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、一覧からウイルス対策製品を選択して をクリックし、 をクリックして をクリックします。

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。

また、よく使用されるクライアントセキュリティ文字列を参照するカスタムクライアントセキュリティ式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 用のカスタムクライアントセキュリティ式を作成し、ウイルス定義が 3 日以上経過していないことを確認したいとします。新しいポリシーを作成し、ウイルス定義を指定するように式を設定します。

次の手順は、事前認証ポリシーでクライアントセキュリティポリシー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クライアントセキュリティ式を作成するには

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］>［認証/承認］の順に展開し、［事前認証EPA］をクリックします。
2. 詳細ペインで、［Add］ をクリックします。 ダイアログボックスが開きます。
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、 に 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。

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

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. 「事前認証ポリシーの作成」ダイアログ・ボックスで、「作成」をクリックし、「閉じる」をクリックします。

カスタム式を構成すると、その式は 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

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。

バインディング事前認証ポリシー

事前認証または Client Security セッションポリシーを作成したら、ポリシーを適用するレベルにポリシーをバインドします。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作成して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。

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

5. 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。

事前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、［ 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、「事前認証」をクリックします。
4. で 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」ダイアログでポリシーを選択し、「ポリシーのバインド解除」をクリックして、「OK」をクリックします。

仮想サーバーから事前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. 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、 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］>［認証/承認］の順に展開し、［事前認証EPA］をクリックします。
2. 詳細ペインでポリシーを選択し、 をクリックします。

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

認証後ポリシーの設定

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。

注：この機能はNetScaler Gateway プラグインでのみ機能します。ユーザーがCitrix Receiver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。

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。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。

認証後ポリシーの設定

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。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。

認証後のポリシーを設定するには

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、 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 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. クライアントセキュリティ式を設定し、 をクリックします。
9. の で、グループを選択します。
10. に、認証後スキャンが失敗した場合にユーザーに受信するメッセージを入力します。
11. 「認証グループ」で、「グローバルを上書き」をクリックしてグループを選択し、「追加」をクリックして「OK」をクリックし、「作成」をクリックします。
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の設定

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、クライアントセキュリティポリシーを構成し、ユーザーデバイスで 10 分ごとに実行するとします。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。

注：認証後ポリシーの頻度チェック機能は、NetScaler Gateway プラグインでのみ機能します。ユーザーがCitrix Receiver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。

クライアントセキュリティポリシーを構成するときに、 認証後ポリシーの構成の手順に従って、頻度 (分単位) を設定できます。次の図は、「式を追加」(Add Expression) ダイアログボックスで頻度値を入力できる場所を示しています。

図1：認証後スキャンの頻度を設定するためのダイアログボックス

検疫グループと承認グループの設定

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

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

あるとします。ユーザーデバイスがNetScaler Gateway で定義したセキュリティ要件を満たすと、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。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。

検疫グループの設定

検疫グループを構成するときは、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、クライアントセキュリティ式を構成します。

検疫グループのクライアントセキュリティ式を構成するには

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. 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. ダイアログボックスで、クライアントセキュリティ式を構成し、 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します。

注

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。

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

グローバル検疫グループを設定するには

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. タブの をクリックします。
4. で、クライアントセキュリティ式を構成します。
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、ユーザーの問題を説明するメッセージを入力し、「OK」をクリックします。

認証グループの設定

エンドポイント分析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、ユーザーを権限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エンドポイント分析スキャンを作成します。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。

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. 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 をクリックします。
7. で、 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、、、 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。

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

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. 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 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、［追加］をクリックし、［OK］を 2 回クリックします。

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、セキュリティ設定-詳細ダイアログボックスで、リストから承認グループを選択し、「削除」をクリックします。

ユーザーデバイスのセキュリティ事前認証式の設定

NetScaler Gateway は、ユーザーログオン時またはセッション中の他の構成時間に、セキュリティの向上に役立つさまざまなエンドポイントセキュリティチェックを提供します。これらのセキュリティ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セキュリティ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

ユーザーデバイスのセキュリティ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、既存の接続を流れるトラフィックは引き続きNetScaler Gatewayを経由します。

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

構成ユーティリティを使用して、ユーザーデバイスでセキュリティ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セキュリティ式を構成できます。

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、またはスパム対策表現の設定

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構成します。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 を確認する場合、セッションまたは事前認証ポリシー内で、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。

事前認証ポリシーまたはセッションポリシーにクライアントセキュリティポリシーを追加するには

1. 構成ユーティリティのナビゲーションペインで、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、［ NetScaler 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。

© 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. 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。
    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」にクライアントのセキュリティ文字列を入力し、「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、［ NetScaler 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、「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。

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

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」に値を入力して「OK」をクリックし、「閉じる」をクリックします。

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：

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、リストされている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、［ NetScaler 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。

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

c. 「演算子」で「EXISTS」または「NOTEXISTS」を選択し、「OK」をクリックして。

プロセスをチェックするエンドポイント分析ポリシー（認証前または認証後）を設定すると、MD5チェックサムを設定できます。

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、クライアントセキュリティ文字列を構成して、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

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

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。**
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、 値フィールドに数値がないと 、**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。

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

レジストリポリシーの設定

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。

- 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NetScaler Gateway プラグインのレジストリキーを検索するレジストリ式です：

CLIENT.REG (セキュアアクセス) .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し、 ダイアログボックスで を選択する場合、 式は CLIENT.REG で始まる必要があります

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。

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

- DWORD

  DWORD タイプの場合、値が比較され、等しくなければなりません。

- 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 バイト未満でなければなりません。

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、［ NetScaler 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形成できます。

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、かっこを使用してセキュリティ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 (&&) 演算子によるポリシーの設定

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、両方のチェックが真の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セキュリティチェックです。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 (\|\|) 演算子によるポリシーの設定

OR (||) 演算子は、2 つのセキュリティ文字列を組み合わせて動作します。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 (||) 演算子をキーワード 'OR' または記号 '||'.

例：

次に、ユーザーデバイス上にファイル c:\file.txt があるか、または 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セキュリティチェックを示します。

```
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 を使ったポリシーの設定

ザ・ない (!)または否定演算子はクライアントセキュリティ文字列を否定します。

例：

次のクライアントセキュリティチェックは、`c:\\sophos\_virus\_defs.dat`ファイルが 2 日以上経過していない場合に合格します：

```
!(client.file(c:\\\\sophos_virus_defs.dat).timestamp==2dy)
```

Advanced Endpoint Analysisスキャン

高度なエンドポイント分析（EPA）は、NetScaler Gateway アプライアンス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 アプライアンスにアクセスしようとすると、管理者がNetScaler Gateway アプライアンス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ブラウザのバージョンなど）がスキャンされます。

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

高度なEPAスキャンは、事前認証セッションと認証後のセッション用にNetScaler Gateway アプライアンスで構成できるポリシーベースのスキャンです。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。

EPA スキャンには、OPSWAT スキャンとシステムスキャンの 2 種類があります。次のセクションでは、スキャンのタイプとその詳細について説明します。

OPSWAT スキャン。スキャンメカニズムは、次のようなさまざまなレベルでセキュリティを提供します。

- 製品固有のスキャン
- ベンダー固有のスキャン
- 汎用スキャン

製品固有のスキャン:特定の製品のスキャン条件を設定できます (例: **アバスト! 特定のベンダー (AVAST Softwareなど) が特定のカテゴリー (アンチ**ウイルスなど) **に対して提供する無料アンチ ****ウイルス**)。アクセスは、指定された条件を満たすコンピュータにのみ付与されます。****

ベンダー固有のスキャン:特定のベンダー (AVAST Software **a.s.など) の**スキャン条件を設定できます。カテゴリの (アンチ**ウイルス**など)。設定されたスキャンは、ベンダーが提供するすべての製品について、指定された基準をチェックします。アクセスは、指定された条件を満たすコンピュータにのみ付与されます。

汎用スキャン:特定のカテゴリ (**ウイルス対策など**) のスキャン条件を設定できます。設定されたスキャンでは、すべての仕入先および仕入先が提供する製品について、指定された基準がチェックされます。アクセスは、指定された条件を満たすコンピュータにのみ付与されます。

システムスキャン。システムスキャンは、MAC アドレスなどのシステムレベルの属性のセキュリティを提供します。システム属性（ **MAC アドレスなど**）のスキャン基準を設定できます。アクセスは、指定された条件を満たすコンピュータにのみ付与されます。

高度なエンドポイント分析スキャンの設定

EPA スキャンには、OPSWAT スキャンとシステムスキャンの 2 種類を設定できます。

OPSWAT スキャンの設定

NetScaler Gateway アプライアンスでは、次のOPSWATスキャンが構成されています。

- 製品固有のスキャン
- ベンダー固有のスキャン

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

- 汎用スキャン

注:特定の製品サポートが GUI に表示されているかどうかをスキャンします。また、次の OPSWAT スキャン設定では、事前認証 EPA を例に挙げています。OPSWAT スキャンは、認証後 EPA にも設定できます。

製品固有の OPSWAT スキャンの設定

NetScaler GUIを使用して製品固有のOPSWAT スキャンを構成するには：

1. **構成 > NetScaler Gateway > グローバル設定に移動します**。
2. 「**グローバル設定** 」ページで 、「**事前認証設定の変更** 」リンクをクリックします。
3. **AAA 事前認証パラメータの設定ページで** 、 **OPSWAT** EPA エディタのリンクをクリックします。
4. 領域で、オペレーティングシステムを選択します。

5. カテゴリを選択します (など)。

6. ベンダーを選択します (例: AVAST Software **a.s.**)。

7. 製品を選択します。たとえば、 **Avast! 無料アンチウイルス**。

8. 製品メニューの横にある をクリックして、製品スキャンを設定します。

9. 定期スキャンを行う場合は、必要に応じて、スキャンの頻度の値を入力します。

ベンダー固有の OPSWAT スキャンの設定

NetScaler GUIを使用してベンダー固有のOPSWAT スキャンを構成するには：

1. **構成 > NetScaler Gateway > グローバル設定に移動します**。
2. 「**グローバル設定** 」ページで 、「**事前認証設定の変更** 」リンクをクリックします。
3. **AAA 事前認証パラメータの設定ページで** 、 **OPSWAT** EPA エディタのリンクをクリックします。
4. 領域で、オペレーティングシステムを選択します。

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

5. カテゴリを選択します (など)。

6. ベンダーを選択します。例：**AVAST Software a.s。**

7. **汎用「AVAST Software a.s」を選択します。ベンダー固有のスキャンをスキャン** 。

8. 製品メニューの横にある をクリックしてスキャンを設定します。

9. 定期スキャンを行う場合は、必要に応じて、スキャンの頻度の値を入力します。

汎用 OPSWAT スキャンの設定

NetScaler GUIを使用して汎用OPSWAT スキャンを構成するには：

1. **構成 > NetScaler Gateway > グローバル設定に移動します。**
2. 「グローバル設定 」ページで 、「 事前認証設定の**変更** 」リンクをクリックします。
3. **AAA 事前認証パラメータ**の設定ページで 、 **OPSWAT EPA エディタ**のリンクをクリックします。
4. 領域で、オペレーティングシステムを選択します。

5. カテゴリを選択します (など)。

6. **汎用アンチウイルス製品スキャンなど、「汎用」**カテゴリ固有のスキャンを選択します。

7. 製品メニューの横にある をクリックしてスキャンを設定します。

8. 定期スキャンを行う場合は、必要に応じて、スキャンの頻度の値を入力します。

システムスキャンの設定

NetScaler Gateway アプライアンスでは、次のシステムスキャンが構成されています。

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

- MACアドレス
- ドメインチェック
- 数値レジストリ
- 数値以外のレジストリ
- Windows Update

NetScaler GUIを使用してOPSWAT システムスキャンを構成するには：

1. **構成 > NetScaler Gateway > グローバル設定に移動します。**
2. 「**グローバル設定** 」ページで 、「**事前認証設定の変更** 」リンクをクリックします。
3. **AAA 事前認証パラメータの設定ページで** 、 **OPSWAT** EPA エディタのリンクをクリックします。
4. 領域で、オペレーティングシステムを選択します。

5. メニューから目的のシステムスキャンを選択します。たとえば、 **MAC アドレスなどです。**

6. 製品メニューの横にある をクリックして、スキャンを設定します。

7. 定期スキャンを行う場合は、必要に応じて、スキャンの頻度の値を入力します。

EPA ライブラリをアップグレードする

NetScaler 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。

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式を使用して事前認証プロファイルを設定するには

1. ［ **NetScaler Gateway >［ポリシー**］に移動します。
2. を選択します。

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

3. 詳細ペインの タブで、 をクリックします。
4. プロファイルの名前を入力します。
5. アクションを選択します。
6. オプションで、クライアントエンドポイントシステムで停止するプロセスまたは削除するファイルの名前を入力します。
7. **［Create］** をクリックします。

これで、プロファイルをリクエストアクションとして事前認証ポリシーで使用できるようになりました

高度なエンドポイント分析式を使用して事前認証ポリシーを設定するには

1. ［ **NetScaler Gateway >［ポリシー**］に移動します。
2. 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、目的のプロファイルを選択します。
6. ペインで、**を選択します。
7. 最初のメニューで、クライアントオペレーティングシステムを選択します。
8. 2 番目のメニューで、スキャンタイプを選択します。
9. ポリシーの作成が完了したら、 をクリックします。

高度なエンドポイント分析事前認証ポリシーをバインドして有効にします。

事前認証ポリシーをバインドするには

1. ［ **NetScaler Gateway >［ポリシー**］に移動します。
2. 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. ［ **操作** ］メニューの［ **グローバルバインド**］を選択します。
5. **［Bind］** をクリックします。
6. 表示される 詳細ペインで、目的のポリシーの横にあるチェックボックスをオンにします。
7. をクリックします。
8. ポリシーには自動的にプライオリティ（重み）が割り当てられます。 エントリをクリックして、必要に応じて編集します。

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

9. **OK** をクリックしてポリシーをバインドします。

特定のセッションに高度なエンドポイント分析ポリシーを設定するには

1. ［**NetScaler Gateway >［ポリシー**］に移動します。
2. 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. メニューで、次のいずれかの操作を行います。
   - a. 既存のアクションを選択します。
   - b. プラスアイコンをクリックすると、セッションポリシーで設定できる設定パラメータが表示されます。構成オプションの右側にある「**グローバルをオーバーライド」(Override Global**) チェックボックスをクリックしてアクティブにします。［**作成**］ を選択します。
6. ペインで、**を選択します。
7. メニューで、クライアントオペレーティングシステムを選択します。
8. 2 番目のプルメニューで、スキャンタイプを選択します。
9. ポリシーの作成が完了したら、 をクリックします。

高度なエンドポイント分析セッションポリシーをバインドして有効にします。

セッションポリシーをバインドするには

1. ［**NetScaler Gateway >［ポリシー**］に移動します。
2. 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. ［**操作** ］メニューの［**グローバルバインド**］を選択します。
5. ［**Bind**］ をクリックします。
6. 表示される 詳細ペインで、目的のポリシーの横にあるチェックボックスをオンにします。
7. をクリックします。
8. ポリシーには自動的にプライオリティ（重み）が割り当てられます。 エントリをクリックして、必要に応じて編集します。
9. **OK** をクリックしてポリシーをバインドします。

© 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

このリファレンスでは、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。ここに含まれる式要素は、NetScaler Gateway 構成ユーティリティによって自動的に作成されるため、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:アプリケーション以外の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 です。

エクスプレッション文字列

アドバンスト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では、式に一意の識別子が使用されます。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
スパイウェア対策	ANTISPY
アンチウイルス	ANTIVIR

© 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
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
数値レジストリスキャン	REG-NUM
非数値レジストリスキャン	REG-NON-NUM

注:macOS X 固有のスキャンでは、式にはメソッドタイプの前にプレフィックス MAC-が含まれます。したがって、ウイルス対策スキャンと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：

```
client.application(MAC-ANTIVIR_2600_RTP_==_TRUE)
```

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

アプリケーションスキャン方法

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、式で使用できるすべてのメソッドをまとめたものです。

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**	指定されたアプリケーションが本物かどうかを確認してください。	==	TRUE
有効	アプリケーションが有効になっているか確認してください。	==	TRUE
RUNNING	アプリケーションが実行中かどうかを確認してください。	==	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。

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限定せずにクライアントマシンをスキャンできます。

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

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。どの製品が特定のスキャン方法をサポートしているかを知るには、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。	すべて、いずれか、どれでもない	**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確認してください。	==	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
VIRDEF-FILE-TIME	**ウイルス定義ファイルが更新されてから何分経過したか** （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

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

方法	説明	コンパレータ	指定可能な値
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てください。	==	TRUE

表5. ヘルスチェックエージェント

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てください。	==	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

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

方法	説明	コンパレータ	指定可能な値
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。	すべて、いずれか、どれでもない	**次のオプション**を含むリスト:非暗号化、部分的、暗号化済み、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

方法	説明	コンパレータ	指定可能な値
SCAN-TIME	パッチの前回スキャンが実行されてから何分経ったか。	<, <=, >, >=, !=, ==	任意の正数
MISSED-PATCH	クライアントシステムには、これらのタイプのパッチがありません。	いずれか、どれでもない	任意の事前選択 (Patch Manager サーバで事前に選択されたパッチ)

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。	いずれか、どれでもない	編集可能なリスト

テーブル 10. ドメインメンバーシップ

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

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。	いずれか、どれでもない	編集可能なリスト

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、HKEY_CURRENT_USER、HKEY_USERS、HKEY_CLASSES_ROOT、HKEY_CURRENT_CONFIG	NO OPERATOR	任意のテキスト
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 リダイレクトが実行されます(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、64 ビットシステムでは WOW リダイレクトパスが	==	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
	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では、この設定は効果がありません。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/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

方法	説明	コンパレータ	指定可能な値

End

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

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

macOS X システム:

\~/ライブラリ/アプリケーション Support/Citrix/EPAPlugin/epaplugin.log

(~ 記号は該当する macOS X ユーザーのホームディレクトリパスを示します。)

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
- 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。

© 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. 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。

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。

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

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

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

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Gateway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。
- ユーザー証明書：ユーザー証明書が認証に使用され、マシン上に証明書が1つしかない場合、NetScaler Gateway 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。NetScaler Gateway クライアントは、次に確立されたトンネルにこの設定を使用します。
- 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。

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

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。この動作をオーバーライドするための追加設定は提供されていません。

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

NetScaler 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。

設定値が「Deny」に設定されている場合、次の変更が適用されます。

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

- 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. 「AlwaysOn プロファイル」ページで、「**追加**」をクリックします。
3. 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VPN**— 次の設定のいずれかを選択します：
     - **リモート**を選択すると 、クライアントは企業ネットワーク内にあるかどうかを検出し、企業ネットワーク内にない場合はトンネルを確立できます。これがデフォルトの設定です。
     - **クライアントの位置に**関係なく、位置検出をスキップしてトンネルを確立できる場所はどこにでもあります
   - 「**クライアント制御** 」— 次の設定のいずれかを選択します：
     - ** 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。これがデフォルトの設定です。
     - **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 — 次の設定のいずれかを選択します：
     - 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。これがデフォルトの設定です。
     - ** 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。

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

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

マシンレベルのトンネルは証明書ベースの認証を使用し、作成されるセッションは証明書の共通名をユーザー名として使用します。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明書を生成するようにしてください。理想的には、デバイス証明書の共通名としてマシン名を使用する必要があります。

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。

© 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
`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 Gateway にのみ与えられます。	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	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。

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

Windows ログオン前に常時接続 VPN (旧式は常時接続サービス)

重要：

NetScaler Gateway 13.0以降にアップグレードして、Windowsログオン前に常時接続VPN機能を使用することを推奨しています。

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

NetScaler Gatewayの構成

NetScaler Gateway搭載Citrix ADC: 1 URL

Citrix ADCとNetScaler Gatewayを組み合わせると、デスクトップユーザーとモバイルユーザーが単一のURLであらゆるアプリケーションに簡単かつ安全にアクセスできます。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。さらに、リモートユーザーは、NetScaler Gateway クライアントプラグインを搭載したiOSまたはAndroidモバイルデバイスとLinux、PC、またはMacシステムを使用して、どこにいてもNetScaler Gateway URLに統一的にアクセスできます。

NetScaler Gateway 環境では、次のカテゴリのアプリケーションへの単一URLアクセスが可能になります：

- 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には 、安全な企業ネットワーク内にある任意のWebベースのアプリケーションを使用できます。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、NetScaler Gatewayが単一の**URLアクセス**を提供するクライアントレスアプリケーションには 、Outlook Web AccessとSharePointがあります。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。

一般にクラウドアプリとも呼ばれるSaaSアプリケーションは、Sharefile、SalesForce、NetSuiteなど、組織が依存する外部の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。

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

組織によっては、 **Citrix ADCサーバーアプリケーション** をCitrix ADC負荷分散構成で展開している場合があります。これは「リバースプロキシ」アプリケーションと呼ばれることもあります。NetScaler Gateway は、展開用の仮想サーバーが同じCitrix ADC NetScaler 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には、NetScaler Gateway 構成とは独立した独自の認証構成がある場合があります。

公開されている**Citrix Virtual Apps and Desktopsの公開**アプリケーションはすべて、NetScaler Gateway URLを介して利用できるよう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。

NetScaler Gateway構成ウィザード

NetScaler Gateway 展開を使用してCitrix ADCを構成するための推奨方法は、NetScaler 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 ：NetScaler Gateway 構成ウィザードでは、初期システム構成は実行されません。NetScaler Gateway アプライアンスまたはVPXインスタンスは、NetScaler Gatewayを構成する前に基本インストールを完了する必要があります。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構成されるNetScaler Gatewayの要素は次のとおりです：

- NetScaler Gateway プライマリ仮想サーバー
- NetScaler Gateway 仮想サーバー用の SSL サーバー証明書
- 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
- NetScaler Gateway ポータルを介してアクセスされるユーザーアプリケーション

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NetScaler Gateway 展開では、次の情報が必要です。

- プライマリNetScaler Gateway 仮想サーバーの場合、展開環境のパブリックIPアドレスとIPポート番号。これは、DNSでNetScaler Gateway URLのホスト名に解決されるIPアドレスになります。たとえば、NetScaler Gateway 環境のURLが`https://mycompany.com/`の場合 、IPアドレスはmycompany.comに解決する必要があります。

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

- 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。LDAP または RADIUS のセカンダリ認証設定も作成できます。認証サーバーのIPアドレスは、関連する管理者資格情報またはディレクトリ属性とともに提供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。
- ポータルのテーマを選択できます。カスタマイズまたはブランド化されたポータルデザインが必要な場合は、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NetScaler Gateway展開を通じて利用できるようにするには、統合ポイント（StoreFront、Web Interface、またはCitrix ADC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、NetScaler Gateway 構成ユーティリティでは使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、NetScaler Gateway 構成ユーティリティで作成されたら、コンテンツスイッチング仮想サーバーまたはVPN仮想サーバーで変更できます。

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。

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

VPN 仮想サーバー

NetScaler Gateway 構成の他のすべてのVPNパラメーター、プロファイル、およびポリシーバインディングは、メインの認証構成を含め、この仮想サーバーで管理されます。このエンティティは、［ NetScaler 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、NetScaler Gateway の初期構成時にコンテンツスイッチ仮想サーバーに指定された名前が含まれます。

注

：NetScaler Gateway 展開用に作成されたVPN仮想サーバーはアドレス指定できず、0.0.0.0の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。

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、Citrix ADCアプライアンスのコンテンツスイッチング機能を活用して機能します。

Unified Gateway の展開の例をいくつか示します：

- Unified Gateway 仮想サーバー-> \[1 台のNetScaler Gateway 仮想サーバー\]
- Unified Gateway 仮想サーバー-> \[1つのNetScaler Gateway仮想サーバー、1つの負荷分散仮想サーバー\]
- Unified Gateway 仮想サーバー-> \[NetScaler Gateway仮想サーバー1台、負荷分散仮想サーバー2台\]
- Unified Gateway 仮想サーバー-> \[NetScaler Gateway仮想サーバー1台、負荷分散仮想サーバー3台\]

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

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の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。

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、トラフィックをNetScaler Gateway 仮想サーバーに転送できませんでした。

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。

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

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に関する軽微な問題 (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アクセス方法でのみトリガーされ、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たにもかかわらず、ユーザーがAAA-TM仮想サーバーにアクセスしようとしても、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。

セットアップ

Unified Gateway のライセンス要件は何ですか。 **

Unified Gateway は、エンタープライズライセンスとプラチナライセンスでのみサポートされています。NetScaler Gateway のみまたは標準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? **

ユニファイドゲートウェイ仮想サーバーと併用する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 仮想サーバー上の 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? **

現在NetScaler Gateway 仮想サーバーに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 証明書は自由に再利用でき、Unified Gateway 仮想サーバにバインドすることもできます。

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？ **

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

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

ただし、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は、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

単一ホスト対複数ホストは、Web サイトが一般的な 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) でホストされる方法と似ています。ホストが 1 つの場合は、Apache でエイリアスや「仮想ディレクトリ」を使用するのと同じ方法で、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。

認証

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で機能する既存の認証メカニズムはすべてUnified Gateway と連携します。

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た認証メカニズムは、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。アドレス指定できない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 の設定には、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 パラメーターの値の 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。

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

「StepUp」認証」って何ですか？ **

AAA-TM リソースにアクセスするために、さらに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。

StepUp 認証は 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。

1 回ログイン/1 回ログアウトとは何ですか? **

一度ログイン：VPNユーザーは、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、AAA-TM StepUp などの特殊なケースでは再認証が行われます。

一度ログアウト：最初のAAA-TMまたはNetScaler Gateway セッションが作成されると、そのセッションを使用してそのユーザーの後続の AAA-TM または NetScaler Gateway セッションが作成されます。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。

Unified Gateway レベルで共通の認証ポリシーを指定し、AAA-TM 負荷分散仮想サーバ固有の認証を負荷分散仮想サーバレベルでバインドすることはできますか。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 AAA-TM 仮想サーバに個別の認証ポリシーを指定する必要がある場合は、個別にアドレス指定可能な認証仮想サーバを個別に用意する必要があります（通常の 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ている必要があります。

バインドされた AAA-TM 仮想サーバに独自の認証ポリシーが適用されるように Unified Gateway をどのように構成しますか。 **

このシナリオでは、負荷分散サーバの認証 FQDN オプションが AAA-TM 仮想サーバを指すように設定されている必要があります。AAA-TM 仮想サーバーには独立した IP アドレスがあり、Citrix ADC およびクライアントからアクセスできる必要があります。

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

Unified Gateway 仮想サーバを経由するユーザを認証するには、AAA-TM 認証仮想サーバが必要ですか。 **

いいえ。NetScaler Gateway 仮想サーバーは、AAA-TM ユーザーであっても認証を行います。

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する必要があります。

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

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。

AAA トラフィック管理

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 AAA-TM 仮想サーバを追加することと、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。

AAA-TM 負荷分散仮想サーバが Unified Gateway 仮想サーバの背後に移動された場合、その仮想サーバ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にポイントすることで、NetScaler Gateway 仮想サーバーによって認証が確実に行われます。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。

AAA-TM セッションのセッションポリシーはどのように設定しますか。 **

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

Unified Gatewayで、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、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。認証仮想サーバーを指定すると、その仮想サーバーにバインドされた AAA-TM セッションポリシーが適用されます。

ポータルのカスタマイズ

Citrix ADC 11.0のNetScaler Gatewayポータルにはどのような変更点がありますか? **

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すると、新しいポータル・テーマ機能を使用して、新しいポータル・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。

カスタマイズはCitrix ADC 11.0のアップグレードプロセスの一部として移行されますか? **

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

いいえ。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ポータルページへの既存のカスタマイズは、Citrix 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すべて rc.conf 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：

［ **構成］>［NetScaler Gateway］>［グローバル設定］**に移動します

をクリックします。「 クライアントエクスペリエンス 」をクリック**し、「 UI テーマ 」**ドロップダウンリストから「 **デフォルト** 」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Citrix ADCハードドライブに保存されていて、そのカスタマイズを引き続き使用したい場合は、11.0 GUIファイルをバックアップして、既存のカスタムテーマファイルに挿入します。ポータル・テーマに移動する場合は、まず、「 クライアント・エクスペリエンス」の「グローバル設定」または「セッション」プロファイルの「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。

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

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。Citrix ADC インスタンスからファイルを取り出すには、SSH または WinSCP などのファイル転送ユーティリティを使用する必要があります。

ポータル・テーマは 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 AAA-TM 仮想サーバーでサポートされています。

RDPプロキシ

NetScaler Gateway 11.0のRDPプロキシでは何が変更されましたか? **

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

Citrix ADC 11.0のRDPプロキシ機能は、プラチナエディションとエンタープライズ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：

RDP プロキシ機能を有効にする

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プロキシの既存のCitrix ADC 10.5.e構成をCitrix ADC 11.0に移行するには、次の詳細を理解して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：

- 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。

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

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：プラチナライセンスまたはエンタープライズライセンスで、RDPプロキシ構成を使用する既存の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）NetScaler Gateway 仮想サーバーのフロントエンドであるユニファイドゲートウェイ仮想サーバーを使用する。

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。

他のCitrix ソフトウェアとの統合

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。

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。

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

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にはなりません。

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

ダブルホップ DMZ への展開

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に展開されたNetScaler Gateway アプライアンス

注

：上の例では説明のため、StoreFront、Web Interface、Citrix Virtual Appsで3つのファイアウォールを使用するダブルホップ構成について説明しましたが、DMZにアプライアンスを1つとセキュアネットワークにアプライアンスを1つずつ含むダブルホップDMZを作成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は、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と連携するように構成できます。ユーザーはCitrix Receiverを使用して接続します。

注

：NetScaler Gateway をStoreFront を使用してダブルホップDMZに展開すると、Receiver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DMZでのNetScaler 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。NetScaler Gatewayは、Citrix Virtual AppsとStoreFront を使用してダブルホップDMZに展開できます。

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3つのファイアウォールとWeb Interfaceを使用する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、安全なネットワークに1つのアプライアンスを持つダブルホップDMZを作成することもできます。DMZ に 1 つのアプライアンスとセ

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

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。

Citrix StoreFront またはWeb Interfaceと連携するようにダブルホップDMZを構成できます。ユーザーはCitrix Receiverを使用して接続します。

注

NetScaler GatewayをStoreFront を備えたダブルホップDMZに展開すると、Receiverの電子メールベースの自動検出は機能しません。

ダブルホップ導入の仕組み

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：

- ユーザーは、Webブラウザーを使用してCitrix Receiverを使用して最初のDMZでNetScaler Gatewayに接続し、公開アプリケーションを選択します。
- Citrix Receiverはユーザーデバイス上で起動します。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。ユーザー接続にはCitrix Receiverのみが使用されます。
- 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。

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

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
Framehawk	いいえ
UDP オーディオ	いいえ

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

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

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：

   - 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。

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

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。
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。

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

- 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。
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、最初のDMZのNetScaler Gatewayと2番目のDMZのNetScaler Gatewayプロキシを経由して、ユーザーデバイスとサーバーの間を流れます。

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

ダブルホップ DMZ 導入の準備

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。

導入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への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。

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

最初のDMZへのNetScaler Gatewayのインストール

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 でのNetScaler Gatewayの設定

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。

2 つ目の DMZ へのNetScaler Gatewayのインストール

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。

「 ハードウェアのインストール」の指示に従って、 各NetScaler Gateway アプライアンスを2つ目の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 に追加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。

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

NetScaler Gateway プロキシ上の仮想サーバーの設定の構成

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。

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。

アプライアンスプロキシと通信するためのアプライアンスの設定

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。

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

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。そのためには、「NetScaler Gateway」>「リソース」を展開 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。

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。

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

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ためのNetScaler Gatewayの構成

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. 構成ユーティリティの［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。
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. 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「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。

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

ファイアウォールの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 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。	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 Receiver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。

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

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。
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.

ダブルホップ DMZ 展開での SSL 証明書の管理

ダブルホップ DMZ 展開のコンポーネント間の接続を暗号化するために必要な SSL 証明書をインストールする必要があります。

ダブルホップ DMZ 展開では、展開に含まれるさまざまなコンポーネント間でいくつかの異なるタイプの接続が発生します。これらの接続にはエンドツーエンド SSL 暗号化はありません。ただし、各接続は個別に暗号化できます。

接続を暗号化するには、接続に関係するコンポーネントに適切な SSL 証明書 (信頼されたルートまたはサーバー証明書) をインストールする必要があります。

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、これらの各接続の暗号化に必要な SSL 証明書を示します。最初のファイアウォールを介した接続の暗号化は、インターネット経由で送信されるトラフィックを保護するために必須です。

最初のファイアウォールを介した接続	暗号化に必要な証明書
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。	最初のDMZのNetScaler Gateway には、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。Webブラウザーには、NetScaler Gateway のサーバー証明書と同じ認証局（CA）によって署名されたルート証明書がインストールされている必要があります。
インターネットからのCitrix Receiverは、最初のDMZでNetScaler Gatewayに接続します。	この接続の証明書管理は、WebブラウザーからNetScaler Gateway への接続と同じです。Web ブラウザ接続を暗号化するために証明書をインストールした場合、この接続もこれらの証明書を使用して暗号化されます。

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、これらの各接続の暗号化に必要な SSL 証明書を示しています。これらの接続を暗号化すると、セキュリティが強化されますが、必須ではありません。

第 2 ファイアウォール経由の接続	暗号化に必要な証明書
最初のDMZのNetScaler Gateway は、2番目のDMZのWeb Interfaceに接続します。	StoreFront またはWeb Interfaceには、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。最初のDMZのNetScaler Gateway には、Web Interface上のサーバー証

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

第 2 ファイアウォール経由の接続	暗号化に必要な証明書
	明書と同じCAによって署名されたルート証明書がインストールされている必要があります。
最初のDMZのNetScaler Gatewayは、2番目のDMZのNetScaler Gatewayに接続します。	2番目のDMZのNetScaler Gateway には、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。最初のDMZのNetScaler Gateway には、2番目のDMZのNetScaler Gateway のサーバー証明書と同じCAによって署名されたルート証明書がインストールされている必要があります。

次の表は、第 3 のファイアウォールを介して発生する接続と、これらの各接続の暗号化に必要な SSL 証明書を示しています。これらの接続を暗号化すると、セキュリティが強化されますが、必須ではありません。

第 3 ファイアウォール経由の接続	暗号化に必要な証明書
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。	XMLサービスがCitrix Virtual Apps サーバー上のMicrosoftインターネットインフォメーションサービス（IIS）サーバー上で実行されている場合は、SSLサーバー証明書をIISサーバーにインストールする必要があります。XML サービスが標準の Windows サービス (IIS に存在しない) の場合、SSL サーバー証明書をサーバーの SSL リレー内にインストールする必要があります。StoreFront またはWeb Interfaceには、Microsoft IISサーバーまたはSSL Relayのいずれかにインストールされたサーバー証明書と同じCAによって署名されたルート証明書がインストールされている必要があります。
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STAに接続します。	この接続の証明書管理は、Web インターフェイスから XML サービスへの接続と同じです。同じ証明書を使用してこの接続を暗号化できます。(サーバー証明書は、Microsoft IIS サーバーまたは SSL リレーのいずれかに存在する必要があります。対応するルート証明書が Web Interface に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.

第 3 ファイアウォール経由の接続	暗号化に必要な証明書
2番目のDMZのNetScaler Gateway は、内部ネットワークのサーバーでホストされているSTAに接続します。	この接続での STA の SSL サーバ証明書管理は、この表で説明した 2 つの接続で説明したものと同じです。(サーバー証明書は、Microsoft IIS サーバーまたは SSL リレーのいずれかに存在する必要があります)。2番目のDMZのNetScaler Gateway には、STAおよびXMLサービスで使用されるサーバー証明書と同じCAによって署名されたルート証明書がインストールされている必要があります。
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へのICA接続を確立します。	SSL サーバー証明書は、公開アプリケーションをホストするサーバーの SSL Relay 内にインストールする必要があります。2番目のDMZのNetScaler Gateway プロキシには、SSL Relay内にインストールされたサーバー証明書と同じCAによって署名されたルート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.

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、次のガイドラインを確認してください：

- 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やコマンドラインインターフェイスを直接使用しない方法 (SSL 証明書のインポートやスタートアップスクリプトへの変更など) を使用してどちらかのノードに構成ファイルを作成する場合は、構成ファイルを他のノードにコピーするか、そのノードに同じファイルを作成する必要があります。
- 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リストを表示できます。詳細については、「インストール前チェックリスト」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、 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。
3. ［高可用性セットアップ］ダイアログボックスの［HA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、リモートノードとして追加するCitrix ADCのNSIPアドレスを入力します。NetScaler 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オンにします。
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. クリックして、ダウンしているインターフェイス/チャネルの を有効にします。
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、「リモートシステムのログオン資格情報」で、「リモートシステムのログイン資格情報がセルフノードと異なる」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、 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 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。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。RPC ノードの設定と変更には、構成ユーティリティを使用します。

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。**
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。

© 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。
   - 「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。

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

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。

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。

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

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 証明書およびキー**(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。

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. 詳細ウィンドウの で、 をクリックします。

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

3. 「ファイル同期の開始」ダイアログの「モード」ドロップダウンリストで、適切な同期タイプ (「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て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。2 次ノードでコマンド伝播を無効にすると、主ノードから伝播されたコマンドは 2 次ノードでは実行されません。

注:伝播を再度有効にした後は、必ず強制的に同期してください。

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. で、次のいずれかを実行します：
   - 高可用性伝達を無効にするには、「プライマリノードは構成をセカンダリに伝達する」チェックボックスをオフにします。
   - 高可用性伝達を有効にするには、「プライマリノードは構成をセカンダリに伝播する」チェックボックスを選択します。
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

次のリストでは、コマンドの伝達が失敗する理由と、設定を復元するための解決策について説明します：

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

- 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

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

© 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
				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にした場合の動作は変更されません。

© 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	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。

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

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

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。

仮想 MAC アドレスを設定するためのパラメータ

VrID

> 仮想 MAC アドレスを識別する仮想ルータ ID。指定できる値は 1 から 255 です。

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

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. 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、 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て をクリックし、 をクリックして をクリックします。

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. 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. 詳細ウィンドウで、アイテムを選択し、 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. 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. 詳細ペインで項目を選択し、 をクリックします。
3. 「設定済みインターフェイス」で、ネットワークインターフェイスを選択して「削除」をクリックし、「OK」をクリックして「閉じる」をクリックします。

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、

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

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 アドレスは、IPv6 仮想ルーター ID を割り当てて作成します。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 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。

IPv6 用の仮想 MAC アドレスを設定するためのパラメータ

仮想ルーター ID

> 仮想 MAC アドレスを識別する仮想ルータ ID。指定できる値は 1 から 255 です。

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. 「アソシエイトインターフェイス」で、「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。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

ルートモニターを使用すると、テーブルに動的に学習されたルートやスタティックルートが含まれているかどうかに関係なく、高可用性の状態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ー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、内部ルーティングテーブルにルートエントリが存在するかどうかに関係なく、常にルートモニターの状態を 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。
NetScaler Gateway が動的ルートを学習できるようにするために、ルートモニターがルートの監視を開始します。これには、最大180秒かかる場合があります。再起動、フェールオーバー、v6ルートでroute6を設定するには、v4ルートのroute msr enable/disableコマンドを設定し、新しいルートモニターを追加します	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。この構成ではR1が唯一のルーターであるため、現在のプライマリノードからR1にアクセスできない場合は常に高可用性セットアップでフェイルオーバーする必要があります。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、いずれかのアプライアンスが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行われます。

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（STAYSECONDARY オプションを使用して）セカンダリのままになるように設定されている場合、ノードは次のエラーメッセージを表示します。「私の状態は無効なので操作できません。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イ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. 「高可用性ステータス」で、「セカンダリのままにする (リッスンモードのまま)」をクリックし、「OK」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、プライマリノードのままにするアプライアンスを選択し、 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。

© 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NetScaler Gateway アプライアンスまたは仮想マシンを最低2つ、最大32台で構成して構築できます

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でサポートされていないため、［**GUI**］**>**［**ナビゲーション**］**ペインの**［**Citrix製品との統合****］セクションにXenApp 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. どのNetScaler Gateway アプライアンスまたは仮想マシンを構成コーディネーターにするかを決定し、そのシステムにクラスターインスタンスを作成します（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。
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。

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

Citrix ADC クラスターの構成には複数の方法があることに注意してください。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

展開の詳細がすべて揃ったら、構成コーディネーターとなる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Citrix 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。これ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。これは、クラスターの構成コーディネーターIPアドレスであり、クラスターの管理IPアドレスになります。
    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. システムが再起動するのを待ちます。利用可能になったら、手順 4b 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。
8. システム情報詳細ペインでは、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ることに注意してください。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。

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

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：NetScaler Gateway セットアップを構成する前に、クラスターへのノードの追加を完了する必要があります。これにより、クラスター構成に問題が発生し、クラスターを削除して最初からやり直したい場合に、NetScaler Gateway 構成を繰り返す必要がなくなります。

1. クラスタ IP アドレスで Citrix 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. 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. プロンプトが表示されたら、［ はい ］をクリックしてシステム構成を保存し、リモートの NetScaler Gateway のウォームリブートを実行します。

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9を繰り返します。

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 IP アドレスで Citrix 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. をクリックします。

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

4. 詳細ペインで、［Add］ 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. 「スティッキー」オプションを選択します。これは、NetScaler Gateway 仮想サーバータイプをサポートするために必要です。
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。これがクラスターグループにバインドされる唯一のノードになります。

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。

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。

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

注：NetScaler Gateway 仮想サーバーがまだ構成されていない場合は、まず > > でNetScaler Gatewayと認証、承認、監査機能を有効にする 必要がある場合があります。

1. クラスタ IP アドレスで Citrix 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. 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.

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。

追加の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人と、NetScaler Gatewayの特定の設定を担当する担当者が1人いるとします。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する必要があります。ユーザーと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。システムコマンドグループと 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を許可します。
- 演算子。読み取り専用アクセスを許可し、サービスの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、設定されているサービスやサーバーへのアクセスも「アクセスダウン」として許可されます。
- Network。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。デフォルトの管理者である nsroot に付与される権限など、すべての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、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. 「パスワード」と「パスワードの確認」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. の で、 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」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。

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場合は、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。高度なポリシーを設定する場合は、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、管理者がそのグループで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. 「 **エンティティグループ** 」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. 「 **オペレーション**」でコマンドを選択し、「 **作成** 」をクリックし、「閉じる」をクリックします。

   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. **［Create］** をクリックしてから、**［Close］** をクリックします。
11. ダイアログボックスで、 をクリックし、 をクリックします。

をクリックすると、 ダイアログボックスの 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 に重大な問題が発生しないように、できるだけ早く是正措置を講じる必要があります。
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 では、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るログ署名SessionIDを使用します。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。
- ログをNetScaler Gatewayに保存するためのログです。

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** のいずれかを選択します。
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** のいずれかを選択します。
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. **Syslog** または **Nslog** のいずれかを選択します。
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、有効にするロギングのタイプ (syslog または nslog) に応じて、Syslog ファイルまたは nslog ファイルのいずれかに格納されます。

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
ログステート	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。
レートリミット	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 のいずれかを選択します。
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.

ロギングを有効にするには

1. ユーザーデバイスで、通知領域の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. ［トレース］タブをクリックし、ログレベルを選択して［OK］をクリックします。

注：

［構成］ダイアログボックスを開くには、NetScaler Gateway プラグインを使用してユーザーがログオンしている必要があります。

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.

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と連携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、どのデバイスからでもShareFileにあるドキュメントを操作できます。

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 MDX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。

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

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：

- 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NetScaler 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NetScaler Gateway プラグインまたはMac用のNetScaler 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、NetScaler Gateway 10.1、ビルド120.1316.e以降をインストールする必要があります。

- Citrix Receiverを使用すると、Endpoint Management を介してShareFileからWeb、SaaS、および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できます。ユーザーがReceiverでログオンすると、NetScaler Gatewayは接続をEndpoint Management にルーティングします。Receiver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Receiverに表示されます。ユーザーがReceiverでログオンしてEndpoint Management に直接接続する場合は、NetScaler 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。この展開にはStoreFront は必要ありません。
- Receiver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します。ユーザーがReceiverでログオンすると、NetScaler Gatewayは接続をStoreFront またはWeb Interfaceにルーティングします。Receiver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Receiverに表示されます。
- Secure Hub：モバイルデバイスからEndpoint Managementを介して、WorxMailやWorxWebなどのiOSおよびAndroidアプリに接続します。ユーザーがSecure Hubにログオンすると、Endpoint Managementで構成したモバイルアプリにアクセスできます。NetScaler Gateway がマイクロ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NetScaler Gateway 経由で接続する場合は、次の操作を行います：

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

- ユーザーは、NetScaler Gateway プラグインまたはReceiverを使用してログオンします。初めてログオンするには、ユーザーはWebブラウザーを開いて、NetScaler Gatewayまたは Receiver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 でログオンします。
- ログオンページで、ユーザーは資格情報を入力して認証されます。
- 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、NetScaler Gateway は展開環境内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は、Endpoint Managementの背後にStoreFront を展開します。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、およびWindowsベースのアプリケーションはすべて、ReceiverまたはSecure Hub に表示されます。

Exchange、ファイル共有、社内Webサイトなど、内部ネットワーク内の他のリソースにアクセスする必要がある場合は、NetScaler 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、コンピューター上で Microsoft Outlook を起動します。安全な接続は、NetScaler Gateway に接続する NetScaler 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 に対して作成され、ユーザは電子メールにアクセスできます。

重要

・NetScaler Gateway 仮想サーバーで認証を構成することをお勧めします。NetScaler Gateway で認証を無効にすると、認証されていないHTTPリクエストは、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。

© 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、ユーザーがCitrix ReceiverまたはSecure Hub を使用して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、ReceiverとStoreFront tを使用して、Citrix Virtual Appsで公開されているWindowsベースのアプリとCitrix Virtual Desktopsで公開されている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、Receiver、または Secure Hub のいずれかで接続して、アプリケーションと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、Receiverを使用してEndpoint Management に直接接続できます。次の図は、Endpoint Management とStoreFront とともに展開された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

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

- 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、「Endpoint Management 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。

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

WebインターフェイスによるCitrix Virtual Apps and Desktops 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およびSecure Ticket Authority（STA）と連携して、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行います。

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、ユーザーはCitrix Receiverを使用して接続します。

NetScaler GatewayとCitrix Virtual Apps and Desktops との統合

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。

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

- 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安全な接続の確立

次の例は、DMZに展開されたNetScaler GatewayがWeb Interfaceとどのように互換性があり、安全な企業ネットワークで利用可能な公開リソースへの安全な単一アクセスポイントを提供するかを示しています。

この例では、次の条件が存在します：

- インターネット上のユーザーデバイスは、Citrix Receiver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。

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

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。
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 Receiver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。

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

Web インターフェイスによるデプロイ

NetScaler Gatewayを導入してCitrix Virtual Apps and Desktopsへの安全なリモートアクセスを提供すると、NetScaler GatewayはWeb InterfaceおよびSecure Ticket Authority（STA）と連携して、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ブラウザーとCitrix Receiver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。
- 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。

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

Web Interfaceを展開する場所は、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 Receiverのいずれかを使用してWeb Interfaceに接続できます。Citrix Receiver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のネットワークアクセスを拡大したりできます。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。

セキュアネットワークへのウェブインターフェースの展開

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が安全な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

DMZ内のNetScaler Gatewayと並行してWebインターフェイスを展開する

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 Receiverを使用してWeb Interfaceに直接接続します。ユーザー接続

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

は、まず認証のためにWeb Interface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 Receiver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内のNetScaler Gatewayの背後にWebインターフェイスを展開する

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 Receiverでログオンすると、最初のユーザー接続はNetScaler Gatewayに送られ、その後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Web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。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。どちらもDMZ内にあるためです。

Web Interfaceの機能

NetScaler Gateway と連携するようにWeb Interfaceを構成する前に、Citrix Virtual Apps Webサイトと Citrix Virtual Apps Servicesサイトの違いを理解する必要があります。

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

- **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ための機能を提供します。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。Citrix Virtual AppsをWeb Interface上のCitrix Virtual Apps Servicesサイトと組み合わせて使用することで、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した場合、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 eDocs ライブラリの「テクノロジー」ノードにある「Web Interface」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「テクノロジー」ノードに ある「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。これには、Webブラウザ、NetScaler Gatewayプラグイン、またはCitrix Receiverを使用できます。詳細については、「 Web インターフェイス機能 」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。

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。

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

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。

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。 > > > > を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 にMMC 3.0がインストールされていることを確認してください。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

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

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。

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

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ペインで、［Citrix Virtual Apps Webサイト］または［Citrix Virtual Apps Services サイト］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。
   - 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。
   - をクリックして、新しいアドレス変換を追加します。
   - リストから既存の住所変換を選択し、 をクリックします。
8. 領域で、次のいずれかのオプションを選択します：

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

- 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。

9. 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。
10. ［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。
11. 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Citrix サーバーで開いたままにするには、［セッション画面の保持を有効にする ］を選択します。
12. セッション信頼性を有効にしていて、2つのSecure Ticket Authority（STA）サーバーからの同時チケット発行を使用する場合は、「利用可能な場合は2つのSTAからチケットをリクエストする」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するため、セッション中に1つのSTAが使用できなくなった場合で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。
13. 「Secure Ticket Authority 設定の指定」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、Web Interfaceが使用できるSTAのURLを指定します。

- 一覧からエントリを選択し、 をクリックします。

  Use the Move Up and Move Down buttons to place the STAs in order of priority. STAs are included with the Citrix XML Service; for example, `http\[s\]://servername.domain.com/scripts/ctxsta.dll`.

  You can specify more than one STA for fault tolerance; however, Citrix recommends that you do not use an external load balancer for this purpose.

14/. STA間の負荷分散を有効にするかどうかを選択するには、「負荷分散に使用」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。 15. 「障害が発生したサーバーをバイパスする」を選択して、到達不能なSTAをバイパスする期間を指定します。

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

```
The Web Interface provides fault tolerance among the servers on the STA
URLs list so that if a communication error occurs, the failed server is
bypassed for the specified time period.
```

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 Receiver、またはCitrix Desktop Receiver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. > > > > 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。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インクリメントが追加されます。

5. 「ユーザー認証が行われる場所の指定」で、次のいずれかを選択します：

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

- 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

：NetScaler Gateway で SmartAccess が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の「認証サービスURL」に、NetScaler Gateway 認証サービスURL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「スマートカード」を選択した場合は、次のいずれかを選択します。

- ユーザーに 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。

設定を示す概要画面が表示されます。「次へ」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。

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

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. ダイアログボックスで、 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。

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。

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

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 Virtual Apps 6.5では、Citrix AppCenterでNetScaler Gateway経由で接続をルーティングするように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。

Citrix Virtual Apps 6.5サーバーのプロパティを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構成するには

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。

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

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。

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。

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

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

   .Receiver for iOSやReceiver for Androidなど、VPN対応のCitrix Receiverをサポートするには、手順3を実行してください。モバイルReceiverをサポートするには、少なくともAccess Gateway 10、ビルド69.6またはAccess Gateway 10、ビルド71.6014.e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。

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。

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

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。
- 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。

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

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。
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。

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

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によるスマートカードアクセスの構成Citrix Receiver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。

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。

© 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。

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 Receiver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と並行している必要があります。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。

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

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。

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

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

- 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、まずセッションプロファイルを作成して、Windows向けNetScaler Gateway 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。

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、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。

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

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、 をクリックし、 **をクリックし**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. 「構成」タブで、「**NetScaler Gateway」>「グローバル設定**」を展開します。
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 つまたは複数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」タブで、「**NetScaler Gateway」>「仮想サーバー**」を展開します。
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. 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、Receiver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

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

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 Receiver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け取ることができます。

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。

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

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設定するには、 **ICA Proxy**設定を有効にするセッションポリシーを作成し 、クライアントのセキュリティ文字列を設定します。

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。

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。

参照先ドキュメント：

- SmartAccess のポリシー式とフィルターを使用してユーザーのアクセスを制限する方法について詳しくは、「デリバリーグループの管理」を参照してください。
- Citrix Virtual Apps のポリシーとフィルターの構成について詳しくは、「ポリシーの作成」を参照してください。

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

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。

Citrix Receiver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 Virtual Apps 6.5では、ユーザ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レターを使用します。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。

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

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 AppCenterを使用して、Citrix Virtual Apps 6.5で制限ポリシーと非制限ポリシーを構成します。

Citrix Virtual Apps 6.5で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. ［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。

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

Citrix Virtual Apps 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。

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。

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

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 Receiver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。
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

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

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アドレスを使用します。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。
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。

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

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 Policy］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。

   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。

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

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。

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。

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

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。

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。

© 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. 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。
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。

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

- 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。
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。

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

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**
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。**

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

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。
   - 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。

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

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。
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

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

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。

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。

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

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。

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

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

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。****

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。

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

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. 「 **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、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。
   - 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。

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

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 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。
`HTTP.REQ.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。
HTTP.REQ.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。

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

HTTP.REQ.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。
HTTP.REQ.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。

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。

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

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。

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。

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

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。
   - **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。

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

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。

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。

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

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。**

   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 (http.req.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チェックできます。
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** 。

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

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。
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。

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

1. ［Citrix NetScaler］>［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。
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** 。

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

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Citrix 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。

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。

© 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、以下のバージョンのWeb Interfaceで動作します：

- 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。

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。

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

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。
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。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

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

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。
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 Receiver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Citrix ADCのWeb Interface機能を有効にすると、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

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

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 グループに属していてシングルサインオンを行うことができます。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行うように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。
- 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、［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.「クライアントエクスペリエンス」タブの「ホーム」の横にある「グローバル上書き」をクリックし、「ホームページの表示」をオフにします。 4.「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「グローバルを上書き」をクリックし、「Web アプリケーションへのシングル

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

サインオン」をクリックします。 5. ［Published Applications］ タブをクリックします。 6. の横にある をクリックし、 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. 「シングル・サインオン・ドメイン」で、「グローバルを上書き」をクリックし、ドメイン名を入力します。

注

.domain.com 形式ではなく、ドメイン形式を使用する必要があります。

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。

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。

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

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。

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会議のレポートを投稿するファイル共有にファイルタイプの関連付けを許可し、ダウンロードやアップロードは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 Receiver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ている仮想サーバーを介して接続し、そのポリシーをCitrix Virtual Apps用に構成します。
- 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 と連携するようにCitrix Virtual Apps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 7でのファイル拡張子の定義。

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

Web インターフェイスサイトの作成

ファイルタイプの関連付けを使用するように Web Interface を設定するには、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
- 認証
- 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 サポートサイト（`<http://support.citrix.com/article/ctx116253>`）からダウンロードできます。

```
pre codeblock

<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"/>
```

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

```
</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。

```
pre codeblock

<location path="site/launch.rad">

        <system.web>

            <httpHandlers>

                <add verb="*" path="*.rad"
type="System.Web.UI.PageHandlerFactory"/>

            </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処理するようにWeb Interfaceサイトを構成してください。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が設定された新しいセッションポリシーとプロファイルの作成。
- 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。

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

ファイルタイプアソシエーションのトラフィックポリシーを設定するときは、ファイル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。
   b. の横にある をクリックし、 または を選択します。
   c. 「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、ユーザー・アカウントが属するドメインの名前を入力して、「**作成**」をクリックします。
7. ダイアログボックスの の横にある 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。

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. 「ファイル・タイプの関連付け」で、「オン」を選択し、「作成」をクリックして、「閉じる」をクリックします。

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。

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

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「**OK**」をクリックします。ここで、「/*.FileExtensionType」は.docや.xlsなどのファイルタイプです。
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. 追加するファイル拡張子ごとに手順4、5、6を繰り返し、「 **作成** 」をクリックし、「 閉じる」をクリックします。

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

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 Receiver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.

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。
- **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。

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

- 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
   - **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。

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

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。**

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。

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

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 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。
- **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

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

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。

- **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、StorageZones Controller環境に関する基本情報を入力するように求められ、次のこと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 ADC 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。

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

- 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。
- Exchange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エンタープライズライセンスが必要です。

Citrix Endpoint Management用のNetScaler ADCウィザード

このセクションでは、NetScaler ADC 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. **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、［ **始める**］をクリックします。
3. 構成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 回しか使用できないため、以降の構成は手動で実行する必要があることに注意してください。この手順では、次の設定を選択することを前提としています。 **NetScaler 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の場合） **負荷分散 Citrix Endpoint Managementサーバー**

4. **［NetScaler Gateway の設定］** ページで、**外部向きのNetScaler Gateway 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** ］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選択します。証明書がローカルマシンにある場合：

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

証明書がアプライアンスにある場合：

6. ページの フィールドで、 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。

   証明書ポリシーを作成する必要がある場合は、 をクリックし、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。 で、要件に応じて **userPrincipalName****または **samAccountName**を指定します。

   - a. **を**選択し、 リストで目的の CA 証明書に移動します。
   - b. 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場合、セカンダリ認証タイプとしてLDPA (またはRADIUS) を設定することもできます。

     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 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、右上隅の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、リストから 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. NetScaler ADCウィザードに戻り、エクスポート（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。

   構成したCitrix Endpoint ManagementのIPアドレスが表示されます。

7. **Citrix Endpoint Managementの［アプリケーション管理］設定を構成します。**

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

- **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。

8. 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。
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、 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のIPアドレスを追加します**。
12. NetScaler ADCダッシュボードで、NetScaler Gateway およびCitrix Endpoint Managementの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。

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

Citrix Endpoint Management または Citrix Endpoint Management 用の負荷分散サーバーの構成

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。

Citrix 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。Citrix Endpoint Management をSSLブリッジモードのCitrix ADC VIPと負荷分散すると、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。
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、セキュリティ基準を満たす必要がある場合は、SSLオフロードを使用してください。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

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

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オフロードモードでのセットアップとトラブルシューティングはさらに複雑です。

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。

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リングを使用したMicrosoft Exchange の負荷分散サーバの構成

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。

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

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 Citrix ADC Connector (XNC) ActiveSync フィルタリングの設定

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。承認は、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って制御されます。

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。
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を使用したモバイルデバイスからのアクセスの許可

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Secure Hub（以前の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

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

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でのSecure Browseの設定

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。

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。

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

- 「**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。
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
```

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

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。
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。

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

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。
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。

© 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。

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

- 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。

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：

© 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の構成

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。

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 ADC 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）

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

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」、「**バインド**」、「**完了**」の順にクリックします。

4. > > に移動し、 **AC_OS**で始まる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、ページの下部に移動します。

6. から 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に個別のNetScaler Gateway VIPを使用するには、［ **式**］で、 **NS_TRUEを次のように置き換えます** 。

   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。 ドロップダウンメニューから、RADIUS サーバ名（この例では **Radius_Server** ）を選択します。

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

14. 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、 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。

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。

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

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の設定

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。
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。

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

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 、 式を **ns_true** に**設定**して をクリックします。

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

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。
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、 で を選択し、 で を選択します。これにより、証明書認証が LDAP 認証タイプと同じプライオリティ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. セクションの 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オンにし、［ **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

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

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.

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NetScaler Gateway プラグインを使用してログオンすると、CloudBridgeからユーザーデバイスにインストールされるCloudBridge プラグインを使用して接続を最適化できます。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NetScaler Gatewayを介して圧縮および高速化されます。CloudBridge が接続に対して有効になっている場合、NetScaler GatewayのTCP圧縮ポリシーは無効になります。

CloudBridge プラグインが展開され、NetScaler Gatewayプラグインと連携して動作します。

NetScaler Gatewayは、リピータープラグインのバージョン5.5と6.1、およびCloudBridge プラグインのバージョン6.2と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NetScaler 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、以下のNetScaler 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
- HTTP 承認

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 での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。NetScaler 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
```

NetScaler Gatewayに設定された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、NetScaler Gateway 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NetScaler Gateway機能に影響を与えることなく、HTTP以外の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またはポリシーに指定したプライオリティ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、［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. 「**ブランチリピータ**」で、「**オン**」を選択し、「**作成**」をクリックします。
7. ダイアログボックスの 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、 をクリックし、 をクリックして 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てください。CloudBridge アクセラレーションを行うには、NetScaler Gatewayで構成されたトラフィックタイプがCloudBridge で設定されたサービスクラスポリシーと一致する必要があります。

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ます。シングルサインオンを使用する場合は、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 トラフィックを高速化しないでください。

© 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。 解決策

  ： ユーザーがGatewayを使用してStoreFront にアクセスすると、RfWebUIテーマには、Gatewayを使用せずに製品にアクセスした場合と同様のユーザーインターフェイスが表示されます。
- ユーザーは、Gatewayを使用してReceiver、StoreFront、Citrix Endpoint Management アプリケーションにアクセスしますが、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ています。

  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
- ユーザー設定の 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 機能では、クライアントレス VPN（CVPN）経由で Web ページにアクセスできます。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、セッションポリシーの *clientlessAccessVPNMode* パラメータが になっている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、リモートデスクトッププロトコル (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: ユーザーが 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。 タブ内のアプリケーションの**横**にある リンクをクリックして、 タブからも同じものを削除できます。

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

© 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.

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。

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

- 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。

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。

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

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。

- 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。

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

- 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。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。

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

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。

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。

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

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>`
   - 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

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

- 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。

```
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>
```

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

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>`
```

`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
```

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

```
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
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。

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

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。
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。

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

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。

    ☐
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。

    ☐

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

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。

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
```

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

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認証システムで認証されると、NetScaler Gateway上のRDPListener を介してアクセスが許可されます。NetScaler Gateway 用RDPListener が必要とする情報は、STA サーバーに安全に保存されます。

ここでは、この機能用に作成されたフローと新しいノブについて説明します。

前提条件

- ユーザーはNetScaler Gatewayオーセンティケーターで認証されます。
- 最初の /rdpproxy URL と RDP クライアントは、別のRDPListener NetScaler Gateway に接続されています。
- RDPListenerゲートウェイ情報は、STA サーバーを使用してオーセンティケーターゲートウェイによって安全に渡されます。

構成

- 新しい *rdpServer*プロファイルを追加します 。サーバープロファイルはRDPListener ゲートウェイで設定されます。

  ```
  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].
  ```

  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/RDPユーザー情報を取得します。

  rdpServerプロファイルは、次のコマンドを使用して VPN 仮想サーバー上で構成されます：

  ```
  add vpn vserver v1 SSL [publicIP] [portforterminatingvpnconnections]
  -rdpServerProfile [rdpServer Profile]
  ```

  警告

  VPN 仮想サーバでrdpServerProfileをいったん設定すると、それを変更することはできません。また、同じserverProfileを別の VPN 仮想サーバーで再使用することはできません。

rdp profile コマンドは **rdpClient** プロファイルに名前が変更され、新しいパラメーターが追加されました 。multiMonitorSupport コマンドが追加されました。また、RDP クライアントプロファイ

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

ルの一部としてサポートされていないカスタムパラメータを設定するオプションが追加されました。接続は常にセキュリティで保護されているため、clientSSL パラメータは削除されました。クライアントプロファイルは、Authenticator Gatewayで設定されます。

```
add rdpClient profile &lt;name> -rdpHost &lt;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
&lt;keyboardHook>] [-audioCaptureMode ( ENABLE | DISABLE )] [-
videoPlaybackMode ( ENABLE | DISABLE )]



        [-rdpCookieValidity &lt;positive_integer>][-multiMonitorSupport
( ENABLE | DISABLE )] [-rdpCustomParams &lt;string>]
```

—rdpHost設定は、単一のゲートウェイ展開で使用されます。

- RDP プロファイルを VPN 仮想サーバーに関連付けます。

これは、sessionAction+sessionPolicy を設定するか、グローバル vpn パラメーターを設定することで実行できます。

例

```
add vpn sessionaction &lt;actname> -rdpClientprofile &lt;rdpprofilename>



add vpn sessionpolicy &lt;polname> NS_TRUE &lt;actname>



bind vpn vserver &lt;vservername> -policy &lt;polname> -priority
&lt;prioritynumber>
```

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

```
OR



set vpn parameter –rdpClientprofile &lt;name>
```

接続カウンター

使用中のアクティブな接続数の記録を保持する新しい接続カウンター ns_rdp_tot_curr_active_conn が追加されました。これは、NetScalerシェルのnsconmsgコマンドの一部として表示できます。後で、このカウンタを表示する新しい CLI コマンドを提供します。

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つ目の接続は、NetScaler Gateway上のRDPリスナー（rdpIPと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、それに続く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. ユーザーはオーセンティケータゲートウェイ VIP に接続し、認証情報を入力します。
2. Gateway へのログインに成功すると、ユーザーはアクセスできるリモートデスクトップリソースを列挙するホームページ/外部ポータルにリダイレクトされます。
3. ユーザーが RDP リソースを選択すると、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` のリクエストが Authenticator Gateway VIP によって受信されます。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. /rdpproxy/ リクエストは認証ゲートウェイによって処理されます。ユーザーは既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。
5. RDPTarget とRDPUser の情報は STA サーバーに保存され、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。オーセンティケータゲートウェイは、ゲートウェイ Vserver に設定されている STA サーバの 1 つを使用します。
6. XML BLOB は次の形式になります

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

\<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「フルアドレス」として入力され、STA チケット (先頭に STA 認証IDが付属) が.rdp ファイルの「loadbalanceinfo」として入力されます。
8. .rdp ファイルがクライアント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ゲートウェイに接続します。STA チケットは最初の x.224 パケットで送信されます。
10. RDPListener ゲートウェイは STA チケットを検証し、RDPTarget とRDPUser 情報を取得します。使用する STA サーバーは、ロードバランシング情報にある「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すでに存在する場合、そのセッションは再利用されます。
12. 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。

シングル・ゲートウェイの互換性

RDP ファイルが /rdpproxy/rdptarget/rdptargetproxy URL を使用して生成されている場合は STA チケットが生成されます。それ以外の場合は、セッションを直接参照する「loadbalanceinfo」の現在の方法が使用されます。

単一ゲートウェイ環境の場合、/rdpproxy URL はオーセンティケータゲートウェイ自体に送られます。STA サーバーは不要です。オーセンティケータゲートウェイは、RDPTarget と AAA セッションCookie を安全にエンコードし、これを.rdp ファイルの「loadbalanceinfo」として送信します。RDP クライアントが x.224 パケットでこのトークンを送信すると、認証ゲートウェイは RDPTarget 情報をデコードし、セッションを検索して RDPTarget に接続します。

アップグレードノート

以前の設定はこの新しいリリースでは動作しません。これは、以前 vpn vserver 上で設定されていた rdPip およびrdpPortパラメータがrdpServerProfile の一部になるように更新され、「rdp Profile」の名前が「rdp ClientProfile」に変更され、古いパラメータ ClientSSL が削除されたためです。

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

RDP サーバープロファイルの作成

1. ［NetScaler Gateway］>［ポリシー］>［RDP］に移動します。

2. タブに移動し、 をクリックします。

3. 次の情報を入力して RDP サーバープロファイルを作成します。

RDP クライアントプロファイルの設定

1. ［NetScaler Gateway］>［ポリシー］>［RDP］に移動します

2. タブに移動し、 をクリックします。

3. RDP サーバープロファイルを設定するには、次の情報を入力します。

仮想サーバーのセットアップ

1. 「NetScaler Gateway」>「仮想サーバー」に移動します。

2. をクリックして新しい RDP サーバーを作成します。

3. この「基本設定」ページのデータを入力し、「 **OK**」をクリックします。

4. **鉛筆**をクリックしてページを編集します 。

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が存在する場合の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

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

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。
- 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、リダイレクターとして機能する宛先サーバーとしてRDPサーバーの1つを指すように構成できます。また、ファーム内の RDP サーバーの 1 つを送信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 セッションを受け付けません。

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

RDP ロードバランシング機能がある場合：

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、Citrix ADCでRDP負荷分散機能を利用できるようにして、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行うことができます。この場合、RDP URL リンクは、RDP ロードバランサーを宛先サーバー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 )



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。アプライアンスは、取得したリストに基づいて、特定のユーザーがアクセスするサーバーの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>
```

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

```
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
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。**

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

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 をもう一度クリックすると、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ための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ファイル名をランダム化することを選択できます。<outputof time ()\ >time () 関数の出力を\ <rdpFileName\ >\ _ \\.rdp 形式で追加することで、ファイル名がランダム化されるようになりました。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
```

Citrix ADC GUIを使用してRDPプロキシによる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。

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

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、 フィールドの横にあるドロップダウンで を選択します。

© 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Citrix 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ポータルテーマ —Web ブラウザで Horizon View にアクセスするには、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.

HDX Enlightened Data Transport サポート

NetScaler Gatewayの拡張Enlightened Data Transport（EDT）サポートにより、Citrix Receiverを実行しているユーザーが仮想デスクトップのセッション中でも高品位なユーザーエクスペリエンスを実現できます。

また、ReceiverとVDA間のEDTターミネーション用の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、「DTLSv1.0 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の両方の条件で優れたユーザーエクスペリエンスを提供します。一方から他方へのローミング時に管理やユーザー構成は必要ありません。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。詳しくは、「HDX」を参照してください。

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。
- リリース12.1ビルド51.x以降、SmartControl ポリシーとICAポリシーがDTLS/EDT接続でサポートされるようになりました。
- 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。

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

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。

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 Receiver 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

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

シナリオ	EDTサポート
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
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仮想サーバーレベルで有効にする必要があります。また、Citrix Virtual Apps and Desktopsコンポーネントは、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ように正しくアップグレードおよび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と連携する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。

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

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。

4. をクリック**する**と、追加の設定オプションが表示されます。

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. 「 **AppFlow コレクターの作成** 」ページで、次のフィールドに入力し、「作成」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-コレクター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

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

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。

4. 「 **AppFlow アクションの作成** 」ページで、次のフィールドに入力し、「**作成**」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

   コレクター — AppFlow アクションに関連付けるコレクター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. 「 **AppFlow ポリシーの作成** 」ページで、次のフィールドに入力し、「**作成**」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場合にこのポリシーに関連付けられるアプリフローアクションの名前。

   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。

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

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。

12. 最後に をクリックします。

CLIを使用してNetScaler Gateway for HDX Insight サポートを構成するには、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>
```

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12.1ビルド63.20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。

しきい値ファクタを超えると、レイテンシー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.

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の統合により、世界クラスのモバイルデバイス管理（MDM）機能が提供され、NetScaler Gatewayクライアント側テクノロジーにより、これらのIntune 対応アプリケーションはNetScaler Gatewayを介して企業のデータやアプリケーションに安全にアクセスできるようになります。

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から直接取得できるADALトークンを使用してNetScaler Gatewayにアクセスします。

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、モバイルデバイスとアプリケーションが、社内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のデータにアクセスできるようにしたいと考えています。

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

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。

NetScaler Gatewayと Intune MDM の統合について

以下は、一般的なNetScaler GatewayとIntune 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（CA）ポリシーを満たしていない場合、NetScaler Gateway VPNクライアントは、デバイスのコンプライアンスステータスを登録または修正するためのIntune がホストするページへのリンクを含むエラーメッセージをユーザーに表示します。

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 にプッシュする際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。

単一要素認証展開用の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の構成

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。
- 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nFactorを搭載したNetScaler Gateway仮想サーバーを追加するには

1. NetScaler Gateway ツリーノードの下にある［仮想サーバー］に移動します。

2. 「**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。

3. を選択します。

4. 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.

5. **［続行］** をクリックします。
6. **［続行］** をクリックします。
7. **［続行］** をクリックします。
8. **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。**
9. の横にあるプラスアイコン ****をクリックします。
10. **［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。
11. ［ **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。
12. 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。
13. 「 **プラグインタイプ** 」の横にあるチェックボックスをクリックし、リストから「Windows/macOS」を選択します。
14. 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。
15. 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。
16. 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。
17. **「 作成」をクリックします。**
18. 「 **NetScaler Gatewayセッションポリシーの作成** 」 ページの「式 」領域に「 **NS_TRUE** 」と入力します。
19. **［Create］** をクリックします。
20. **［Bind］** をクリックします。
21. で を選択します。

    ▢
22. 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。

    ▢
23. 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。

    ▢
24. ［ **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** 。

    ▢
25. をクリックします。

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

26. 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。
27. 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。
28. **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。

    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。

    問題を解決して`https://login.microsoftonline.com/`、`https://graph.windows.net/`、*.manage.microsoft.comにアクセスできるように、アプライアンス上に適切なDNSネームサーバーが設定されていることを確認してください。
29. **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")))
    ```
30. 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。
31. 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。
32. 認証スキーマとして **noschema** を選択し、「 **作成**」をクリックします。
33. 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。

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

34. ** 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設定」を参照してください。

    ☐

35. ［Bind］ をクリックします。

    ☐

    をクリックします](/ja-jp/netscaler-gateway/media-2/intune_21.jpg)

36. ［完了］ をクリックします。

    ☐

37. ［Bind］ をクリックします。

    ☐

    をクリックします](/ja-jp/netscaler-gateway/media-2/intune_23.jpg)

38. ［続行］ をクリックします。

    ☐

39. ［完了］ をクリックします。

    ☐

40. ［Create］ をクリックします。

    ☐

41. ［OK］ をクリックします。

    ☐

42. ［完了］ をクリックします。

    ☐

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。

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

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。

   説明した導入では、NAC OAuth アクションポリシーとともに単一要素認証（LDAP）が使用されているため、 **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-2/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
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

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

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
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。

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

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 インテグレーションを行うには、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
  - 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。

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

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。

   a. 下にスクロールして、 を選択します。

   b. を選択し、 を選択して、 をクリックします

   c. をクリックし、 を選択します。

   d. テナントに権限が付与されていることを確認します。

   注:

   `https://login.microsoftonline.com` または `https://graph.windows.net` 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 を呼び出すことができるように API 権限が割り当てられている必要があります。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。
   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`

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

- Profile
- Directory.AccessAsUser.All
- User.Read
- User.Read.All
- User.ReadBasic.All

INTUNE NAC チェックの追加許可:

`https://login.microsoftonline.com` または `https://graph.windows.net` 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 を呼び出すことができるように API アクセス許可が割り当てられている必要があります。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。
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>`

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

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

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。

> **（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する必要があります。NetScaler Gateway アプライアンスfor Intune でOAuthアクションを構成するときは、新しく登録し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てください。

これで、Azure Portalのアプリケーション構成は完了です。

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。

© 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

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 Web キー (JWK) を含むエンドポイントの URL。
- 対象者：アプリがADALトークンを送信するNetScaler 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。
- tenantiID: Azure ADAL 登録のテナント ID。
- ClientSecret: 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。
- ClientSecret: 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。

1. OAuthActionの作成：

   add authentication OAuthAction \<oauth_action_name> **-OAuthType INTUNE –clientid** \<client_id> - **clientsecret** \<client_secret> **-audience** \<audience\> **-tenantid** \<tenantID\> **-issuer** \<issuer_name> - **userNameField upn-certEndpoint** \<certEndpoint_name>

   例：

   add authentication OAuthAction tmp_action -OAuthType INTUNE -clientid id 1204 -clientsecret a -audience " http://hello" -tenantid xxxx -issuer " https://hello" -userNameField upn -certEndpoint `<https://login.microsoftonline.com/common/discovery/v2.0/keys>`

2. 新しく作成した OAuth 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>

   例：

   add authentication Policy oauth_intune_pol -rule true -action tmp_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 EN**D

   例：

   bind authentication vserver auth_vs_for_gw1_intune -policy oauth_pol -priority 2 -gotoPriorityExpression END

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

4. LoginSchemaの作成：

   add authentication loginSchema \<loginSchemaName\> **-authenticationSchema** <authenticationSchema”location”>

   add authentication loginSchemaPolicy \<loginSchemaPolicyName\> **-rule true -action** \<loginSchemaName\>

   例：

   add authentication loginSchema oauth_loginschema -authenticationSchema "/nsconfig/loginschema/LoginSchema/OnlyOAuthToken.xml"

   add authentication loginSchemaPolicy oauth_loginschema_pol -rule true -action oauth_loginschema

5. AuthVS をLoginSchemaでバインド：

   bind authentication vserver \<auth_vs> **-policy** \<oauth_pol> **-priority 2 -gotoPriorityExpression END**

   例：

   bind authentication vserver auth_vs_for_gw1_intune -policy oauth_loginschema_pol -priority 2 -gotoPriorityExpression END

6. 認証プロファイルを追加して VPN 仮想サーバーに割り当てます：

   add authnprofile \<nfactor_profile_name>**-authnvsName** \<authvserver\>

   set vpn vserver \<vserverName\>**-authnprofile** <nfactor_profile_name>

   例：

   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.

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.

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.

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。

アウトバウンドICAプロキシの構成

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、次の手順に従います：

1. キャッシュリダイレクト Vserver の追加：

   add cr vserver \<name\> \<serviceType\> \<IPAddress\> \<port\> -**cacheType** \<cacheType\>

   サービスはHDXである必要があります

   キャッシュタイプはフォワードである必要があります

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

例:

add cr vserver CR_LAN_Proxy HDX 10.217.208.197 8080 -cacheType FORWARD

2. ICA SmartControl プロファイルの追加：

   add ica accessprofile \<name\> -**ConnectClientLPTPorts** (DEFAULT | DISABLED) **ClientAudioRedirection** (DEFAULT | DISABLED) -**LocalRemoteDataSharing** (DEFAULT | DISABLED) -**ClientClipboardRedirection** (DEFAULT | DISABLED) -**ClientCOMPortRedirection** (DEFAULT |DISABLED) -**ClientDriveRedirection** (DEFAULT | DISABLED) -**ClientPrinterRedirection** (DEFAULT |DISABLED) -**Multistream** (DEFAULT | DISABLED) -**ClientUSBDriveRedirection** (DEFAULT | DISABLED)

   例:

   ```
   add ica accessprofile disableCDM -ConnectClientLPTPorts DEFAULT
   -ClientAudioRedirection DEFAULT –LocalRemoteDataSharing DEFAULT
   -ClientClipboardRedirection DEFAULT -ClientCOMPortRedirection DEFAULT –
   ClientPrinterRedirection DEFAULT -Multistream DEFAULT
   -ClientUSBDriveRedirection DEFAULT
   ```

3. ICA アクションの追加：

   add ica action \<name\> **-accessProfileName** \<string\>

   例:

   ```
   add ica action disableCDM\_action -accessProfileName disableCDM
   ```

4. ICA ポリシーの追加：

   add ica policy \<name\> **-rule** \<expression\> **-action** \<string\> **-comment** \<string\> **-logAction** \<string\>

5. ICAポリシーを仮想サーバーまたはグローバルにバインドします：

   a. 仮想サーバーにバインド

   ```
   **bind cr vserver** \&lt;name\> **-policyName** \&lt;string\> **-
   priority** \&lt;positive\_integer\>
   ```

   例:

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

```
bind cr vserver CR\_LAN\_Proxy –policyname disableCDM\_pol –priority 10
```

b. グローバルにバインド

```
**bind ica global -policyName** \&lt;string\> -**priority**
\&lt;positive\_integer\>
```

例:

```
bind ica global –policyName disableCDM\_pol –priority 10
```

注

セキュアICAポートの設定：この値は、LANプロキシがアウトバウンド接続を行うNetScaler Gatewayのポート番号です。デフォルトでは443に設定されています。次のコマンドを使用してポートを変更します。

set ns param -secureicaPorts\<port\>

例：

set ns param -secureicaPorts 8443

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

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 Receiver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.

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。

注

：サードパーティサーバーが不要になったため、NetScaler 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。

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 をサポートすることの利点

- 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

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

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、任意の数の要素を使用して実行できます。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。

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。

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

- 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。**
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 lpol_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. 「 **バインド**」をクリックします。
7. 上にスクロールして、 で 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。

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

9. の下にある アイコンをクリックし、** を作成し、 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。
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。

© 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。
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

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

- 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

```
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
```

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

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"
```

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

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

- 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。

```
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、新しいパラメーター `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 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 16 桁の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。

© 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「client hello」パケットにサーバー名表示（SNI）拡張子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た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.

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ーは非常に強力な表現言語で構成されています。エクスプレッション言語を使用して、ポリシー内のルールを定義したり、アクションのさまざまな部分を定義したり、サポートされているその他のエンティティを定義したりできます。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。Citrix ADCは拡張性が高く、多種多様なクライアントに対応しているため、高度なポリシーをはるかに超える表現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。
- 多くの追加プロトコルをサポートします。
- システムの多くの追加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。
- 高速な並列マルチストリングマッチング (パッチセットなど) 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 Gateway ログオン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確認されます。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入力する前に行われます。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 。

アドバンスド EPA を使用した事後認証 EPA

認証後の EPA スキャンは、ユーザーの資格情報が確認された後に行われます。従来のポリシーインフラストラクチャでは、認証後の EPA は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設定されていました。高度なポリシーインフラストラクチャでは、EPAスキャンをNファクター認証のEPAファクターとして構成する必要があります。 認証要素の1つとして認証後のEPAスキャンを使用するNファクター認証用に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

クラシック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設定されていました。高度なポリシーインフラストラクチャでは、Nファクター認証のEPAファクターの一部として構成できます。

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。
- すべての PI ポリシーには優先度が必須です。
- 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。
- 同じ優先度の Advance Policy を 1 つのバインドポイントにバインドできます。
- 設定された認証ポリシーがどれもヒットしない場合は、VPN パラメータで設定されたグローバル認証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 (「バー」) [「.」の使用に注意してください。]
REQ.IP	CLIENT.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
RES.IP	SERVER.IP
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.

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：次のセクションでは、テンプレートを使用してアプリを構成および公開するためにNetScaler Gateway で実行する手順について説明します。アプリケーションサーバーで実行する構成手順については、次のセクションで説明します。

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

以下の設定は、テンプレートを使用してアプリを設定および公開する例として AWS コンソールアプリを取り上げています。

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

1. **Unified Gateway > 認証**をクリックします。

   Unified Gateway 設定画面が表示されます。

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

2. 「**アプリケーション**」セクションで、編集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 エクスプレッション — ステップ 3 で示したように、 ロール ARN、IdP ARN

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、 **AWS** コンソールテンプレートをクリックします 。 ウィンドウが表示されます。 リンクをクリックします。

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

以下は、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アプリサーバー固有の構成に関するガイダンスが記載されたpdfのリンクです。

- 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
- Criconus
- 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
- Sumologic
- 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.

EPA コンポーネントとしての nFactor のデバイス証明書

デバイス証明書は、EPA コンポーネントとして nFactor で設定できます。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。

次に、nFactor でデバイス証明書を EPA コンポーネントとして構成する利点を示します。

- デバイス証明書の検証に失敗しても、ログオンは失敗しません。構成に基づいて、ログオンを続行でき、ユーザーはアクセスが制限されたグループの下に配置されます。
- デバイス証明書のチェックはポリシー駆動型であるため、デバイス証明書認証に基づいて、社内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、企業の管理対象ラップトップ上でのみ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。

デバイス証明書の検証は、定期的な EPA スキャンの一部にはできません。

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、EPA プラグインと同じバージョンの VPN プラグインをデバイスにインストールする必要があります。
- 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。

nFactor のデバイス証明書を EPA コンポーネントとして設定する

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
```

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

Citrix ADC GUIを使用してnFactorのデバイス証明書をVPN仮想サーバーのEPAコンポーネントとして構成するには：

1. NetScaler GUIで、［構成］**>［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 、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. ページで、 アイコンをクリックします。

4. **［詳細］** クリックします。
5. 「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。

   「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、クラシック 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］>［詳細ポリシー］>［アクション］［EPA**］に移動します。
7. ページで、 をクリックします。 をクリックして、既存の EPA アクションを編集できます。
8. 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に値を入力し、 リンクをクリックします。
9. **エクスプレッションエディタメニューから** を選択します。

10. 表示される次のメニューから を選択し、 をクリックして設定を完了します。

Citrix ADC GUI を使用して nFactor のデバイス証明書を Citrix ADC AAA 仮想サーバーの EPA コンポーネントとして構成するには：

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**］に移動します。
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. ページで、 アイコンをクリックします。

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

4. **［詳細］** 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**］ をクリックして設定を完了します。

7. **前のセクションに示したステップ 6 ～ 10** を繰り返して、設定を完了します。

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

__index__

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。

NetScaler Gatewayは、Endpoint Management およびStoreFront と連携するように構成できます。NetScaler GatewayをEndpoint Management またはStoreFront と連携するように構成する場合、Citrix 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のモバイルアプリ、およびShareFileからドキュメントを入手できます。ユーザーは、Secure Hub、Citrix Receiver、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、StoreFront へのReceiver接続とSecure Hub 接続を管理します。このセッションポリシーは、Receiver for Windows、Receiver for Mac、Receiver for

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

Android、Receiver for iOS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。Secure Browse を設定する必要があるのは iOS デバイスのみです。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は、Receiver for Web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Receiver for Web
- NetScaler Gateway プラグイン
- Receiver for Android
- Receiver for iOS
- Receiver for Mac
- Receiver for Windows
- 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 Receiverでは、StoreFront FQDNは、内部ネットワークに接続された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、Receiver for Windows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リストがReceiver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。

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

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：

- StoreFront へのSecure Hub およびReceiver接続を管理するための1つのセッションポリシー。このセッションポリシーは、Receiver for Windows、Receiver for Mac、Receiver for Android、Receiver for iOSをサポートしています。ユーザーがReceiver for AndroidまたはReceiver for iOSに接続する場合、NetScaler Gateway経由の接続を許可するには、クライアントレスアクセスとSecure Browse を有効にする必要があります。
- Receiver for Webへのブラウザー接続を管理するための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、Receiver for Android、Receiver for iOS、および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1つのセッションポリシーで管理します。PNAサービスのセッションポリシーを構成した場合、Receiver for Windows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Receiver接続を管理するための1つのセッションポリシー。このセッションポリシーは、Receiver for Windows、Receiver for Mac、Receiver for Android、Receiver for iOSをサポートしています。ユーザーがReceiver for AndroidまたはReceiver for iOSに接続する場合は、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。Receiver for iOSからの接続では、NetScaler Gateway経由の接続を許可するためにSecure Browse を有効にする必要があります。
- Receiver for Webへのブラウザー接続を管理するための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。

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

- 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、ユーザーがレガシーバージョンのReceiverに接続する場合、Secure Browseを有効にしていない場合は、Receiver for Android、Receiver for iOS、およびその他のモバイルデバイスを介した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した場合、Receiver for Windows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。

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