Adaptive Authentication service

Contents

Release notes 2

Configure Adaptive Authentication service 3

Related Adaptive Authentication configurations 16

Disk space management for instances 33

Troubleshoot Adaptive Authentication issues 35

Smart access using Adaptive Authentication 41

Sizing and performance guidelines 53

Data Governance 54

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Release notes

February 6, 2024

Adaptive Authentication release note is a subset of the NetScaler release notes. Adaptive Authentication customers must use NetScaler release notes to learn about the enhancements, issues fixed, and the issues known to exist in the Adaptive Authentication service.

> **Note:**
>
> The date in this document refers to the last upgrade date of the service.

16 Jan 2024

What's new

- **Auto upgrade of the Adaptive Authentication instances**

Adaptive Authentication instances are auto upgraded to build 14.1–12.35 and later that addresses the security vulnerabilities described in CTX584986.

26 Sep 2023

What's new

- **Auto upgrade of the Adaptive Authentication instances**

Adaptive Authentication instances are auto upgraded to build 14.1–8.50 and later that addresses the security vulnerabilities described in CTX579459.

18 July 2023

What's new

- **Auto upgrade of the Adaptive Authentication instances**

Adaptive Authentication instances are auto upgraded to build 13.1–49.101 and later that addresses the security vulnerabilities described in CTX561482.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

28 April 2023

What's new

- **LDAP and LDAPS support with load balancing**

  The Citrix Adaptive Authentication instance provides LDAP and LDAPS support using a load balancing virtual server. For more details, see Sample LDAP and LDAPS load balancing configuration.

  [AAUTH-2067]

- **Mapping backend AD or RADIUS server subnets with resource locations**

  Admins can choose the connectors through which back-end AD and RADIUS servers must be reached. For more details, see Provision Adaptive Authentication.

Fixed issues

- Smart Access policies and OAuth authentication policies configured for Adaptive Authentication are missing in the NetScaler GUI.

  [AAUTH-68]

Known issues

- For an Adaptive Authentication instance, when you use the **Test connection** option in the LDAP profile (NetScaler admin GUI) to check the connectivity, the LDAP server is incorrectly displayed as reachable even though it is not reachable.

  [AAUTH-2111]

Configure Adaptive Authentication service

February 6, 2024

The following high-level steps are involved in configuring the Adaptive Authentication service.

1. Provision Adaptive Authentication
2. Configure Adaptive Authentication policies
3. Enable Adaptive Authentication for Workspace

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Prerequisites

- Reserve an FQDN for your Adaptive Authentication instance. For example, `aauth.xyz.com`, assuming `xyz.com` is your company domain. This FQDN is referred as the Adaptive Authentication service FQDN in this document and is used when provisioning the instance. Map the FQDN with the IdP virtual server public IP address. This IP address is obtained after provisioning in the **Upload Certificate** step.
- Procure a certificate for aauth.xyz.com. Certificates must contain the SAN attribute. Else the certificates aren't accepted.
- Adaptive Authentication UI does not support uploading of certificate bundles. To link an intermediate certificate, see Configure intermediate certificates.
- Choose your connectivity type for the on-premises AD/RADIUS connectivity. The following two options are available. If you do not want data center reachability, use the connector connectivity type.
  - **Citrix Cloud Connector** - For details, see Citrix Cloud Connector.
  - **Azure VNet peering** - For details, see Setup connectivity to on-premises authentication servers using Azure VNet peering.
- Configure a network time protocol (NTP) server to avoid time skews. For details, see How to synchronize system clock with servers on the network.

Points to note

- Citrix recommends not to run clear config for any Adaptive Authentication instance or modify any configuration with the prefix `AA` (example, AAuthAutoConfig) including certificates. This disrupts Adaptive Authentication management and user access is impacted. The only way to recover is through reprovisioning.
- Do not add SNIP or any additional routes on the Adaptive Authentication instance.
- User authentication fails if the customer ID isn't in all lowercase. You can convert your ID to all lowercase and set it on the NetScaler instance by using the command `set cloud parameter -customerID <all_lowercase_customerid>`.
- The nFactor configuration that is required for the Citrix Workspace or the Citrix Secure Private Access service is the only configuration customers are supposed to create directly on the instances. Currently there are no checks or warnings in NetScaler that prevents admins from making these changes.
- It's recommended that all custom configurations are made in the user interface and not directly on the Adaptive Authentication instances. This is because the changes made on the instances aren't auto-synced with the user interface and hence the changes are lost.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Do not upgrade the Adaptive Authentication instances to random RTM builds. All upgrades are managed by Citrix Cloud.
- Only a Windows-based cloud connector is supported. Connector appliance isn't supported in this release.
- If you're an existing Citrix Cloud customer and have already configured Azure AD (or other authentication methods), to switch to Adaptive Authentication (for example, device posture check), you must configure Adaptive Authentication as your authentication method and configure the authentication policies in the Adaptive Authentication instance. For details, see Connect Citrix Cloud to Azure AD.
- For RADIUS server deployment, add all connector private IP addresses as the RADIUS clients in the RADIUS server.
- In the current release, the external ADM agent isn't allowed and therefore Citrix Analytics (CAS) is not supported.
- NetScaler Application Delivery Management service collects the backup for your Adaptive Authentication instance. To extract the backup from ADM, onboard the ADM service. For details, see Config backup and restore. Citrix does not take the backups explicitly from the Adaptive Authentication service. Customers must take the backup of their configurations from the Application Delivery Management service if necessary.
- The Adaptive Authentication instances fail to establish the tunnel if a proxy is configured in the customer's setup. Therefore, it is recommended that you disable proxy configuration for Adaptive Authentication.
- If you are using third-party authentication services such as SAML, authentication might fail if all claims are not found. Therefore, it is recommended that customers add an additional factor such as NOAUTH in the multifactor authentication configuration to pass all the claims.
- It is recommended that you keep the debug log level disabled during normal operations and only enable as required. If the debug log level is enabled always, it causes a tremendous load on the Management CPU. This can result in system crashes during high traffic loads. For details, see CTX222945.

How to configure the Adaptive Authentication service

Access the Adaptive Authentication user interface

You can access the Adaptive Authentication user interface by one of the following methods.

- Manually type the URL https://adaptive-authentication.cloud.com.
- Log in using your credentials and select a customer.

  After you're successfully authenticated, you're redirected to the Adaptive Authentication user interface.

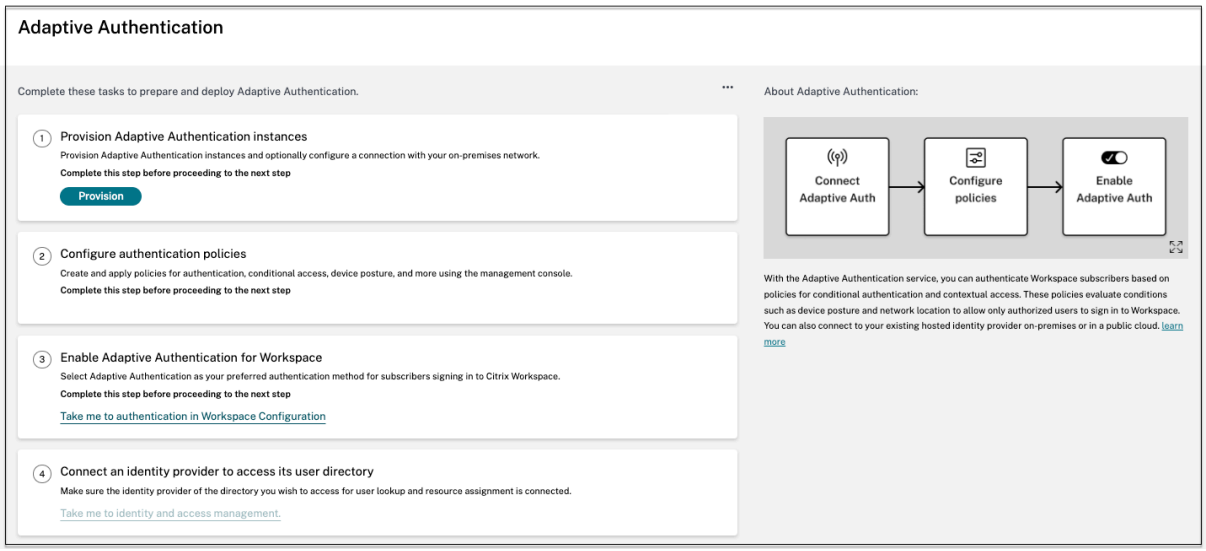
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

OR

- Navigate to **Citrix Cloud > Identity and Access Management**.
- In the Authentication tab, in **Adaptive Authentication**, click the ellipsis menu and select **Manage**.

The Adaptive Authentication user interface appears.

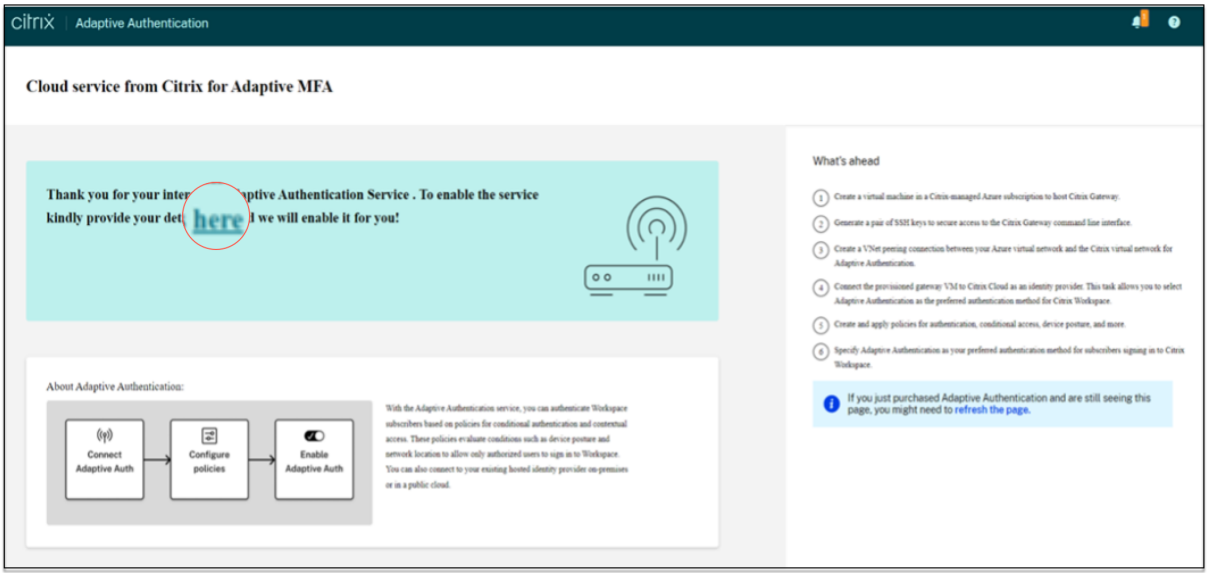
The following figure illustrates the steps involved in configuring Adaptive Authentication.



Step 1: Provision Adaptive Authentication

> **Important:**
>
> Customers interested in the Adaptive Authentication service are required to click the link as shown in the following screenshot and complete the Podio form. The Citrix Adaptive Authentication team then enables the provisioning of Adaptive Authentication instances.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Perform the following steps to provision the Adaptive Authentication instance:

1. On the **Adaptive Authentication** UI, click **Provision**.
2. Select the preferred connection for Adaptive Authentication.

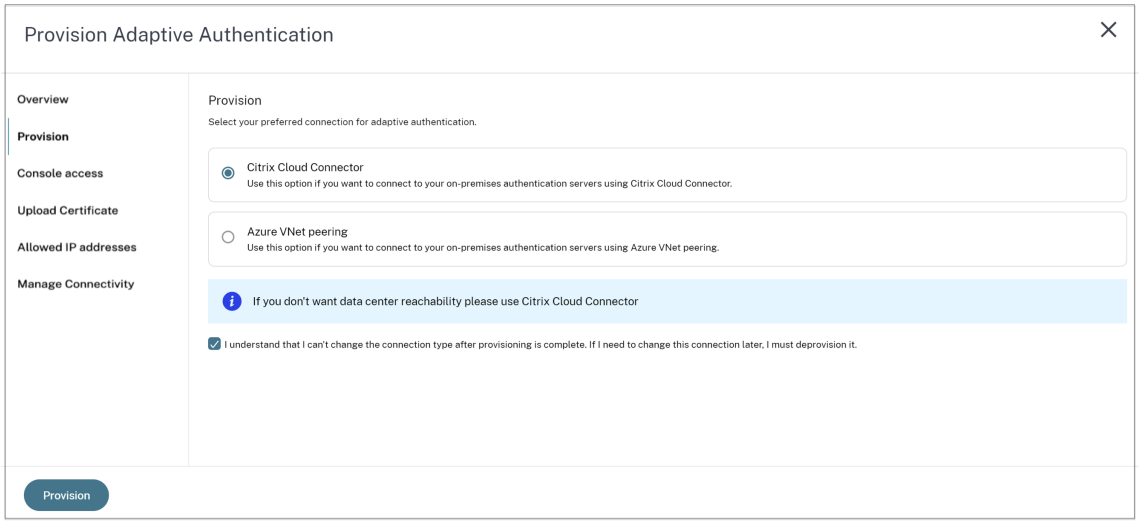
    - **Citrix Cloud Connector:** For this connection type, you must set up a connector in your on-premises network. Citrix recommends that you deploy at least two Citrix Cloud Connectors in your environment to set up connection to the Citrix Gateway hosted on Azure. You must allow your Citrix Cloud Connector to access the domain/URL you've reserved for the Adaptive Authentication instance. For example, allow https://aauth.xyz.com/*.

      For details on Citrix Cloud Connector, see Citrix Cloud Connector.

    - **Azure VNet peering** - You must set up the connectivity between the servers using Azure's VNet peering.

        - Ensure that you have an Azure subscription account to set up the connectivity.
        - The customer VNet that is being peered must already have an Azure VPN gateway provisioned. For details, see https://docs.microsoft.com/en-us/azure/vpn-gateway/tutorial-site-to-site-portal.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



To add a Citrix Cloud Connector as your preferred connection:

Perform the following steps.

- Select the **Citrix Cloud Connector** option, and then select the end user agreement checkbox.
- Click **Provision**. Provisioning might take up to 30 minutes to set up.

> **Note:**
>
> For connector connectivity type, make sure that your Adaptive Authentication FQDN is reachable from the connector virtual machine after provisioning.

To set up Azure VNet peering:

If you select **Azure VNet peering** as your connection, you must add a subnet CIDR block that must be used to provision the Adaptive Authentication instance. You must also ensure that the CIDR block does not overlap with your organization's other network ranges.

For details, see Set up connectivity to on-premises authentication servers using Azure VNet peering.

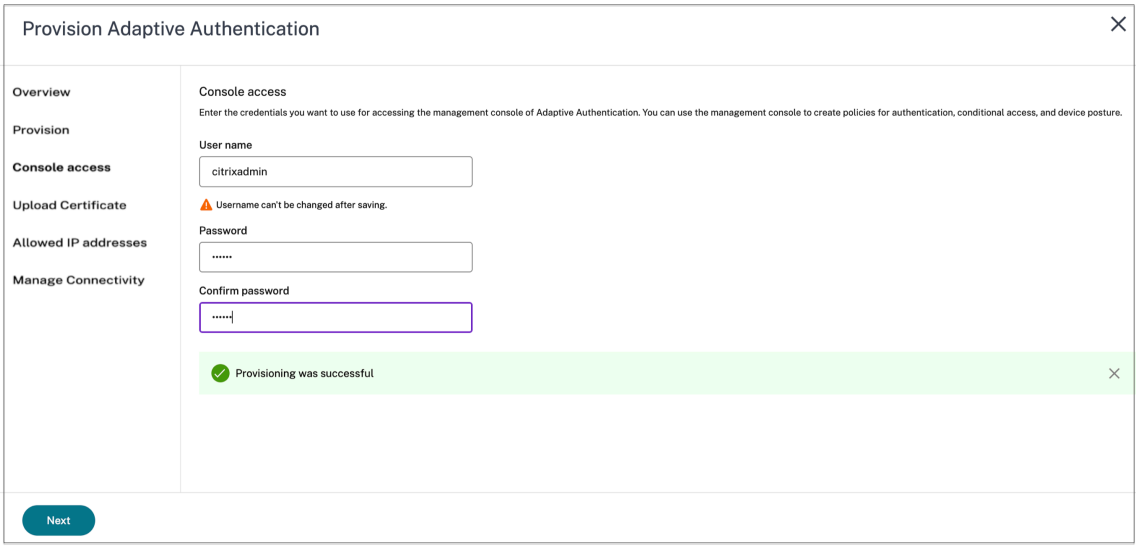
3. Set up credentials to access the instances that you've enabled for Adaptive Authentication. You need the management console access for creating policies for authentication, conditional access, and so on.

   a) In the **Console access** screen, enter the user name and password.
   b) Click **Next**.

> **Note:**

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> Users created from the **Console access** screen are provided with "SuperUser"privileges that have the shell access.



4. Add the Adaptive Authentication service FQDN and upload the certificate-key pair.
   You must enter the Adaptive Authentication service FQDN of your choice for the publicly accessible authentication server. This FQDN must be publicly resolvable.

   a) In the **Upload Certificate** screen, enter the FQDN that you've reserved for Adaptive Authentication.

   b) Select the certificate type.

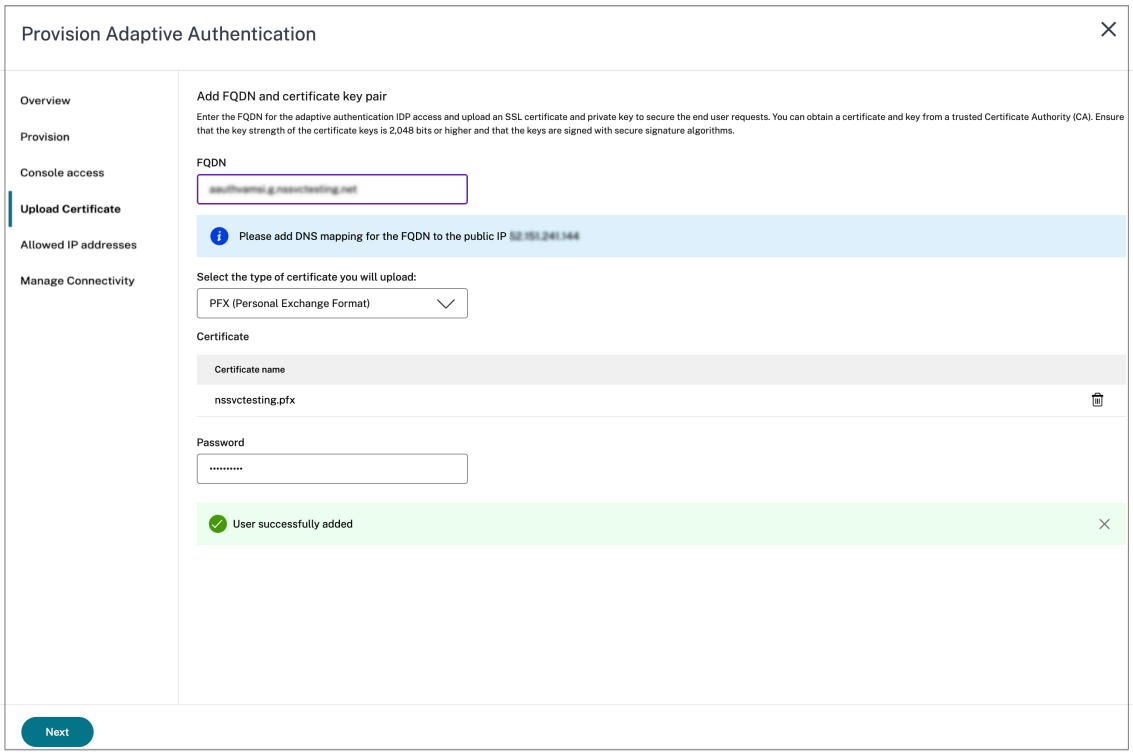
      - Adaptive Authentication service supports certificates of type PFX, PEM, DER for provisioning of instances.
      - Certificate bundle is only supported for certificates of type PEM. For other bundle types, Citrix recommends installing the root and intermediate certificates and linking them to the server certificate.

   c) Upload the certificate and the key.

> **Note:**
>
> - Install your intermediate certificate on the Adaptive Authentication instance and link it with the server certificate.
>
>   a) Log in to the Adaptive Authentication instance.
>   b) Navigate to **Traffic Management > SSL**.
>   For details, see Configure intermediate certificates.
>
> - Only public certificates are accepted. Certificates signed by private or unknown CAs aren't accepted.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

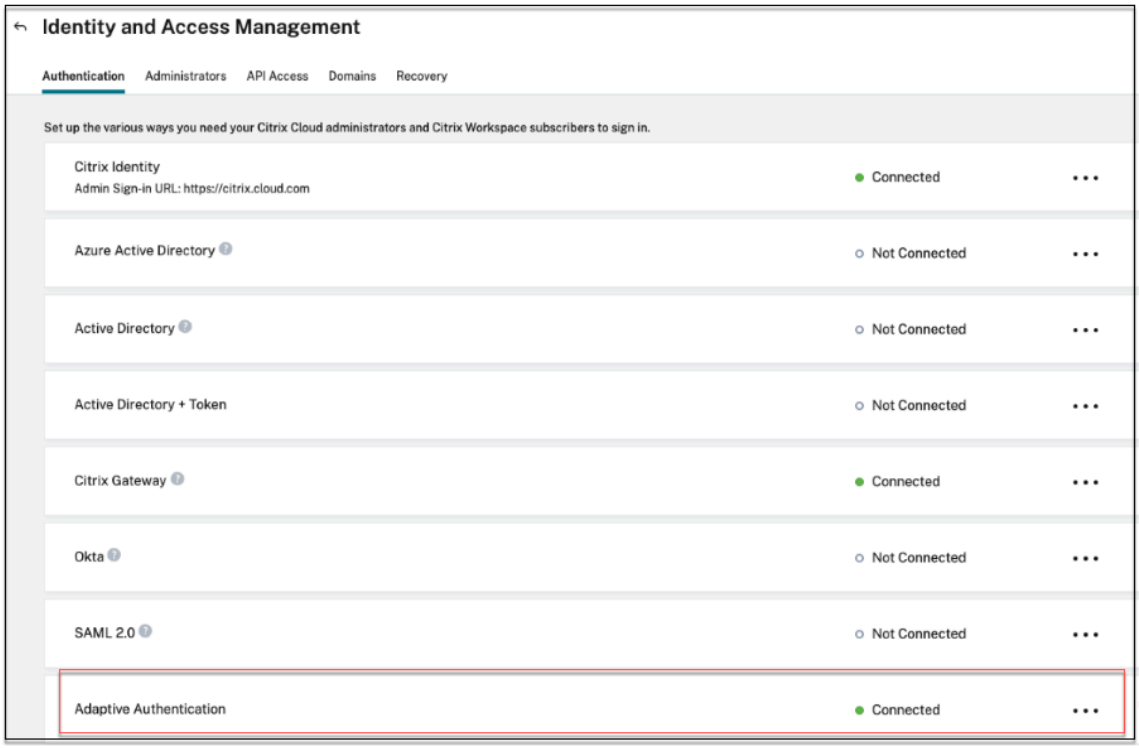
> - Certificate configuration or certificate updates must be done using the Adaptive Authentication UI only. Do not change it directly on the instance as this might result in inconsistencies.



5. Upload the certificate and the key.

   The Adaptive Authentication instance now is connected to the Identity and Access Management service. The **Adaptive Authentication** method status is displayed as **Connected**.

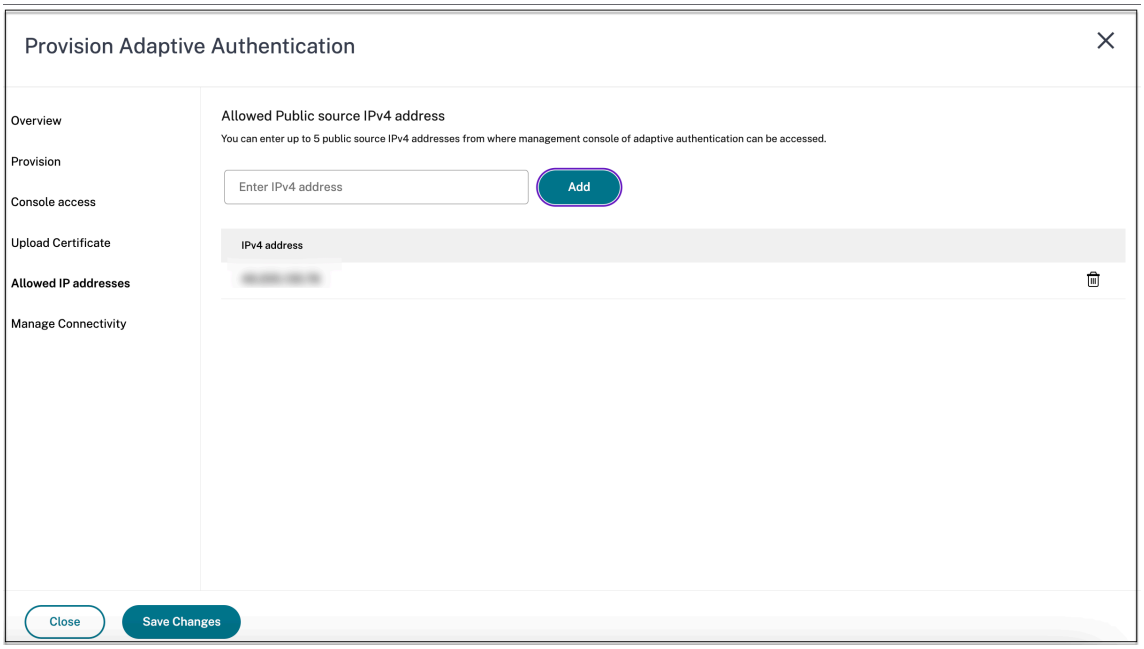
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



6. Set up an IP address through which the Adaptive Authentication management console can be accessed.

    a) In the **Allowed IP addresses** screen, for each instance, enter a public IP address as the management IP address. To restrict the access to the management IP address, you can add multiple IP addresses that are allowed to access the management console.
    b) To add multiple IP addresses, you must click **Add**, enter the IP address, and then click **Done**. This must be done for every IP address. If you do not click the **Done** button, the IP addresses aren't added to the database but are only added in the user interface.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



7. If you're using the connector connectivity type, then specify a set of resource locations (connectors) through which AD or RADIUS servers can be reached. If you're using the VNet peering connectivity type, then you can skip this step.

   Admins can choose the connectors through which back-end AD and RADIUS servers must be reached. To enable this feature, customers can set up a mapping between their back-end AD/RADIUS server subnets such that if the authentication traffic falls under a specific subnet, then that traffic is directed to the specific resource location. However, If a resource location isn't mapped to a subnet, then admins can specify to use the wildcard resource location for those subnets.

   Previously, Adaptive Authentication traffic for on-premises AD/RADIUS was directed to any available resource location using the round robin method. This caused issues for customers with multiple resource locations.

   a) On the Adaptive Authentication UI, click **Manage Connectivity**.

   b) Enter the subnet details and select the respective resource location.

      > **Note:**
      >
      > If you clear the **Use any available resource location for remaining subnets** checkbox, only the traffic directed towards the configured subnets is tunneled.

   c) Click **Add**, and then click **Save Changes**.

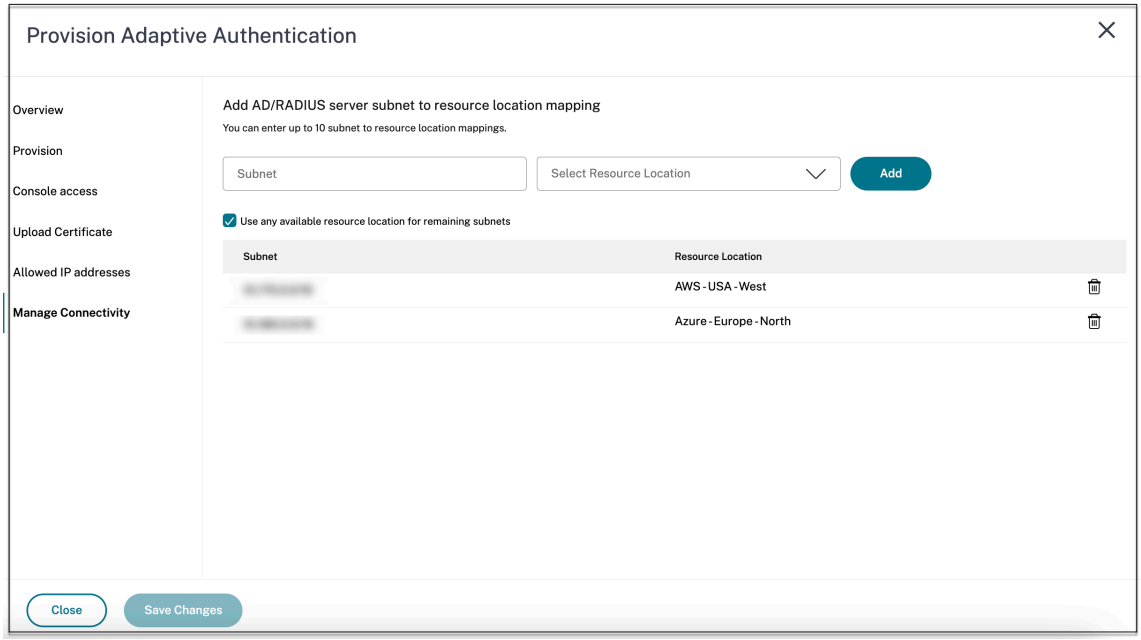
> **Note:**
>
> - Only RFC1918 IP address subnets are allowed.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- The number of subnet-resource location mappings per customer is limited to 10.
- Multiple subnets can be mapped to a single resource location.
- Duplicate entries aren't allowed for the same subnet.
- To update the subnet entry, delete the existing entry and then update.
- If you rename or remove the resource location, make sure to remove the entry from the **Manage Connectivity** screen in the Adaptive Authentication user interface.
- Any changes made to the resource location mapping by using the following CLI commands are overwritten by the changes pushed from the user interface (**Adaptive Authentication Provisioning > Manage Connectivity**).

```
- set cloudtunnel parameter -subnetResourceLocationMappings

- set policy expression aauth_allow_rfc1918_subnets <>
- set policy expression aauth_listen_policy_exp <>
```



Provisioning Adaptive Authentication is now complete.

Step 2: Configure Adaptive Authentication policies

How to connect to your Adaptive Authentication instance:

After the provisioning, you can access the Adaptive Authentication management IP address directly. You can access the Adaptive Authentication management console using the FQDN or your primary IP address.

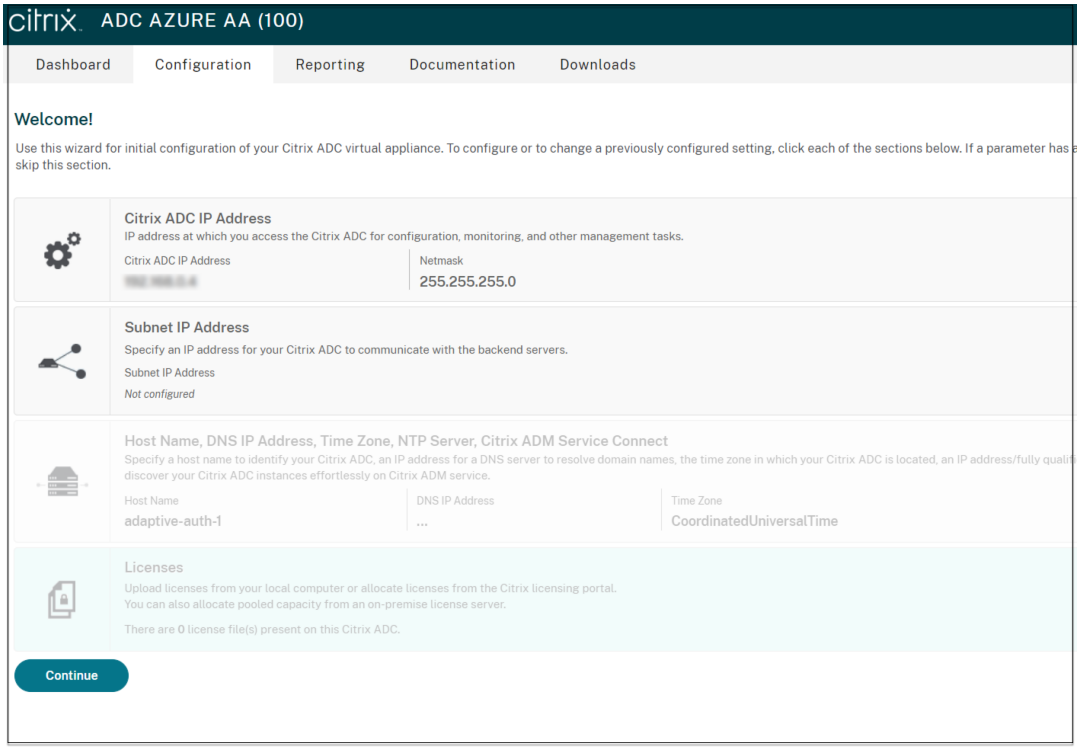
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Important:**
>
> - In a high availability setup, as part of the synchronization process, the certificates are also synchronized. So ensure that you use the wildcard certificate.
> - If you need a unique certificate for each node, upload the certificate files and keys in any folder that doesn't get synchronized (for example, create a separate folder (nosync_cert) in the nsconfig/SSL directory) and then upload the certificate uniquely on each node.

Access the Adaptive Authentication management console:

- To access the Adaptive Authentication management console using the FQDN, see Configure SSL for ADC Admin UI access.
- To access the Adaptive Authentication using your primary address, do the following:

  1. Copy the primary IP address from the **Configure Authentication policies** section in the GUI and access the IP address in your browser.
  2. Log in using the credentials that you've entered while provisioning.
  3. Click **Continue**.



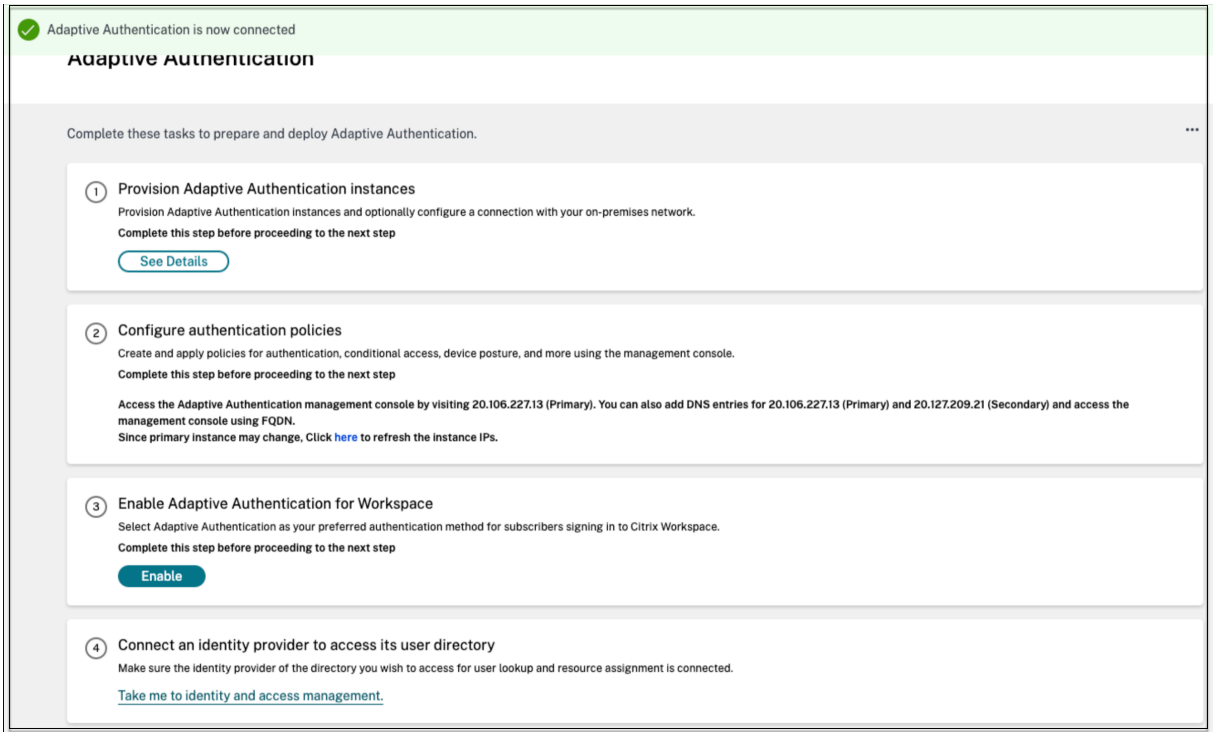
  4. Navigate to **Configuration > Security > AAA - Application Traffic > Virtual Servers**.
  5. Add the authentication policies. For various use cases, see Sample authentication configurations.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Note:**
>
> Accessing the Adaptive Authentication instance using the IP address isn't trusted and many browsers block the access with warnings. We recommend that you access the Adaptive Authentication management console with FQDN to avoid any security barriers. You must reserve the FQDN for the Adaptive Authentication management console and map it with the primary and secondary management IP address.
>
> For example, if your Adaptive Authentication instance IP is 192.0.2.0 and Secondary: 192.2.2.2, then;
>
> - primary.domain.com can be mapped to 192.0.2.0
> - secondary.domain.com can be mapped to 192.2.2.2

Step 3: Enable Adaptive Authentication for Workspace

After provisioning is complete, you can enable authentication for Workspace by clicking **Enable** in the **Enable Adaptive Authentication for Workspace** section.



> **Note:**
>
> With this, the Adaptive Authentication configuration is completed. When you access your workspace URL, you must be redirected to the Adaptive Authentication FQDN.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Related references

- Edit an FQDN
- Schedule upgrade of your Adaptive Authentication instances
- Deprovision your Adaptive Authentication instances
- Enable secure access to the gateway
- Set up connectivity to on-premises authentication servers using Azure VNet peering
- Custom workspace URL or vanity URL
- Config backup and restore
- Sample load balanced LDAPS configuration
- Migrate your authentication method to Adaptive Authentication
- Sample authentication configurations

Related Adaptive Authentication configurations

November 24, 2023

Edit an FQDN

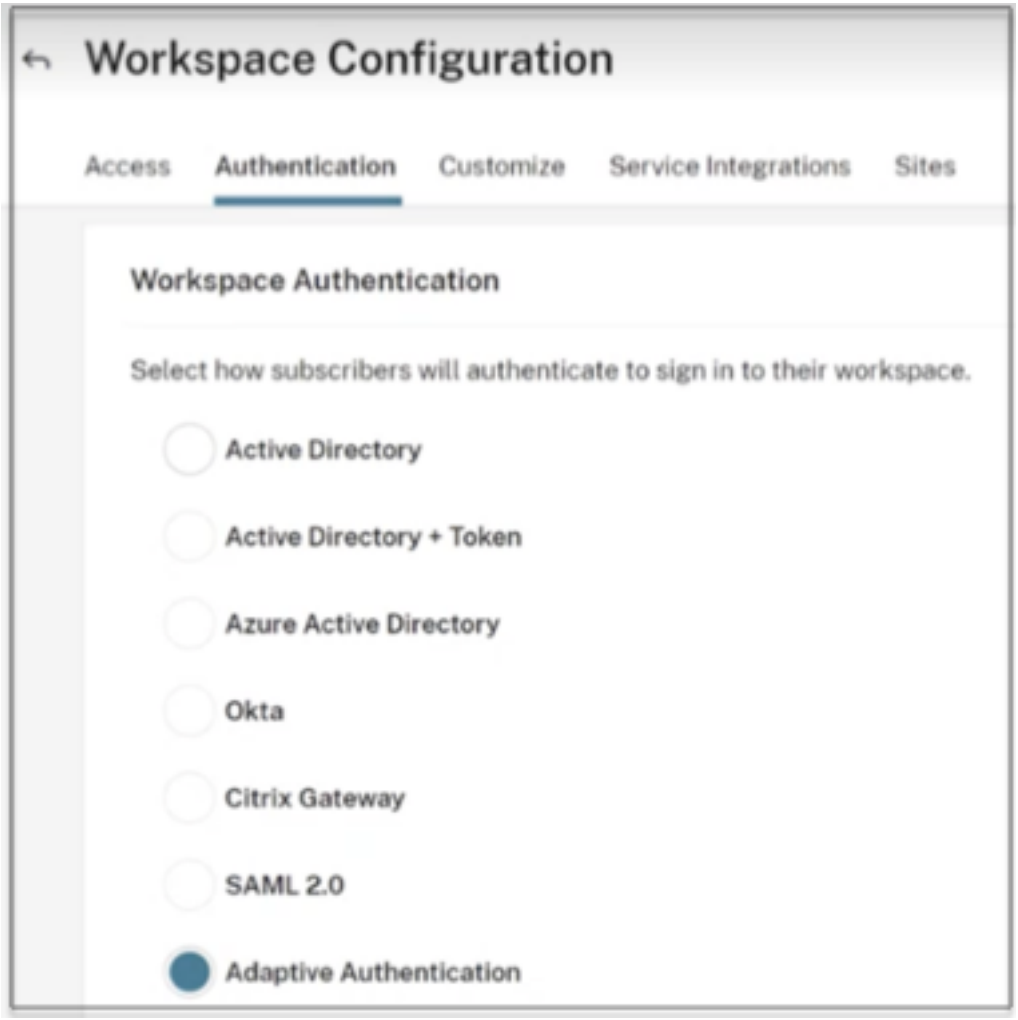
You cannot edit an FQDN if **Adaptive Authentication** is selected as the authentication method in the Workspace configuration. You must switch to a different authentication method to edit the FQDN. However, you can edit the certificate if necessary.

> **Important:**
>
> - Before modifying the FQDN, ensure that the new FQDN is mapped to the IdP virtual server public IP address.
> - Existing users who are connected to **Citrix Gateway** using OAuth policies must migrate your authentication method to **Adaptive Authentication**. For details, see Migrate your authentication method to Adaptive Authentication.

To edit an FQDN, perform the following:

1. Switch to a different authentication method from **Adaptive Authentication**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

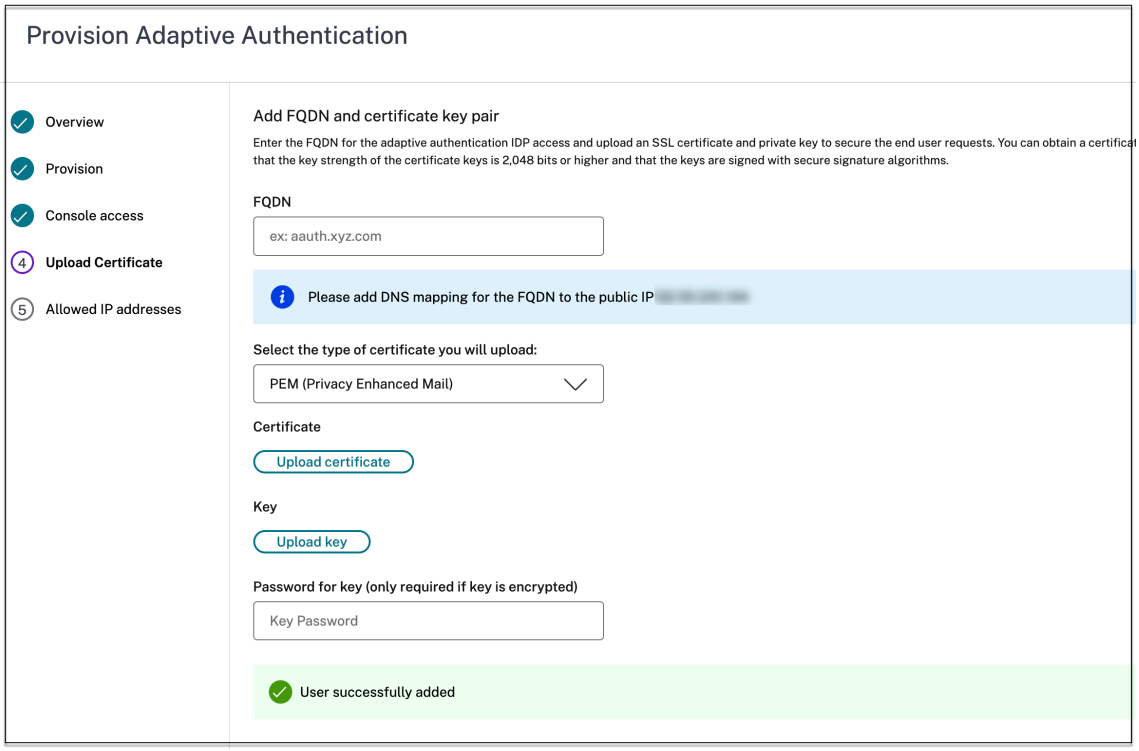


2. Select **I understand the impact on the subscriber experience,** and then click **Confirm**.

   When you click **Confirm**, the workspace login to end users is impacted and Adaptive Authentication is not used for authentication until Adaptive Authentication is enabled again. Therefore, it is recommended that you modify the FQDN during a maintenance window.

3. In the **Upload Certificate** screen, modify the FQDN.

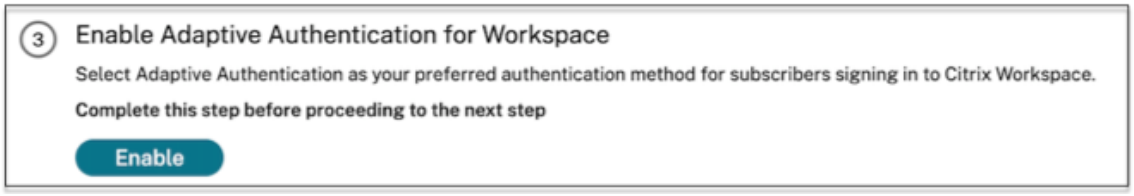
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



4. Click **Save Changes**.

> **Important:**
>
> If you edit an FQDN, you must also upload the certificate again.

5. Enable the Adaptive Authentication method again by clicking **Enable** (step 3) in the Adaptive Authentication home page.



6. Click **Refresh**.

Custom workspace URL or vanity URL

A custom workspace URL allows you to use a domain of your choice to access your Citrix Workspace store. Users can access Workspace using the default Workspace URL or the custom workspace URL or both.

To configure a custom workspace URL or vanity URL, you must perform the following:

1. Configure your custom domain. For details, see Configuring your custom domain.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

2. Configure a new OAuthIDP profile with the same client ID, secret, and audience as your current or default profile (AAuthAutoConfig_oauthIdpProf) but with a different redirect URL. For details, see Configuring OAuth Policies and Profiles.

   Example:

   Current profile:

```
-add authentication OAuthIDPProfile AAuthAutoConfig_oauthIdpProf
 -clientID xxxx -clientSecret yyyy -encrypted -encryptmethod
ENCMTHD_3 -kek -suffix 2023_07_09_20_09_30 -redirectURL "https
://accounts-internal.cloud.com/core/login-cip"-audience zzzz -
sendPassword ON

add authentication OAuthIdPPolicy AAuthAutoConfig_oauthIdpPol -
rule true -action AAuthAutoConfig_oauthIdpProf

bind authentication vserver auth_vs -policy AAuthAutoConfig_oauthIdpPol
 -priority 100 -gotoPriorityExpression NEXT
```

   New profile:

```
add authentication OAuthIDPProfile AAuthAutoConfig_oauthIdpProf_Custom1
 -clientID xxxx -clientSecret yyyy -encrypted -encryptmethod
ENCMTHD_3 -kek -suffix 2023_07_09_20_09_30 -redirectURL "https://
custom_domain/core/login-cip"-audience zzzz -sendPassword ON

add authentication OAuthIdPPolicy AAuthAutoConfig_oauthIdpPol_Custom1
 -rule true -action AAuthAutoConfig_oauthIdpProf_Custom1

bind authentication vserver auth_vs -policy AAuthAutoConfig_oauthIdpPol_Cu
 -priority 101 -gotoPriorityExpression NEXT
```

> **Important:**
>
> - The OAuth policy and profile is created by the Adaptive Authentication service during the provisioning phase. As a result, the Citrix Cloud admin does not have access to the unencrypted client secret. You can obtain the encrypted secret from the ns.conf file. To create an OAuth profile, you must use the encrypted secret and create the profile using only the CLI commands.
> - You cannot create an OAuth profile using the NetScaler user interface.

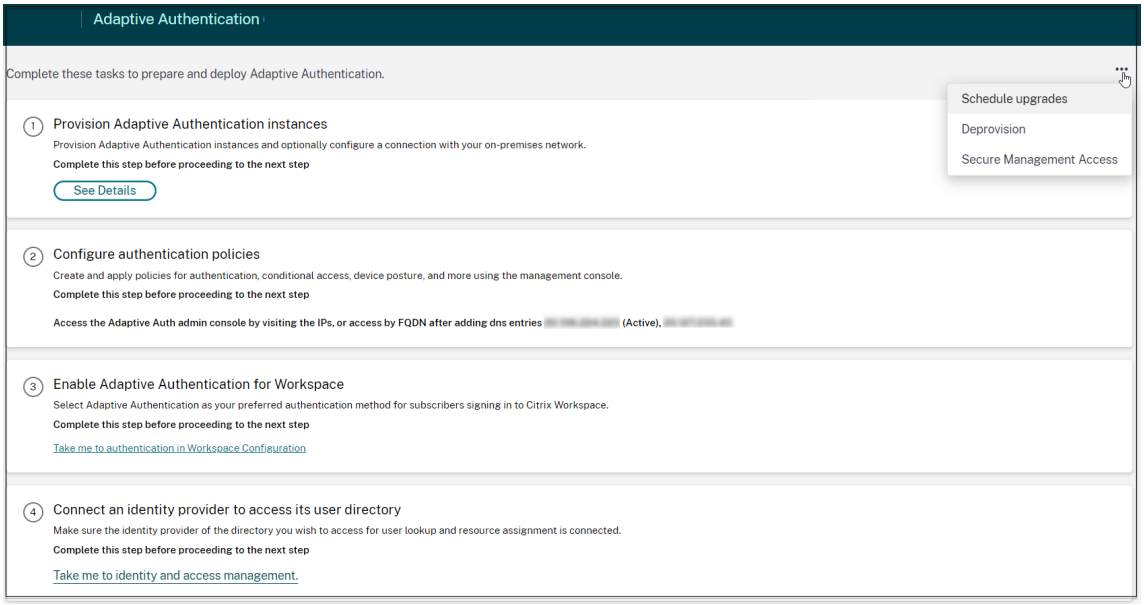
Schedule upgrade of your Adaptive Authentication instances

For the current site or deployment, you can select the maintenance window for upgrade.

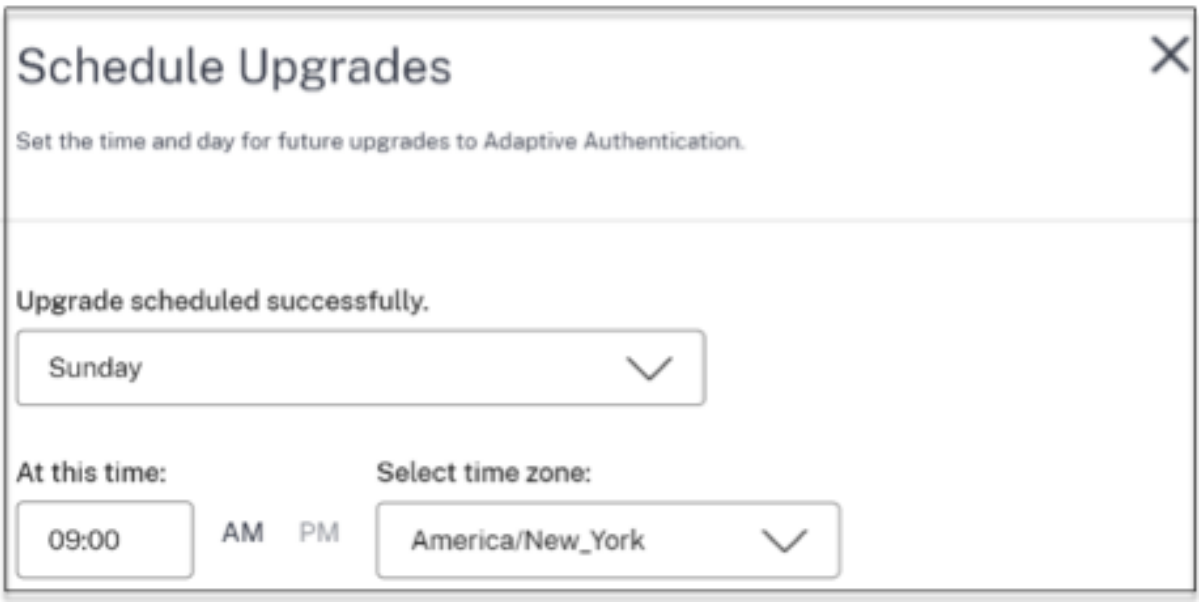
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> **Important:**
>
> Do not upgrade the Adaptive Authentication instances to random RTM builds. All upgrades are managed by Citrix Cloud.

1. On the **Adaptive Authentication** UI, in the **Provision Adaptive Authentication instances** section, click the ellipsis button.



2. Click **Schedule upgrades**.
3. Select the day and time for the upgrade.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Deprovision your Adaptive Authentication instances

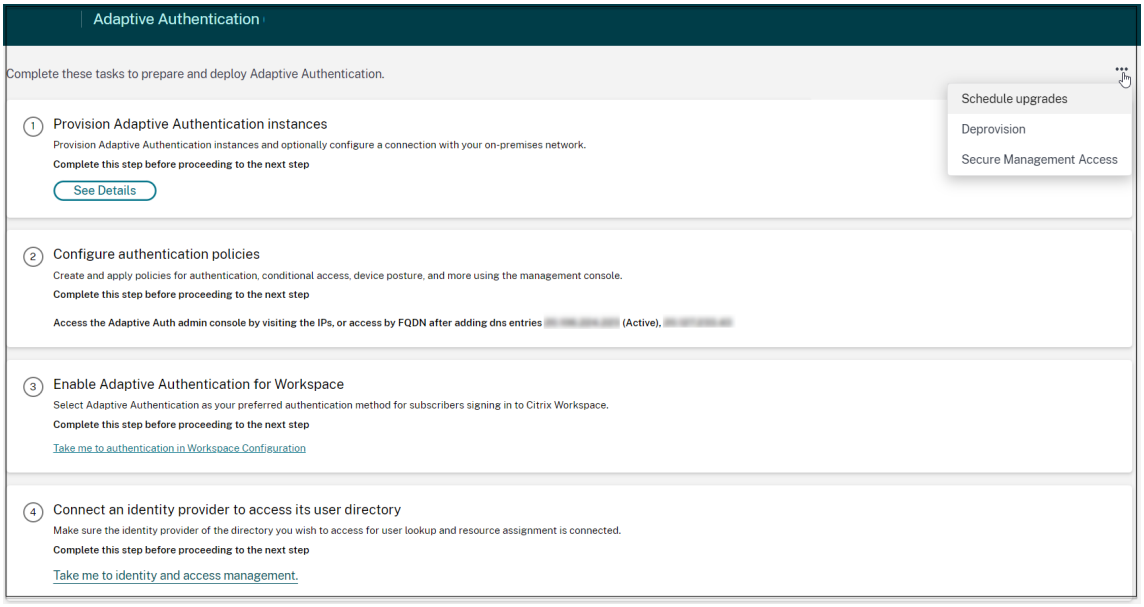
Customers can deprovision the Adaptive Authentication instances in the following cases and as per the suggestion from Citrix support.

- The Adaptive Authentication instances are not accessible (especially after a scheduled upgrade), though this scenario might not occur.
- If the customer has to switch from VNet peering mode to connector mode or conversely.
- If the customer selected a wrong subnet at the time of provisioning VNet peering mode (the subnet conflicts with other subnets in their data center or Azure VNet).

> **Note:**
>
> Deprovisioning also deletes the config backup of the instances. Therefore you must download the backup files and save it before you deprovision your Adaptive Authentication instances.

Perform the following to deprovision an Adaptive Authentication instance:

1. On the **Adaptive Authentication** UI, in the **Provision Adaptive Authentication instances** section, click the ellipsis button.

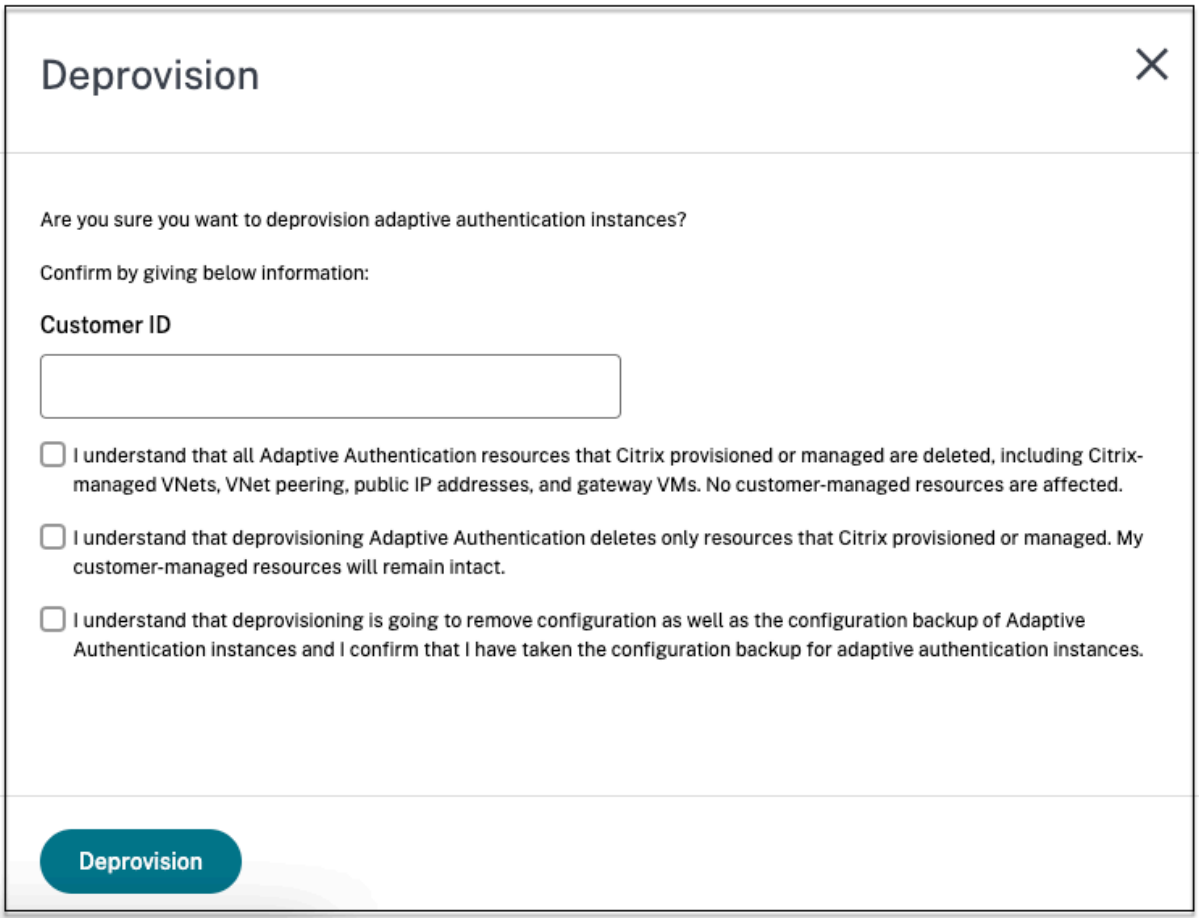


2. Click **Deprovision**.

> **Note:**
>
> Before deprovisioning, you must disconnect **Citrix Gateway** from the Workspace Configuration.

3. Enter the customer ID to deprovision the Adaptive Authentication instances.

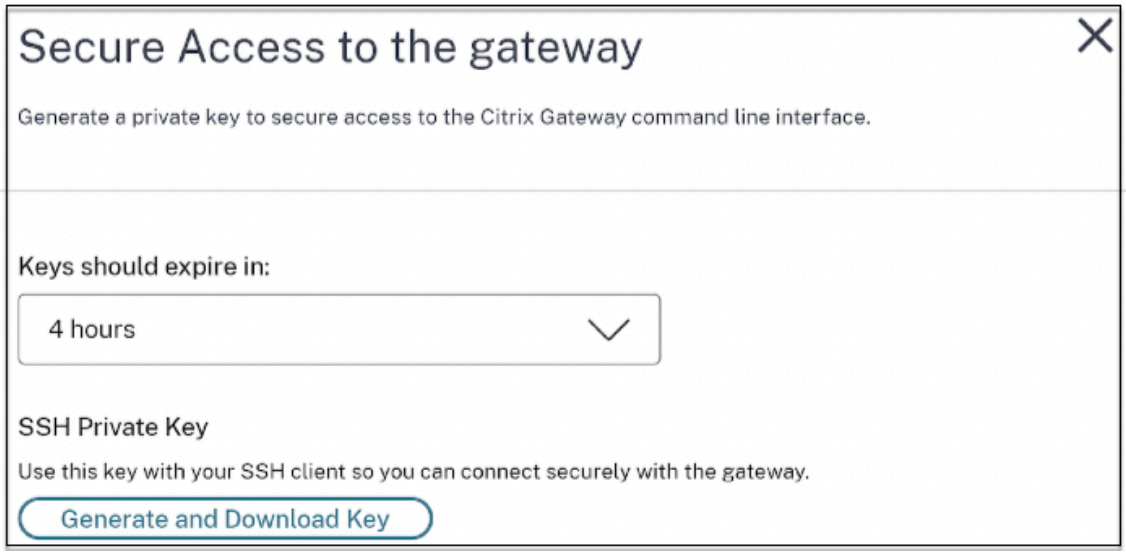
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Enable secure access to the gateway

1. On the **Adaptive Authentication** UI, in the **Provision Adaptive Authentication instances** section, click the ellipsis button.
2. Click **Secure Management Access**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



3. In **Keys should expire in**, select an expiration duration for the new SSH key.
4. Click **Generate and Download keys**.
   Copy or download the SSH private key for later use as it is not displayed after the page is closed. This key can be used to log in to the Adaptive Authentication instances with the user name `authadmin`.

   You can click **Generate and Download keys** to create a new key pair if the earlier key pair expires. However, only one key pair can be active.
5. Click **Done**.

Important:

- If you are using PuTTY on Windows to connect to Adaptive Authentication instances, you must convert the downloaded private key to PEM. For details, see https://www.puttygen.com/convert-pem-to-ppk.
- It is recommended to use the following command to connect to the Adaptive Authentication instances via the terminal from the MAC or PowerShell/Command prompt from Windows (version 10).
  `ssh -i <path-to-private-key> authadmin@<ip address of ADC>`
- If you want the AD users to access the Adaptive Authentication GUI, you must add them as new administrators to the LDAP group. For details, see https://support.citrix.com/article/CTX123782.
  For all other configurations, Citrix recommends that you use the Adaptive Authentication GUI and not the CLI commands.

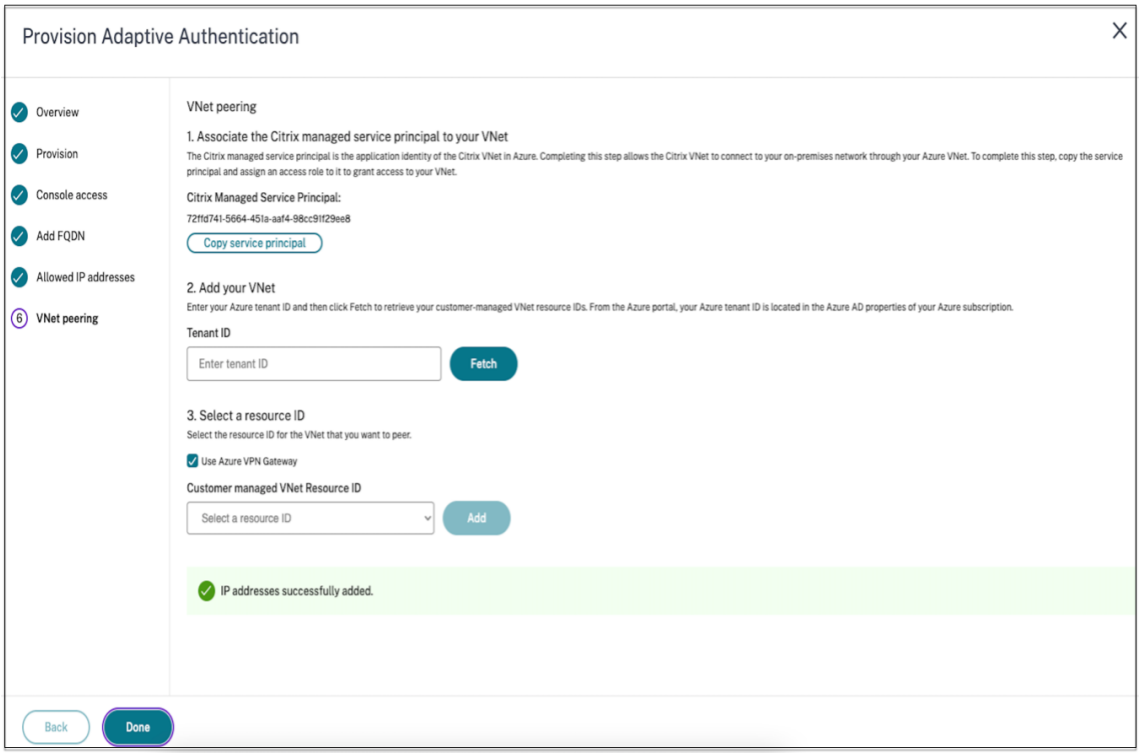
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Set up connectivity to on-premises authentication servers using Azure VNet peering

You must set up this configuration only if you have selected the connectivity type as Azure VNet peering.

> **Note:**
>
> If you are using third-party IDPs like Okta, Azure AD, Ping, this step is not required.

1. On the Connect Adaptive Authentication UI, click **Provision**, and then click **Azure VNet Peering**.



The **Citrix Managed Service Principal** field contains the application ID of an Azure Service Principal created by Citrix for your customer. This service principal is required to allow Citrix to add a VNet peering to a VNet in your subscription and tenant.

To allow this service principal to log in to the customer tenant, the admin at the customer site (global admin of the tenant) must run the following PowerShell commands to add the SPN to the tenant. CloudShell can also be used.

```
Connect-AzureAD
New-AzureADServicePrincipal -AppId $App_ID
```

Where `$App_ID` is an SPN Application ID shared by Citrix.

> **Note:**
>
> - The earlier-mentioned command outputs a service principal name that must be used

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> for the role assignments.
> - To allow this service principal to add an Azure VNet peering, the admin at the customer site (not limited to global admin) must add a "Network Contributor"role to the VNet that must be linked to the Citrix Managed VNet.
> - SPN is a unique identifier that is used to associate the Citrix virtual network in Azure. Associating the SPN with VNet enables Citrix virtual network to connect to the customers'on-premises network through Azure's VNet.

2. Create a VNet peering.

   - Enter the tenant ID for which the earlier steps were run and click **Fetch**.

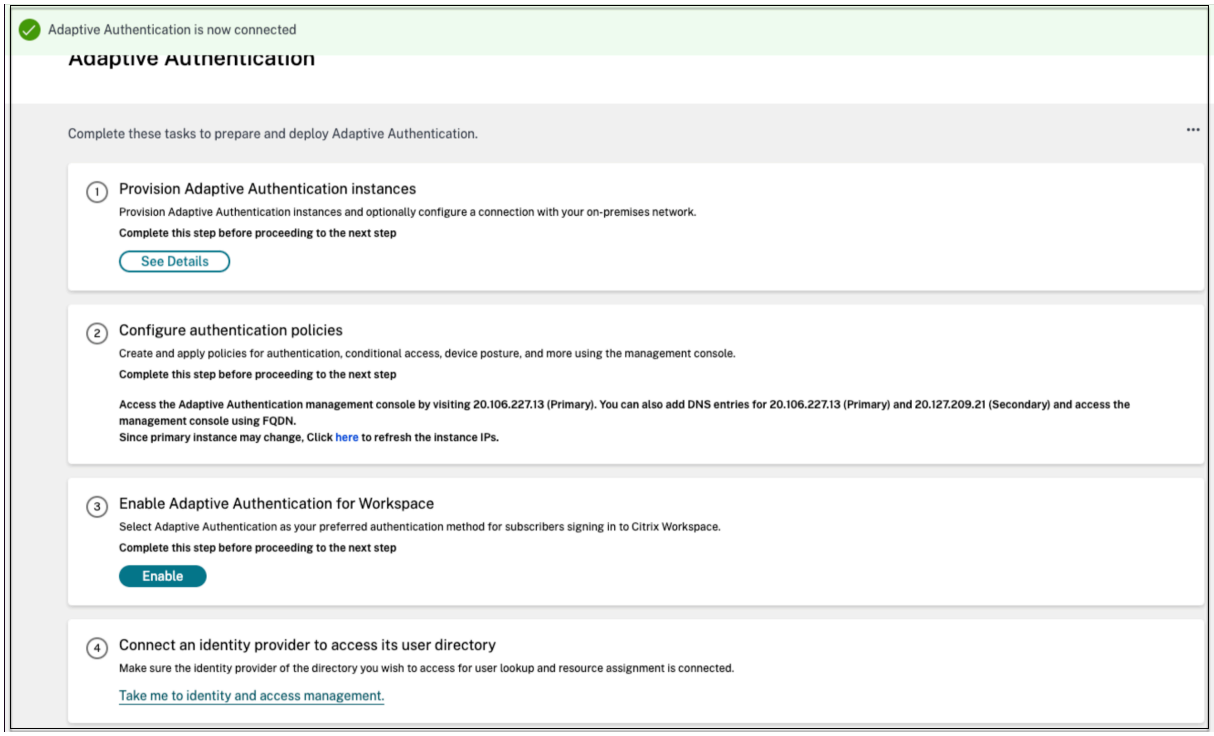
   This populates the customer-managed VNet resource ID with the candidate VNets for which the network contributor role is added for the SPN. If you do not see your VNet, make sure that the earlier steps are run correctly or repeat the steps.

   > **Note:**
   >
   > For details on how to find your tenant ID, see https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-how-to-find-tenant.

3. Select **Use Azure VPN Gateway** to connect your on-premises networks to Azure.
4. In **Customer managed VNet Resource ID**, select the VNet identified for peering, and click **Add**. The VNet is added to the table with the status initially as **In Progress**. Once the peering is completed successfully, the Status changes to **Done**.
5. Click **Done**.
6. Continue with the configuration, see Step 1: Provision Adaptive Authentication.

   > **Important:**
   >
   > - For traffic to flow between the Citrix managed VNet and the on-premises network, firewall and routing rules might be changed on the on-premises to direct the traffic to the Citrix Managed VNet.
   > - You can add only one VNet peer at a time. Multiple VNet peerings are not allowed currently. You can delete a VNet peering or create one as required.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Config backup and restore

Application Delivery Management service performs backup management for the Adaptive Authentication instances. For details, see Back up and restore NetScaler instances.

1. On the Application Delivery Management tile, click **Manage**.
2. Navigate to **Infrastructure > Instances** and access the backups.

> **Note:**
>
> If you do not see the service onboarded, onboard the Application Delivery Management service. For details, see Getting started.

Sample LDAP and LDAPS load balancing configuration

The Citrix Adaptive Authentication instance provides LDAP/LDAPS support using a load balancing virtual server.

> **Note:**
>
> - If you are not using load balancing for LDAP/LDAPS, avoid creating a service or a server for an LDAP server as this might break the Adaptive Authentication tunnel.
> - If you are using load balancing for LDAP, create a service group and bind it to the load bal-

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> ancing service and not to a standalone service.
> - When using load balancing virtual server for authentication, ensure that you add the load balancing virtual server IP address instead of the actual LDAP server IP address in the LDAP action.
> - By default, a TCP monitor is bound to the service that you create. On the Adaptive Authentication NetScaler instances, the service is marked as UP by default if a TCP monitor is used.
> - For monitoring, it is recommended that you use custom monitors.

Prerequisites

Private IP address (RFC1918 address) of the load balancing virtual server. It can be a dummy IP address as this address is used for internal configuration.

Load balancing LDAP servers

For load balancing LDAP servers, create a service group and bind it to the load balancing virtual server. Do not create a service for load balancing LDAP servers.

Configure LDAP by using the NetScaler CLI:

You can use the following CLI commands as a reference to configure LDAP.

1. `add serviceGroup <serviceGroupName> <serviceType>`
2. `bind servicegroup <serviceGroupName> (<IP> | <serverName>)<port>`
3. `add lb vserver <name> <serviceType> <ip> <port>` - The port must be 389. This port is used for internal communication and connection to an on-premises server is over SSL based on the port configured for the service group.
4. `bind lb vserver <name> <serviceGroupName>`
5. `add authentication ldapAction <name> { -serverIP } <ip_addr> | { -serverName <string> } } <lb vserver ip>`
6. `add authentication policy <ldap_policy_name> -rule <expression> -action <string>`
7. `bind authentication vserver auth_vs -policy <ldap_policy_name> -priority <ldap_policy_priority> -gotoPriorityExpression NEXT`

Configure LDAP by using the NetScaler GUI:

1. Navigate to **Traffic Management > Load Balancing** and then click **Virtual Servers**.
2. Create a virtual server of type TCP and port 389.

   Do not create a load balancing virtual server of type SSL/SSL_TCP.
3. Navigate to **Traffic Management > Load Balancing** and then click **Service Groups**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

4. Create a service group of type TCP and port 389.
5. Bind the service group to the virtual server that you have created in step 1.

For details on the procedures, see Set up basic load balancing.

Load balancing LDAPS servers

For load balancing LDAPS servers, you must create a load balancing virtual server of type TCP to avoid internal SSL encryption or decryption into the Adaptive Authentication instance. The load balancing virtual server handles the TLS encryption/decryption in this case. Do not create a load balancing virtual server of type SSL.

Configure LDAPS by using the NetScaler CLI:

You can use the following CLI commands as a reference to configure LDAPS.

1. `add lb vserver <name> <serviceType> <ip> <port>` - The port must be 636.
2. `bind lb vserver <name> <serviceGroupName>`
3. `add authentication ldapAction <name> { -serverIP } <ip_addr> | { -serverName <string> } } <lb vserver ip>`
4. `add authentication policy <ldap_policy_name> -rule <expression> -action <string>`
5. `bind authentication vserver auth_vs -policy <ldap_policy_name> -priority <ldap_policy_priority> -gotoPriorityExpression NEXT`

Configure LDAPS by using the NetScaler GUI:

1. Navigate to **Traffic Management > Load Balancing** and then click **Virtual Servers**.
2. Create a virtual server of type TCP and port 636.

   Do not create a load balancing virtual server of type SSL/SSL_TCP.
3. Navigate to **Traffic Management > Load Balancing** and then click **Service**.
4. Create a service of type SSL_TCP and port 636.
5. Bind the service to the virtual server that you have created in step 1.

For details on the procedures, see Set up basic load balancing.

Create custom monitors

Create custom monitors by using the NetScaler GUI:

1. Navigate to **Traffic Management > Load Balancing > Monitors**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

2. Create a monitor of type LDAP. Ensure that you set the monitor probe interval to 15 seconds and the response timeout to 10 sec.
3. Bind this monitor to your service.

For more details, see Custom monitors.

Provision to add up to 15 admin IP addresses

Adaptive Authentication service allows you to enter up to 15 Public IP subnets and individual IP addresses to access the Adaptive Authentication management console.

Points to note while entering the IP addresses/subnets:

- Ensure that the CIDRs of the public IP subnets are between /20 to /32.B.
- Ensure that there is no overlap between the entries.

Examples:

- 192.0.2.0/24 and 192.0.2.8 are not accepted because 192.0.2.8 lies within 192.0.5.0/24.
- Overlapping Subnets :192.0.2.0/24 and 192.0.0.0/20 are not accepted because the subnets overlap.
- While entering a network subnet value, enter the network IP address as the IP address value.

  Example:

  - 192.0.2.2/24 is incorrect, instead use 191.0.2.0/24
  - 192.0.2.0/20 is incorrect, instead use 192.0.0.0/20

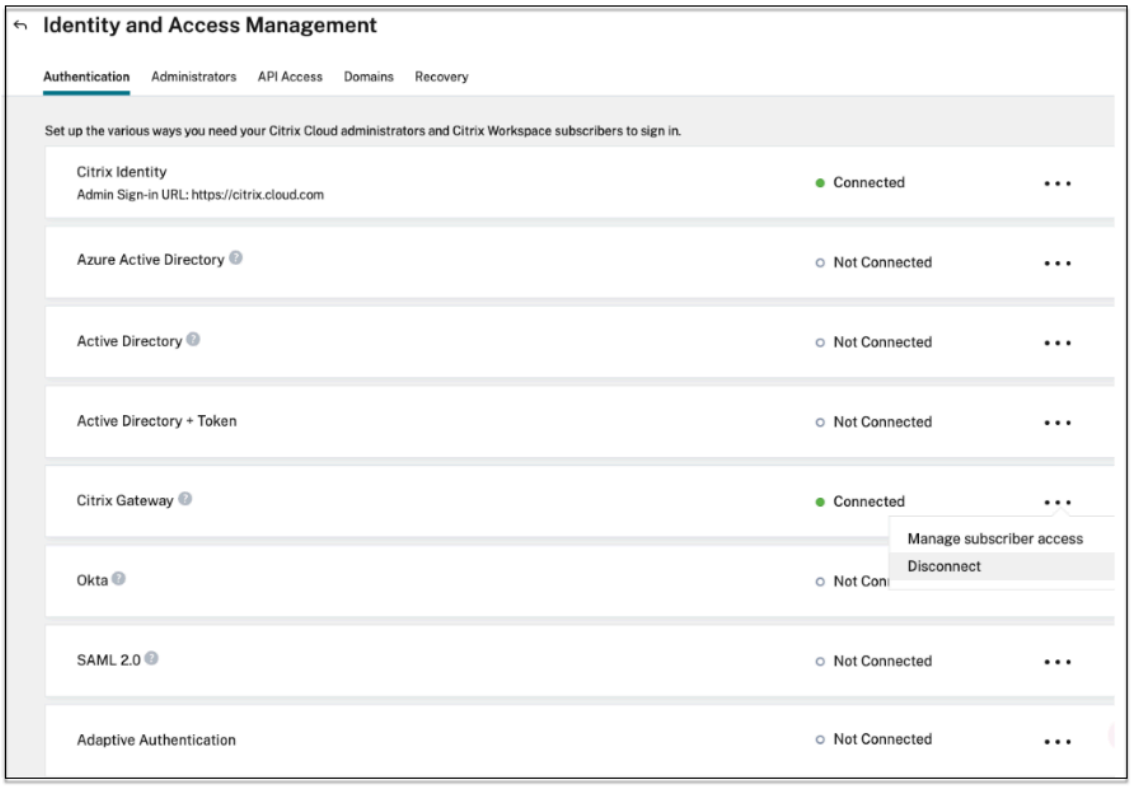
To get this feature enabled, reach out to Citrix Support.

Migrate your authentication method to Adaptive Authentication

Customers already using Adaptive Authentication with authentication method as **Citrix Gateway** must migrate **Adaptive Authentication** and then remove the OAuth configuration from the Adaptive Authentication instance.

1. Switch to a different authentication method other than Citrix Gateway.
2. In **Citrix Cloud > Identity and Access Management**, click the ellipsis button corresponding to Citrix Gateway and then click **Disconnect**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



3. Select **I understand the impact on the subscriber experience**, and then click **Confirm**.

   When you click **Confirm**, the workspace login to end users is impacted and Adaptive Authentication is not used for authentication until Adaptive Authentication is enabled again.

4. In the Adaptive Authentication instance management console, remove the OAuth related configuration.

   By using the CLI:

   ```
   unbind authentication vs <authvsName> -policy <oauthIdpPolName>
   rm authentication oauthIdpPolicy <oauthIdpPolName>
   rm authentication oauthIdpProfile <oauthIdpProfName>
   <!--NeedCopy-->
   ```

   By using the GUI:

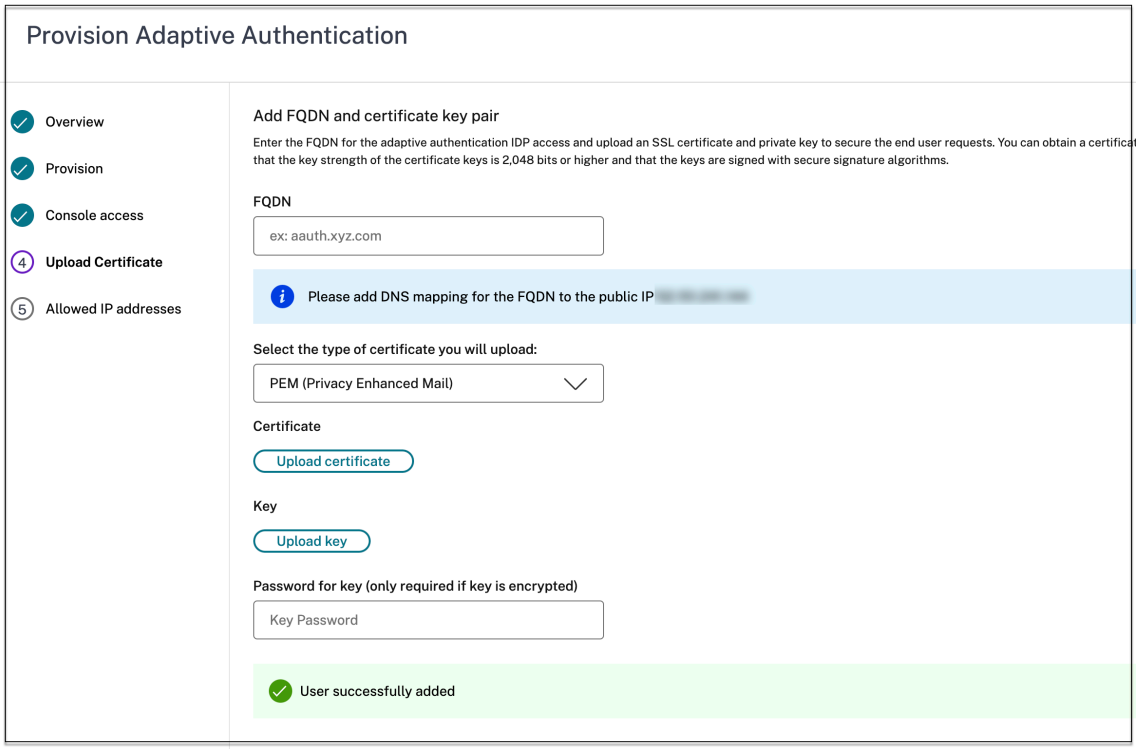
   a) Navigate to **Security > AAA - Application Traffic > Virtual Servers**.
   b) Unbind the OAuth policy.
   c) Navigate to **Security > AAA - Application Traffic > Policies > Authentication > Advanced Policies > OAuth IDP**.
   d) Delete the OAuth policy and profile.

5. Navigate to **Citrix Cloud > Identity and Access Management**.
   In the Authentication tab, in Adaptive Authentication, click the ellipsis menu and select **Manage**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

OR access https://adaptive-authentication.cloud.com

6. Click **See Details**.
7. In the **Upload Certificate** screen, do the following:
   - Add the Adaptive Authentication FQDN.
   - Remove the certificates and key files and upload it again.



> **Important:**
>
> If you edit an FQDN or the certificate-key pair directly without migrating to **Adaptive Authentication**, connection to Identity and Access Management fails and the following errors are displayed. You must migrate to the Adaptive Authentication method to fix these errors.
>
> - ADC command failed with an error. A policy is already bound to the specified priority.
> - ADC command failed with an error. Cannot unbind a policy that is not bound.

8. Click **Save Changes**.

   At this point, Identity and Access Management displays **Adaptive Authentication** as **Connected** and the Adaptive Authentication instance has the OAuth profile auto configured.

   You can validate this from the GUI.

   a) Access your Adaptive Authentication instance and log in with your credentials.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

b) Navigate to **Security > AAA - Application Traffic > Virtual Servers**. You must see that the OAuth IdP profile created.
c) Navigate to **Citrix Cloud > Identity and Access Management**. Adaptive Authentication is in the **Connected** status.

9. Enable the Adaptive Authentication method again by clicking **Enable** (step 3) in the Adaptive Authentication home page.

This step enables the authentication method as Adaptive Authentication in your workspace configuration.

10. Click the workspace link on step 3 after clicking **Enable**. You must see that the authentication method is changed to Adaptive Authentication.

> **Note:**
>
> New users must follow the same steps excluding the step to remove the OAuth related configuration.

Sample authentication configurations

Customers can configure an authentication policy of their choice and bind it to the authentication virtual server. Authentication profile bindings are not required for the authentication virtual server. Only the authentication policies can be configured. The following are some of the use cases.

> **Important:**
>
> Authentication configuration must be done on the primary nodes only.

Multifactor authentication with conditional authentication

- Dual factor authentication with LDAP and RADIUS using dual factor schema (taking user input only once)
- Authentication log on method according to user's departments (Employee, Partner, Vendor) in organization with drop-down menu to select the department
- Authentication log on method according to user domains with drop-down menu
- Configure email ID (or user name) input as first factor with conditional access based on group extraction with email ID at first factor and provide different logon type for each group

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Multifactor authentication using Certificate authentication for users with user certificates and Native OTP registration for non-cert users
- Different authentication type with conditional authentication according to user host name inputs
- Dual factor authentication with Native OTP authentication
- Google Re-CAPTCHA

Third-party integration with multifactor authentication

- Configure Azure AD as SAML IdP (Configure next factor as LDAP policy - NO_AUTH to complete OAuth trust)
- Conditional authentication with First factor as SAML and then custom login to certificate or LDAP based on SAML attributes
- First factor as webauth login followed by LDAP

Device posture scans (EPA)

- Device posture check for version check followed by customized login for compliant (RADIUS) and non-compliant users(LDAP)
- LDAP authentication followed by mandatory device posture scan
- Device posture check before and after AD authentication - Pre and Post-EPA as a factor
- Device Certificate as an EPA factor

Miscellaneous scenarios

- Add EULA with authentication
- Customize nFactor policy labels, login schema

Disk space management for instances

February 22, 2024

The Adaptive Authentication team manages all upgrades and maintenance of Adaptive Authentication instances. Therefore, it is recommended that you do not upgrade or downgrade the Adaptive Authentication instances to random RTM builds. Citrix manages the Adaptive Authentication instances, by default.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

For the instance upgrades, a minimum of 7 GB space is required in the VAR directory. Therefore, the Adaptive Authentication service team clears the disk space on the instances before applying upgrades. It is recommended that you do not keep any sensitive, proprietary, or personal information in the following directories:

- /var/core
- /var/crash
- /var/tmp
- /var/nsinstall
- /var/nstrace
- /var/nslog

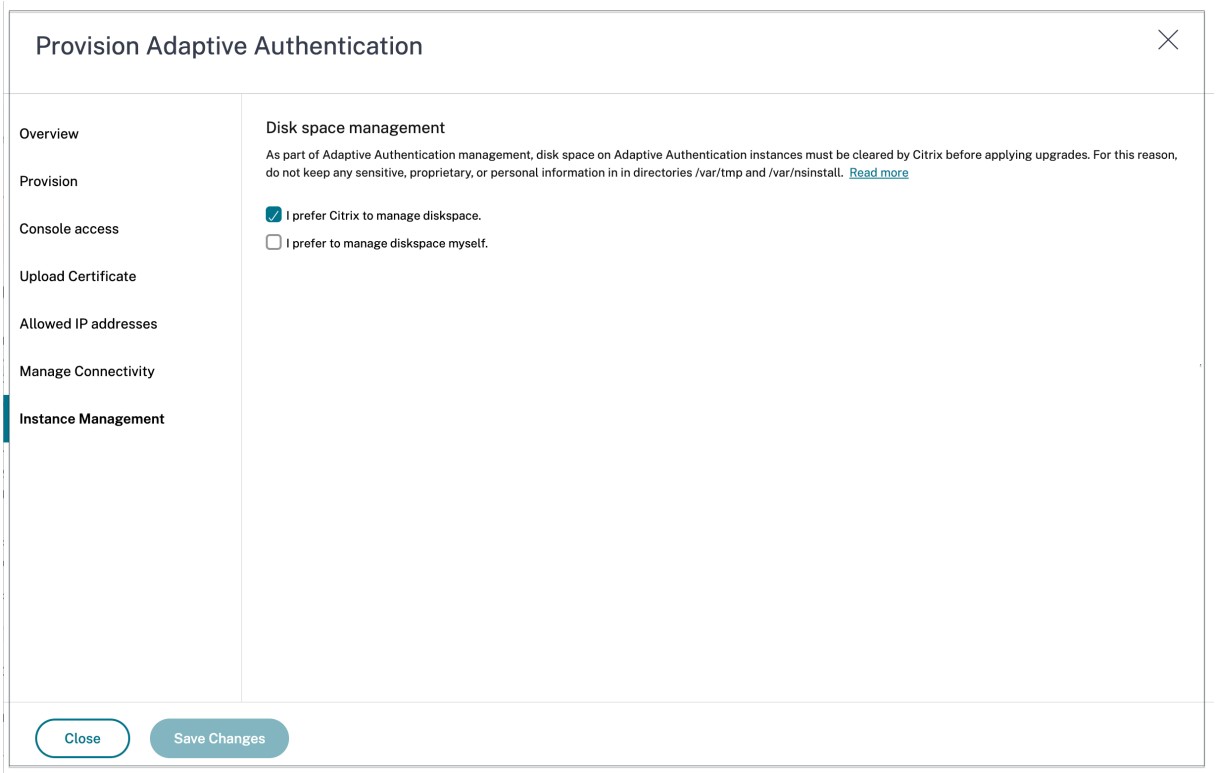
> **Note:**
>
> - The /var/nsinstall directory is cleared first during the upgrade followed by the /var/tmp directory. If the minimum space requirement is still not met, then the other directories (/var/-core, /var/crash, /var/nstracem, and /var/nslog) are cleared as well.
> - The customer is responsible for managing and maintaining the NetScaler disk space and disk clean-up.

Option to manage disk space yourself

Though Citrix manages the Adaptive Authentication instances, by default, you can prefer to clean up the disk space on the instances yourself. You can opt out of the default method by doing the following:

1. In the Adaptive Authentication navigation pane, click **Instance Management**.
2. Select **I prefer to manage diskspace myself** and then click **Confirm** in the confirmation message dialog box.
3. Click **Save Changes**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



> **Note:**
>
> You can also schedule upgrades according to your customer traffic. The Citrix Cloud team then upgrades your instances accordingly.
> For information about scheduling upgrades, see Schedule upgrade of your Adaptive Authentication instances.

Troubleshoot Adaptive Authentication issues

August 17, 2023

The issues are categorized based on the different stages in the configuration:

- Provisioning
- Instance accessibility issue
- AD/Radius connectivity and authentication issue
- Authentication issues
- EPA/device posture-related issues
- Smart tag-related issues
- Log collection

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

You can troubleshoot the issues using the Adaptive Authentication CLI as well. To connect to the CLI, do the following:

- Download SSH client like putty/securecrt on your machine.
- Access the Adaptive Authentication instance using the management IP (primary) address.
- Login with your credentials.

For details, see Access a NetScaler appliance.

Enable logging of adaptive authentication logs

Make sure that you enable the log levels to capture the adaptive authentication logs.

Enable logs using CLI:

1. Log in to the Adaptive Authentication instance CLI.
2. Using PuTTY, enter the management credentials.
3. Run the command `set audit syslogParams logLevel ALL`

Enable logs using GUI:

1. Log in to the Adaptive Authentication instance using a browser.
2. Navigate to **Configuration > System > Auditing**.
3. In the Auditing page, under **Settings**, click **Change Auditing syslog Settings**.
4. In **Log Levels**, select **ALL.**

Provisioning issues

- **Unable to access the Adaptive Authentication UI**

  Check if the entitlement is enabled for your customer ID/tenant.

- **Stuck in the provisioning page for more than 45 min**

  Collect the screenshot of the error, if any, and then contact Citrix Support for assistance.

- **VNet peer is down**

  - Check if there are alerts in the Azure Portal corresponding to this peering and take the recommended actions.
  - Delete the peering, add it again from the Adaptive Authentication UI.

- **Deprovisioning is not complete**

  Contact Citrix Support for assistance.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Instance accessibility issue

- **Management IP address is not accessible for the instance**
  - Check if the client's public IP address used for access is among the allowed source IP addresses.
  - Validate if there is any proxy changing the client source IP address.
- **Unable to log in to the instance**

  Make sure that the admin access is working fine with the credentials you entered during provisioning.
- **End users do not have complete rights**

  Make sure while adding the user, you have bound the suitable command policy for access. For more information, see User, user groups, and command policies.

AD or RADIUS connectivity issue

Issue with Azure Vnet peering connectivity type:

- Check if the customer managed Azure VNet is reachable from the Adaptive Authentication instances.
- Check if connectivity/reachability from customer managed Azure VNet to AD is working.
- Ensure that appropriate routes are added to direct traffic from on-premises to Azure VNets.

Windows based Connector:

- All logs are available in the directory /var/log/ns.log and each log is prefixed with [NS_AAUTH_TUNNEL].
- ConnectionID from logs can be used to correlate different transactions.
- Ensure that the private IP address of the connector virtual machine is added as one of the RADIUS clients in the RADIUS server because that IP address is the source IP address for the connector.

  For every authentication request, the tunnel is established between the Adaptive Authentication Instance (NS - AAAD process) and the authentication server. Once the tunnel is established successfully, authentication occurs.

  Make sure that the connector virtual machine can resolve the Adaptive Authentication FQDN.
- Connector is installed however the on-premises connectivity fails.

  Validate if NSAUTH-TUNNEL is getting established.

  ```
  cat ns.log | grep -I “tunnel”
  ```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

If the following sample log is not printed in the ns.log file for the authentication request, then there might be an issue while establishing a tunnel or some issue from the connector side.

```
LDAP:
[NS_AAUTH_TUNNEL] Entering bitpump for
Connection1 => Src : 192.168.0.7:28098, Dst : 10.106.103.60:636 ,
    Connection2 => Src : 10.106.103.70:2271, Dst :
   10.106.103.80:443"
RADIUS:
[NS_AAUTH_UDP_TUNNEL] MUX channel established"
<!--NeedCopy-->
```

Check the log details and take actions appropriately.

Log details	Corrective action
No logs with prefix `[NS_AAUTH_TUNNEL]` are included in the log file	Run the `show cloudtunnel vserver` command. This command must list both (TCP and UDP) cloud tunnel virtual server with the state "UP."
`[NS_AAUTH_TUNNEL] Waiting for outbound from connector` For this log, if the following response is not received: `[NS-AAUTH-TUNNEL] Received connect command from connector and client connection lookupsucceeded"`	Check if the connector machine is able to reach to the Adaptive Authentication FQDN **OR** check the connector side firewall for outbound connections to the Adaptive Authentication FQDN
`[NS_AAUTH_TUNNEL] Server is down or couldn't create connection to ip 0.0.0.0` and `[NS_AAUTH_TUNNEL] Connect response code 401 is not 200 OK, bailing out"`	Reach out to Citrix Support.

No response from connector:

- Make sure that Adaptive Authentication FQDN is reachable from the connector virtual machine.
- Make sure that you have an intermediate certificate bound and linked to the server certificate on the Adaptive Authentication instance.

Incorrect LDAP/RADIUS settings:

If your AD/RADIUS server IP address is a public IP address, you must add the subnet or the IP addressing the expressions in NetScaler. Do not edit the existing ranges.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- To add a subnet or IP address by using the CLI:

```
set policy expression aauth_allow_rfc1918_subnets "(CLIENT.IP.DST
    .BETWEEN(10.0.0.0,10.255.255.255) || CLIENT.IP.DST.BETWEEN
    (172.16.0.0,172.31.255.255) || CLIENT.IP.DST.BETWEEN
    (192.168.0.0, 192.168.255.255) || CLIENT.IP.DST.BETWEEN
    (13.14.0.0, 13.14.255.255)||CLIENT.IP.DST.EQ(1.2.5.4))"
<!--NeedCopy-->
```

- To add a subnet or IP address by using the GUI:

  1. Navigate to **Appexpert > Expressions**.
  2. Add expression **aauth_allow_rfc1918_subnets**.

If the tunnel is established but still authentication fails, use the following steps to troubleshoot the issue.

LDAP:

- Validate the Bind DN details.
- Use test connectivity to confirm the error.
- Validate the errors using `aaad` debug.
- Log in to the Adaptive Authentication instance by using the CLI.

```
shell
cd /tmp
cat aaad.debug
<!--NeedCopy-->
```

Common LDAP errors:

- Server time out –No response from the connector for the LDAP query.
- Other LDAP errors, see https://support.citrix.com/article/CTX138663.

Radius:

- Connector IP address must be added as the RADIUS client source IP address in the RADIUS server configuration.

Authentication issues

- **Post assertion errors for OAuth**
  - Make sure that all the claims are provided by AD. You need 7 claims for this to be successful.
  - Validate the logs in /var/log/ns.log to locate the error for OAuth failures.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
cat /var/log/ns.log
<!--NeedCopy-->
```

  - Validate the OAuth profile parameters.

- **Azure AD authentication stuck at post assertion**

  Add AD authentication as the next factor with authentication set to off. This is to get all the required claims for successful authentication.

EPA related issues

- **Plug-in is already present but the user is getting a prompt to download the plug-in.**

  Possible causes: Version mismatch or corrupt files

  - Run developer tools and validate if the plug-in list file contains the same version as that of the NetScaler and your client machine.
  - Make sure that the client version on the NetScaler is the same as on the client machine.

    Update the client on the NetScaler.

    On the Adaptive Authentication instance, navigate to **Citrix Gateway > Global Settings > Update client libraries**.

    The EPA plug-in libraries page on Citrix Downloads provides you the detailed information.
  - At times, the request can be cached on NetScaler even if the version is updated.

    `show cache object` displays the cached plug-in details. You can delete it by using the command;

    ```
    flush cache object -locator 0x00000023345600000007
    ```

  For details on EPA log collection, see https://support.citrix.com/article/CTX209148.

- **Is there a way to revert the EPA settings (Always, Yes, No) after the user has selected an option.**

  Currently, EPA settings revert is done manually.

  - On the client machine, navigate to C:\Users<user_name>\AppData\Local\Citrix\AGEE.
  - Open the `config.js` file and set trustAlways to null - `"trustAlways":null`

Smart access tag issues

- **After configuring the smart access, applications are not available**

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Make sure that the tags are defined on both the Adaptive Authentication instance and the Citrix VDA delivery groups.

Check that the tags are added on the Workspace delivery group in all capitals.

You can collect the ns.log and reach out to Citrix Support if this does not work.

General log collection for Adaptive authentication instance

- Technical support bundle: For details, see How to collect the technical support bundle from SDX and VPX appliances for insight analysis.
- Trace files. For details, see How to record a packet trace on NetScaler.

Contact Citrix Support for guidance.

Smart access using Adaptive Authentication

December 20, 2023

Citrix Cloud customers can provide smart access (Adaptive Access) to the Citrix DaaS resources (virtual apps and desktops) or the Secure Private Access service using Adaptive Authentication as an IdP to Citrix Workspace.

The Smart Access feature allows the Adaptive Authentication service to surface all the policy information about the user to Citrix Workspace or Citrix DaaS. The Adaptive Authentication service can provide device posture (EPA), network location (inside or outside the corporate network, geo-location), user attributes like user groups, time of day or a combination of these parameters as part of the policy information. The Citrix DaaS administrator can then use this policy information to configure contextual access to the virtual apps and desktops. The virtual apps and desktops can either be enumerated or not based on the earlier parameters (access policy). Some user actions such as clipboard access, printer redirection, client drive, or USB mapping can also be controlled.

Example use cases:

- The administrator can configure the group of apps to be displayed or accessed only from specific network locations like the corporate network.
- The administrator can configure the group of apps to be displayed or accessed only from corporate managed devices. For example, EPA scans can check whether the device is a corporate managed or BYOD. Based on the EPA scan result, the relevant apps can be enumerated for the user.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Pre-requisites

- Adaptive Authentication as an IdP must be configured for Citrix Workspace. For details, see Adaptive Authentication service.
- Adaptive Authentication service with Citrix DaaS is up and running.
- The Adaptive Access feature is enabled. For details, see Enable Adaptive Access.

Understanding the flow of events for smart access

1. The user logs in to Citrix Workspace.
2. The user gets redirected to the Adaptive Authentication service configured as an IdP.
3. The user is prompted for pre-authentication (EPA) or authentication.
4. The user is successfully authenticated.
5. Smart access policies are evaluated according to the configuration and tags are associated with the user session.
6. The Adaptive Authentication service pushes the tags to the Citrix Graph service. The user is redirected to the Citrix Workspace landing page.
7. Citrix Workspace fetches the policy information for this user session, matches the filter, and evaluates the apps or desktops that must be enumerated.
8. Admin configures the access policy on Citrix DaaS to restrict the ICA access for users.

Configuration of Smart access policies on Adaptive Authentication instances

Configuring smart access policies on an Adaptive Authentication instance is a two-step process:

1. Define smart access policies with smart access tags on Adaptive Authentication instances. For example, see *Step 1*.
2. Define the same tags on your DaaS/Secure Private Access for resource access. For example, see *Step 2*.

Use case 1: Configure a smart access policy to allow access to users logging in from the Chrome browser and block clipboard access for them

Step 1: Configure smart access policies with smart tags on Adaptive Authentication instance

1. Log in to the Adaptive Authentication instance.
2. Navigate to Adaptive Authentication virtual server (**Security > AAA - Application Traffic > Virtual Servers**).
3. Select the authentication virtual server and then click **Edit**.

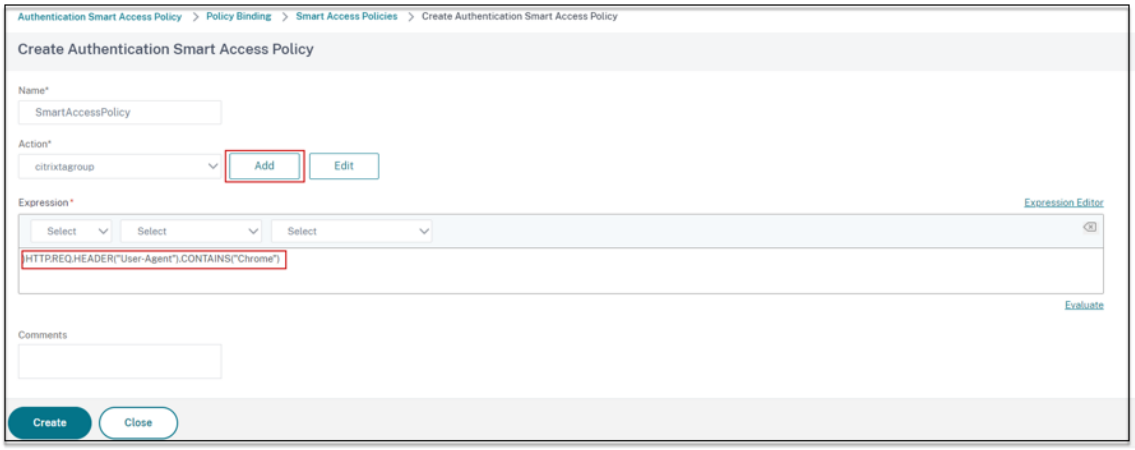
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

4. Click **Smart Access Policies**.
5. Define the expression of the policy according to your requirement.

    a) Click **Add Binding**.
    b) In **Select Policy**, click **Add**.
    c) Enter a name for the smart access policy.
    d) Define the expression.

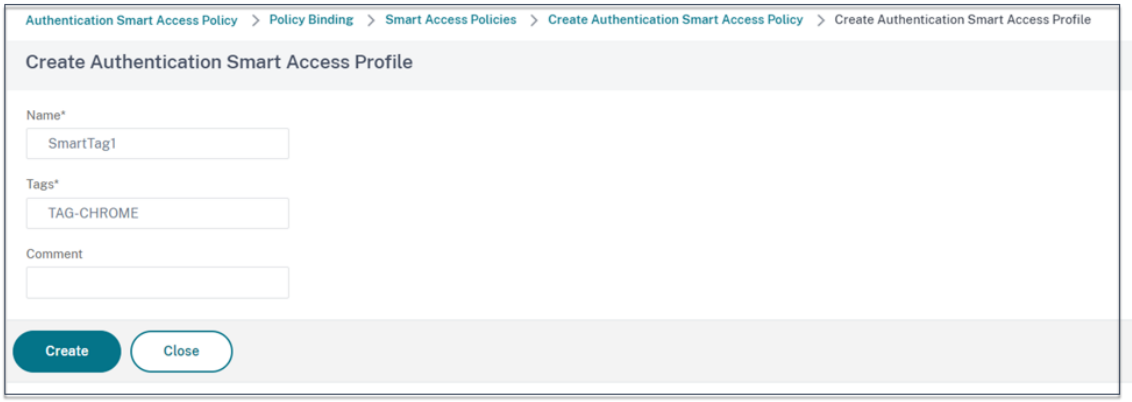
    For the example of allowing access for users logging in from a Chrome browser, enter the expression `HTTP.REQ.HEADER("User-Agent").CONTAINS("Chrome")`

    Similarly, you can create expressions based on the time, user login, authentication and authorization group, and other options.



6. Now, create smart tags and bind these tags to the smart access policy.

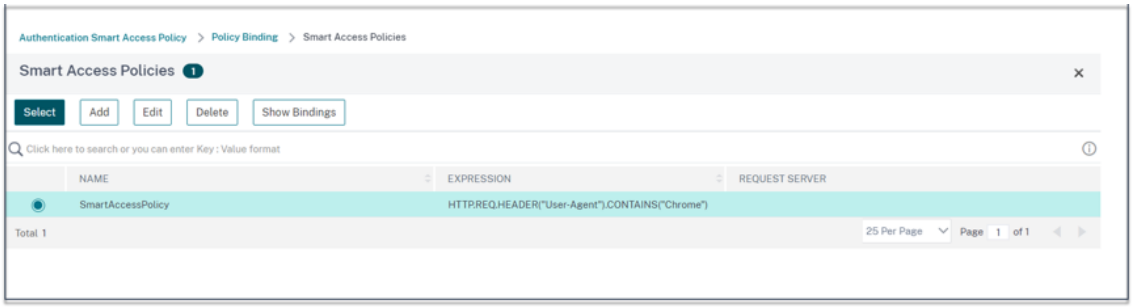
    a) In **Action**, click **Add**.
    b) In **Name**, type a name for the smart access profile.
    c) In **Tags**, define the smart access tags. For example, TAG-CHROME.



    a) Click **Create**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

b) Select the smart access policy and click **Add Binding**.
c) Bind this smart access tag to the smart access policy created earlier.



> **Note:**
>
> You can also create a smart access policy from **Security >AAA - Application Traffic > Policies > Authentication > Advanced Policies > Smart Access > Policies** and then bind it to the authentication virtual server.

Step 2: Define smart access tags in DaaS Studio

1. Add the policies with the smart tag "TAG-CHROME". For details, see Define tags in Citrix Studio.

Use case 2: Configure smart access policies based on EPA results, for post authentication

Step 1: Configure smart access policies with smart tags on Adaptive Authentication instance
For smart access based on conditions like end point analysis, configure nFactor flow, define an EPA action, and then add the default group.

To configure EPA as a factor in nFactor flow, see Configure EPA as a factor.

Logical flow

1. The user accesses the Workspace URL.
2. The user is redirected to Adaptive Authentication for authentication/EPA.
3. End point analysis is done on the end user and the results are stored by adding the user to the defined default group.
4. The user is prompted for the next authentication flow.
5. Smart access policies are evaluated and the user is assigned the smart access tags.

Configuration

Users accessing from a machine with antivirus installed must be marked as compliant and provided with full access. However, user machines without antivirus must be marked non-compliant and pro-

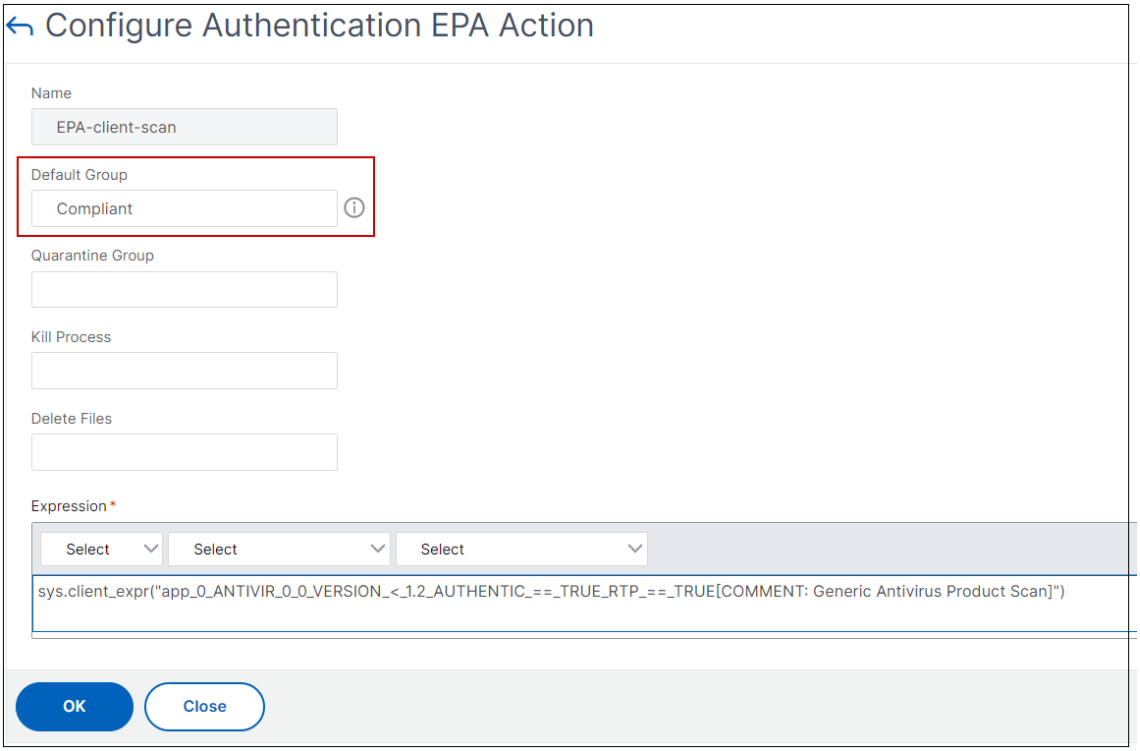
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

vided with limited access.

1. Create an nFactor policy for EPA. For details, see Configure EPA as a factor.

   In the nFactor flow, ensure that the first is a user authentication factor.

2. Select the EPA expression to check if the antivirus is present or not.
3. In the EPA action define the default group.



   User is added to this default group if EPA runs as success.

4. Now, create smart access policies

   a) Log in to the Adaptive Authentication instance.

   b) Navigate to Adaptive Authentication virtual server (**Security > AAA - Application Traffic > Virtual Servers**).

   c) Select the Adaptive Authentication virtual server and click **Edit**.

   d) Click **Smart Access Policies**.

   e) Create two smart access policies with the following expressions.

      - AAA.USER.IS_MEMBER_OF (“Compliant”) - For the user EPA pass condition
      - !AAA.USER.IS_MEMBER_OF (“Compliant”) –For the user EPA fail condition

   f) Define smart access tags for both of these policies.

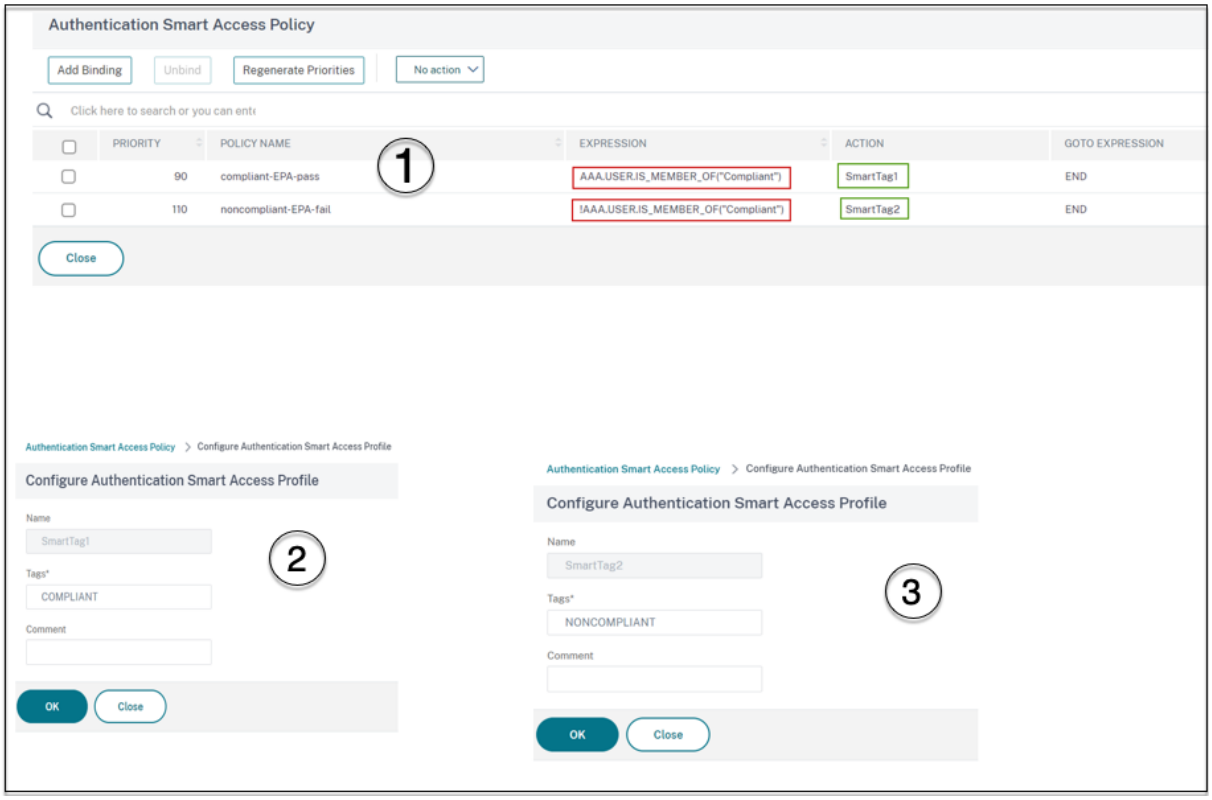
      Example:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Tag name `SmartTag1` with the tag COMPLIANT for `AAA.USER.IS_MEMBER_OF ("Compliant")`
- Tag name `SmartTag2` with the tag NONCOMPLIANT for `!AAA.USER.IS_MEMBER_OF ("Compliant")`

Adaptive Authentication instance configuration with conditions as EPA for smart access is now complete.

You can configure the tags and expression according to your requirements.



Step 2: Configure smart access tags in DaaS Studio Add the policies with smart tags "COMPLIANT"and "NONCOMPLIANT"in the respective delivery groups. For details, see Define tags in Citrix Studio.

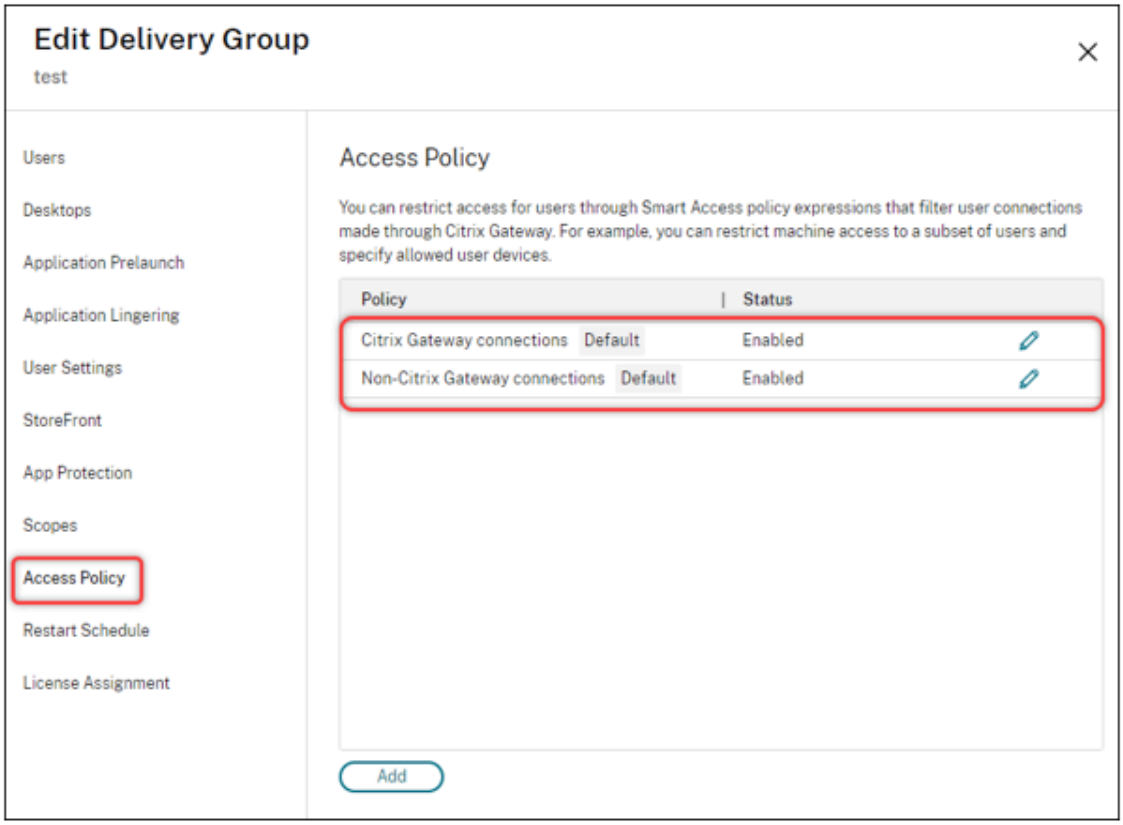
Define tags in DaaS studio

Define tags in delivery groups to restrict the application enumeration for users.

Example: BranchOffice users must see applications from the **Adaptive Access Delivery group** which has all the applications.
Whereas, WorkfromHome users must see applications from **WFH Delivery Group**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

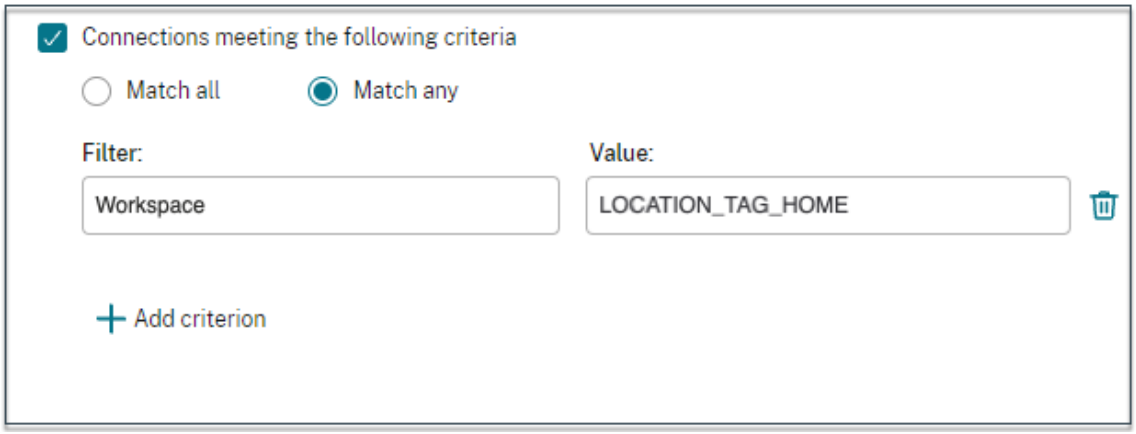
1. Sign into Citrix Cloud.
2. Select **My Services > DaaS**.
3. Click **Manage**.
4. Create delivery groups as per your requirement. For details, see Create delivery groups.
5. Select the delivery group that you have created and click **Edit Delivery Group**.



6. Click **Access Policy**.
7. For customers using adaptive access within the Citrix Workspace platform, perform the following steps to restrict access for a delivery group to internal networks only:

    a) Right-click the delivery group and select **Edit**.
    b) Select the access policy in the left pane.
    c) Click the edit icon to modify the default Citrix Gateway connections policy.
    d) On the Edit policy page, select **Connections meeting the following criteri**a, select **Match any**, and then add the criteria.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



For WorkFromHome users, enter the following values in the respective delivery controller.

Farm: Workspace

Filter: LOCATION_TAG_HOME

For BranchOffice users, enter the following values in the respective delivery controller.

Filter: Workspace

Value: LOCATION_TAG_BRANCHOFFICE

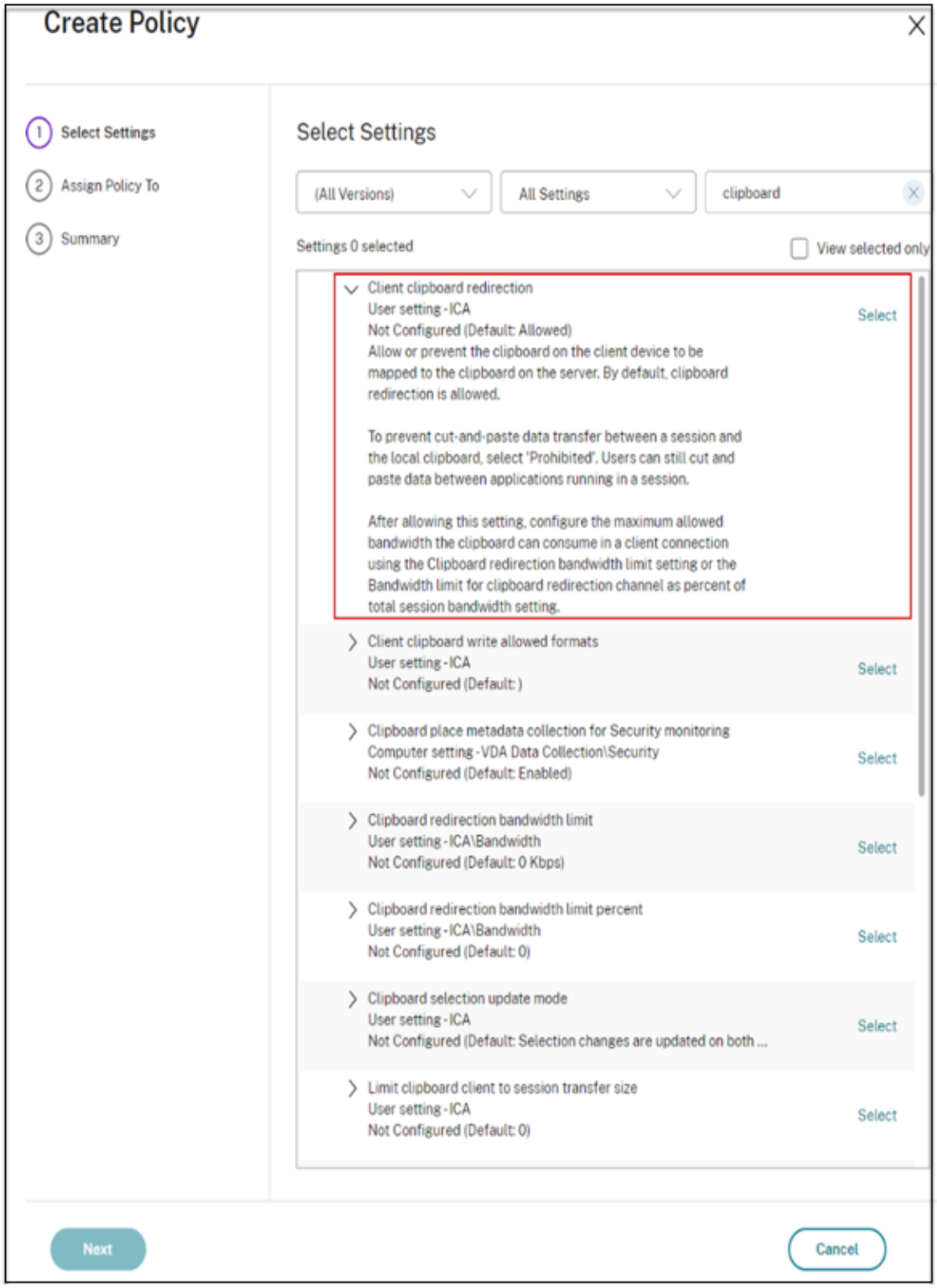
You can now use these tags to restrict access to your applications.

Restrict the type of access for the provided applications

Example: Work from home users must not have clipboard rights.

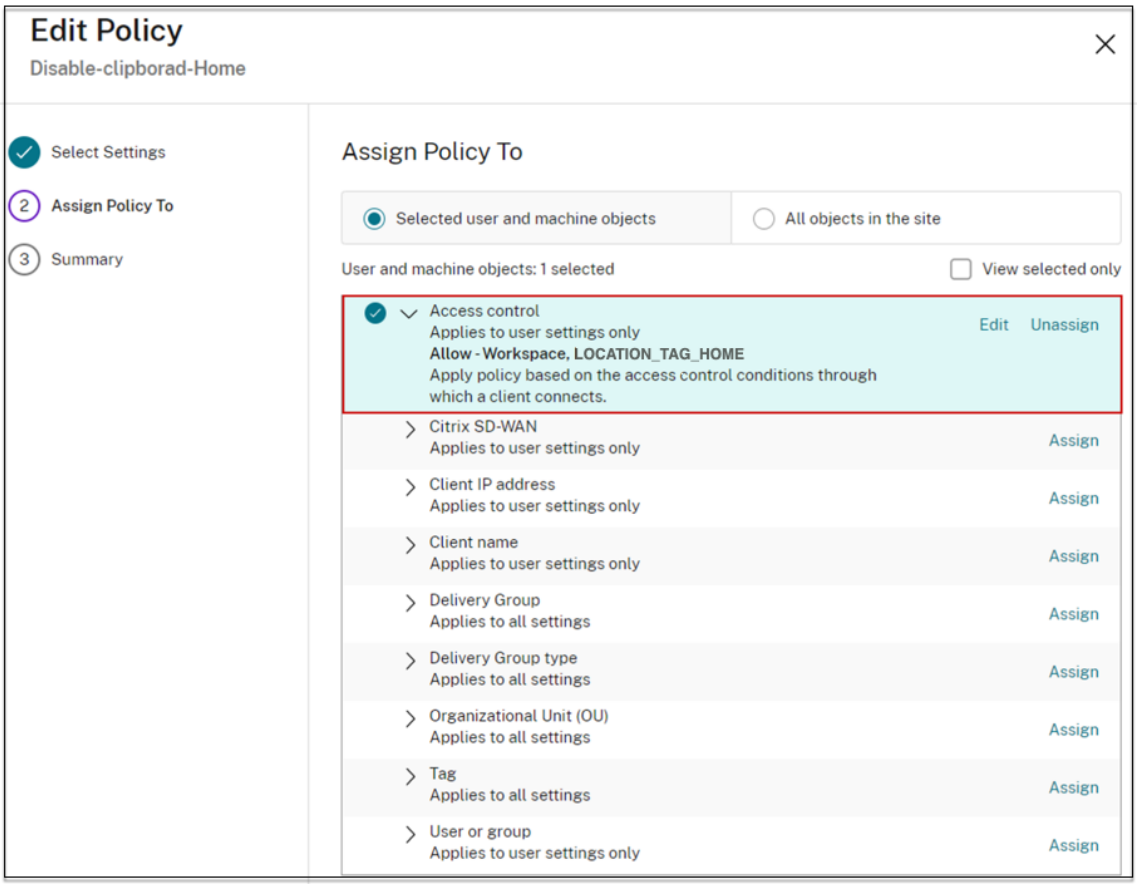
1. In DaaS Studio, navigate to **Policies** and click **Create Policy**.
2. In the **Create Policy** page, select the setting for which you want to allow or prohibit access.
3. click **Select**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



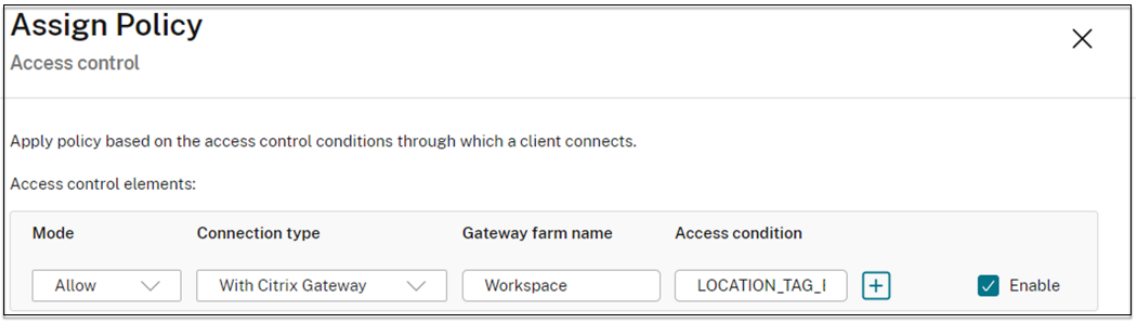
4. In the **Edit Setting** page, click **Allowed** or **Prohibited** and then click **Save.**
5. Click **Next**.
6. In the **Assign Policy to** page, select **Access control** and then click **Next**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



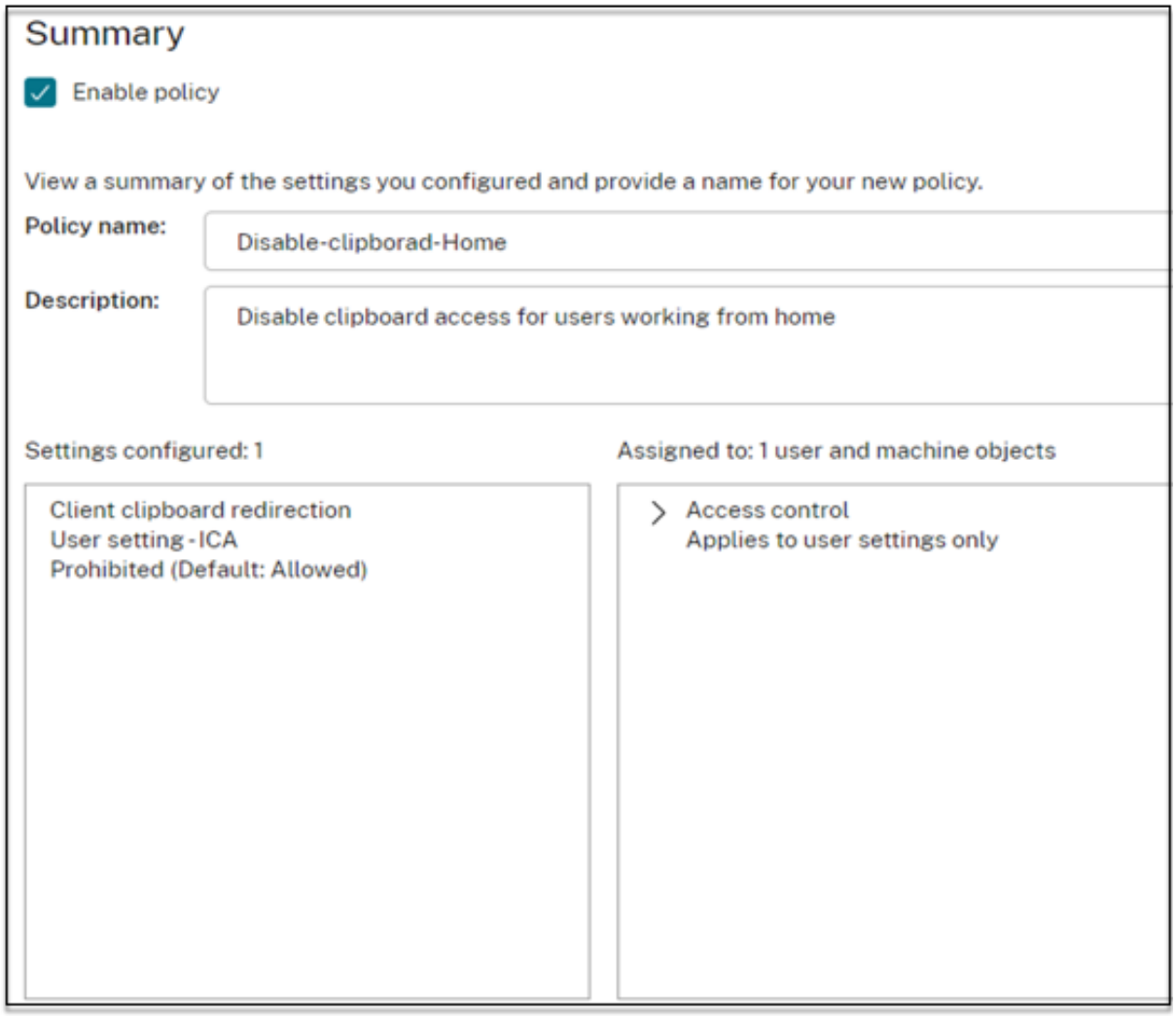
7. Define a policy with the following details:

   - **Mode**: - Allow
   - **Connection type**: - With Citrix Gateway
   - **Farm name**: - Workspace
   - **Access Condition**: LOCATION_TAG_HOME (all upper case)



8. Click **Next** and enter a name for the policy.
9. Click **Finish**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



You're now all set to test your access.

Troubleshooting common errors

- **Issue:** You see the message "Cannot Complete your Request".

  Resolution

  1. Ensure that Adaptive Access is enabled. For details, see Enable Adaptive Access.
  2. If the feature isn't enabled, Contact Citrix Support.

- **Issue:** No apps or desktops are published.

  This issue might occur if the smart tags aren't pushed from Adaptive Authentication to the workspace or aren't received at DaaS or Secure Private Access.

  Resolution:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Check if smart access policies are getting hit. For details see https://support.citrix.com/article/CTX138840.
- Check if the Citrix Adaptive Authentication instance is able to connect to `cas.citrix.com`.
- Check the Adaptive Authentication instance for details on the smart tags.
  * Ensure that in the `set audit syslogParams` command, the logLevel parameter is set to `ALL` on all instances.
  * Log in to the Adaptive Authentication primary instance using putty.

    Type shell
    `cd /var/log`cat ns.log | more or cat ns.log | grep -I “smartaccess”‘
- If these do not resolve the issue, contact Citrix Support.

Configuration changes for a high availability setup

Sometime there might be a delayed file synchronization in a high availability setup in the following directories. As a result, the keys created during Citrix ADM registration aren’t read on time.

- /var/mastools/conf/agent.conf
- /var/mastools/trust/.ssh/private.pem
- /var/mastools/trust/.ssh/public.pem

To address the file synchronization issue, perform the following steps to rerun the `set cloud` command on the secondary.

```
> shell cat /var/mastools/conf/agent.conf
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<mps_agent>
<uuid>temp_str</uuid>
<url>fuji.agent.adm.cloud.com</url>
<customerid>customer_id</customerid>
<instanceid>instance_id</instanceid>
<servicename>MAS</servicename>
<download_service_url>download.citrixnetworkapistaging.net</
   download_service_url>
<abdp_url>fuji.agent.adm.cloud.com</abdp_url>
<msg_router_url>fuji.agent.adm.cloud.com</msg_router_url>
</mps_agent> Done
> set cloud param -CustomerID customer_id -InstanceID instance_id -
   Deployment Production
<!--NeedCopy-->
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Sizing and performance guidelines

November 2, 2023

Adaptive Authentication provides customers access to their on-premises authentication servers using either Cloud Connectors deployed in their data centers or Azure VNet Peering in case data center reachability is already established from the customer managed VNet. This topic contains information on the performance numbers for both Citrix Cloud Connector and Azure VNet Peering deployments and also the recommended scale and size configurations for Citrix Cloud Connector machines.

User authentication rate

A connector virtual machine of size 2 vCPUs and 7 GB RAM can authenticate 14 users/sec.

By default, the connector service is configured to auto-restart twice if there's a failure or a crash. In the subsequent failure or a crash, the service stops. Also currently, the connector service fails if the authentication rate is increased beyond 4 authentications/sec. This rate can be achieved by configuring the connector service to restart after any number of failures (**Citrix Netscaler Cloud Gateway > Recovery > Restart the service**). If this setting isn't configured, the rate drops to 4 authentications/sec.

Traffic latency and user authentication rate when using Citrix Cloud Connectors

The following table displays the traffic latency and the user authentication rate when using Citrix Cloud Connectors:

Authentication type	Authentication latency (p95) in ms	Authentication or user login rate per second
LDAP	5.99	14
RADIUS	3.17	14
LDAP+RADIUS	4.59	14
LDAPS	26.75	14
LDAPS+RADIUS	15.61	14

Traffic latency and user authentication rate when using Azure VNet Peering

The following table displays the traffic latency and the user authentication rate when using Azure VNet peering:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Authentication type	Request latency(p95) in ms	Authentication or user login rate per second
LDAP	6.95	17.54
LDAPS	7.19	16.98

Data Governance

February 6, 2024

This topic provides information regarding the collection, storage, and retention of logs by the Citrix Adaptive Authentication service and the Adaptive Authentication instances. Any capitalized terms not defined in Definitions carry the meaning specified in the Citrix End User Services Agreement.

- Adaptive Authentication services: Citrix Cloud service that administrators can log in to deploy and manage Adaptive Authentication instances.
- Adaptive Authentication instances: NetScaler virtual machines deployed by the Adaptive Authentication service to allow administrators to manage user authentication.

Data residency

Adaptive Authentication services

The Citrix Adaptive Authentication service customer content data resides in the Azure Cloud Services East region. They are replicated to the following Azure regions for availability and redundancy:

- US West
- North Europe

The following are the different destinations for the service configuration and runtime logs.

- Splunk service for system monitoring and debugging logs, in the US and EU (European Union) locations only.
- NetScaler Application Delivery Management service for the aggregated user access logs. For details, see NetScaler ADM Data Governance.
- Citrix Cloud System Logs service for admin audit logs. For details, see Citrix Cloud Services Customer Content and Log Handling and Geographical Considerations.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Adaptive Authentication instances

NetScaler Application Delivery Management service for backing up all configurations, instance specific artifacts. For details, see NetScaler ADM Data Governance.

Data collection

Citrix Adaptive Authentication service allows the customer administrators to configure the service through the Adaptive Authentication UI and the companion Connector Appliances through the console. The following customer content is collected:

- Adaptive Authentication service
  - FQDN (fully qualified domain name) and IP address of the IdP (identity provider) endpoint.
  - IP addresses/ranges, ports, and protocols
  - Certificates used to access the IdP authentication virtual server
  - Public IP address of the management endpoint
  - For Azure VNet peering, service principal with network contributor role. For details, see Set up connectivity to on-premises authentication servers using Azure VNet peering.
- User identifiers for app entitlements
- Citrix Cloud Connector related details. For details, see Citrix Cloud Connector.
  - IP addresses or FQDNs
  - Users, devices, and resource location identifiers
  - Internal proxy configuration

For runtime logs collected by the service components, the key information consists of the following:

- Client IP address and port
- Destination FQDN/address and port
- Client User-Agent
- Application URL path
- Application access time and duration
- Request byte count
- Response byte count
- HTTP transaction ID
- Deployment mode (Connector or Azure VNet peering)
- Azure resources
  - Resource group names
  - VNets (IP addresses, CIDRs)
  - Subnets (IP addresses, CIDRs)
  - Virtual machine names

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Data transmission

Citrix Adaptive Authentication service sends logs to the destinations (Splunk) protected by the transport layer security.

Data control

Citrix Adaptive Authentication service does not currently provide options for the customers to turn off sending logs or prevent customer content from being replicated globally.

Data retention

Based on the Citrix Cloud data retention policy, the customer configuration data is purged from the service 90 days (about 3 months) after subscription has expired.

The log destinations maintain their service-specific data retention policy.

- For the events stored in Citrix Application Delivery Management. See Citrix ADM Data Governance.
- The Splunk logs are archived and eventually removed after 90 days (about 3 months).
- The Adaptive Authentication instances are deallocated 30 days (about four and a half weeks) after the subscription has expired.

Data export

There are different data export options for several types of logs.

- The admin audit logs are accessible from the Citrix Cloud System Log console.
- The Splunk logs are not for customers to consume. These events can also be exported from Splunk as a CSV file.

Definitions

- Customer content means any data uploaded to a customer account for storage or data in a customer environment to which Citrix is provided access to perform the services.
- Log means a record of events related to the services, including records that measure performance, stability, usage, security, and support.
- Services mean that the Citrix Cloud services outlined earlier for the purposes of facilitating the customer use cases.

© 2024 Cloud Software Group, Inc. All rights reserved. Cloud Software Group, the Cloud Software Group logo, and other marks appearing herein are property of Cloud Software Group, Inc. and/or one or more of its subsidiaries, and may be registered with the U.S. Patent and Trademark Office and in other countries. All other marks are the property of their respective owner(s).