



Product Documentation

Configuring Remote Access with Citrix NetScaler Gateway

Imprivata Enterprise Access Management 24.2

Before You Begin

**NOTE:**

Beginning with 24.2, Imprivata OneSign and Imprivata Confirm ID have been renamed to Imprivata Enterprise Access Management.

Some interfaces in the Imprivata Admin Console, Imprivata Appliance Console, and documentation may retain the older Imprivata OneSign and Imprivata Confirm ID product names.

Before you begin your integration with Imprivata Confirm ID, familiarize yourself with the features of the product and how it affects your current remote access experience.

New Cloud Experience

- The Imprivata Cloud experience is a more robust architecture where the user authenticates with Imprivata directly with less chance of timeout or failure. Imprivata's connection to Active Directory means your AD group attributes are sent directly to Imprivata with less configuration required;
- You do not have to replace the LDAP connection between your gateway and Active Directory: You can easily maintain your existing single-factor remote access login experience while you roll out Imprivata Confirm ID Remote Access.
- The Imprivata cloud provides access to cloud-based features delivered in future versions of Imprivata Confirm ID.

How To Use Imprivata Confirm ID Remote Access

Before enabling Imprivata Confirm ID Remote Access, there are major decisions you need to make about how to use it.

- **Who do I want to use Imprivata Confirm ID Remote Access?** You control who uses Remote Access by organizing them into User Policies. If you want to roll out Remote Access to one department at a time, you will organize each department into a user policy.
- **How do I want users to enroll?** Your users need to enroll the Imprivata ID app, and/or their phone number for SMS code authentication. Your users can enroll remotely or on premises. For example, if a subset of your users rarely come into the office and must enroll from outside your network, place them into a user policy that allows enrolling remotely. You will configure these options for each user policy.
- **Do I want users logging in with password only?** Remote Access can be configured to allow users access into the VPN (RADIUS client) with password only until they enroll Imprivata ID or their phone number. This allows your users a grace period if they aren't ready or interested in enrolling right away. If you want to enforce stricter security, you can turn this off so users must use two-factor authentication for access into the VPN.
- **Do I want to prompt users to enroll?** You can turn off an enrollment reminder that appears each time users log into a computer with the Imprivata agent on premises.

- **What to do when a device is lost or stolen?** When a user calls in to report their device was lost or stolen, you can offer to generate a temporary code to allow two-factor authentication when logging in remotely. Set up this feature in advance of your deployment. See "Imprivata Temporary Codes" in the Imprivata Online Help.
- **Vendors with shared accounts?** If a temporary worker must use two-factor authentication but they should not install Imprivata ID, you can issue them a temporary code to use as their second factor. See "Imprivata Temporary Codes" in the Imprivata Online Help.
- **Does my solution organize remote access by Active Directory groups?** (Remote Access via RADIUS only) Review your current remote access policies to determine whether you limit remote access by AD groups. You need to configure Imprivata Confirm ID to send extended attributes via its RADIUS server so your gateway can allow and deny access by AD groups.

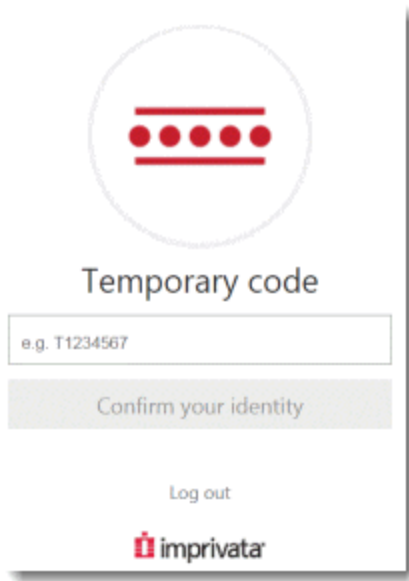
Optional — Temporary Codes

When Imprivata ID authentication is required to log in, but the user doesn't have his device or OTP token, Imprivata has made it easy for your enterprise to issue a temporary code allowing your user to continue their work virtually uninterrupted. Temporary codes can also be used when you need to provide remote access to a temporary user such as a contractor.

How It Works

In a typical Imprivata two-factor authentication workflow, the user must enter his password, then complete a second factor authentication via Imprivata ID, SMS code, or OTP token. If he doesn't have his device or token, he cannot log in. If he contacts your enterprise's helpdesk, you can issue him a temporary code:

1. The user contacts your help desk to report his device or OTP token was misplaced or stolen.
2. Your helpdesk verifies the user's identity and generates a temporary code with an expiration date.
3. The user logs in, using the temporary code when prompted (see image below).



He can use the temporary code until:

- The code expires
- He enrolls an Imprivata ID, phone number, or OTP token via the Imprivata agent
- He resumes using his typical second factor: Imprivata ID, SMS code, or OTP token authentication.

Who's Eligible

Temporary codes are only available for Remote Access and Imprivata ID for Windows Access. Temporary codes cannot be used for order signing or any other Imprivata workflow.

For complete details, see the Imprivata Online Help.

Optional: Skip Second Factor

1. In the Imprivata Admin Console, go to **Users > Workflow policy**.
2. Go to **Remote access workflows > Log In** and check **Allow users to skip the second factor on remembered devices for...**
3. Select how long the user can skip second factor (1 hour minimum — 120 days maximum). The default is 30 days.
4. Click **Save**.

About Skip Second Factor

- This feature does not turn off second factor for all remote access users: each user will be presented with the option **Remember device for X days** (30 days is the default).
- Skip Second Factor is an option for all users associated with the Remote Access Log In workflow.
- Skip Second Factor is available only for remote access gateways that use Imprivata cloud-based authentication with the Imprivata Confirm ID graphical user interface. The legacy RADIUS remote access experience does not support Skip Second Factor.

- **Remember device** — when selected, the user will not be prompted for a second factor on this browser on this computer for this Imprivata Confirm ID enterprise. Any other browsers and any other computers this user logs into will still enforce two factor authentication.

If the user logs in from other browsers (on the same computer or another computers) she can choose to skip second factor again.

- If she logs into another Imprivata Confirm ID enterprise from the same browser, her **Remember device** selection will not apply.
- **Cookies** — Skip Second Factor is not supported if cookies or local storage is disabled or deleted in the browser:
 - The browser must be able to create cookies when the user enables Skip Second Factor.
 - Later, the browser must be able to access those cookies when the user expects to skip second factor at subsequent logins.

Typical User Workflow

1. The user enters her username and password in the Imprivata Confirm ID interface at her remote access gateway.
2. She clicks **Log in**.
3. The interface for her second authentication method appears. With this feature enabled, she will also see a new option: **Remember device for 30 days** (the duration you selected above will appear here). A popup help message recommends **Use only for trusted workstations**.
4. The user selects this option.
5. The user completes her second factor authentication.

The user will not have to complete two factor authentication at this browser on this computer again until the period elapses.

Enforce Two Factor Authentication Again for One User

At any time, you can enforce two factor authentication again for a user that has selected to skip it. For example, if a user reports someone has access to her browser, or you have any other security concerns about a specific user:

1. In the Imprivata Admin Console, go to **Users > Users** and find the specific user.
2. Open the Edit User page.
3. In the section **Require second factor for log in**, click **Require 2FA on all devices**.
4. Click **Save**.

Two factor authentication is now enforced for this user; the next time this user completes two factor authentication, she can again choose to skip.

Revoking Skip Second Factor for All Users

At any time, you can enforce two factor authentication again for all users:

1. In the Imprivata Admin Console, go to **Users > Workflow policy**.
2. Go to **Remote access workflows > Log In** and un-check **Allow users to skip the second factor on remembered devices for...**
3. Click **Save**.

Two factor authentication is now enforced for all users. They will not be presented with the **Remember device** option again.

Revising Skip Second Factor for All Users

At any time, you can shorten or lengthen the duration of Skip Second Factor for all users:

1. In the Imprivata Admin Console, go to **Users > Workflow policy**.
2. Go to **Remote access workflows > Log In** and edit the value for **Allow users to skip the second factor on remembered devices for...**
3. Click **Save**.

If you have reduced the duration for Skip Second Factor, two factor authentication will be enforced for all users who already selected it if the new time period is already elapsed. The next time users complete two factor authentication, they can again choose to skip.

If you have extended the duration for Skip Second Factor, the new duration will be enforced for all users who already selected it and all forthcoming users.

Remote Access with Citrix NetScaler Gateway

Imprivata Confirm ID integrates with Citrix NetScaler Gateway to streamline authentication management and simplify two-factor authentication for remote access for employees. In addition to logging in remotely, Imprivata Confirm ID users can also enroll authentication methods from outside your network.

Imprivata Confirm ID also offers a customized user interface for Citrix NetScaler. When logging in remotely and enrolling authentication methods, the user interface resembles the Imprivata Confirm ID enrollment utility on the Imprivata agent.

Before You Begin

Review [Imprivata Confirm ID Supported Components](#) to confirm that your version of Citrix NetScaler Gateway is supported. Fully configure your Citrix NetScaler Gateway environment for remote access with single-factor username and password authentication before configuring its connection to Imprivata.

Diagram: Two-Factor Remote Access Authentication

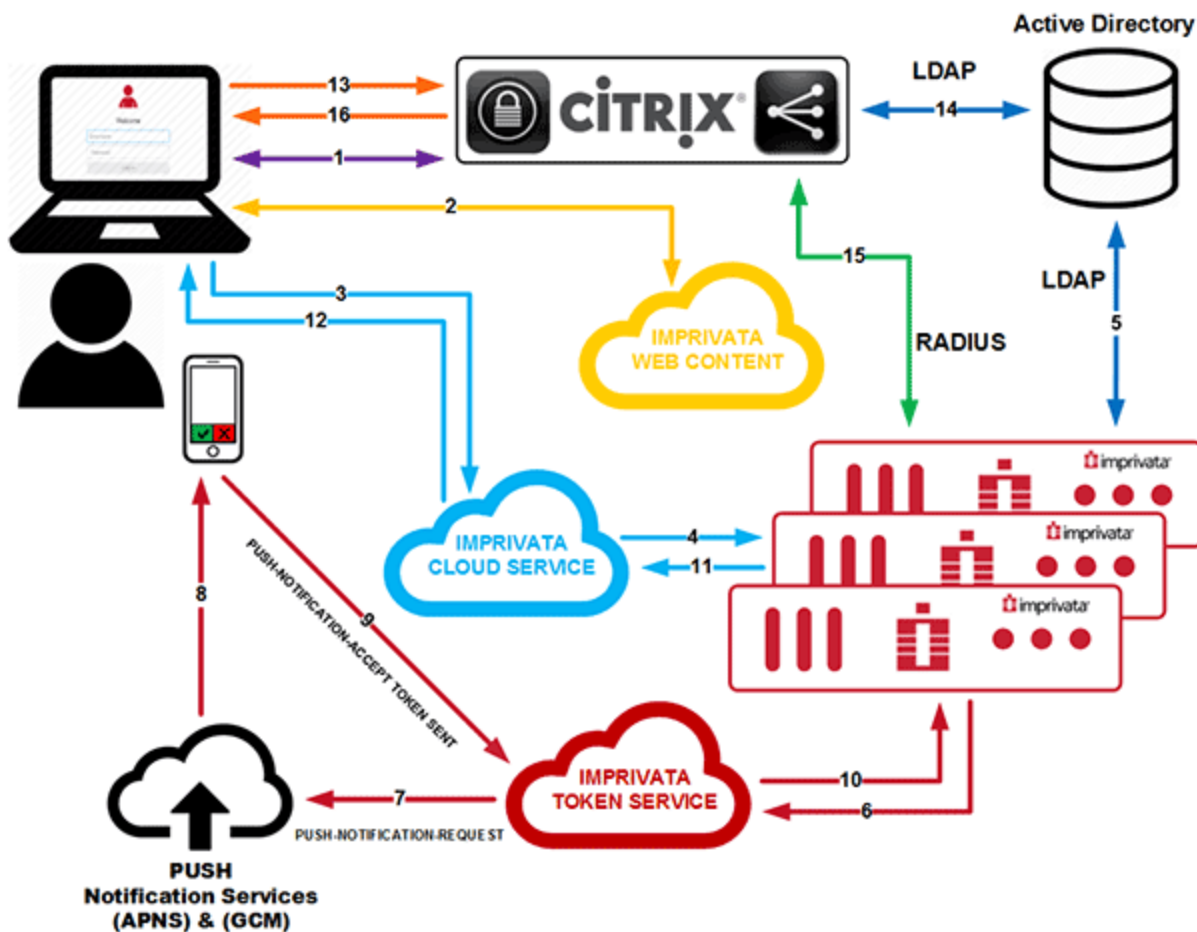
The Imprivata Cloud Remote Access experience overlays an Imprivata-powered graphical login screen on top of the NetScaler default login screen.

This graphical login screen authenticates the user with Imprivata Confirm ID via the Imprivata Cloud. Only after the authentication is complete, Imprivata Confirm ID sends the following to Citrix NetScaler:

- Username and Password go to the Citrix LDAP primary authentication
- Username and an authentication success token go to the Citrix RADIUS secondary authentication

Unlike the legacy Remote Access experience that required 30 seconds for the users to respond and complete the authentication, the Imprivata Cloud Remote Access experience only requires time to send this one message to Citrix NetScaler.

Also, you do not have to replace the LDAP connection between your gateway and Active Directory: You can easily maintain your existing single-factor remote access login experience while you roll out Imprivata Confirm ID Remote Access.



1. Primary authentication initiated to the Citrix NetScaler Gateway. In the background, the browser renders the login page with three fields (e.g. username, password1, password2.)
2. The browser downloads Imprivata web content. The initial login page is overlaid with Imprivata's custom login featuring only username and password fields.
3. The user enters his username and password. This information is sent to the Imprivata Cloud Service.
4. The Imprivata Cloud Service sends the user's credentials to the customer's on-premises Imprivata appliance.
5. The Imprivata appliance verifies the username and password with Active Directory (or another directory service.)
6. The Imprivata appliance sends a push token request to the Imprivata Cloud Token Service.
7. The Imprivata Cloud Token Service sends a push notification to the proper notification service (e.g. APNS or GCM.)
8. The notification service sends the push notification to the user's phone.
9. The user accepts the push notification. The user's phone sends a token back to the Cloud Token Service.
10. The Cloud Token Service sends a 'push token accepted' to the Imprivata appliance.
11. The Imprivata appliance sends an 'access accept' with a secure token to the Imprivata Cloud Service.
12. The Imprivata Cloud Service forwards the secure token to the user's browser.

13. The user's browser sends his username, password, and the secure token in the second password field.
14. Citrix NetScaler Gateway verifies the username and password. The group and other attributes are sent back to the gateway for authorization.
15. Citrix NetScaler Gateway verifies the Imprivata secure token over RADIUS to the Imprivata appliance.
16. Citrix NetScaler Gateway access granted to the user.

Cloud-Based Remote Access Integration

Integrate your Imprivata Confirm ID environment with Citrix NetScaler.

1. In the Imprivata Admin Console, go to **Applications > Remote access integrations**.
2. Click **Citrix NetScaler > Add new integration**.

If your connection to the Imprivata cloud looks good, your Customer ID will appear.

Cloud Connection

Imprivata Services will enter the Enterprise ID and one-time cloud provisioning code required to establish trust between your Imprivata enterprise and the Imprivata cloud:

1. If you're not on the Cloud Connection page already: In the Imprivata Admin Console, click the **gear icon > Cloud connection**.
2. Services will enter your **Enterprise ID** and **cloud provisioning code**.
3. Click **Establish trust**.



BEST PRACTICE:

The cloud connection must be established by Imprivata Services.

Cloud Connection Status

You can review the status of your enterprise's connection to the Imprivata cloud at any time. Status notifications are displayed on the Imprivata Admin Console, and the cloud connection status of every appliance at every site is also available:

1. In the Imprivata Admin Console, go to the **gear icon > Cloud connection**.
2. Every appliance host is listed with its status. If there are problems with a connection, recommendations for resolving the problem are displayed here.

Add New Citrix NetScaler Integration

1. On the **Add new Citrix NetScaler integration** page:

- Enter a descriptive **Nickname**
- Enter the **Hostname or IP address** of the Citrix NetScaler client. (The Citrix NetScaler client may also be referred to as the Network Access Server (NAS) or RADIUS client);
- Enter the **Encryption key** (shared secret).



BEST PRACTICE: This encryption key will be used as a shared secret between your RADIUS server (Imprivata appliance) and RADIUS client (Citrix NetScaler). Use a computer-generated string 22-30 characters in length.

You do not need to repeat this process for each Imprivata appliance. This client configuration is distributed to all Imprivata appliances in your enterprise.

2. **Optional** — Some RADIUS clients demand return information about authenticating users in the form of RADIUS attributes. You can add these attributes here. See "Managing RADIUS Connections" in the Imprivata Online Help.
3. Click **Save and get integration script**. Contact your Citrix administrator to include the script in a rewrite script (see below). This script is also available on the Imprivata Admin Console > **Applications** > **Remote access integrations** page.

Configure Two Factor Authentication via the Imprivata Cloud

In the following sections, you will create a new rewrite action, create a new secondary authentication RADIUS policy, and bind it to your NetScaler Gateway virtual server.

This rewrite policy is triggered when a user visits your NetScaler Gateway login page. The rewrite overlays an Imprivata-powered graphical login screen over the NetScaler default login screen. The integration script points Citrix NetScaler to the Imprivata Cloud to grab the Imprivata Confirm ID user interface.



NOTE: This topic offers instructions on making these configurations via CLI commands, or in the Citrix NetScaler graphical user interface console. When using the console, Citrix may present a warning message "Classic authentication policies are deprecated". You can safely ignore these messages.

Your Current Citrix NetScaler Environment

Before you add two-factor authentication, Your Citrix NetScaler production environment should be configured with an LDAP policy for primary authentication. You will be adding a secondary authentication RADIUS policy below.

Create Rewrite Action

In the Citrix NetScaler console, go to **AppExpert > Rewrite > Actions > Add**.

Configure the fields as follows:

Name	sample-rewrite-action	Give your rewrite action a descriptive name.
Type	INSERT_BEFORE_ALL	Inserts the expression before the search text.
Expression to choose target location	HTTP.RES.BODY (1000000)	1 million characters in the HTTP response body.
Expression to insert with	Enter the integration script here.	The integration script is available on the Imprivata Admin Console #160; Applications > Remote access integrations page.

Search type = Text	</body>	<input checked="" type="radio"/> Search <input type="radio"/> Pattern <div>Text</div> <div></body></div>
--------------------	---------	---

Create Rewrite Action using the CLI

Edit the sample command below to create the rewrite action via the command line:

- Replace the code in **blue** with your enterprise's unique integration script. The integration script is available on the Imprivata Admin Console > **Applications** > **Remote access integrations** page.
- The integration script needs to be surrounded with **single quotes**.
- Single quotes inside the integration script need to be 'escaped' with a **backslash**.

```
add rewrite action sample-rewrite-action insert_before_all HTTP.RES.BODY(1000000)
'"<script
src=\'https://cidra.integration.common.imprivata.com/static/js/embed/netscaler.js\'
data-access-token=
\'eyJ0ZW5hbnRJZCI6IjQyNTQ3NzU5ODUwMDM2MzUzNiIsCiJjb250ZXh0RGF0YSI6CnsiYXV0aEFwcElkIjoiTm
V0c2NhbGVyIiwKIjF1dGhJbnN0YW5jZUlkIjoIMDkxNDdiNzktYjEwNS00\" +
\"NWQzLTk0N2ItNzliMTA1NjVhM2VhIn19\'></script>'" -search "text(\"</body>\")"
```

Create Rewrite Policy

In the Citrix NetScaler console, go to **AppExpert > Rewrite > Policies > Add**.

Configure the fields as follows:

Name	sample-rewrite-policy	Give your rewrite policy a descriptive name.
Action	sample-rewrite-action	Select the rewrite action you created in the previous section.
Expression	HTTP.REQ.URL.ENDSWITH ("vpn/index.html") HTTP.REQ.URL.ENDSWITH ("logon/LogonPoint/index.html")	If expression is true, then the rewrite action is performed: This will ensure the rewrite action is only triggered on pages that end with these strings: <ul style="list-style-type: none">vpn/index.html — Default login, Green Bubble login, and X1 login pagelogon/LogonPoint/index.html — RfWebUI login page

Create Rewrite Policy using the CLI

Use the sample command below to create the rewrite policy via the command line. Inner quotes, single and double need to be 'escaped' with a **backslash**:

```
add rewrite policy sample-rewrite-policy "HTTP.REQ.URL.ENDSWITH  
(\"vpn/index.html\")||HTTP.REQ.URL.ENDSWITH(\"logon/LogonPoint/index.html\")" sample-  
rewrite-action
```

Bind Policy to Virtual Server

In the Citrix NetScaler console, go to **Netscaler Gateway > Virtual Servers > Edit > Policies > Add (+)**

Configure the fields as follows:

Choose Policy	Rewrite	
Choose Type	Response	Action will be applied to the HTTP response.
Select Policy	Rewrite Policy	Select the rewrite policy created above.
Priority	100	
Goto Expression	END	Because there are no additional rewrite policies. (If you add subsequent rewrite policies, this value must be set to NEXT.)

Bind Policy to Virtual Server using the CLI

Use the sample command below to bind the policy to the virtual server via the command line:

```
bind vpn vserver sample-virtual-server -policy sample-rewrite-policy -priority 100 -  
gotoPriorityExpression END -type RESPONSE
```

Create RADIUS Server

In the Citrix NetScaler console, go to **Netscaler Gateway > Policies > Authentication > RADIUS > Servers**

Click **Add**.

Configure the fields as follows:

Name	sample-radius-server	Give your server a descriptive name.
Server Name or IP Address	server1.sample.com	
Port	1812	
Secret Key	Enter the Secret Key , and again in the Confirm Secret Key field.	This is the same key as the "encryption key" entered in the Imprivata Admin Console > Applications > Remote access integrations.
Time-out (seconds)	3	

Create Authentication RADIUS Policy

In the Citrix NetScaler console, go to Netscaler Gateway > Policies > Authentication > RADIUS > Policies"

Configure the fields as follows:

Name	Example Auth RADIUS Policy	Give your policy a descriptive name.
Server	server1.sample.com	
Expression	ns-true	

Bind RADIUS Policy as a Secondary Authentication

In the Citrix NetScaler console, go to **Netscaler Gateway > Virtual Servers > Edit > Policies > Add (+)**

Configure the fields as follows:

Choose Policy	RADIUS	
Choose Type	Secondary	
Select Policy	Example Auth RADIUS Policy	Select the Secondary Authentication RADIUS policy above.
Priority	100	

Create RADIUS Server and Policy using the CLI

Use the sample command below to create a secondary RADIUS server via the command line.

- Replace the server name in **blue** with the name of your authentication RADIUS server.
- Replace **<shared secret>** with the secret key / shared secret you created in the Imprivata Admin Console:

```
add authentication radiusAction sample-radius-server -serverName server1.sample.com -
serverPort 1812 -radKey <shared secret>
add authentication radiusPolicy sample-radius-policy ns_true sample-radius-server
```

Create Bind Policy for the Secondary using the CLI

Use the sample command below to create the bind policy for the secondary via the command line.

```
bind vpn vserver "Example vpn virtual server" -policy "Example auth radius policy" -  
priority 100 -secondary
```

Optional — Number Matching

Multi-factor authentication fatigue attacks, also known as "MFA bombing", are a common cyberattack strategy. In an MFA fatigue attack, the attacker sends MFA push notifications to a registered user. The user may accidentally or absent-mindedly accept one of these push notifications, giving the attacker access to protected resources. This type of attack is generally preceded by phishing of the registered user's login credentials.

With Imprivata's Number Matching authentication enabled, users must enter a 2-digit code into Imprivata ID that matches the randomly generated number displayed on the application being accessed. This reduces the risk of the user accepting a push notification they did not initiate, and keeps your digital assets out of the hands of bad actors.



NOTE:

In the Imprivata Confirm ID Legacy Remote Access experience, users will not receive a push notification. They must manually enter the Imprivata ID token code from their mobile device. In this environment, Imprivata does not control the user interface, so Imprivata cannot provide same workflow used in Imprivata's Remote Access Cloud implementation.

Setup

1. In the Imprivata Admin Console, go to **Users > Workflow Policy**.
2. On the **Confirm ID workflow policy** page > **Authentication Options**, select **Require Web SSO and remote access users to enter a code when using Imprivata ID for MFA (number matching)**



NOTE:

Number Matching authentication is available for Imprivata Confirm ID Remote Access and Imprivata WebSSO only. Number Matching authentication is not available for the feature Imprivata ID for Windows Access.

This feature does not add Imprivata ID push notifications with number matching to workflows that do not already require the user to accept push notifications. This feature only requires users to enter a 2-digit code within workflows that already require the user to accept Imprivata ID push notifications. See **Expected Workflow**, below.

Expected Workflow

In this example, the user is at an endpoint computer where the Imprivata Agent is not present, and/or they are completing WebSSO or Remote Access workflows that require the user to accept an Imprivata ID push notification:

1. The user is logging in remotely, or provides the URL for an app enabled for Imprivata Web SSO.
2. The user is prompted to enter their username and password.
3. After the user successfully enters their username and password, they are prompted to approve a push notification sent to their enrolled Imprivata ID. A two-digit code will be shown on the application or resource being accessed.
4. Imprivata ID will display the username and the application the user is accessing.

The code expires in 30 seconds.

5. After the user accepts the push notification, they are given access to the application/resource.

When authenticating to some sites, the user may need to manually enter the six-digit Token Code from Imprivata ID app.

For WebSSO, subsequent apps are automatically authenticated within the same browser and the same session.

If the user closes an app without logging out of the app, he can return to the app during the same session without logging in again.

If the user fails to enter the code correctly, or the code expires, the user must begin authentication again.



CAUTION:

For this workflow, users must upgrade to the latest version of Imprivata ID on their mobile device. Users with versions of Imprivata ID before 2023.2 (iOS) or 2023.1 (Android) will not have the option to simply accept a push notification; they must manually enter the six-digit Token Code to authenticate to all sites.

Optional — Non-Licensed User Access

When you integrate Imprivata Confirm ID Remote Access with your gateway, the following users will be blocked from logging in:

- Imprivata Confirm ID and OneSign users who are not licensed for Remote Access, and
- All non-Imprivata users: users not synced with the Imprivata users list.

However, you can override this default behavior and allow remote access for these users:

1. In the Imprivata Admin Console, go to **Applications > Remote access integrations**
2. Select an integration.
3. In the section **Non-licensed user access**, select **Allow remote access for users without an Imprivata Confirm ID for Remote Access license**.
4. Click **Save**.

This option uses Active Directory authentication for these users only, bypassing Imprivata Confirm ID authentication.

Active Directory Groups Queried

When searching for a user in Active Directory, Imprivata will query Active Directory groups as follows:

Users synced with the Imprivata appliance — The Imprivata appliance will query direct group and nested group memberships.

Users not synced with the Imprivata appliance — The Imprivata appliance will only query direct group memberships.

Troubleshooting — Nested Groups Not Queried

Nested groups are not queried in the Remote Access Log In workflow. If you allow non-licensed user access but a non-Imprivata user is still blocked from Remote Access, the cause may be because their Active Directory group is nested.

Example

- A user is a member of Group1.
- Group1 is a member of Group2 = Group1 is nested in Group2.
- Group1 is not queried for non-Imprivata users attempting Remote Access.

Solution

If you need to provide remote access to non-Imprivata users in nested groups, sync them with the Imprivata appliance. You do not need to license them for any Imprivata features. The sync alone will cause them to be queried by Imprivata Confirm ID for Remote Access.



CAUTION: All users synced with the Imprivata appliance must be added to a user policy. If you do not want these users consuming any licenses, verify that the user policy they're added to consumes no licenses (the Imprivata Admin Console may present a Caution on this user policy stating these users will not be able to log in; this message can be ignored in this specific case). See "Creating and Managing User Policies" and "Synchronizing the Users List" in the Imprivata Online Help.

Optional — Native Citrix Workspace App Support

This section describes how to enable Native Citrix Workspace app support in addition to the browser-based access documented above:

- Set up another rewrite policy to the secondary authentication. This rewrite tells Citrix Workspace app that if it receives a username and password but no token, to initiate authentication via RADIUS with the native client.
- Add another LDAP connection to be used only for authorization group extraction. Unlike the legacy experience, group information is not sent over RADIUS.



NOTE:

This topic offers instructions on making these configurations via CLI commands, or in the Citrix NetScaler graphical user interface console. When using the console, Citrix may present a warning message "Classic authentication policies are deprecated". You can safely ignore these messages.

Create Another Rewrite Action

In the Citrix NetScaler console, go to **AppExpert > Rewrite > Actions > Add**.

Configure the fields as follows:

Name	sample-receiver-rewrite-action	Give your rewrite action a descriptive name.
Type	INSERT_AFTER_ALL	Inserts the expression after the search text.
Expression to choose target location	HTTP.RES.BODY(1000000)	1 million characters in the HTTP response body.
Expression to insert with	"\r\n" + "<META http-equiv="X-Citrix-AM-GatewayAuthType" content="SMS">"	If expression is true, then rewrite action is performed.
Search type = Text	</title>	If found, insert content before </title> tag.

Create Another Rewrite Action in CLI

Use the sample command below to create another rewrite action via the command line. Single quotes need to be escaped with a backslash:

```
add rewrite action sample-receiver-rewrite-action insert_after_all "HTTP.RES.BODY(1000000)" q/"\r\n" + "<META http-equiv=\"X-Citrix-AM-GatewayAuthType\" content=\"SMS\">"/ -search "text(\"</title>\")"
```

Create Another Rewrite Policy

In the Citrix NetScaler console, go to **AppExpert > Rewrite > Policies > Add**.

Configure the fields as follows:

Name	sample-receiver-rewrite-policy	Give your rewrite policy a descriptive name.
Action	Rewrite Action	Select the rewrite action created above.
Expression	HTTP.REQ.HEADER("User-Agent").CONTAINS("CitrixReceiver")	If expression is true, then rewrite action is performed. This will ensure this policy is only triggered for the native Receiver.

Create Another Rewrite Policy in CLI

Use the sample command below to create another rewrite policy via the command line. Inner single and double quotes need to be 'escaped' with a backslash:

```
add rewrite policy sample-receiver-rewrite-policy "HTTP.REQ.HEADER(\"User-Agent\").CONTAINS(\"CitrixReceiver\")" sample-receiver-rewrite-action
```

Bind the Policy to the Virtual Server

In the Citrix NetScaler console, go to **NetScaler Gateway > Virtual Servers > Policies > Add (+)**

Configure the fields as follows:

Choose Policy	Rewrite	
Choose Type	Response	
Select Policy	Rewrite Policy	Select the rewrite policy created above.
Priority	110	To ensure this policy is enforced second, set the policy binding to 110 (the first LDAP policy is already set to 100).
Goto Expression	END	This is the final rewrite policy.

Bind the Policy to the Virtual Server in CLI

Use the sample command below to create another rewrite policy via the command line:

```
bind vpn vserver sample-virtual-server -policy sample-receiver-rewrite-policy -priority 110 -gotoPriorityExpression END -type RESPONSE
```

Edit the Original Rewrite Policy Binding

To prompt the policy to complete both rewrites, edit the existing rewrite policy binding:

In the Citrix NetScaler console, go to **NetScaler Gateway > Virtual Servers > Edit > Policies**

Configure the fields of the first policy as follows:

Policy Name	Existing Policy Name	
Priority	100	
Goto Expression	NEXT	Allows the second rewrite policy to run (example: sample-receiver-write-policy)

Edit the Original Rewrite Policy Binding in CLI

Use the sample command below to edit the original rewrite policy via the command line:

```
bind vpn vserver sample-virtual-server -policy sample-rewrite-policy -priority 100 -gotoPriorityExpression NEXT -type RESPONSE
```

Add a Second LDAP Connection

Add another LDAP connection to be used only to retrieve group membership and user attributes that can be used for authorization policies. Unlike the legacy experience, group membership and user attribute information is not sent over RADIUS.

1. In the Citrix NetScaler console, go to **NetScaler Gateway > Policies > Authentication > LDAP > Servers > Add**
2. In the list of LDAP servers, check the box for your LDAP server and click **Add**.
The configuration of your LDAP server is copied to this new server.
3. Give the server a different name. Example: sample-ldap-server2
4. Uncheck the **Authentication** box.
5. Click **Create**.

Add a Second LDAP Connection in CLI

Use the sample command below to create a second LDAP connection via the command line. Replace the code in **blue** with your enterprise password:

```
add authentication ldapAction sample-ldap-server2 -serverName imprivata.com -ldapBase "dc=imprivata,dc=com" -ldapBindDn "cn=administrator,cn=users,dc=imprivata,dc=com" -ldapBindDnPassword <mypassword> -ldapLoginName sAMAccountName -groupAttrName memberOf -authentication DISABLE
```

Create a Second LDAP Policy

In the Citrix NetScaler console, go to **NetScaler Gateway > Policies > Authentication > LDAP > Policies > Add**

Configure the fields as follows:

Name	sample-ldap-policy2	Give your LDAP policy a descriptive name.
Server	LDAP Server	Select the second LDAP server created in the previous section.
Expression	REQ.HTTP.HEADER User-Agent CONTAINS CitrixReceiver	Ensures this policy is only triggered when logging in at the native Receiver.

Create a Second LDAP Policy in CLI

Use the sample command below to create a second LDAP policy via the command line. Inner single and double quotes need to be escaped with a backslash:

```
add authentication ldapPolicy sample-ldap-policy2 "REQ.HTTP.HEADER User-Agent CONTAINS CitrixReceiver" sample-ldap-server2
```

Bind the Second LDAP Policy to the Virtual Server

In the Citrix NetScaler console, go to **NetScaler Gateway > Virtual Servers > Basic Authentication > Add (+)**

Configure the fields as follows:

Choose Policy	LDAP	
Choose Type	Primary	Adding a second LDAP server without authentication.
Select Policy	LDAP Policy	Select the second LDAP policy created in the section above.
Priority	110	To ensure this policy is enforced second, set the policy binding to 110 (the first LDAP policy is already set to 100).

Bind the Second LDAP Policy to the Virtual Server in CLI

Use the sample command below to bind the second LDAP policy to the virtual server via the command line:

```
bind vpn vserver sample-virtual-server -policy sample-ldap-policy2 -priority 110
```


Optional — RADIUS Load Balancing



BEST PRACTICE: In large deployments, configure load balancing to distribute RADIUS authentications among Imprivata appliances within the Imprivata enterprise.

This section describes how to configure the Citrix NetScaler Gateway load balancer to distribute the traffic load to all your Imprivata appliances in production. If your Citrix NetScaler Gateway license does not include load balancing, another load balancing solution should be used.

In a large deployment, you should not configure the Citrix NetScaler Gateway to send all RADIUS requests to one Imprivata appliance.



NOTE:

This topic offers instructions on making these configurations via CLI commands, or in the Citrix NetScaler graphical user interface console. When using the console, Citrix may present a warning message "Classic authentication policies are deprecated". You can safely ignore these messages.

Add Load Balancing Servers

1. In the Citrix NetScaler console, go to **Traffic Management > Load Balancing > Servers > Add**.
2. Configure the fields as follows:

Name	sample-aap1-server1
Select Domain Name > FQDN	Enter the FQDN of an Imprivata appliance in production.

Repeat this process to add all the Imprivata appliances in production.

Add Load Balancing Servers in CLI

Edit the sample command below to add load balancing servers via the command line. Replace the code in **blue** with the FQDNs of your Imprivata appliances in production:

```
add server sample-appl-server1 server1.sample.eng
add server sample-appl-server2 server2.sample.eng
```

Add Load Balancing Service Group

1. In the Citrix NetScaler console, go to **Traffic Management > Load Balancing > Service Groups > Add**.
2. Configure the fields as follows:

Name	sample-service-group
------	----------------------

Protocol	RADIUS
Cache Type	SERVER

Add Load Balancing Service Group in CLI

Edit the sample command below to add a load balancing service group via the command line:

```
add serviceGroup sample-service-group RADIUS -maxClient 0 -maxReq 0 -cip DISABLED -usip NO -useproxyport NO -cltTimeout 120 -svrTimeout 120 -CKA NO -TCPB NO -CMP NO
```



NOTE:

This Load Balancing Service Group does not have any 'service group members' yet. You will add the Imprivata production appliances in the next section.

Add Load Balancing Service Group Members

Add the Imprivata production appliances (the 'service group members' you created above) to the currently-empty Service Group:

1. In the Citrix NetScaler console, go to **Traffic Management > Load Balancing > Service Groups**.
2. Select your Load Balancing Service Group.
The section **Load Balancing Service Group > Service Group Members** lists no service group members.
3. Click the > link.
4. On the **Create Service Group Member** page, select **Server Based**.
5. You don't actually have to 'create' the members (you did this already), so click the > to select them.
6. Check each of the Imprivata production appliance servers, and click **Select**.
7. Back on the **Create Service Group Member** page, set the Port to **1812**.
8. Click **Create**.
9. Back on the **Load Balancing Service Group** page, click **OK**.

Add Load Balancing Service Group Members in CLI

Edit the sample commands below to bind the Imprivata production appliances to the load balancing service group via the command line. Add another line of code for each Imprivata production server you need to bind to the load balancing server:

```
bind serviceGroup sample-service-group sample-appl-server1 1812
bind serviceGroup sample-service-group sample-appl-server2 1812
```

Add Load Balancing Virtual Server

In the Citrix NetScaler console, go to **Traffic Management > Load Balancing > Virtual Servers**

Configure the fields as follows:

Name	sample-lb-virtual-server	
Protocol	RADIUS	
IP Address Type	IP Address	Enter the IP address of the NetScaler load balancer.
Port	1812	

Add Load Balancing Virtual Server in CLI

Edit the sample command below to add the load balancing virtual server via the command line.

Replace the code in **blue** with the IP address of your load balancing server:

```
add lb vserver sample-lb-virtual-server RADIUS 10.1.1.1 1812 -persistenceType NONE -
cltTimeout 120
```

Bind Virtual Server Service Group

1. In the Citrix NetScaler console, go to **Traffic Management > Load Balancing Virtual Server** page > **Service Groups**:
2. In the section **Services and Service Groups**, Click > to select the Service Group.
3. Select the Service Group you created and click **Select**.
4. On the **ServiceGroup Binding** page, your service group is displayed. Click **Bind**.

Bind Load Balancing Virtual Server Service Group in CLI

Edit the sample command below to bind the load balancing virtual server service group via the command line:

```
bind lb vserver sample-lb-virtual-server sample-service-group
```

Configure RADIUS Server to Point to Load Balancer

Edit the Authentication RADIUS Server to point to the NetScaler load balancer instead of the Imprivata appliance.

In the Citrix NetScaler console, go to **VPN Virtual Server Authentication RADIUS Policy Binding > Configure Authentication RADIUS Server**.

Configure the fields as follows:

Server IP	IP Address	Enter the IP address of the NetScaler load balancer.
Secret Key	Enter the Secret Key , and again in the Confirm Secret Key field.	This is the same key as the "encryption key" entered in the Imprivata Admin Console > Applications > Remote access integrations .
Click Test Connection .		
Time-out (seconds)	3	

Configure RADIUS Server to Point to Load Balancer in CLI

Edit the sample command below to configure the RADIUS server to point to the load balancer via the command line.

- Replace the server name in **blue** with the IP address of the NetScaler load balancer.
- Replace **<shared secret>** with the secret key / shared secret you created in the Imprivata Admin Console:

```
set authentication radiusAction sample-radius-server -serverIP 10.1.1.1 -serverPort 1812 -radKey <secretkey>
```

Imprivata Admin Console — Add SNIP to RADIUS Client Integration

Edit the Citrix NetScaler integration to point to the Subnet IP (SNIP) address. (You can find the SNIP address in the Citrix console > **System** > **Network** > **IPs** > **IPv4s**):

1. In the Imprivata Admin Console, go to **Applications** > **Remote access integrations**.
2. In the section **Your integrations**, click on the **Nickname** for your Citrix NetScaler integration.
3. In the section **RADIUS client information**, add the SNIP address.
4. Click **Save**.

Optional — Web Apps Secure Access via AAA

The Imprivata Cloud experience also supports two factor authentication for web apps via AAA. There are no prerequisites for configuring this experience — none of the above Remote Access configuration is required.

Without the Imprivata Cloud experience, users outside your enterprise firewall cannot log in directly to web apps.

With the Imprivata Cloud experience, the user opens the login screen for the web app, completes two-factor authentication, and Imprivata passes the username and password to the app. The user only has to log in once.

In the following sections, you will create a new secondary authentication RADIUS policy for your AAA virtual server, and create a new rewrite policy.

This rewrite policy is triggered when a user visits a web app login page. The rewrite replaces the NetScaler default login screen with an Imprivata-powered graphical login screen. The integration script points Citrix NetScaler to the Imprivata Cloud to grab the Imprivata Confirm ID user interface.

Add a Form SSO Profile

In the Citrix NetScaler console, go to **Security > AAA – Application Traffic > Policies > Traffic > Form SSO Profiles > Add**

Configure the fields as follows:

Name	sample-form-sso-profile	Give the Form SSO Profile a descriptive name.
Action URL	/action_page.php	Web page form action to log into the application
User Name Field	username	Input field for the username
Password Field	password	Input field for the password
Success Criteria Expression	True	Checks to see if the SSO is successful
Submit Action	POST	This sample application uses a POST action

Add a Form SSO Profile via the CLI

Use the code sample below to add a form SSO profile via the command line:

```
add tm formSSOAction sample-form-sso-profile -actionURL "/action_page.php" -userField username -passwdField password -ssoSuccessRule True -nvtype STATIC -submitMethod POST
```

Add a Traffic Profile

In the Citrix NetScaler console, go to **Security > AAA – Application Traffic > Policies > Traffic > Traffic Profiles > Add**

Configure the fields as follows:

Name	sample-traffic-profile	Give the traffic profile a descriptive name.
Single Sign-on	ON	Enable SSO
Form SSO Profile	sample-form-sso-profile	Select the SSO profile you created above
Enable Persistent Cookie	Checked	Send session cookie with each http request

Add a Traffic Profile via the CLI

Use the code sample below to add a traffic profile via the command line:

```
add tm trafficAction sample-traffic-profile -SSO ON -formSSOAction sample-form-sso-profile -persistentCookie ON -InitiateLogout OFF -kcdAccount NONE
```

Add a Traffic Policy

In the Citrix NetScaler console, go to **Security > AAA – Application Traffic > Policies > Traffic > Traffic Policy > Add**

Configure the fields as follows:

Name	sample-traffic-policy	Give the traffic policy a descriptive name.
Profile	sample-traffic-profile	Select the traffic profile you created above.
Expression	True	

Add a Traffic Policy via the CLI

Use the code sample below to add traffic policy via the command line:

```
add tm trafficPolicy sample-traffic-policy True sample-traffic-profile
```


Add a AAA Virtual Server

In the Citrix NetScaler console, go to Security > AAA – Application Traffic > Virtual Servers > Add
Configure the fields as follows:

Name	sample-aaa-virtual-server
IP Address Type	IP Address
IP Address	Enter the IP address for the AAA virtual server.
Protocol	SSL
Port 443	

Add a AAA Virtual Server via the CLI

Use the code sample below to add a AAA virtual server via the command line:

```
add authentication vserver sample-aaa-virtual-server SSL 10.153.166.125 443
bind ssl vserver sample-aaa-virtual-server -certkeyName integ-wildcard-cert
bind authentication vserver sample-aaa-virtual-server -policy sample-ldap-policy1 -
priority 100
bind authentication vserver sample-aaa-virtual-server -policy sample-radius-policy -
priority 100 -secondary
```

Add a Load Balancing Server

In the Citrix NetScaler console, go to **Traffic Management > Load Balancing > Servers**

Configure the fields as follows:

Name	sample-app-server
Domain Name	Radial Button
FQDN	appserv1.integ.sample.eng

Add a Load Balancing Server via the CLI

Use the code sample below to add a load balancing server via the command line:

```
add server sample-app-server appserv1.integ.sample.eng
```

Add a Load Balancing Service Group

In the Citrix NetScaler console, go to **Traffic Management > Load Balancing > Service Groups**

Configure the fields as follows:

Name	sample-lb-server-group
Protocol	HTTP

Add a Load Balancing Service Group via the CLI

Use the code sample below to add a load balancing service group via the command line:

```
add serviceGroup sample-lb-service-group HTTP -maxClient 0 -maxReq 0 -cip DISABLED -  
usip NO -useproxyport YES -cltTimeout 180 -svrTimeout 360 -CKA NO -TCPB NO -CMP NO  
bind serviceGroup sample-lb-service-group sample-app-server 80
```

Add a Load Balancing Virtual Server

In the Citrix NetScaler console, go to **Traffic Management > Load Balancing > Virtual Servers**

Configure the fields as follows:

Name	sample-lb-virtual-server
Protocol	Radial Button
IP Address Type	IP Address
IP Address	Enter the IP address of the load balancing virtual server

Authentication Section

Go to the Authentication section.

Configure the fields as follows:

Type	Form Based Authentication	
Authentication FQDN	ns1-aaa-vs1-integ.sample.eng	
Choose Virtual Server Type	Authentication Virtual Server	
Authentication Virtual Server	sample-aaa-virtual-server	Created above

via the CLI

Use the code sample below to add a load balancing virtual server via the command line:

```
add lb vserver sample-lb-virtual-server HTTP 10.153.66.104 80 -persistenceType NONE -  
cltTimeout 180 -AuthenticationHost ns1-aaa-vs1.integ.sample.eng -Authentication ON -  
authnVsName sample-aaa-virtual-server  
bind lb vserver sample-lb-virtual-server sample-lb-service-group  
bind lb vserver sample-lb-virtual-server -policyName sample-traffic-policy -priority  
100 -gotoPriorityExpression END -type REQUEST
```

Configure AAA Support via the Citrix GUI

Configure a Citrix AAA Virtual Server

1. Go to your load balancing server.
2. In the Authentication section, click Add to add a AAA virtual server:
 - Enter the Authentication FQDN for the AAA server you're about to create.
 - Virtual server type = Authentication Virtual Server
 - Authentication Virtual Server field = click the + to create it now.
3. Create the Authentication Virtual Server:
 - Give the server a descriptive name.
 - Enter the IP address for the server (SSL port 443)

- Upload a server certificate (Because it's a security server, this AAA server creates an SSL session to an authentication server.)

Create Secondary RADIUS Authentication

Go to your Citrix NetScaler Gateway Load Balancing virtual server > Basic Authentication.

Create RADIUS Policy

1. On the Basic Authentication title bar, click +
2. In the Choose Type screen:
 - Choose Type = RADIUS
 - Choose Type = Secondary
3. Click **Continue**.
4. In the **Policy Binding > Select Policy** section, click the + to create a policy.
5. On the **Create Authentication RADIUS Policy** screen:
 - Give the policy a descriptive **Name**;
 - Enter the **IP address** of the Imprivata appliance or load balancer;
 - Set the Expression to **ns_true**
6. Click **Create**.

Create Authentication RADIUS Server

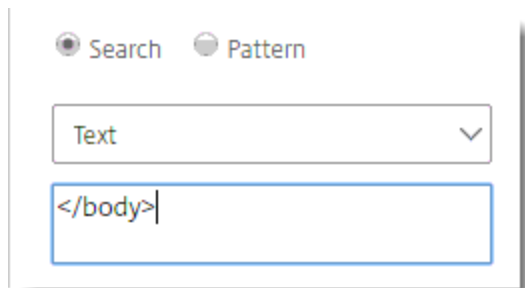
1. On the **Create Authentication RADIUS Server** screen:
 - Give the server a descriptive **Name**;
 - Enter the **Server Name**;
 - Port = **1812**
 - Enter the Secret Key (the **Encryption key** / shared secret you created on the Imprivata Admin Console)
 - Set the Time-out to **3** seconds;
 - Click **Create**.
2. Back on the **Choose Type** screen, select the policy you just created and click **Bind**.
You should now see your Secondary Authentication RADIUS Policy listed below your Primary Authentication LDAP Policy.

Create Rewrite Policy

This rewrite policy will ensure the policy is only triggered on the HTML pages where users log in:

1. Go to AppExpert > Rewrite > Actions > Rewrite Policies.
2. Click Add.
3. Give the policy a descriptive name.
4. In the Action section, click the + to create a rewrite action.
5. On the Create Rewrite Action screen:

- Give the action a descriptive **Name**;
 - Type = INSERT_BEFORE_ALL
 - Use the following code for the **Expression to choose target location**:
 - HTTP.RES.BODY(1000000)
6. In the field **Expression to Insert with**, enter the **Integration Script** available on the Imprivata Admin Console **Remote access integrations** page. This code replaces the NetScaler default login screen with an Imprivata-powered graphical login screen. The code points Citrix Netscaler to the Imprivata Cloud to grab the Imprivata Confirm ID user interface. (The lengthy token code identifies your unique instance to Imprivata.)
 7. In the **Search** section, select the **Text** drop-down and enter `</body>` (all lower case) in the field provided.



8. Click **Create**.
9. Back on the **Create Rewrite Policy** screen:
 - Give the policy a descriptive **Name**;
 - Undefined-Result Action = **-Global-undefined-result-action-**
10. In the **Expression** field, enter the following code. This will ensure the policy is only triggered on the HTML pages where users log in:
`HTTP.REQ.URL.ENDSWITH("/vpn/tmindex.html")`
 (tmindex.html is the default HTML filename NetScaler uses for AAA authentication.)
11. Click OK.

Bind Rewrite Policy Globally

You cannot bind a rewrite policy to the AAA server, so you must apply the rewrite policy globally to all servers. However, the rewrite policy won't affect any other servers because of the policy expression you created above limits it to pages with the **tmindex.html** filename.

1. In your list of rewrite policies, click Policy Manager.
2. In the Rewrite policy manager:
 - Bind Point = Default Global
 - Protocol = Select HTTP to support web apps, for example.
 - Connection type = Response
3. Click Continue.
4. On the Policy Binding screen:

- Select your rewrite policy
- Priority = 100
- Goto expression END
- Invoke LabelType = NONE

5. Click Bind.

Optional — Advanced Authentication with nFactor

Preserving Your Current NetScaler Login Experience

Imprivata Confirm ID Remote Access with Citrix NetScaler uses a rewrite policy to replace the NetScaler default login screen with an Imprivata-powered graphical login screen. The integration script points Citrix NetScaler to the Imprivata Cloud to grab the Imprivata Confirm ID user interface.

Imprivata Confirm ID supports Basic Authentication by default.

However, only Citrix NetScaler nFactor (Advanced Authentication) can handle:

- policy-based authentication (off premises or on premises)
- including additional factors (sending the user domain as a separate value, for example)

This topic describes how to configure NetScaler to complete Advanced Authentication and transfer user credentials to the Imprivata login page to complete two-factor authentication.

Create the LDAP Server

Create the LDAP server receive and cache the username and password, then send the result of the authentication + the RADIUS secure token from Imprivata Confirm ID to NetScaler:

1. In the Citrix NetScaler console, go to **Security > AAA - Application Traffic > Policies > Authentication > Advanced Policies > Actions > LDAP > Add**
2. Give the LDAP server a descriptive name, and enter your existing settings here.
3. Click **Create**.

The screenshot displays the Citrix NetScaler console interface for configuring an LDAP server. The top navigation bar includes 'Citrix ADC VPX (1000)' and tabs for 'Dashboard', 'Configuration', 'Reporting', 'Documentation', and 'Downloads'. The 'Configuration' tab is active, leading to the 'Create Authentication LDAP Server' page.

The configuration page is divided into several sections:

- Name***: A text field containing 'Example Auth LDAP Server'.
- Server Name / Server IP**: Radio buttons for 'Server Name' (selected) and 'Server IP'.
- Server Name***: A text field containing 'ldap.example.com'.
- Security Type**: A dropdown menu set to 'TLS'.
- Port**: A text field containing '389'.
- Server Type**: A dropdown menu.
- Time-out (seconds)**: A text field containing '3'.
- Authentication**: A checked checkbox.
- SSH Public Key**: A text field.

The **Connection Settings** section includes:

- Base DN (location of users)***: A text field containing 'dc=ldap,dc=example,dc=com'.
- Administrator Bind DN***: A text field containing 'cn=admin,dc=example,dc=com'.
- Administrator Password***: A password field with masked characters.
- Confirm Administrator Password***: A password field with masked characters.
- Test LDAP Reachability**: A button.
- Test End User Connection**: A link.

The **Other Settings** section includes:

- Server Logon Name Attribute**: A dropdown menu set to 'sAMAccountName'.
- Default Authentication Group**: A text field.

Create the RADIUS Server

Create the RADIUS server to send the secure token from Imprivata Confirm ID to NetScaler.

In the Citrix NetScaler console, go to **Security > AAA - Application Traffic > Policies > Authentication > Advanced Policies > Actions > RADIUS > Add**

Name	Give your server a descriptive name.	
Port	1812	
Secret Key	Enter the Secret Key , and again in the Confirm Secret Key field.	This is the same key as the "encryption key" entered in the Imprivata Admin Console > Applications > Remote access integrations.
Time-out (seconds)	3	

Click **Create**.

Citrix ADC VPX (1000)

DashboardConfigurationReportingDocumenta

Create Authentication RADIUS Server

Name*

Example Auth RADIUS Server

Server NameServer IP

Server Name*

imprivata-appl.example.com

Port

1812

Secret Key*

Confirm Secret Key*

Test RADIUS Reachability

Test End User Connection

Time-out (seconds)

3

More

CreateClose

Create the LDAP Authentication Policy

In the Citrix NetScaler console, go to **Security > AAA - Application Traffic > Policies > Authentication > Advanced Policies > Policy > Add**

Name	Give the policy a descriptive name.
Action Type	LDAP
Action	Select the LDAP server you created above.
Expression	True

Click **Create**.

Citrix ADC VPX (1000)

Dashboard

Configuration

Reporting

Create Authentication Policy

Name*

Example Auth LDAP Policy

?

Action Type*

LDAP

?

Action*

Example Auth LDAP Server

Add

Edit

Expression*

Select

Select

Select

True

More

Create

Close

Create the RADIUS Authentication Policy

In the Citrix NetScaler console, go to **Security > AAA - Application Traffic > Policies > Authentication > Advanced Policies > Policy > Add**

Name	Give the policy a descriptive name.
Action Type	RADIUS
Action	Select the RADIUS server you created above.
Expression	True

Click **Create**.

Citrix ADC VPX (1000)

Dashboard

Configuration

Reporting

Create Authentication Policy

Name*

Example Auth RADIUS Policy

Action Type*

RADIUS

Action*

Example Auth RADIUS Server

Add

Edit

Expression*

Select

Select

Select

True

More

Create

Close

Create the Authentication Policy Label

To send the LDAP authentication approval to the next step (RADIUS authentication), create the Authentication Policy label and bind it to the RADIUS policy:

In the Citrix NetScaler console, go to **Security > AAA - Application Traffic > Policies > Authentication > Advanced Policies > Authentication Policy Labels > Add**

Name	Give the label a descriptive name.
Login Schema	No schema is needed here. The "no schema" value = LSCHEMA_INT
Feature Type	AAATM_REG

Click **Continue**.

Citrix ADC VPX (1000)

DashboardConfigurationReporting

Authentication Policy Label

Create Authentication Policylabel

Name*

Example Auth Policy Label?

Login Schema*

LSCHEMA_INT

AddEdit

Feature Type

AAATM_REQ

Comment

Continue

Cancel

Bind the Authentication Policy Label

Bind the policy label to the RADIUS policy:

1. In the Citrix NetScaler console, go to **Security > AAA - Application Traffic > Policies > Authentication > Advanced Policies > Authentication Policy Labels > Bind**
2. Select the RADIUS policy you created above.
3. Priority — **100**
4. Goto Expression — **END**
5. Click **Bind**.

Citrix ADC VPX (1000)

Dashboard

Configuration

Reporting

Documentation

Downloads

←

Authentication Policy Label

Create Authentication Policylabel

Name

Example Auth Policy Label

Login Schema

LSCHEMA_INT

Feature Type

AAATM_REQ

Policy Binding

Select Policy*

Example Auth RADIUS Policy

>

Add

Edit

?

► More

Binding Details

Priority*

100

Goto Expression*

END

?

Select Next Factor

Click to select

>

Add

Edit

Bind

Close

Complete the Authentication Policy Label

1. In the Citrix NetScaler console, go to **Security > AAA - Application Traffic > Policies > Authentication > Advanced Policies > Authentication Policy Labels**

The Login Schema, RADIUS policy, and Feature Type are now listed in the Authentication Policy Label.

2. Click **Done**.

Citrix ADC VPX (1000)

HA Status
Not configured

Partition
default

nsroot

Dashboard

Configuration

Reporting

Documentation

Downloads

Authentication Policy Label

Create Authentication Policylabel

Name

Example Auth Policy Label

Login Schema

LSCHEMA_INT

Feature Type

AAATM_REQ

Add Binding

Unbind

Regenerate Priorities

No action

	Priority	Policy Name	Expression	Action	Goto Expression	Next Factor
<input type="checkbox"/>	100	Example Auth RADIUS Policy	True	Example Auth RADIUS Server	END	

Done

Create the Login Schema Profile

To tell the AAA server how the users should authenticate, create the login schema profile:

1. In the Citrix NetScaler console, go to **Security > AAA - Application Traffic > Login Schema > Profiles > Add**

Name	Give the profile a descriptive name.
Authentication Schema	Select a Dual Authentication schema XML file. You can select an existing file from a list. The IDs of the three fields must be login , passwd , and passwd1 .
Enable Single Sign On Credentials	Select

2.



NOTE: Selecting **Single Sign On Credentials** is used to pass usernames and passwords to SSO applications and resource services such as Citrix StoreFront. When AAA is used for authentication, the user's credentials are not passed back to the remote access virtual server by default. By enabling **Single Sign On Credentials** here, user credentials will be sent back to the Remote Access Virtual Service.

3. Click **Create**.

Citrix ADC VPX (1000)

HA Status
Not configured

Partition
default

nsroot

DashboardConfigurationReportingDocumentationDownloads

Create Authentication Login Schema

Name*

Example Auth Login Schema Profile

Authentication Schema*

/nsconfig/loginschema/LoginSchema/DualAuth.xml

User Expression

Expression Editor

Select Select Select

Press Control+Space to start the expression and then type ':' to get the next set of options

Evaluate

Password Expression

Expression Editor

Select Select Select

Press Control+Space to start the expression and then type ':' to get the next set of options

Evaluate

User Credential Index

Password Credential Index

Authentication Strength

0

Enable Single Sign On Credentials

More

CreateClose

Create the Login Schema Policy

- 1. In the Citrix NetScaler console, go to **Security > AAA - Application Traffic > Login Schema > Policies > Add**

Name	Give the policy a descriptive name.
Profile	Select the login schema profile you created above.
Rule	True

- 2. Click **Create**.

Citrix ADC VPX (1000)

Dashboard

Configuration

Reporting

Documentation

Create Authentication Login Schema Policy

Name*

Example Auth Login Schema Policy

Profile*

Example Auth Login Schema Policy

Add

Edit

Log Action

Add

Edit

Undefined-Result Action

Rule*

Select

Select

Select

True

Comments

Create

Close

Create the AAA Virtual Server

1. In the Citrix NetScaler console, go to **Security > AAA - Application Traffic > Authentication Virtual Servers > Add**

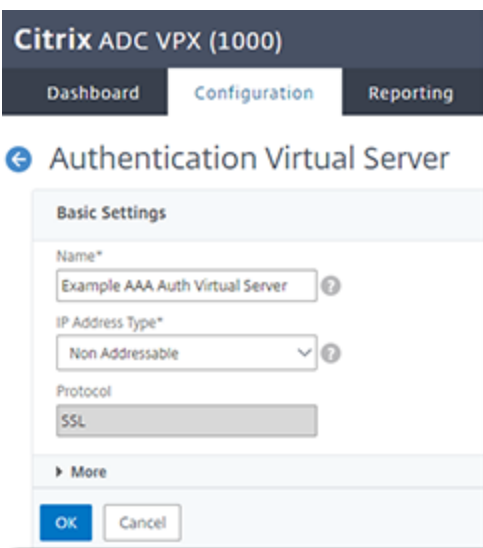
Name	Give the server a descriptive name.
IP Address Type	Non-Addressable
Protocol	SSL

2. Click **OK**.



NOTE:

Since the AAA virtual server is local, this server can be non-addressable and does not require an SSL server certificate.



Citrix ADC VPX (1000)

Dashboard Configuration Reporting

← Authentication Virtual Server

Basic Settings

Name*
Example AAA Auth Virtual Server ?

IP Address Type*
Non Addressable ?

Protocol
SSL

► More

OK Cancel

Add the LDAP Policy to Bind

- 1. In the Citrix NetScaler console, go to **Security > AAA - Application Traffic > Authentication Virtual Servers > Advanced Authentication Policies > Authentication Policy**

Select Policy	Select the LDAP policy you created above.
Priority	100
Goto Expression	NEXT
Select Next Factor	Select the Authentication Policy Label you created above.

- 2. Click **Bind**.

Policy Binding

Policy Binding

Select Policy*

Example Auth LDAP Policy

>

Add

Edit

?

► More

Binding Details

Priority*

100

Goto Expression*

NEXT

▼

Select Next Factor

Example Auth Policy Label

>

Add

Edit

?

Bind

Close

Bind the Schema Policy

1. In the Citrix NetScaler console, go to **Security > AAA - Application Traffic > Authentication Virtual Servers > Login Schemas > Login Schema > Policies > Select**
2. Select the Login Schema Policy you created above.
3. Click **Select**.
4. Go to **Policy Binding**.
5. Click **Bind**.

Policy Binding

Policy Binding

Select Policy*

> Add Edit ?

► More

Binding Details

Priority*

Bind Close

Create the Authentication Profile

Create the profile for Advanced Authentication on the AAA server. This profile is used on the VPN virtual server to send users to the AAA server:

- 1. In the Citrix NetScaler console, go to **Security > AAA - Application Traffic > Authentication Profile > Add**

Name	Give the profile a descriptive name.
Choose Virtual Server Type	Authentication Virtual Server
Authentication Virtual Server	Select the AAA virtual server you created above.

- 2. Click **Create**.

Citrix ADC VPX (1000)

Dashboard

Configuration

Reporting

←

Create Authentication Profile

Name*

Example Auth Profile

?

Authentication Host

Choose Virtual Server Type

Authentication Virtual Server

▼

Authentication Virtual Server*

Example AAA Auth Virtual Ser...

>

Add

Edit

?

Authentication Domain

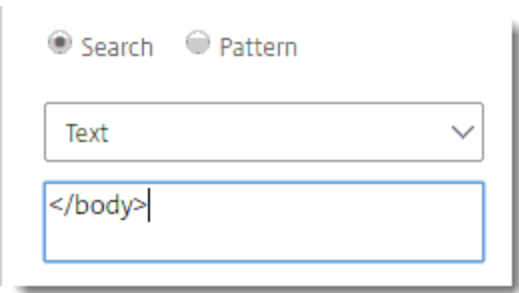
Authentication Level

Create

Close

Create the Rewrite Action

The rewrite action inserts Imprivata's graphical login screen for users to complete Imprivata Confirm ID authentication. In the Citrix NetScaler console, go to **AppExpert > Rewrite > Rewrite Actions > Add**. Configure the fields as follows:

Name	Example Rewrite Action	Give your rewrite action a descriptive name.
Type	INSERT_BEFORE_ALL	Inserts the expression before the search text.
Expression to choose target location	HTTP.REQ.BODY (1000000)	1 million characters in the HTTP response body.
Expression to insert with	Enter the integration script here.	The integration script is available on the Imprivata Admin Console > Applications > Remote access integrations page.
Search type = Text	</body>	

← Create Rewrite Action

Name*

 ?

Type*

 ?

Use this action type to insert a custom text in request/response before all references of specified text.

Expression to choose target location*

Expression Editor

Evaluate

Expression to Insert with

Expression Editor

Evaluate

☒ Search ☐ Pattern

Create the Rewrite Policy

1. In the Citrix NetScaler console, go to **AppExpert > Rewrite > Rewrite Actions > Add**

Name	Give the rewrite policy a descriptive name.	
Action	Select the rewrite action you created above.	
Undefined Result Action	-Global-undefined-result-action-	
Expression	<code>HTTP.REQ.URL.ENDSWITH("vpn/index.html") HTTP.REQ.URL.ENDSWITH("logon/LogonPoint/index.html")</code>	<p>If expression is true, then the rewrite action is performed: This will ensure the rewrite action is only triggered on pages that end with these strings:</p> <ul style="list-style-type: none">• <code>vpn/index.html</code> — Default login, Green Bubble login, and X1 login page• <code>logon/LogonPoint/index.html</code> — RfWebUI login page

2. Click **Create**.

← Create Rewrite Policy

Name*



Action*

[Add](#)[Edit](#)

Log Action

[Add](#)[Edit](#)

Undefined-Result Action*



Expression*



HTTP.REQ.URL.ENDSWITH("/vpn/tmindex.html") || HTTP.REQ.URL.ENDSWITH("/logon/LogonPoint/tmindex.html")

Comments

[Create](#)[Close](#)

Bind the Rewrite Policy Globally

1. In the Citrix NetScaler console, go to **AppExpert > Rewrite > Rewrite Actions > Policy Manager > Add Binding**

Select Policy	Select the rewrite policy you created above.
Priority	100
Goto Expression	END
Invoke LabelType	None

2. Click **Bind**.

Citrix ADC VPX (1000)

Dashboard

Configuration

Reporting

Documentation

Downloads

← Rewrite Policy Manager

Bind Point

Bind Point

Default Global

Protocol

HTTP

Connection Type

Response

Policy Binding

Select Policy*

Example Rewrite Policy

>

Add

Edit

?

► More

Binding Details

Priority*

100

Goto Expression*

END

▼

Invoke LabelType*

None

▼

Bind

Close

Bind AAA Authentication Policy to Gateway Virtual Server

Bind the policy to the server at **Citrix Gateway > Citrix Gateway Virtual Servers > Authentication Profile > Bind**

Rolling Out Remote Access

Now that the gateway software and the Imprivata appliance are configured to communicate with each other, you can roll out Imprivata Confirm ID to your users.

Step 1: Organize Users

You control how your users enroll and log in with Imprivata Confirm ID by organizing users into user policies, then associating those user policies with the Remote Access workflow and enroll rules.

Some examples of how you may want to organize your users:

- **IT pilot** — If you'd like to validate your configuration through an IT pilot, create a user policy that contains only your pilot users. Later in this process you can activate Remote Access for only the pilot group.
 - **Phased rollout** — After you've validated your enrollment, you can introduce Imprivata Confirm ID Remote Access one department at a time. Organize departments into user policies, and associate them with the Remote Access workflow and your enroll rule when you're ready to "go live".
 - **Off-site users** — If some of your users rarely come into the office, organize them into a user policy; you can allow them to enroll Imprivata ID and their phone number before they access the VPN (RADIUS client).
1. In the Imprivata Admin Console, go to **Users > User Policies** select the user policies that will be associated with Remote Access. Use existing policies, make copies of existing policies, or create policies from scratch.
 2. Go to **Users > Users**. Choose who will be using Remote Access, and apply a user policy to them. Every user in a policy will receive Remote Access when it's associated with the Remote Access workflow (later in this process).

For complete details on organizing users, see "Managing User Accounts" in the Imprivata Online Help.

Step 2: Select Remote Access Authentication Methods

Confirm authentication methods required for Remote Access.

1. In the Imprivata Admin Console, go to **Users > Workflow policy**.
By default, the **Remote Access Log in** workflow is configured for:
 - Password + Imprivata ID, and
 - Password + SMS code
2. If you want to change how your users access the VPN (RADIUS client), go to the section **Remote access workflows** and make your changes. For complete details on configuring workflow policies, see "Configuring the Imprivata Confirm ID Workflow Policy" in the Imprivata Online Help.
3. Do not associate any user policies with this workflow yet; you will "go live" with Remote Access later in this section.
4. Click **Save**.



NOTE: If you have users who cannot use a mobile device in the workplace, Imprivata Confirm ID Remote Access also supports native integration with VASCO tokens. See "Managing VASCO OTP Tokens" in the Imprivata Online Help.

Step 3: Configure Enrollment Rule

Your users need to enroll the Imprivata ID app, and/or their phone number for SMS code authentication. Remote Access enables enrolling while logging in to your VPN gateway, and enrolling at the Imprivata agent connected to your enterprise network.

Provide a descriptive name and configure an enrollment rule. You will associate one or more user policies with this rule later. You can add additional rules with different options for other user policies.

Access for Unenrolled Users

Before enrolling Imprivata ID or SMS code, users can access the VPN with password alone.

Or you can require "a different login method" for your unenrolled users. This setting is intended for users logging in with:

- Password + OTP token,
- PIN + OTP token, or
- an OTP token.

When configuring the enroll rules, if you select "a different login method" but don't select one of these methods in the **Log in** section, these users will be blocked. Users who have been assigned a temporary code will still have access.



NOTE: If you have users who have already enrolled Imprivata ID (providers who already use Imprivata ID for signing orders, for example), they won't have the option to access the VPN (RADIUS client) with password only – they must use password + Imprivata ID to sign in if the Remote Access workflow includes Imprivata ID.

To view a list of users who have already enrolled Imprivata ID— in the Imprivata Admin Console, go to **Reports > Enrolled users report**, customize the report as needed, and click **Run**. For more details, see

Choose Where Users Can Enroll

Imprivata Confirm ID Remote Access offers options for enrolling Imprivata ID and phone numbers for SMS authentication:

A user can always enroll in the Imprivata agent — A user can always enroll at a computer with the Imprivata agent connected to the Imprivata appliance, or they're outside your enterprise network using a virtual desktop connection. They can access the Imprivata Confirm ID enrollment utility and enroll their Imprivata ID and/or phone number. You have the option of prompting unenrolled users to do so.

Prompt the user at the remote client — This method is ideal for users who do not come into the office often: a user is logging into your VPN (RADIUS client) from outside your enterprise network. After the user has successfully entered their username and password, your gateway will prompt the user to enroll their Imprivata ID and/or phone number.



NOTE:

In this scenario, users can enroll Imprivata ID and their phone number remotely by providing their username and password only. For added security during remote enrollment, you can generate a temporary code for each user and place them in a user policy that allows remote enrollment but requires two-factor authentication when logging in remotely. In this scenario, they would enter their username, password, and temporary code before they could remotely enroll Imprivata ID or their phone number. See "Temporary Codes for Remote Access" in the Imprivata Online Help.

Do not prompt — With this selection, users will not be prompted, but they can still enroll authentication methods when the Imprivata agent is connected to the Imprivata appliance, or they're outside your enterprise network using a virtual desktop connection. Users cannot enroll in the remote client unless you prompt them.

Choose Whether Users Can Delay

If you discover some users delay enrollment and continue to log in using their username and password only, you can force them to enroll before they access the VPN. If you allow users to delay enrollment, they can delay indefinitely; to track these users who have not enrolled, see [Step 6: Who Hasn't Enrolled Yet?](#)

Optional — IT Pilot

Validate your Remote Access configuration by piloting it with a small group of users. If you did not create a user policy dedicated exclusively to this IT pilot, [return to Step 1](#) and create one now.

Associate an IT pilot user policy with the Remote Access workflow and Enroll rules:

1. In the Imprivata Admin Console, go to **Users > Workflow Policy > Remote access workflows**.
2. In the section **Log In**, click **Associate user policies**.
3. Choose your IT pilot user policy from the list.
4. In the section **Enroll**, click **Associate user policies**.
5. Choose your IT pilot user policy from the list.
6. Click **Save**. Imprivata Confirm ID enrollment and remote access are now live only for the users in the pilot.

Step 4: Notify Users

Before you "go live" with Imprivata Confirm ID Remote Access, introduce this new system to your users. Let them know what to expect; request users enroll Imprivata ID and/or their phone number by a certain date, after which two-factor authentication will be enforced.

Step 5: Go Live

Associate user policies with the Remote Access workflow, and associate user policies with an enroll rule:

1. In the Imprivata Admin Console, go to **Users > Workflow Policy > Remote access workflows**.
2. In the section **Log In**, click **Associate user policies**.
3. Choose user policies from the list.
4. In the section **Enroll**, select an enroll rule and click **Associate user policies**.
5. Choose user policies from the list.
6. If you have more than one Enroll rule and need some users to use it, select another enroll rule and click **Associate user policies**.
7. Choose user policies from the list. A user policy can only be associated with one enroll rule.
8. Click **Save**.

Step 6: Who Hasn't Enrolled Yet?

Generate a list of users that haven't enrolled yet. When you're ready to enforce two-factor authentication, you can then contact these users directly, and/or enforce enrollment.

1. In the Imprivata Admin Console, go to **Reports > Add New Report**.
2. On the **Add New Report** page, go to **Confirm ID > Unenrolled users (Remote access)**.
3. On the **Add report** page, customize the report and filters as needed.
 1. Run, save, and/or export the report results to a CSV file.
 2. The report includes the unenrolled users' email addresses; use the CSV file to bulk email all unenrolled users and instruct them to enroll.

For complete details on Imprivata reporting, see "Using Reporting Tools" in the Imprivata Online Help.

Prompt Users to Enroll

Prompt users to enroll Imprivata ID and/or their phone number:

1. In the Imprivata Admin Console, go to **Users > Workflow Policy > Remote access workflows**.
2. In the section **Enroll > Enroll prompts**, select prompts in the Imprivata agent and/or the remote client.
3. In the section **Enroll > Delay**, you can require them to enroll Imprivata ID or their phone number before accessing the VPN.
4. Click **Save**.

After a user enrolls Imprivata ID or their phone number, this prompt will no longer appear.

Step 7: Future Rollouts

You can repeat steps 5 and 6 with more users in your enterprise, and new hires in departments already using Remote Access.