imprivata®

Product Documentation

Remote Access with Citrix NetScaler Gateway - Legacy Experience

Imprivata Enterprise Access Management 24.1

Before You Begin

> **NOTE:**
> Beginning with 24.1, 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.
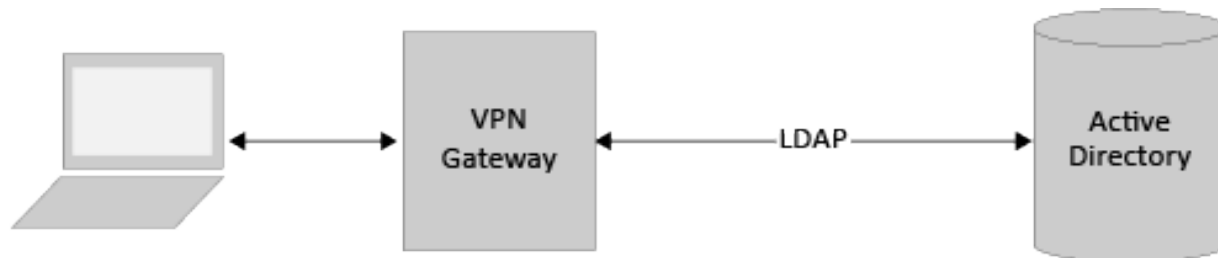
How To Use Imprivata Confirm ID Remote Access

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.

Imprivata Confirm ID as RADIUS Server

In a typical enterprise, the remote access gateway communicates with Active Directory via LDAP:

After integrating with Imprivata Confirm ID, your remote access gateway will send all requests to the RADIUS server built into the Imprivata appliance.
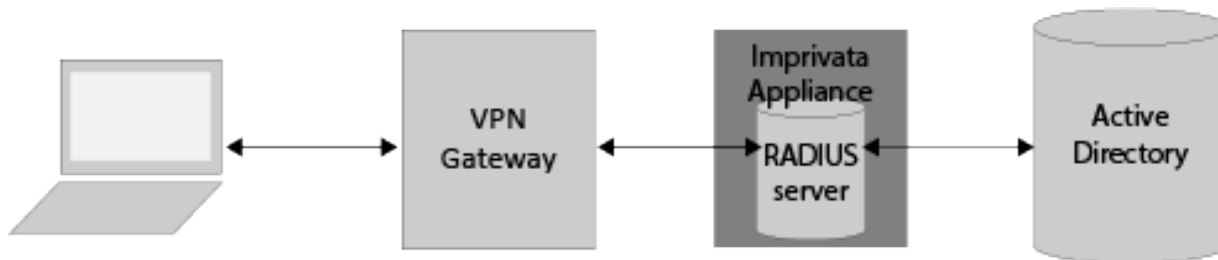
Imprivata Confirm ID handles all authentications with Active Directory:

• Your LDAP binding with AD is replaced with a connection to Imprivata's RADIUS server.
• Do not configure your gateway for two-factor authentication; the complete two-factor authentication is configured on the Imprivata Admin Console and handled between Imprivata Confirm ID and AD.
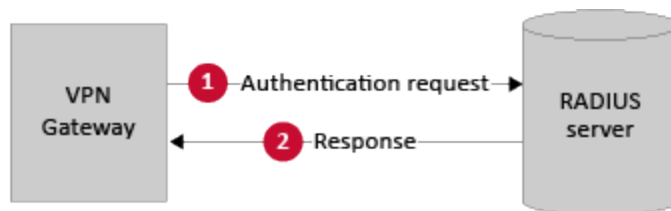
Imprivata Confirm ID authenticates remote access users via RADIUS, but the transaction stays open longer than a typical RADIUS authentication.

The connection must stay open so the user has time to respond to the notification.

Review Imprivata Confirm ID Push Authentication below and configure your retry and timeout settings accordingly.

Typical RADIUS Transaction

In a typical RADIUS transaction, the VPN gateway sends an authentication request to the RADIUS server (1) and milliseconds later, the server responds to the request (2): the transaction is complete.

RADIUS Transaction with Imprivata Confirm ID Push Authentication

Imprivata Confirm ID Push Authentication also uses the RADIUS server on the Imprivata appliance, but the transaction takes much more time to complete.

In this scenario, the user has entered their first factor credentials at the VPN gateway, and the user is configured for push authentication:
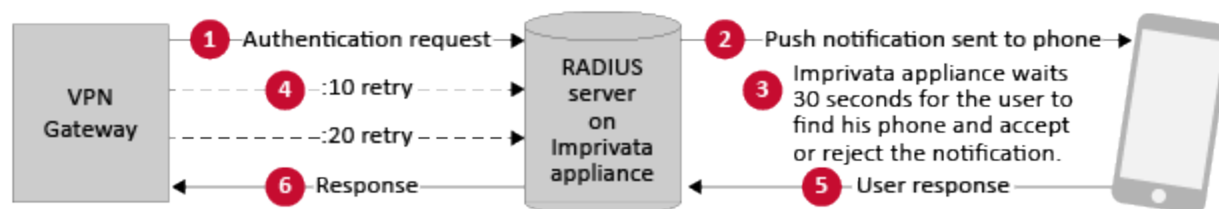
1. The VPN gateway sends an authentication request to the RADIUS server on the Imprivata appliance.

2. The Imprivata appliance sends a push notification to the Imprivata ID on the user's device.

3. The Imprivata appliance waits 30 seconds for the user to find his device and accept or reject the notification.

4. Meanwhile, the VPN gateway must wait for at least 30 seconds for a response from the Imprivata appliance. The gateway may be configured to retry the request, but it must not timeout before 30 seconds have elapsed.

5. The user accepts or rejects the push notification.

6. If the user responds within 30 seconds, the Imprivata appliance sends the response to the VPN gateway.

   If the user takes longer than 30 seconds to respond, the Imprivata appliance sends a failure notification to the VPN gateway. The user must try again, or try another authentication method (if available).

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).
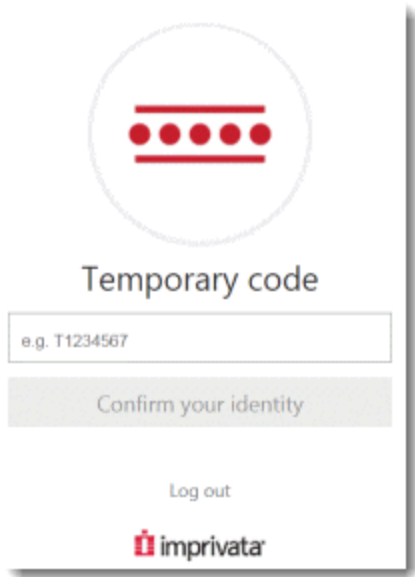
He can use the temporary code until:

- 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.

Remote Access with Citrix NetScaler Gateway — Legacy RADIUS Experience

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 will closely resemble 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.

This document contains the following sections:

© 2024 Imprivata, Inc. All Rights
Reserved.

Imprivata Enterprise Access Management
24.1

Remote Access with Citrix NetScaler Gateway - Legacy
Experience | 8

Best Practice — Use Graphical User Interface on the Web Portal

Imprivata Confirm ID offers a graphical user interface for your users when logging in remotely and enrolling authentication methods. You can enable this interface with one click when setting up the Imprivata RADIUS host below.

Diagram: Two-Factor Remote Access Authentication
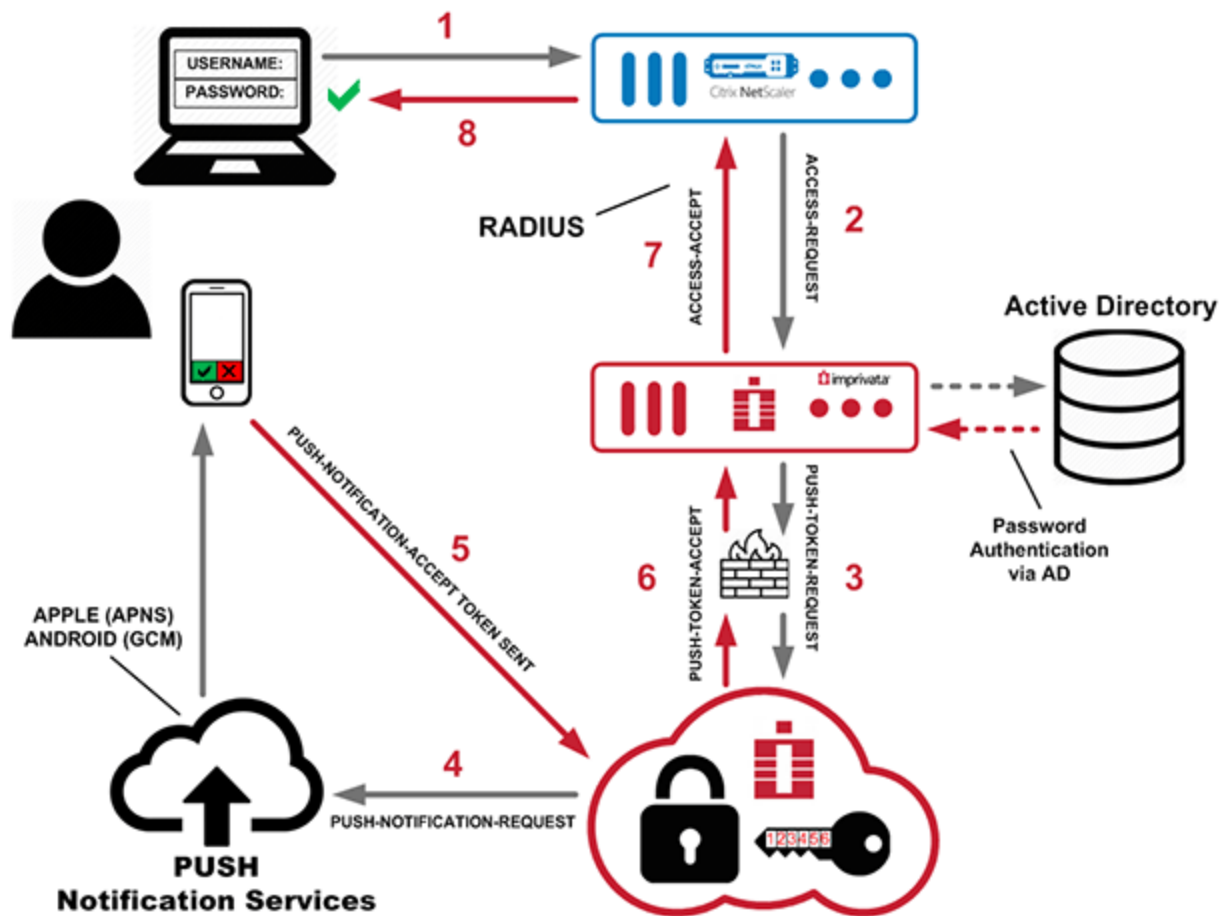
1. The user initiates primary authentication to the Citrix NetScaler Gateway.
2. The Citrix NetScaler Gateway sends a RADIUS access request to the Imprivata appliance.
3. The Imprivata appliance sends a push token request to the Imprivata Cloud Token Service.
4. Imprivata Cloud Token Service sends a push notification to the Imprivata ID app on the user's device.
5. The user accepts the push notification from the Imprivata ID app, and the device sends a token to the Imprivata Cloud Token Service.
6. The Imprivata Cloud Token Service sends a push token accept to the Imprivata appliance.
7. The Imprivata appliance sends RADIUS access accept to the Citrix NetScaler Gateway.
8. The Citrix NetScaler Gateway access granted to the user.

Configure Imprivata Remote Access

Add a New RADIUS Client

To enable Imprivata to serve your RADIUS client, name your RADIUS client and configure the NAS address / SNIP address on the Imprivata Admin Console:

1. In the Imprivata Admin Console, go to **Applications** > **Remote access integrations.**
2. Click **Add new integration**.
3. On the **Add new integration** screen:
   - Enter a descriptive **Nickname**
   - Enter the **Hostname or IP address** of the RADIUS client. (The RADIUS client may also be referred to as the Network Access Server (NAS) or VPN Server);
   - Enter the **Encryption key** (shared secret).

> **BEST PRACTICE**: This encryption key will be used as a shared secret between your server and RADIUS client. Use a computer-generated string of 22 to 64 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.

4. Click **Save**.

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 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 the RADIUS client.
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

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

If you allow non-licensed user access and a non-Imprivata user is still blocked from Remote Access, their Active Directory group may be nested and not queried in this Remote Access Log In workflow.

Example — A user who is a member of Group1, where Group1 is a member of Group2 is not considered to be a member of Group2 and will not be queried for non-Imprivata users attempting Remote Access.

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 - Configure RADIUS Group Attributes

Some RADIUS clients demand return information about authenticating users in the form of RADIUS attributes. See "Managing RADIUS Connections" in the Imprivata Online Help.

Troubleshooting The RADIUS Connection

You can troubleshoot the connection between your RADIUS client and the Imprivata appliance by viewing **serverProxy.log**:

1. On the Imprivata appliance, go to **System** > **Logs**.
2. In the section **Log data export**, export the log data for the period you wish to troubleshoot.
3. Click **View files**.
4. In the index of logs, open **RadiusENA/serverProxy.log.gz**
5. The communication between the RADIUS client and the Imprivata appliance is logged here.

Examples

- If you see the message **Source IP address [*ip address*] does not have a NAS entry**, the IP address for the RADIUS client may have been entered incorrectly or not configured at all.
- If you see **no entries in the log**, and the Imprivata appliance does not respond to the request from the RADIUS client, this may mean:
  - The IP address for the Imprivata appliance was not entered properly on the RADIUS client.
  - The authentication port for the Imprivata appliance was not set to **1812** on the RADIUS client.
- If you see the message **The Remote Authentication failed, either because the assigned user policy has no permission configured in the Authentication subtab OR the user's credentials failed**, this may mean:
  - The encryption key (shared secret) does not match on the RADIUS client and the Imprivata appliance; or
  - The RADIUS client is configured to use an unsupported protocol.
- **Push Notifications** — If the Imprivata Admin Console reports an authentication via push notification succeeded, but the RADIUS client reports the authentication timed out, the timeout value on the RADIUS client may need to be increased.

To create and run a RADIUS Activity report, in the Imprivata Admin Console, go to **Reports** > **Add new report**.

Configure the Citrix NetScaler Gateway VPN

Add a virtual server, configure RADIUS as your primary authentication method, and create a secret key.

1. On the Citrix NetScaler Gateway Configuration Utility, go to the **Configuration** tab > **NetScaler Gateway** > **Virtual Servers**.
2. Click **Add**.
3. Enter a name and IP address for your virtual server.
4. Set the port to **443**.
5. Click **OK**.
6. Set the binding to your server certificate.
7. In the section **Authentication**, click the plus sign to add a primary authentication method.
8. Select **RADIUS** Policy and set the Type to **Primary**.
9. In the section **Authentication**, click the name **RADIUS Policy**. The **VPN Virtual Server Authentication RADIUS Policy Binding** window opens.
10. Click the policy to highlight it and then cllick **Edit** > **Edit neo.server label**.
11. In the **Configure Authentication RADIUS Server** window, enter a name.
12. In the **IP Address** field, enter Imprivata appliance / RADIUS server IP address.

> ⓘ **NOTE**: If you will be using Citrix NetScaler Gateway to configure load balancing directly, enter the SNIP for RADIUS source IP address (NAS) here. See Citrix NetScaler RADIUS Load Balancing.

13. The Port for Imprivata appliances = **1812**.
14. Create a secret key to enter here. You will also enter this key as the "encryption key" in the Imprivata Admin Console (see Imprivata Remote Access).
15. Click **Done**.
16. In the **Policies** section, click the policy to highlight it, and then click **Edit** > **Edit Policy**.
17. If your RADIUS server is not selected, select it now.
18. Set the **Expression** to **ns_true**.
19. Click **OK**.

> ⓘ **NOTE**: The Imprivata Confirm ID RADIUS server only supports PAP protocol. CHAP protocols are not supported. Configure your RADIUS clients for PAP protocol to support Imprivata Confirm ID.

Optional — Native Citrix Workspace app Support

Imprivata Confirm ID supports remote access via native Citrix Workspace app, but the following configuration is required if you need to provide remote access via native Citrix Workspace app <u>and</u> remote Citrix access via the web portal.

In this section, configure one Citrix server for the web portal, and direct the native Citrix Workspace app to a subnet IP address. Then configure Imprivata Confirm ID for two separate Remote Access clients.

NetScaler Network IP Addresses

1. Log into the Citrix NetScaler Admin page > Configuration > System > Network > IPs
2. Make a note of the IP addresses: **NetScaler IP** and **Subnet IP**.

Add Two RADIUS Clients

In this section, set up two RADUIS clients: one for traffic from the Citrix web portal, and one for traffic from the native Citrix Workspace app. The web portal can use Imprivata Confirm ID's graphical user interface, while the native Citrix Workspace app must use the text-based interface.

1. In the Imprivata Admin Console go to **Applications** > **Remote access integrations**.
2. Click **Add new RADIUS client**.
3. Add a Citrix NetScaler RADIUS client using the NetScaler IP.
4. Select the graphical user interface.
5. Add a second Citrix NetScaler RADIUS client using the Subnet IP.
6. Select the Text-based user interface.
   For more details, see Add a New RADIUS Client above.

Create a Load Balancing Server

1. Log into the Citrix NetScaler **Admin** page > **Configuration** > **Traffic Management** > **Load Balancing** > **Server** and click **Add**.
2. Create a load balancing server: Enter your Imprivata appliance information.
3. Click **Create**.

Create a Load Balancing Service

1. Go to the Citrix NetScaler **Admin** page > **Configuration** > **Traffic Management** > **Load Balancing** > **Services** and click **Add**.
2. Create a load balancing service: Use the just-created load balancing server as the service provider.
3. Click **OK**.

Dashboard	Configuration	Reporting

← | Load Balancing Service

Basic Settings

Service Name*

Radius Server

○ New Server ● Existing Server

Server*

10.113.219.15 (10.113.219.15) ▼

Protocol*

RADIUS ▼

Port*

1812 ✕ ❓

▶ More

[OK] [Cancel]

Create a Load Balancing Virtual Server

1. Go to the Citrix NetScaler **Admin** page > **Configuration** > **Traffic Management** > **Load Balancing** > **Virtual Servers** and click **Add**.
2. Create a load balancing virtual server:
   a. Protocol = **RADIUS**;
   b. Enter a domain IP address;
   c. RADIUS port = **1812**
   d. Bind the just-created load balancing service to the virtual server.
3. Click **Done**.

Create an Authentication RADIUS Server

1. Go to the Citrix NetScaler **Admin** page > **Policies** > **Authentication** > **RADIUS** > **Servers**.
2. Create an authentication RADIUS server by using the just-created Load Balancing Virtual Server:
   a. Create a secret key to enter here. You will also enter this key as the "encryption key" in the Imprivata Admin Console (see Imprivata Remote Access).
   b. Change the Time-out value to 30 seconds or greater.
3. Click **Create**.

Create Two RADIUS Authentication Policies

1. Go to the Citrix NetScaler **Admin** page > **Policies** > **Authentication** > **RADIUS** > **Policies**.
2. Bind one policy to the normal Imprivata appliance, and the other policy to the just-created RADIUS "load balancing" virtual server which is, in reality, also pointing to the Imprivata appliance.

☐	VS201_WebPortal	REQ.HTTP.HEADER User-Agent NOTCONTAINS CitrixReceiver	VS201_RADIUS_SERVER ✖
☐	VS201_CitrixReceiver	REQ.HTTP.HEADER User-Agent CONTAINS CitrixReceiver	VS201_RADIUS_LB ✖

Bind RADIUS Authentication Policies to the Virtual Server

Bind the two RADIUS authentication policies to the NetScaler Gateway Virtual Server for the user login interface:

1. Go to the Citrix NetScaler **Admin** page > **Virtual Gateways**.
2. Add or configure a gateway virtual server and bind the two RADIUS authentication policies to the virtual server.

Optional — Citrix NetScaler 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 to distribute RADIUS traffic from the Citrix NetScaler Gateway to all your Imprivata appliances in production.

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

On the Citrix NetScaler Gateway Configuration Utility, go to the **Configuration** tab > **Traffic Management** > **Load Balancing** > **Servers**:

1. **Create Servers**: Add the names and IP addresses or domain names for each Imprivata production appliance in your enterprise.
2. **Add A Service Group**: Add your Imprivata appliances into a service group. Configuring a service group enables you to manage a group of Imprivata appliances as easily as a single appliance.
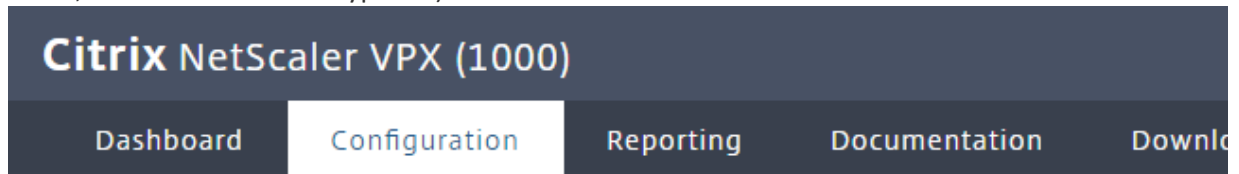3. **Add a Virtual Server**: Add a Virtual Server for your service group.

Optional — Returning An Active Directory Password in the RADIUS Response

Imprivata Confirm ID can be configured to return the authenticating user's Active Directory (AD) password back to the RADIUS client as part of the RADIUS Accept-Accept response.

The objective of this functionality is to eliminate the need for users to provide their AD password when authenticating to their VPN or VPN SSL box with other authentication methods such as VASCO, RSA, Imprivata ID, or SMS authentication. Allowing the VPN client to use the user's cached AD password to avoid challenging the user when they access AD-based resources. The AD password will be returned using the RADIUS PAP protocol. Due to limitations in the PAP protocol, the AD password will <u>not</u> be encrypted.

To configure the Citrix NetScaler Gateway to consume the user's AD password via a RADIUS attribute, set the **Password Vendor Identifier** and **Password Attribute Type** when configuring the RADIUS server. The RADIUS attribute will need to be added to the RADIUS host on the Imprivata appliance to send the AD password. The following steps demonstrate how to configure the Citrix NetScaler Gateway and the Imprivata appliance.

1. On the Citrix NetScaler Gateway, configure the Authentication RADIUS server (Password Vendor Identifier = **398**; Password Attribute Type = **5**)

2. In the Imprivata Admin Console, go to **Applications** > **Remote access integrations** > **RADIUS attributes**.
3. Add attribute (Attribute Number = **26**, Vendor Code = **398**, Vendor-Specific Attribute Number = **5**, and Attribute Value = **%password%**

RADIUS global attributes (optional)

26	%password%
398	5

Add attribute

Allow or Restrict Access Based on RADIUS Attributes

Review your Authorization Policy to determine if Citrix Netscaler limits remote access by Active Directory groups. If yes, then you need to configure Imprivata Confirm ID to send specific extended attributes so Citrix receives this information via the Imprivata RADIUS server.

If you review your Authorization Policy and determine Citrix Netscaler does not limit remote access by Active Directory groups, skip this section.

1. Configure the group attributes that the RADIUS client (NetScaler) will receive from the RADIUS server (Imprivata). This can be vendor-specific attributes (VSA) or RADIUS well-known attributes such Class attribute type 25, shown:

Configure Authentication RADIUS Server

Name

PER60_RADIUS_SERVER

○ Server Name   ● Server IP

IP Address*

| 10 | . | 113 | . | 204 | . | 60 | ☐ IPv6

Port*

1812

Time-out (seconds)

60

Secret Key*

••••••••••••••••••••••••••••

Confirm Secret Key*

••••••••••••••••••••••••••••

☐ Send Calling Station ID

NAS ID

☐ Enable NAS IP address extraction

Group Vendor Identifier

Group Prefix

Group Attribute Type

25

NetScaler client will listen for this attribute type when receiving group information from the Imprivata appliance. Attribute type 25 is a well-known RADIUS class attribute.

NetScaler will listen for this attribute type when receiving group information from the Imprivata appliance. Attribute type 25 is a well-known RADIUS class attribute.

2. Edit the NetScaler session policy for the virtual server. Go to the **Security** tab > **Advanced Settings**:

3. Next to the "Allow Groups to Login" textbox, click the checkbox to enable the field.
4. Enter the names of the Class Attributes that will be allowed to log into the VPN.
   This attribute value is sent in the RADIUS Access-Accept packet during a successful authentication. If the Class attribute matches the value sent, the user will be allowed to login.

5. Server Group configuration:
   - Sending groups using RADIUS well-known attribute type **25**
   - The group attribute value will be sent to the RADIUS client if the user is a member of anyone of the AD groups selected.

Optional — Configure the VPN via the CLI

You may find it easier to configure Citrix NetScaler via the CLI.

Parameters (example)

- virtual server name = VS191
- virtual server IP address = 10.113.213.191
- certificate name = MyCompanyCert
- radius server name = VS191_RADIUS_SERVER
- radius server IP address = 10.113.204.60
- radius policy name = VS191_RADIUS_POLICY

Command Line Configuration

```
config> vpn vserver VS191 ssl -state enabled 10.113.213.191 443

config> exit

config> bind ssl vserver VS191 -certkeyName "MyCompanyCert"

config> authentication radiusACtion VS191_RADIUS_SERVER -serverIP 10.113.204.60
-radKey password

config> serverPort 1812

config> authTimeout 60

config> exit

config> authentication radiusPolicy VS191_RADIUS_POLICY ns_true VS191_RADIUS_SERVER

config> exit

config> bind vpn vserver VS191 -policy VS191_RADIUS_POLICY -priority 100

config> bind vpn vserver VS191 -policy SETVPNPARAMS_POL -priority 100
```

© 2024 Imprivata, Inc. All Rights
Reserved.

Imprivata Enterprise Access Management
24.1

Remote Access with Citrix NetScaler Gateway - Legacy
Experience | 30

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 <u>not</u> associate any user policies with this workflow yet; you will "go live" with Remote Access later in this section.
4. Click **Save**.

> (i) **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.

> **(i)** **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, <u>or</u> 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.

Supporting Citrix NetScaler Gateway RfWebUI Portal Theme

Imprivata Confirm ID supports Remote Access integration with Citrix NetScaler Gateway 11.1.

However, if you have enabled Imprivata's graphical user interface for your RADIUS client, and you are using NetScaler 11.1's **RfWebUI Portal Theme** (Receiver for Web UI), configuration of a Rewrite Action and Policy applied to your virtual server is required. If you must use NetScaler's RfWebUI Portal Theme, users will not be able to log in without the configuration described in this topic.

Example: Configuration Required

When you have integrated Citrix NetScaler with Imprivata Confirm ID, but you have not successfully configured the Rewrite Policy and Action as described below: After users enter their username and first factor authentication (password, for example),

- The RfWebUI theme will <u>not</u> display the Imprivata Confirm ID graphical user interface;
- A string of JSON code will appear in the NetScaler user interface;
- The user will be unable to enter their second-factor authentication;
- The user will be unable to proceed.

Example: Configuration Success

When you have integrated Citrix NetScaler with Imprivata Confirm ID, and you have successfully configured the Rewrite Policy and Action as described below:

After users enter their username and first factor authentication (password, for example), the Imprivata Confirm ID user interface will appear and prompt the user to complete second factor authentication (Imprivata ID in this example):
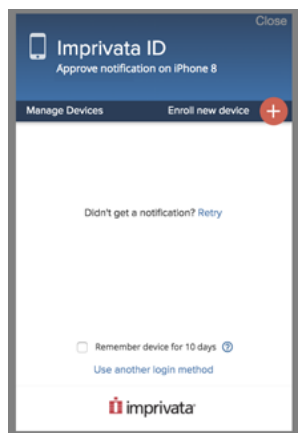
Configure the Rewrite Policy and Action

To configure the rewrite policy and action via the command-line interface, SSH into the NetScaler server and enter the following commands <u>with specific customizations for your enterprise</u>:

```
config> add rewrite action example_rewrite_action INSERT_BEFORE_ALL HTTP.RES.BODY
(1000000)
'"<script src=\'https://impr1.co/3/nr.js\'></script>"' -search Text("</body>")

config> add rewrite policy example_rewrite_policy HTTP.REQ.URL.ENDSWITH
("logon/LogonPoint/index.html") example_rewrite_action

config> bind vpn vserver example_server -policy example_rewrite_policy -type RESPONSE
-priority 100 -gotoPriorityExpression end
```

Edit these commands as follows:

- **example_rewrite_action** — Give the Rewrite Action a descriptive name;
- **example_rewrite_policy** — Give the Rewrite Policy a descriptive name;
- **example_server** — Use the actual vserver name;
- **logon/LogonPoint/index.html** — this the default path to the NetScaler login screen. If your login screen URL is different, edit this string to match.

Configure the Rewrite Policy and Action via GUI

You can configure these same settings manually in the Citrix NetScaler VPX graphical user interface:

Create A Rewrite Policy

1. In the Citrix NetScaler VPX, select the virtual server where the RfWebUI Theme is in use.
2. In the **Policies** section, click the **+ button** to add a policy.
3. In the **Choose Type** window, choose **Policy: Rewrite** and **Type: Response**.
4. Click **Continue**.
5. On the **Choose Type** screen > **Policy Binding** section, click the **+ button** to create the policy.
6. Edit the policy you've just created:
   a. Give the policy a descriptive name.
   b. Leave the **Undefined-Result-Action** as the default
   c. Set the **Expression** as: `HTTP.REQ.URL.ENDSWITH("logon/LogonPoint/index.html")`

      The string inside the quotes is the default path to the NetScaler login screen. If your login screen URL is different, edit this string to match.
   d. Click **Create**.

      After this policy is created, you will see it listed on the virtual server page > **Policies** > **Response Policies** ("**1 Rewrite Policy**", for example).
7. To continue creating this policy you need to create a Rewrite Action and select it for this policy. See Create A Rewrite Action below.

Create A Rewrite Action

This Rewrite Action will insert an Imprivata script into your login page HTML code. When successful, you can view the source of your login page HTML and find this code (usually very close to the end, near the </body> tag).

1. In the **Configure Rewrite Policy** window, go to the **Action** field and click the **+ button** to create a Rewrite Action.

2. Configure the Rewrite Action you've just created:

   a. Give the policy a descriptive name.

   b. Set the **Type** as **INSERT_BEFORE_ALL**

   c. Set the **Expression to choose target location** as `HTTP.RES.BODY(10000000)`

   d. Set the **Expression** as: `"<script src='https://impr1.co/3/nr.js'></script>"` (including the double quotes)

   e. Select the **Search** radio button, set the field to **Text**, and the string `</body>`

   f. Click **Create**.

3. Return to the Rewrite Policy you created earlier and in the **Action** field, select this Rewrite Action and then click **OK** to save your change.

4. To complete creating this policy you need to bind the rewrite policy and action to the virtual server. See Bind Policy to Virtual Server below.

Bind Policy to Virtual Server

After the rewrite policy and action have been created, your new rewrite policy will appear on the **Choose Type** screen. If necessary, change the priority and/or goto expression, then click **Bind** to bind the policy to the virtual server.