imprivata®

Product Documentation

Configuring Remote Access with Microsoft Active Directory Federation Services

Imprivata Enterprise Access Management 24.1

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.

Imprivata Confirm ID integrates with Microsoft Active Directory Federation Services (AD FS) to streamline authentication management and simplify two-factor authentication for Microsoft Office 365, cloud applications, and remote access for employees. In addition to logging in remotely, Imprivata Confirm ID users can also enroll authentication methods from outside your network.

When logging in remotely and enrolling authentication methods, the user interface will closely resemble the Imprivata Confirm ID enrollment utility on the Imprivata agent.

Review Imprivata Confirm ID Supported Components to confirm that your version of AD FS is supported. Fully configure your AD FS environment for remote access with single-factor username and password authentication before configuring its connection to Imprivata.

This document contains the following sections:

Optional — Load Balancing

BEST PRACTICE: In large deployments, a load balancing solution should be used to distribute RADIUS traffic from AD FS to all your Imprivata servers in production. In a large deployment, you should not configure AD FS to send all RADIUS requests to one Imprivata server. For users to authenticate successfully, a user session should be persistent to one Imprivata appliance.

Troubleshooting — Imprivata GUI Does Not Appear

Your browser may be blocking Imprivata Confirm ID's login user interface because the browser's Content Security Policy prohibits content that the user did not request from the Imprivata cloud.

1. Run the following Powershell command to inject a script that adds an exception to the Content Security Policy:

   ```
   Set-AdfsResponseHeaders -SetHeaderName "Content-Security-Policy" -SetHeaderValue
   "default-src 'self' 'unsafe-inline' 'unsafe-eval' impr1.co; img-src 'self' data:;"
   ```

2. Restart all your AD FS servers for this exception to take effect.

Add AD FS 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 RADIUS client**.
3. On the **Add new RADIUS client** screen:
   - Select **Microsoft AD FS**
   - Enter a descriptive **Client name**
   - 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 22-31 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**.
5. A message will appear onscreen with a link to download the **Imprivata Connector for AD FS**. You can also download this software from the Imprivata Customer Experience Center.
   The Imprivata Connector for AD FS is required to enable the connection between AD FS and Imprivata Confirm ID. You will install the Connector later in this process.

> **NOTE**: Some RADIUS clients demand return information about authenticating users in the form of RADIUS attributes. The Imprivata Connector for AD FS handles RADIUS communication directly so RADIUS attribute settings are not manually configurable for AD FS.

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.

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 a 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.

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.

NOTE: Passwords are authenticated directly by your Microsoft Active Directory server, not by the Imprivata appliance. If your users authenticate with password, you must select password in their Imprivata Confirm ID Remote Access workflow even though the Imprivata appliance is not authenticating it.

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. Later, you will need to organize the same users in your Microsoft AD FS environment. To enable multi-factor authentication, it is critical for these users and groups to match exactly.

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).

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,
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.

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. .

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 Optional — Load Balancing

Install and Activate the Imprivata Connector for AD FS

After adding Microsoft AD FS as a RADIUS client, a message will appear on the Imprivata Admin Console with a link to download the Imprivata Connector for AD FS. You can also download this software from the Imprivata Customer Experience Center.

The Imprivata Connector for AD FS is required to enable the connection between AD FS and Imprivata Confirm ID.

> **NOTE:**
> The Imprivata Connector for AD FS requires that your servers' system locale (or the service account user) is set to EN-US.

Add Exception To Content Security Policy

Your browser may be blocking Imprivata Confirm ID's login user interface because the browser's Content Security Policy prohibits content that the user did not request from the Imprivata cloud.

1. Run the following Powershell command to inject a script that adds an exception to the Content Security Policy:

   ```
   Set-AdfsResponseHeaders -SetHeaderName "Content-Security-Policy" -SetHeaderValue
   "default-src 'self' 'unsafe-inline' 'unsafe-eval' impr1.co; img-src 'self' data:;"
   ```

2. Restart all your AD FS servers for this exception to take effect.

Install the Connector

Run the InstallShield wizard to set up the Imprivata Connector for AD FS. The following information is required during the installation of the Connector:

- Your primary Imprivata server FQDN or IP address. You can find this on the Imprivata Admin Console > Applications > **Remote access integrations** page.
- Best Practice — Also configure a secondary (backup) Imprivata server.
- The RADIUS encryption key (shared secret) — the same key you set when adding this RADIUS client on the Imprivata Admin Console.

When the InstallShield wizard is complete, you will be asked to restart AD FS and enable Imprivata Confirm ID:

- **Automatically Restart and Enable** — The AD FS service will restart (causing AD FS downtime), the Imprivata Connector for AD FS installation will be completed, and Imprivata Confirm ID will "go live" for all users and groups selected in your AD FS Global Authentication Policy.
- **Perform these steps later** — you must manually restart the AD FS service (perhaps during a scheduled "maintenance window"). To "go live", you must manually activate the Imprivata Connector in the AD FS Global Authentication Policy.

AD FS 3.0 — Enable/Disable Multi-Factor Authentication with Imprivata Confirm ID

Manually enable or disable the connection to Imprivata Confirm ID at any time:

1. On the AD FS console, go to **AD FS Management** > **Edit Global Authentication Policy** > **Multi-Factor** tab.
2. Select or deselect **Imprivata Authentication** to turn Imprivata Confirm ID on or off.

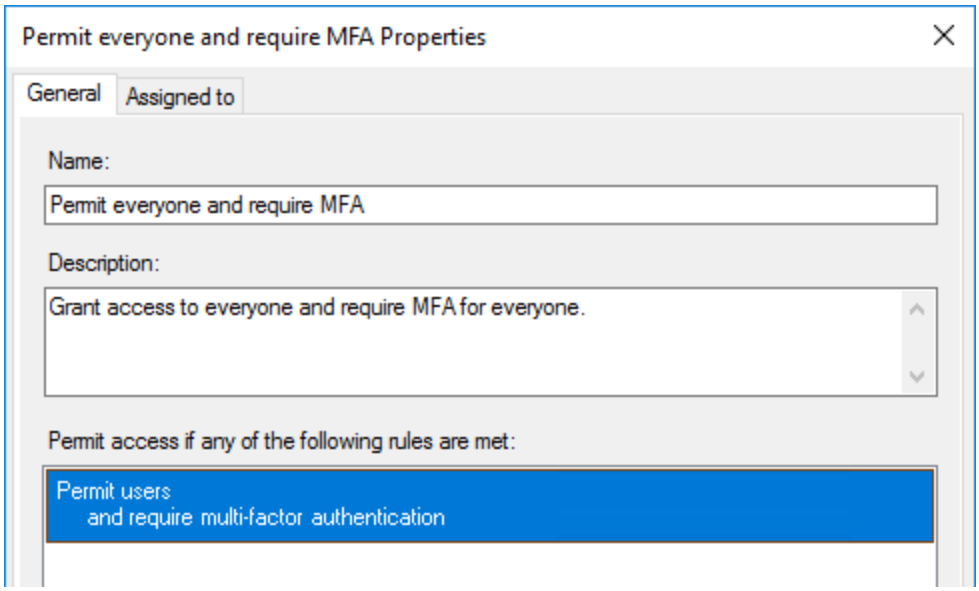
   When **Imprivata Authentication** is not selected, AD FS users will not be prompted for two factor authentication with Imprivata Confirm ID.
3. Turn on Imprivata Confirm ID for users, groups, or locations:
   - To assign specific domain users or groups for multi-factor authentication, click **Add...**
     - This is a global setting for your whole AD FS enterprise, whether they are at home or at work.
     - Making a selection here takes precedence over the **Device** and **Location** settings below.
   - If you just want to turn on Imprivata Confirm ID for unregistered devices, click **Devices** > **Unregistered devices**. Making a selection here takes precedence over the **Locations** setting below.
   - If you just want to turn on Imprivata Confirm ID for users outside your network, select **Locations** > **Extranet**.
4. Click **OK**.

AD FS 4.0 — Enable/Disable Multi-Factor Authentication with Imprivata Confirm ID

Manually enable or disable the connection to Imprivata Confirm ID at any time:

1. On the AD FS console, go to **Service** > **Authentication Methods** > **Edit Multi-factor authentication methods** > **Multi-Factor** tab.
2. Select or deselect **Imprivata Authentication** to turn Imprivata Confirm ID on or off.

   When **Imprivata Authentication** is not selected, AD FS users will not be prompted for two factor authentication with Imprivata Confirm ID.
3. To assign only specific domain users or groups for multi-factor authentication, go to **AD FS** > **Access Control Policies**, and add or edit a policy.



4. Go to **AD FS** > **Relying Party Trusts** and right-click the Display Name to edit. Select **Edit Access Control Policy**.
5. Select the access control policy that meets your needs. Click **OK**.

Optional — Edit Connector Settings After Installation

After your initial setup with the InstallShield wizard, you can change the shared secret, add Imprivata servers to your configuration, edit the list of servers, and edit the failover settings for each.

To edit Connector settings, edit the Imprivata Config JSON formatted file (take care to use proper JSON syntax) to add/drop Imprivata servers and edit failover settings if needed.

Your config JSON file comprises the current configuration of your AD FS / Imprivata enterprise. It is located in the default install folder: **C:\ProgramFiles(x86) \Imprivata\ADFS\Imprivata_ADFS_Config.json**

Sample: Imprivata_ADFS_Config.json

```
{
                                "Servers": [
                                {
                                "Host": "server1.domain.eng",
                                "RetryCount": 3,
                                "RetryInterval": 3
                                },
                                {
                                "Host": "server2.domain.eng",
                                "RetryCount": 3,
                                "RetryInterval": 3
                                }
                                ],
                                "UnavailableInterval": 30
                }
```

Shared Secret: For security reasons you cannot view or edit the shared secret in the config JSON file. The PS1 script will prompt you to change the shared secret if needed. See the following section.

Default failover settings: the Imprivata Connector for AD FS will retry three times to contact the Imprivata server, waiting three seconds between each retry. If a server is still unresponsive after three attempts, the Connector will mark that server unavailable for 30 seconds. Then the Connector will failover to the next available server in the failover server list.

Run the PS1 Script

After editing and saving the JSON file, run **configure_adfs_plugin.ps1**

If necessary, you can enter a new shared secret.

The AD FS service must be restarted for the changes to take effect.

NOTE: When you run the PS1 script, your existing configuration is replaced with the contents of the JSON file. For example, if you want to keep two existing servers and add another, you must list all three in the JSON file.

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.

Configure AD FS Users/Groups for Multi-Factor Authentication

To enable multi-factor authentication, your users / groups must be added to the Multi-factor tab. It is critical for these users and groups to match exactly.

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, create one now.

Go to your **AD FS Global Authentication Policy**. On the **Multi-factor** tab > **Users/Groups** section, do not select all your users / groups. Instead, select only a pilot group of users. When your pilot is complete and you are ready to "go live" to a larger group, add those users / groups on the **Multi-factor** tab > **Users/Groups** section.

- Users/Groups selected in **AD FS Global Authentication Policy**. On the **Multi-factor** tab > **Users/Groups** section, select only the users and groups that will be using Imprivata Confirm ID Remote Access.
  AND
- When you organize your **Imprivata Confirm ID users/groups** into user policies, you must associate the exact same users/groups with your Remote Access workflow.

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.

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**.

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.

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.

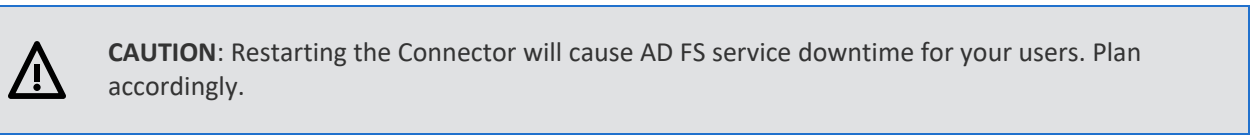
Step 7: Future Rollouts

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

Troubleshooting: "An error occurred"

If the user sees the message "An error occurred. Contact your administrator for more information", it's possible the Imprivata Connector for AD FS event log does not exist, and the Connector must be restarted:

1. Open Powershell as an administrator. Check if the Imprivata AD FS event log exists:
   `> Get-EventLog -LogName "Imprivata ADFS"`
2. If the event log exists, the events in the log may help you diagnose the issue; or you may see the following:
   `Get-EventLog : The event log 'imprivata ADFS' on computer '.' does not exist.`
3. If the event log does not exist, run the following command to create the event log:
   `>New-EventLog -LogName "Imprivata ADFS" -Source "ImpADFSLog"`
4. Run the Get command again to confirm the event log was created. Because no events have occurred, you will see an empty log.
5. Restart the Imprivata Connector for AD FS.

   `> Restart-Service adfssrv`
6. Run the get command again, or refresh the event viewer and look for any entries in AD FS event log:
   `> Get-EventLog -LogName "Imprivata ADFS"`
7. Confirm the successful restart: Attempt to log in with Imprivata two-factor authentication.