Product Documentation

Remote Access with F5 BIG-IP

Imprivata Enterprise Access Management 25.2

Contacting Imprivata

20 CityPoint, 480 Totten Pond Road, 6th Floor

Waltham, MA 02451 USA

Phone: 781-674-2700

Toll-Free: 1-877-OneSign

Fax: 1 781 674 2760

Support: 1 800 935 5958 (North America)

Support: 001 408-987-6072 (Outside North America)

https://www.imprivata.com

support@imprivata.com

Copyright and Legal Information

Trademark Information

Legal Notices

Document revision 25.2

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 Enterprise Access Management for MFA (formerly 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 Enterprise Access Management Remote Access.
- The Imprivata cloud provides access to cloud-based features delivered in future versions of Enterprise Access Management.

How To Use Enterprise Access Management Remote Access

Before enabling Enterprise Access Management Remote Access, there are major decisions you need to make about how to use it.

- **Who do I want to use Enterprise Access Management 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 Enterprise Access Management to send extended attributes via its RADIUS server so your gateway can allow and deny access by AD groups.

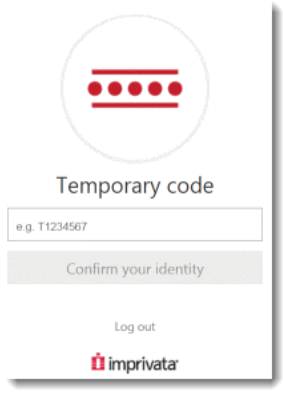
Optional — Temporary Codes

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 Enterprise Access Management 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 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 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 Enterprise Access Management 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 F5 BIG-IP VPN

Imprivata Enterprise Access Management (formerly Imprivata Confirm ID) integrates with F5 BIG-IP VPN to streamline authentication management and simplify two-factor authentication for remote access for employees. In addition to logging in remotely, Enterprise Access Management users can also enroll authentication methods from outside your network.

Before You Begin

Fully configure your F5 BIG-IP VPN environment for remote access with single-factor username and password authentication before configuring its connection to Imprivata.

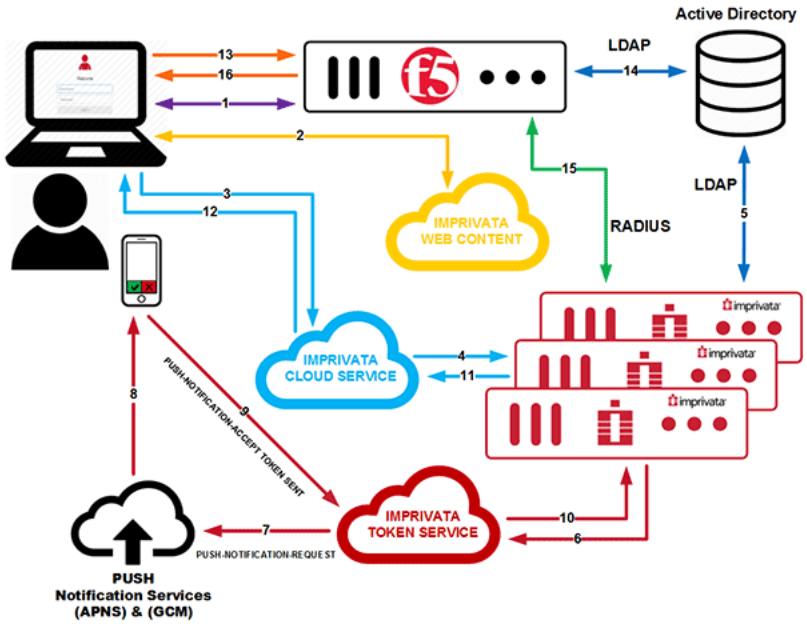
Diagram: Two-Factor Remote Access Authentication

The Imprivata Cloud Remote Access experience replaces the F5 BIG-IP default login screen with an Imprivata-powered graphical login screen.

This graphical login screen authenticates the user with Enterprise Access Management via the Imprivata Cloud. Only after the authentication is complete, Enterprise Access Management sends the following to F5 BIG-IP:

- Username and Password go to the F5 BIG-IP LDAP primary authentication
- Username and authentication success token go to the F5 BIG-IP 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 F5 BIG-IP.



1. Primary authentication initiated to the F5 BIG-IP. 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. F5 BIG-IP verifies the username and password. The group and other attributes are sent back to the gateway for authorization.
15. F5 BIG-IP verifies the Imprivata secure token over RADIUS to the Imprivata appliance.
16. F5 BIG-IP VPN access granted to the user.

Cloud-Based Remote Access Integration

Integrate your Enterprise Access Management environment with F5 BIG-IP.

1. In the Imprivata Admin Console, go to **Applications** > **Remote access integrations**.
2. Click **f5** > **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 F5 BIG-IP Integration

1. On the **Add new F5 BIG-IP integration** page:
   - Enter a descriptive **Nickname**
   - Enter the **Hostname or IP address** of the F5 BIG-IP client. (The F5 BIG-IP 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 (F5 BIG-IP). Use a computer-generated string at least 22 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 F5 BIG-IP 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 the F5 BIG-IP VPN

There are five configuration steps to integrate Enterprise Access Management Remote Access with F5 BIG-IP:

- Add the RADIUS Client to point to the Imprivata appliance
- Edit the login page to include a third login field
- Add token authentication via the RADIUS server as a second factor to your Access Policy
- Customize the logon page by pasting in the integration script
- Increase the logon page session timeout to allow time for the user to enroll IID

Add RADIUS Client

1. On the F5 console, go to **Access** > **Authentication** > **RADIUS** > **Create...**
2. Configure the fields as follows. Click **Finished** when you're done:

Name	`impr-radius-server`	
Server Connection	Direct	
Server Address	Enter the IP address of the Imprivata appliance.	
Authentication Service Port	1812	
Secret	Enter the **Secret**, and again in the **Confirm Secret** field.	This is the same key as the "encryption key" entered in the Imprivata Admin Console > **Applications** > **Remote access integrations**.
Timeout	5 seconds (default)	
Retries	3 (default)	

Edit Logon Page to Include Third Logon Field

1. On the F5 console, go to **Access** > **Profiles / Policies** > **Access Profiles (Per-Session Policies)**
2. In the row for your existing Access Profile for LDAP authentication, in the Per-Session Policy column, click **Edit...**
3. Click the **Logon Page** action. Configure the fields as follows:

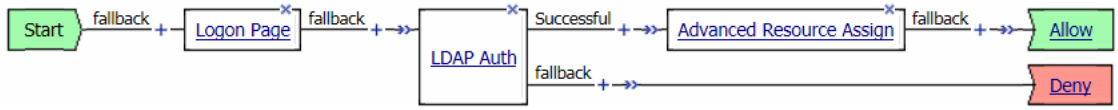
Third field Type:	password
Post Variable Name	`password1`
Session Variable Name	`password1`
Logon Page Input Field #3	Token (default)

4. **Save** your changes when you're done.
5. **Apply** the saved changes to the Access Policy: click **Apply Policy** next to the F5 logo at the top of the page (this click redirects you to **Access** > **Profiles / Policies** > **Access Profiles (Per-Session Policies)**).
6. Select the Access Policy and click **Apply**.

Add Token Authentication As A Second Factor

1. On the F5 console, go to **Access** > **Profiles / Policies** > **Access Profiles (Per-Session Policies)**
2. In the row for your existing Access Profile for LDAP authentication, in the Per-Session Policy column, click **Edit...**

   Your existing Access Policy should look something like this:

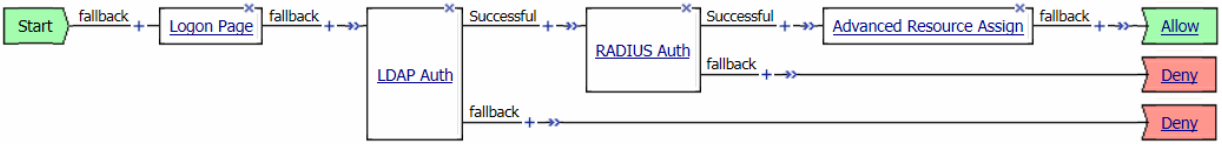


3. Just to the right of **LDAP Auth** action **Successful** , click **+** to add a new action.
4. Click the **Authentication** tab, select **RADIUS Auth** from the list, and click **Add Item**.
5. Configure the fields as follows.

AAA Server	`impr-radius-server`	Select the server you created above.
Password Source	`%{session.logon.last.password1}`	Add a "1" to "password" to match the variable name you created above

6. Click **Save**.

   Your revised Access Policy should look like this:



7. **Apply** the saved changes to the Access Policy.

Add Integration Script to Logon Page

1. In the Imprivata Admin Console, copy the Remote Access Integration script. Go to **Applications** > **Remote access integrations** page.
2. On the F5 console, go to **Profiles / Policies** > **Customization** > **Advanced**
3. In the **Form Factor** navigation, go to **Customization Settings** > **Access Profiles** > ***your policy name*** > **Access Policy** > **Logon Pages** > **logon.inc**
4. Paste the Imprivata integration script manually before the close body tag. Example (your token code will be different):

```
<!--Imprivata F5 Integration Script -->
<script src='https://cidra.integration.common.imprivata.com/static/js/embed/f5.js'
data-access-token='eyJ0ZW5hbnRJZCI6IjQyNTQ3NzU5ODUwMDM2MzUzNiIsCiJjb250ZXh0RGF0YSI
6CnsiYXV0aEFwcElkIjoiTmV0c2NhbGVyIiwKImF1dGhJbnN0YW5jZUlkIjoiMDkxNDdiNzktYjEwNS00N
WQzLTk0N2ItNzliMTA1NjVkM2VhIn19'></script>
</body>
</html>
```

5. Click **Save**.
6. **Apply** the saved changes to the Access Policy.

Repeat for every server's access policy where you need to integrate with Imprivata Confirm ID. This script only affects servers using this access policy.

Best Practice: Increase Logon Page Session Timeout

Enterprise Access Management enables your users to enroll Imprivata ID when logging in remotely. However, unless you increase F5's default five minute session timeout, the user's session may time out when they turn away from their browser to install the Imprivata ID app on their device.

1. On the F5 console, go to **Access** > **Profiles / Policies** > **Access Profiles (Per-Session Policies)**
2. Click on the Access Profile **Name** (not the **Edit** link)
3. Go to **Settings** > **Access Policy Timeout**. This value is set to **300** seconds by default. Best Practice: increase value to to **900** seconds.
4. Click **Update**.
5. **Apply** the saved changes to the Access Policy.

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 their username and password on their endpoint computer, then 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.

Setup

1. In the Imprivata Admin Console, go to **Users** > **Workflow Policy**.
2. On the **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 Enterprise Access Management 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 enters the two-digit code on Imprivata ID, they are given access to the application/resource.

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 Enterprise Access Management Remote Access with your gateway, the following users will be blocked from logging in:

- Imprivata MFA and SSO 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 Enterprise Access Management 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 Enterprise Access Management 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.

Rolling Out Remote Access

Now that the gateway software and the Imprivata appliance are configured to communicate with each other, you can roll out Enterprise Access Management for MFA to your users.

Step 1: Organize Users

You control how your users enroll and log in with Enterprise Access Management 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 Enterprise Access Management 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 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, Enterprise Access Management 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

Enterprise Access Management 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 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**. Enterprise Access Management enrollment and remote access are now live only for the users in the pilot.

Step 4: Notify Users

Before you "go live" with Enterprise Access Management 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 **MFA** > **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.