



Product Documentation

Enrollment Guide for Remote Access

Imprivata Enterprise Access Management 24.3

Enrolling Authentication Methods for Remote Access Workflows



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.

The following sections explain how to enroll your Imprivata ID and phone number for Imprivata Enterprise Access Management Remote Access (formerly Confirm ID Remote Access).

The authentication methods you are allowed to use may vary in your organization, so both Imprivata ID and SMS authentication may be available to you.



NOTE: These workflows are for users who do not require or have already completed identity proofing.

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

To open the Imprivata enrollment utility, click the Imprivata icon in the Windows notification area (Imprivata agent menu), and then click **Enroll Authentication Methods**.



NOTE: You will receive a confirmation email for each authentication method you enroll. If you receive an email confirmation for an authentication method that you did not enroll, or you believe you received an email in error, contact your Imprivata Enterprise Access Management administrator.

Enrolling Your Imprivata ID

Based on the required Imprivata ID feature, make sure that the following requirements are met.



NOTE: Unless otherwise noted, a requirement applies to all Imprivata ID features.

iOS Requirements

- iOS 11 or later installed.
- An active Internet connection is required to enroll Imprivata ID, as well as to send log files to Imprivata.
- **Hands Free Authentication:**
 - Bluetooth enabled.
 - Access to Location Services (Always).
 - An active Internet connection is not required for Hands Free Authentication or manual token code entry.
- **Remote Access:**
 - Notifications enabled.
 - An active Internet connection is required for push notifications.
- **Secure Walk Away**
 - iPhone 6s or later.
 - Access to Location Services (Always), Bluetooth Sharing, and Motion & Fitness is required.
- QR code for direct access to the download page on the [iTunes App Store](#):



Android Requirements

- Android 6 or later installed.
- An active Internet connection is required to enroll Imprivata ID, as well as to send log files to Imprivata.
- **Hands Free Authentication:**
 - Bluetooth enabled.
 - An active Internet connection is not required for Hands Free Authentication or manual token code entry.
- **Remote Access:**
 - Notifications enabled.
 - An active Internet connection is required for push notifications.
- **Secure Walk Away:**
 - Samsung Galaxy S7 or later.
 - Google Pixel 1 or later.
 - OnePlus 6 or later.
 - Bluetooth enabled.
- QR code for direct access to the download page on [Google Play](#):



Typical Imprivata ID Enrollment

1. Open the Imprivata ID app on your device.
2. Log into the Imprivata enrollment utility on a computer: Click the Imprivata icon in the Windows notification area (Imprivata agent menu), and then click **Enroll Authentication Methods**.
The authentication methods available for you to enroll are displayed:
3. Click **Get Started!** or **Enroll your Imprivata ID** on the enrollment utility home screen. The **Enroll your Imprivata ID** screen opens.
4. Enter the 12 character serial number and six digit token code displayed on the Imprivata ID app screen.
5. Click **Done**.
6. When your Imprivata ID is successfully enrolled, your device's name appears on the Imprivata enrollment utility screen. Click **Done**.



NOTE: You can enroll multiple Imprivata IDs. To enroll another Imprivata ID on a different device now, click **Enroll another**. If you want to enroll later, perform the steps in this section again when you are ready.

7. If you are enrolling in the presence of an enrollment supervisor, the supervisor authenticates to witness your enrollment.

Enroll Imprivata ID During Remote Access Log In

You can allow users to remotely enroll Imprivata ID after enrolling at least one second factor. After a user replaces their device, they can enroll Imprivata ID on the new device without calling your IT helpdesk first:

1. In the Imprivata Admin Console, go to **Users > Workflow policy**.
 2. Go to **Remote access workflows > Log In > Self-service** and check **Allow users to remotely enroll and manage authentication methods**
 3. Click **Save**.
- When enabled, Self Service Enrollment is an option for all users associated with the Remote Access **Log In** workflow (if your Log In workflow includes Imprivata ID.)
 - Self Service Enrollment is available only for remote access gateways that use Imprivata cloud-based authentication with the Imprivata graphical user interface. The legacy RADIUS remote access experience does not support Self Service Enrollment.

**CAUTION:**

When clinicians replace their device with a new model, their EPCS Allowed Imprivata ID enrollment is not carried forward to the new device. Self service enrollment of Imprivata ID does not replace the EPCS Allowed enrollment required for Imprivata ID.

These users can enroll Imprivata ID on their new device for remote access as described below, but before they can use Imprivata ID on their new device for EPCS workflows, they will first need to confirm their email and phone number.

Typical User Workflow

A user has upgraded to a new device. Imprivata ID was restored from a backup automatically to the new device. The user may not realize Imprivata ID must be re-enrolled on the new device.

1. The user enters his username and password in the Imprivata Enterprise Access Management interface at his remote access gateway.
2. He clicks **Log in**. Imprivata Enterprise Access Management sends a push notification to his old device only.
3. The user sees onscreen that Imprivata ID is waiting for him to approve the notification, but the model of his old device is displayed. This visual cue is designed to prompt the user to take action. (The onscreen model display is a feature improvement for all push notifications.)
4. The user does not have to call your helpdesk. The user clicks **Add new device** instead.

The user must complete a second authentication before they can enroll Imprivata ID.



BEST PRACTICE:

When rolling out Imprivata ID to your users, require users to enroll their phone number for SMS authentication. SMS authentication is the easiest method in this case; the user could also authenticate with Imprivata ID on their old device (if he still has it) or call your helpdesk for a temporary code.

5. The user clicks **SMS code**. Imprivata Enterprise Access Management sends an SMS code to his device (the user kept his phone number when he upgraded his device, so his SMS enrollment is unchanged.)
6. The user receives the SMS message on his new device, enters the verification code onscreen, and clicks **Confirm your identity**.
7. The **Enroll your Imprivata ID** screen opens. The user opens the Imprivata ID app on his new device, enters the serial number and token code from the app, and clicks **Submit**.
The user's Imprivata ID is enrolled. After he clicks **Done** his remote access gateway opens as usual. The next time he logs in remotely, Imprivata ID on his new device will receive the push notification by default.

Imprivata ID on his old device is still enrolled, will continue to receive push notifications, and can continue to be used unless deleted by the user or your Imprivata Enterprise Access Management administrator.

EPCS — Clinician Enrolling Imprivata ID on a New Phone

When a clinician replaces her device with a new model, or she restores, replaces, or reinstalls Imprivata ID for any reason, her EPCS-allowed Imprivata ID enrollment is not carried forward to the new device.

For an Institutionally identity proofed provider, the clinician must have at least two EPCS-allowed methods available to self-enroll a new Imprivata ID, if self-enrollment is allowed by their organization.

Alternatively, if a provider does not have enough EPCS-allowed methods to self-enroll, or self-enrollment is not enabled, then the provider can enroll a new Imprivata ID with a supervisor who witnesses the enrollment.

For an Individually identity proofed provider, the clinician does not need to repeat identity proofing, but before she can use Imprivata ID on her new device for EPCS workflows, she will need to confirm the same email and phone number as she did during Identity Proofing.

Enrolling Your Phone Number

Imprivata Enterprise Access Management supports SMS text notifications to any device that accepts SMS messaging, including devices not supported by Imprivata ID.



NOTE: You must have your device with you to enroll your phone number.

To enroll a phone number:

1. Log into the Imprivata enrollment utility on a computer: Click the Imprivata icon in the Windows notification area (Imprivata agent menu), and then click **Enroll Authentication Methods**.

The authentication methods available for you to enroll are displayed.

2. Select **Enroll your mobile phone number**.
3. Enter your mobile phone number with area code (Message and data rates may apply).

Enroll SMS code

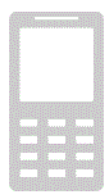
SMS is a way to confirm your identity with a one-time code delivered to your mobile phone via a text message (SMS).

Enter your mobile phone number with area code.
Message and data rates may apply.

E.g. (999) 999 - 9999

Next

[Do this later](#)



4. A text message is sent to your device. Enter the verification code from that message.
You will receive a confirmation email after the enrollment is complete. If you receive a confirmation email for an authentication method that you did not enroll, contact your Imprivata Enterprise Access Management administrator immediately.



NOTE: If you need to change to a different phone number in the future, contact your help desk.

Enrolling Your Phone Number While Logging In Remotely

Imprivata Enterprise Access Management Remote Access Users may also be configured to enroll their phone number while logging into their VPN gateway or Microsoft AD FS client. The workflow is identical.

Close

Enter phone number


We will send a code via SMS to your phone to enroll you in SMS as a log in method

e.g. (000) 000-0000

Standard message and data rates may apply

Submit

Back

 imprivata