imprivata®

Product Documentation

Enrollment and Signing Guide for Providers

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

Enrolling Authentication Methods for MFA 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 authentication methods for authenticating with Imprivata Enterprise Access Management for MFA (formerly Imprivata Confirm ID). The authentication methods you are allowed to use vary from role to role in your organization, so not all authentication methods described in this document may be available to you.

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

You enroll Imprivata Enterprise Access Management authentication methods using the Imprivata enrollment utility. (If your enterprise has enabled Imprivata Enterprise Access Management Remote Access, you may be able to enroll while logging into your VPN gateway instead.)

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

If you are enrolling authentication methods in the presence of an enrollment supervisor, then you can log into the enrollment utility using any of your enrolled authentication methods, in addition to your username and password.

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:

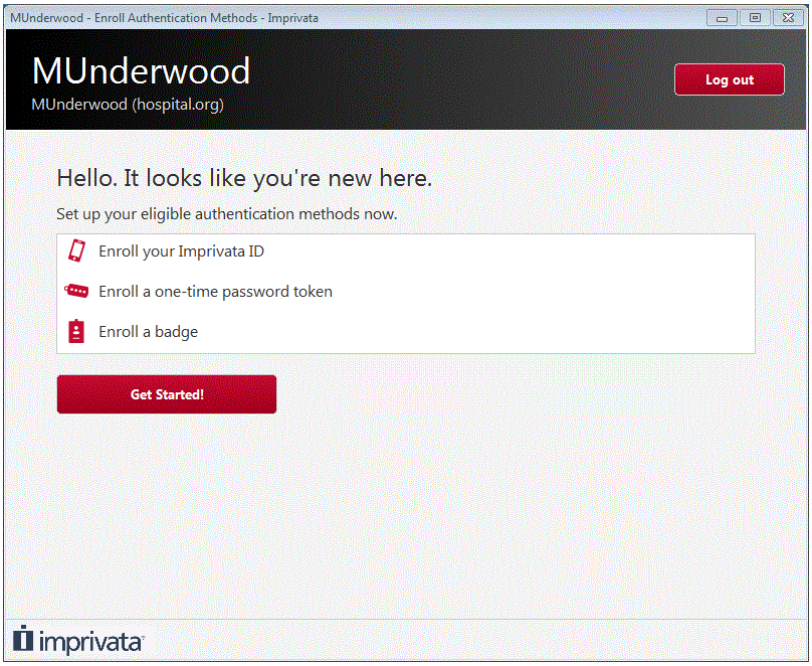
Android Requirements

- 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:

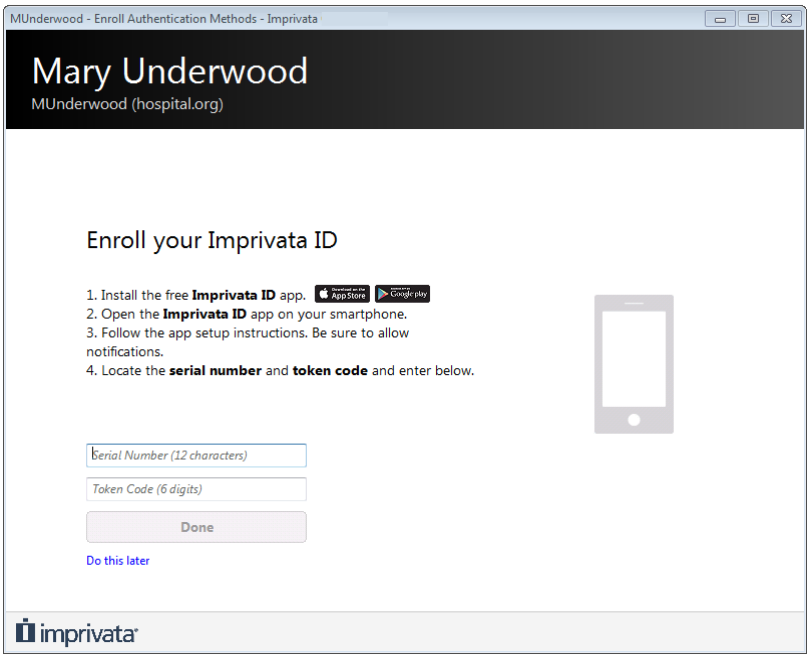
Typical Imprivata ID Enrollment

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**.

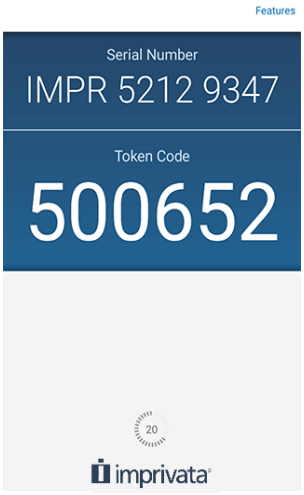
   The authentication methods available for you to enroll are displayed:



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.

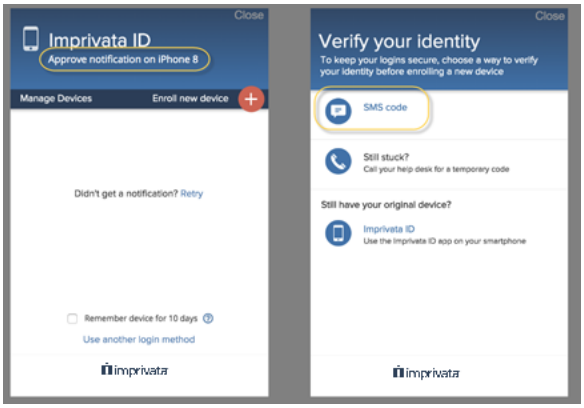
   The user must complete a second authentication before they can enroll Imprivata ID.

   > **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

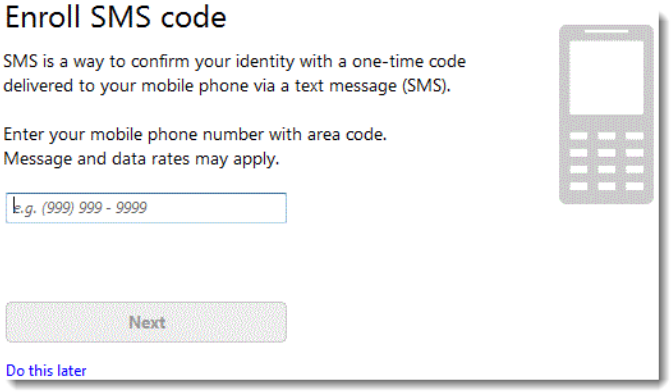
Imprivata Enterprise Access Management supports SMS text notifications to any device that accepts SMS messaging, including devices not supported by Imprivata ID.

> **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).



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 an confirmation email for an authentication method that you did not enroll, contact your Imprivata Enterprise Access Management administrator immediately.

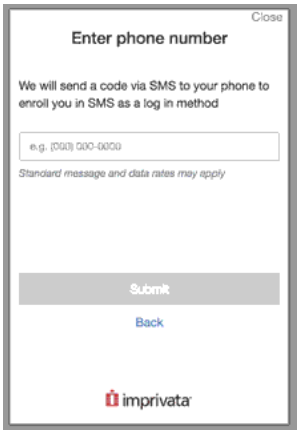
Troubleshooting

Changing Phone Numbers — If you need to change to a different phone number in the future, contact your help desk.

SMS Enrollment Deleted — If you enroll your phone number for SMS authentication, then do not use SMS authentication for a year, that enrollment is deleted. You will not receive SMS messages for authentication. 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.



NOTE:
International-based phone numbers are supported. For a list of supported countries, see "Credential Types" under "Remote Access" in Imprivata Enterprise Access Management with MFA Supported Components.

Enrolling Your Fingerprints

NOTE: You may be required to enroll in the presence of an enrollment supervisor.

To enroll one finger, the enrollment utility must successfully scan the finger three times to learn the fingerprint, then a fourth time to verify that the scanned fingerprint has been successfully enrolled.

BEST PRACTICE: Enroll two fingers (preferably both index fingers) in case a single finger authentication fails.

To enroll fingers:

1. Click **Get Started!** or **Enroll your fingerprints** on the enrollment screen.
2. Click the onscreen finger you will use to identify yourself.
3. Place and hold or swipe your finger on the reader. Each scan is not successfully completed until a green check mark appears.
4. When prompted, place and hold or swipe the same finger a second time.
5. When prompted, place and hold or swipe the same finger a third time.
6. Place and hold or swipe the same finger on the reader a fourth time to confirm Imprivata Enterprise Access Management can use the first three scans to authenticate you in the future.
7. Click another onscreen finger to enroll, or click **Done**.
8. If you are enrolling in the presence of an enrollment supervisor, the supervisor authenticates to witness your enrollment.

   You will receive a confirmation email after the enrollment is complete. If you receive an confirmation email for an authentication method that you did not enroll, contact your Imprivata Enterprise Access Management administrator immediately.

Enrolling Your Fingerprints with a Symantec VIP Credential or Imprivata ID

You can enroll your fingerprints if you have completed identity proofing and have a Symantec VIP credential or Imprivata ID.

To enroll one finger, Imprivata Enterprise Access Management must successfully scan the finger three times to learn the fingerprint, then a fourth time to verify that the scanned fingerprint has been successfully enrolled.

> **BEST PRACTICE:** Enroll two fingers (preferably both index fingers) in case a single finger authentication fails.

To enroll fingers:

1. Click **Enroll your fingerprints** on the enrollment screen.
2. Click the onscreen finger you will use to identify yourself.
3. Enter your Symantec VIP credential or Imprivata ID and your password.
4. Place or swipe your finger on the reader. Each scan is not successfully completed until a green check mark appears.
5. When prompted, place and hold or swipe the same finger a second time.
6. When prompted, place and hold or swipe the same finger a third time.
7. Place and hold or swipe the same finger on the reader a fourth time to confirm Imprivata Enterprise Access Management can use the first three scans to authenticate you in the future.
8. Click another onscreen finger to enroll, or click **Done**.
9. When you're done, log out of the enrollment utility.

   You will receive a confirmation email after the enrollment is complete. If you receive an confirmation email for an authentication method that you did not enroll, contact your Imprivata Enterprise Access Management administrator immediately.

Enrolling Your One-Time Password (OTP) Token

NOTE: You may be required to enroll in the presence of an enrollment supervisor.

To enroll a one-time password token ("OTP," "token," or "keyfob"):

1. Click **Get Started!** or **Enroll a one-time password token** on the enrollment screen.
2. Select the type of token to enroll.
3. Follow the on-screen directions to enter the device serial number, token passcode, or Symantec credential token, as needed.
4. Click **Done**.
5. If you are enrolling in the presence of an enrollment supervisor, the supervisor authenticates to witness your enrollment.

   You will receive a confirmation email after the enrollment is complete. If you receive an confirmation email for an authentication method that you did not enroll, contact your Imprivata Enterprise Access Management administrator immediately.

Enrolling Your Badge (Proximity Card)

To enroll a badge (proximity card):

1. Select **Enroll a badge** on the Imprivata enrollment screen.
2. Tap the badge on the reader when prompted.
3. After the badge has been successfully enrolled, click **I'm done** or **Enroll another badge** to continue.

   You will receive a confirmation email after the enrollment is complete. If you receive an confirmation email for an authentication method that you did not enroll, contact your Imprivata Enterprise Access Management administrator immediately.

Enrolling Your Facial Biometric

This enrollment of Imprivata ID does not require a fingerprint reader or a supervisor witness, nor does it require the provider to still have their old mobile device if they have replaced it.

Requirements

- For mobile device and mobile operating system requirements, see Imprivata Enterprise Access Management Supported Components.
- The latest version of Imprivata ID.
- ◦ Agent version 7.4 or later for supervised (witnessed) enrollment of a facial biometric.
  ◦ Agent version 7.5 or later for unsupervised (unwitnessed) enrollment or unsupervised deletion of a facial biometric.
- You must have already enrolled Imprivata ID as an authentication method on your mobile device. This enrolled authentication method does ***not*** have to be allowed for EPCS.
- To perform unsupervised enrollment or unsupervised deletion of your facial biometric, administrator configuration setting **Facial biometric must always be supervised** must be deselected (unchecked) on the **MFA enrollment supervisors** page. An Imprivata administrator can access the **MFA enrollment supervisors** page using the Imprivata Admin Console > **Users** menu > **Enrollment Supervisors**.
- To perform unsupervised enrollment of your facial biometric, you must have two or more authentication methods that are EPCS allowed (one of these may be a password). Otherwise, your enrollment must be supervised (enabled and witnessed) by an enrollment supervisor. EPCS allowed authentication methods are selected by your organization and may include Imprivata ID, fingerprints, and One-Time Password (OTP) tokens.

Two-Part or Four-Part Procedure

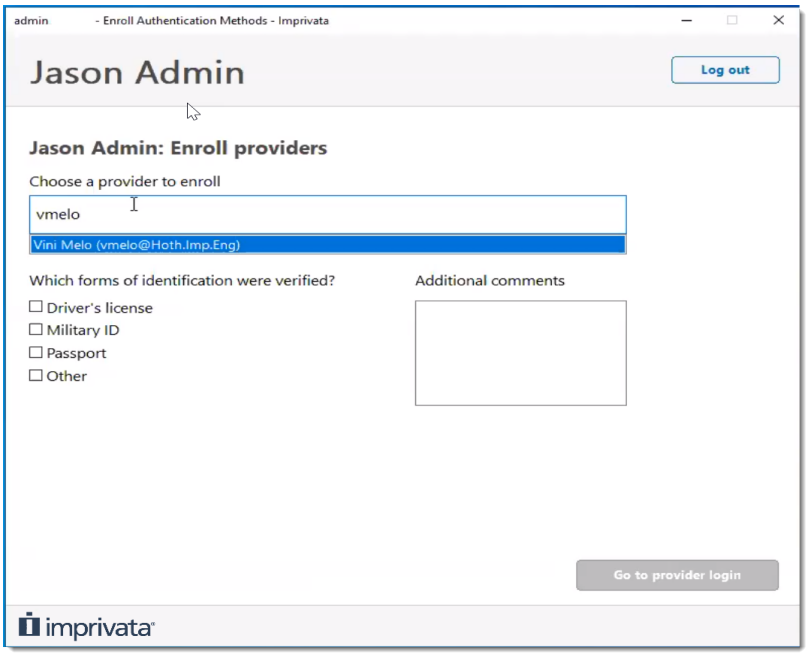
The procedure to enroll your facial biometric has either two or four parts, depending on whether your enrollment must be supervised (see Requirements). For unsupervised enrollment, perform only parts 2 and 3. For supervised enrollment, complete all four parts. You must complete the parts in sequence.

1. Supervisor Enabling Facial Biometric Enrollment.
2. Provider Enrolling Their Facial Biometric.
3. Provider Verifying Their Facial Biometric.
4. Supervisor Witnessing Facial Biometric Enrollment.

Supervisor Enabling Facial Biometric Enrollment

For a supervised enrollment, an enrollment supervisor must perform these steps to enable a provider's facial biometric enrollment:

1. Access the Imprivata enrollment utility by clicking on the Imprivata agent icon in the computer system tray and selecting **Enroll Authentication Methods**.
   The enrollment utility launches.
2. The supervisor logs into the enrollment utility.
3. Click **Enroll providers**. The **Enroll providers** window opens:



4. Enter the provider's username and select the matching name from the drop-down list.
5. Optionally or if required by your organization, select the form of identification that you verified and enter any comments in the Additional comments field.
6. Click **Go to provider login**. The enrollment utility login window appears for the provider, who must now proceed to Provider Enrolling Their Facial Biometric. When the provider is done enrolling and verifying their facial biometric, the supervisor must witness the provider's enrollment in Supervisor Witnessing Facial Biometric Enrollment.

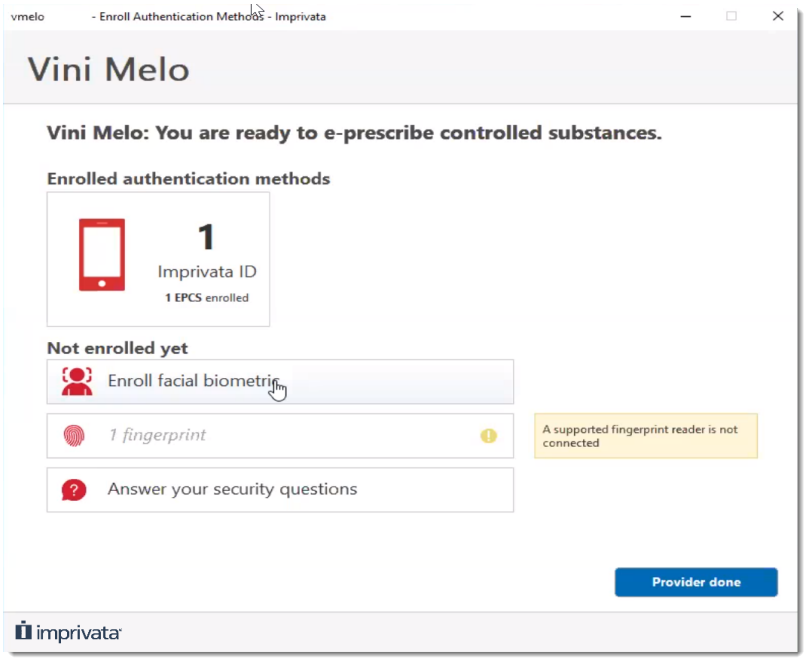
Provider Enrolling Their Facial Biometric

The provider must perform these steps to enroll their facial biometric:

1. **For an unsupervised enrollment:** access the Imprivata enrollment utility by clicking on the Imprivata agent icon in the computer system tray and selecting **Enroll Authentication Methods**. The enrollment utility launches. Log into the enrollment utility using your provider password.

   For a supervised enrollment: on the computer used in the previous section, log into the displayed enrollment utility using your provider password.

   Your provider enrolled and enrollable authentication methods are displayed, for example:

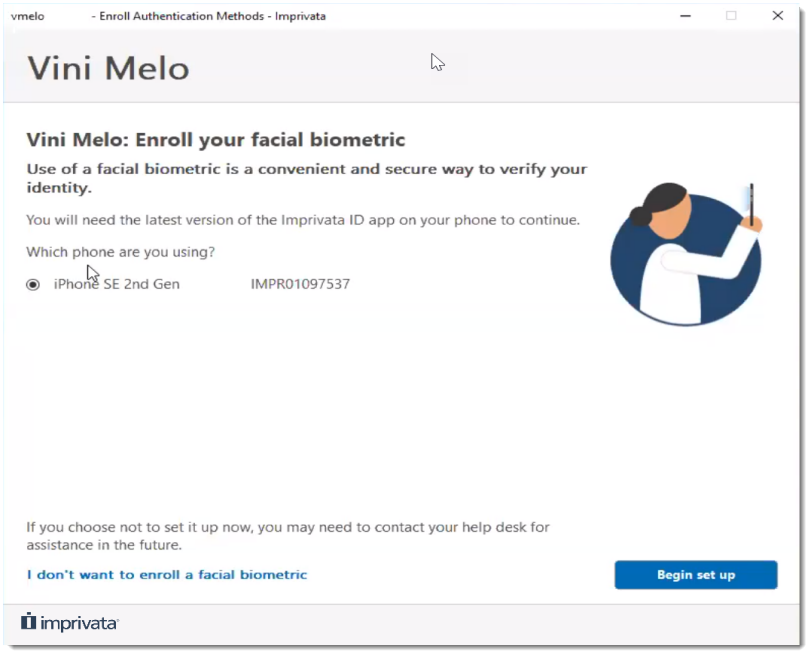


2. Click **Enroll facial biometric**. (If this option is disabled, see Troubleshooting.)

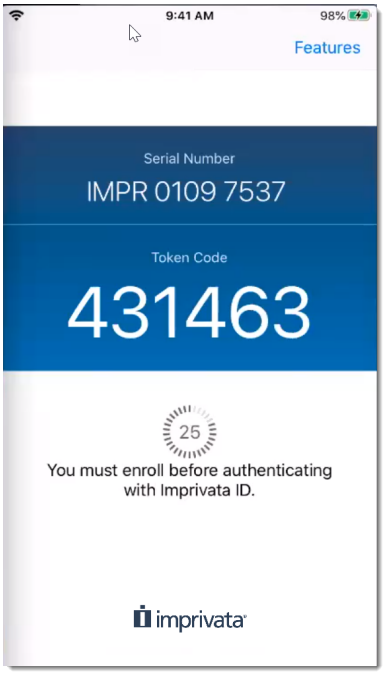
   For an unsupervised enrollment: the two-factor authentication page displays. Complete that authentication.

   For a supervised enrollment: two-factor authentication is not required.

   A list of your mobile devices that contain an enrolled Imprivata ID is displayed:



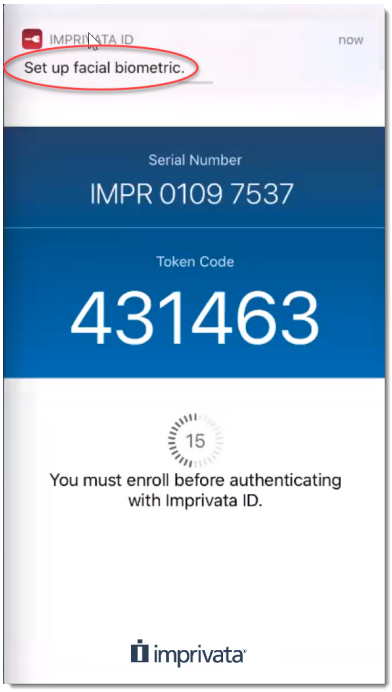
3. Select the device you will use to enroll your facial biometric and click **Begin set up**.
4. *On your mobile device*, open Imprivata ID:



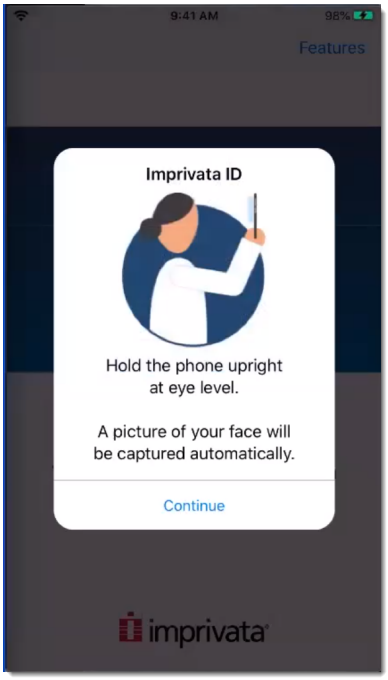
5. *On your computer*, enter the token code from Imprivata ID and click **Continue**.

   The application instructs you to accept notification from Imprivata ID on your mobile device and to follow the instructions on that device to continue.

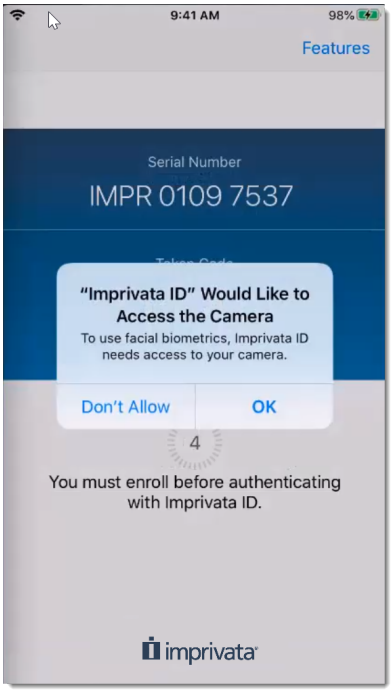
6. *On your mobile device*, tap on the notification that says **Set up facial biometric**:



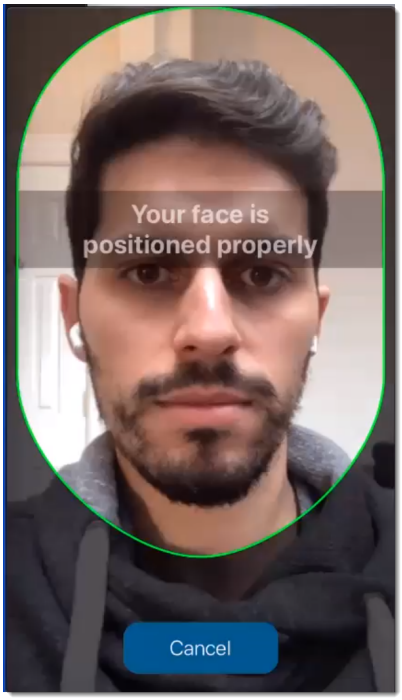
   The mobile display changes to:



7. Click **Continue**. The mobile display changes to:



8. Click **OK**. The camera activates.
9. Follow the displayed instructions to properly position the device to capture an image of your face. The app then takes the picture automatically and reports that it is processing the image:



If the image was captured successfully, the display shows **Face captured, Continue enrolling on your desktop workstation**.

On your computer, the Imprivata enrollment utility also indicates that your face was captured successfully.

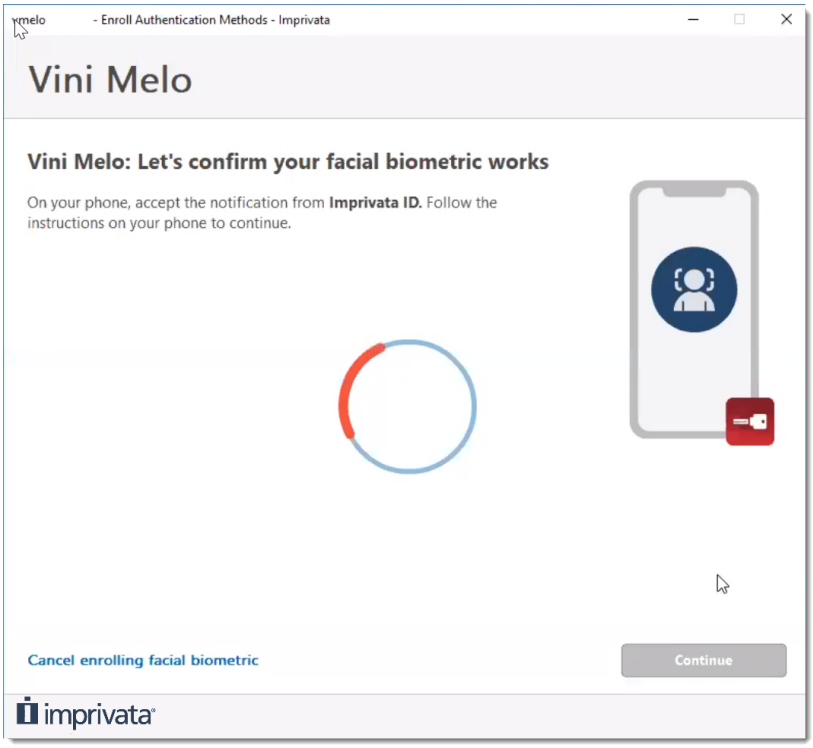
If the image was not captured successfully, then *on your computer*, click **Try again** and return to Step 4.

10. After the image is captured successfully, continue to the next section.

Provider Verifying Their Facial Biometric

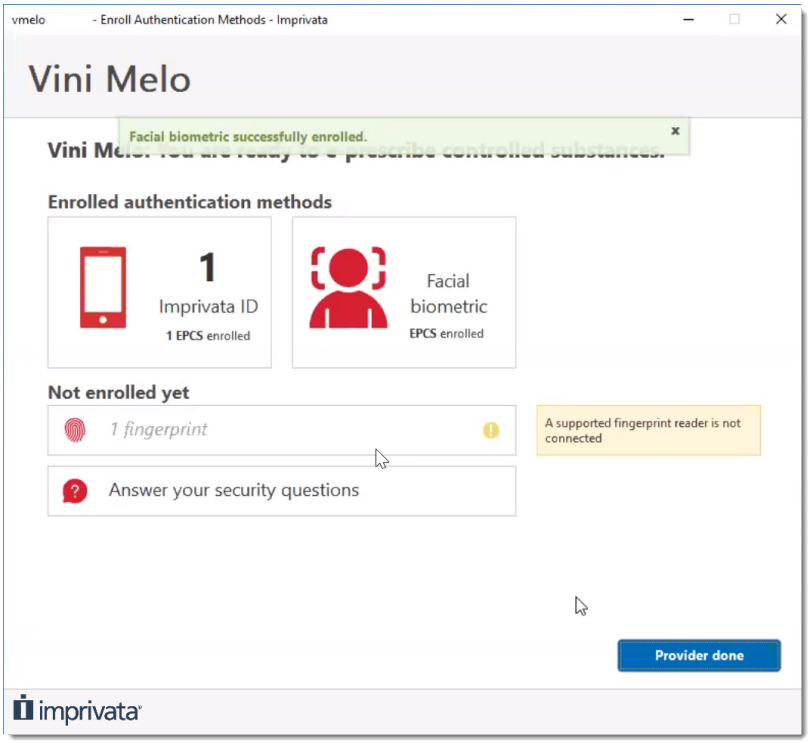
The provider must perform these steps to verify their facial biometric:

1. *On your computer*, the Imprivata enrollment utility indicates that your face was captured successfully. Click **Continue**. A confirmation window directs you to your mobile device:



2. *On your mobile device*, accept the notification prompt from Imprivata ID that says to verify your identity by taking a photograph of your face.
3. Follow the displayed instructions to correctly position the device to capture an image of your face.
4. When the image is captured successfully, then *on your computer*, click **Continue**.

   For an unsupervised enrollment: the computer shows **Facial biometric EPCS enrolled** under **Enrolled authentication methods**, and you are done with this procedure:

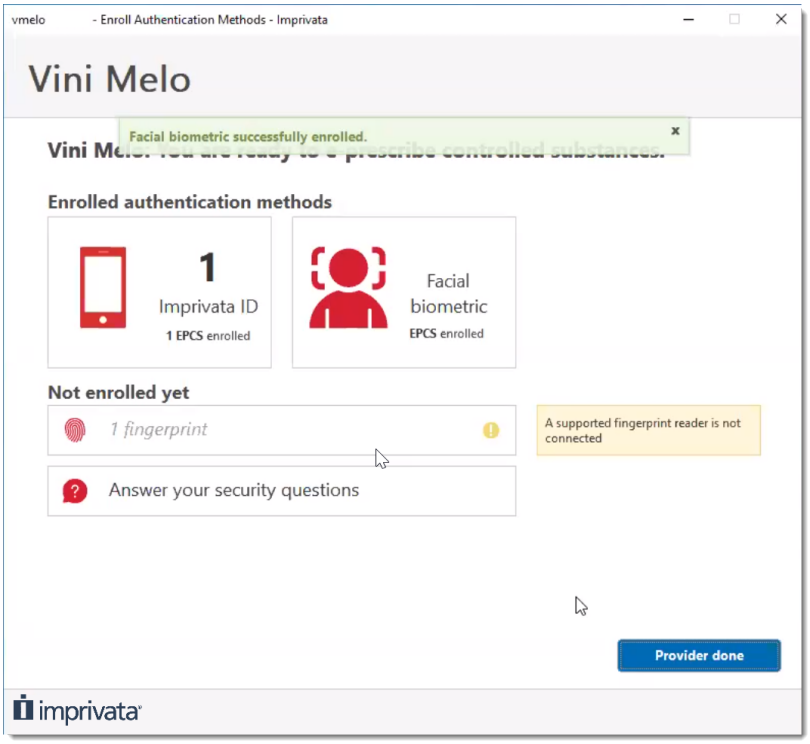


For a supervised enrollment: the computer displays a window for your supervisor to witness your facial biometric enrollment. Continue to the next section.

Supervisor Witnessing Facial Biometric Enrollment

On the **You must witness this enrollment** window, the supervisor can enter or review the forms of identification they verified and the comment fields if required by your organization, and then witness the enrollment by authenticating.

After that authentication, the computer shows that the facial biometric is successfully enrolled:



Troubleshooting

- If you cannot access the Imprivata enrollment utility and the utility pop-up **Status** area shows **Imprivata Agent disconnected**, check your network connections.
- If your mobile device does not receive notifications from the Imprivata enrollment utility on your computer, check the settings of Imprivata ID on your mobile device to ensure that Notifications are allowed for the app. Also, in that app, select **Features** and ensure that **Fast Access** is enabled. Disabling Fast Access also disables notifications for this app.
- Check the settings of Imprivata ID on your mobile device to ensure you have version 7.4 or later.
- Check the version of the Imprivata agent on your computer. Agent version 7.4 or later is required for supervised (witnessed) facial biometric enrollment. Agent version 7.5 or later is required for unsupervised (unwitnessed) enrollment or unsupervised deletion of a facial biometric.
- If you are trying to do unsupervised enrollment of your facial biometric, and one of the authentication methods you are using for two-factor authentication is being rejected, then your

organization may not allow that method for EPCS. Try using a different authentication method (see the list in Requirements).

- If you are trying to do unsupervised enrollment of your facial biometric, and the **Enroll facial biometric** option is disabled, then you may not have an authentication method that is EPCS allowed. If you are unable to use two authentication methods that are EPCS allowed (one of which may be a password), then your enrollment must be supervised (enabled and witnessed) by an enrollment supervisor.
- Check Imprivata Enterprise Access Management Supported Components to ensure that facial biometric enrollment is supported for your mobile device and mobile operating system.
- To capture an acceptable facial biometric (facial image), good lighting is very important. If your mobile device fails repeatedly to capture an acceptable facial biometric, try improving the lighting in the room where you are taking the picture or move to an area where your face is lit evenly. You can also try to remove any facial coverings, dark-tinted eyeglasses or sunglasses, or heavy-framed eyeglasses.
- Significant changes in your facial appearance, such as growing or removing a heavy beard, may require that you delete your facial biometric and enroll a new facial biometric. To delete your facial biometric, see Deleting a Facial Biometric.

Deleting a Facial Biometric

Significant changes in facial appearance, such as growing or removing a heavy beard, may require that a provider delete their facial biometric and enroll a new facial biometric. Depending on a configuration setting (specified in Requirements), a provider may be able to delete their facial biometric unsupervised or they may require a supervisor to enable the deletion.

To delete their facial biometric unsupervised, a provider follows this procedure:

1. Log into the Imprivata enrollment utility.
2. Under **Enrolled authentication methods**, select **Facial Biometric**.
3. Select **Remove facial biometric.**
4. Confirm the removal in the confirmation pop-up.

If during step 3 above the **Remove facial biometric** option is not present, then a supervisor must enable the deletion.

To enable a supervised deletion, the supervisor follows the procedure described in Supervisor Enabling Facial Biometric Enrollment, and then the provider follows the deletion procedure above, logging into the same instance of the utility as the supervisor. When the deletion is done, the supervisor does not need to authenticate again to witness the deletion. If desired, the provider can enroll a new facial biometric as described in Provider Enrolling Their Facial Biometric.

A supervisor should always be able to enable deletion of a provider's facial biometric. However, if a provider and supervisor are unable to delete a provider's facial biometric, they can contact their Imprivata system administrator, who can delete it for them. An administrator deletes a facial biometric for a provider using the Imprivata Admin Console. In that console, the administrator:

1. Locates the Provider's user account and selects **Edit user**.
2. In the user details page, under **Authentication Methods**, checks **Delete enrollment** for the facial biometric, then clicks **Save** on the page to implement the deletion.

Enrolling Your Imprivata ID for EPCS Using Your Facial Biometric

This section describes how to enroll Imprivata ID on a mobile device you will use for EPCS (electronic prescription of controlled substances) using your facial biometric (facial image). This enrollment does not require a fingerprint reader or a supervisor witness, nor does it require you to still have your old mobile device if you have recently replaced it.

NOTE:
You must have your mobile device with you.

Confirm with your system administrator that the Imprivata system is configured to allow unsupervised (unwitnessed) Imprivata ID enrollment.

Requirements

- For mobile device and mobile operating system requirements, see Imprivata Enterprise Access Management Supported Components.
- You must have previously enrolled your facial biometric as an authentication method, as described in Enrolling Your Facial Biometric.
- If you have not yet installed Imprivata ID on your mobile device, then you must install it before or during this procedure. Imprivata ID version 7.4 or later is required.
- If you have replaced an older mobile device, you must enroll Imprivata ID again on the new device.

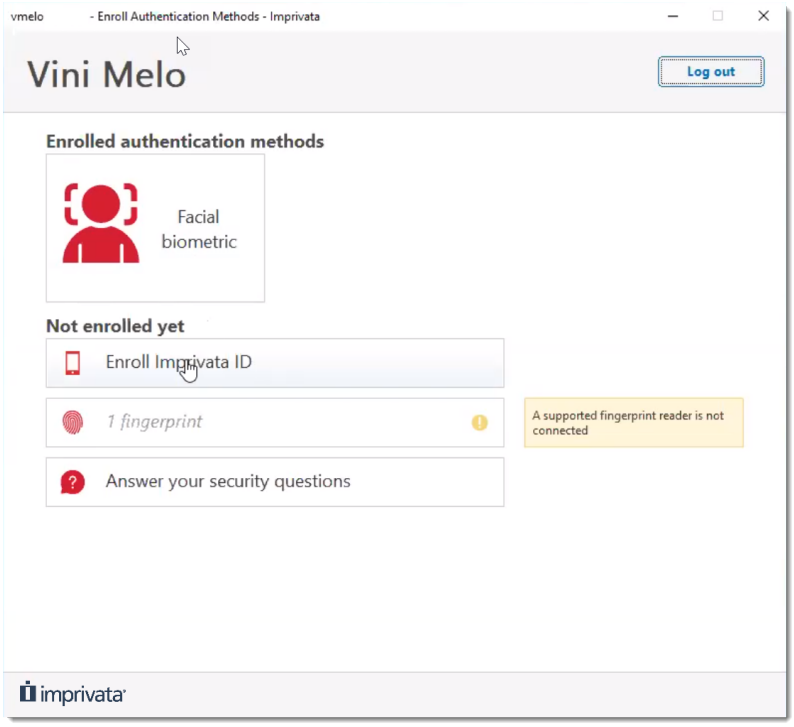
Procedure

To enroll your Imprivata ID on a mobile device for EPCS using your facial biometric:

1. *On your computer*, click on the Imprivata agent icon in your computer system tray and select **Enroll Authentication Methods**.

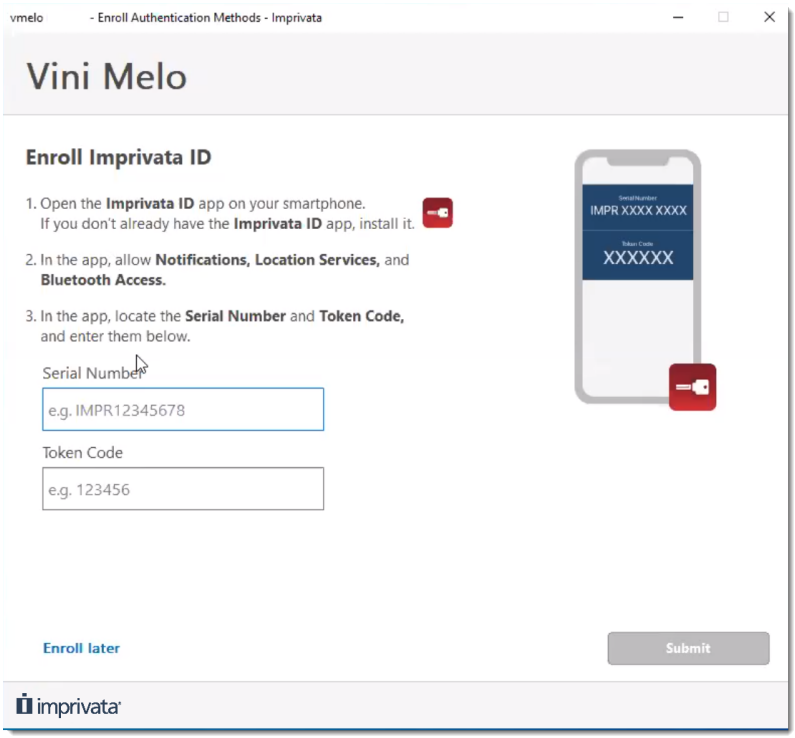
   If this option is disabled and the utility pop-up **Status** area shows **Imprivata Agent Connected**, then the Imprivata system may not be configured to allow unsupervised (unwitnessed) Imprivata ID enrollment. Contact your system administrator.
2. Log into the enrollment utility.

   The app shows your enrolled authentication methods, including facial biometric, for example:



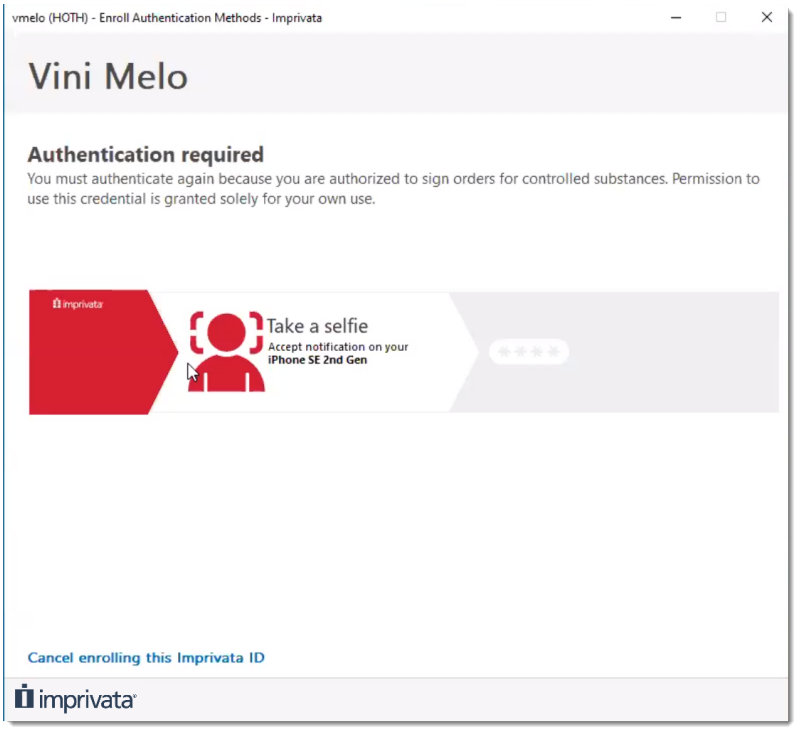
3. Click **Enroll another Imprivata ID** or **Enroll Imprivata ID**.

   The Enroll Imprivata ID window displays:

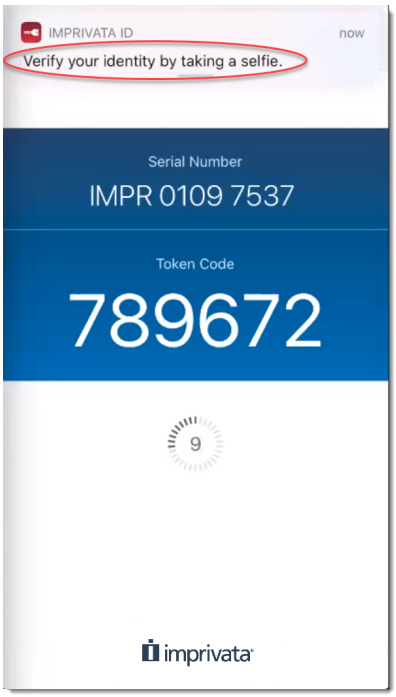


4. If Imprivata ID is not yet installed on your mobile device, install it and follow the instructions shown to set a few settings in that app.
5. Also in that app, select **Features** and ensure that **Fast Access** is enabled. Disabling Fast Access also disables notifications for this app.
6. *On your computer*, enter your Imprivata ID serial number and token code and click **Submit**.

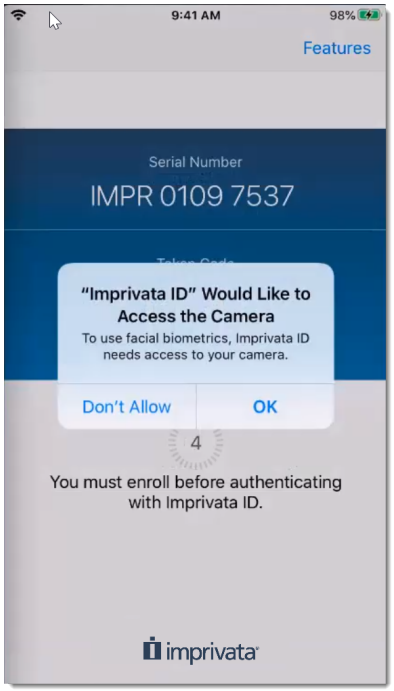
The following window is displayed:



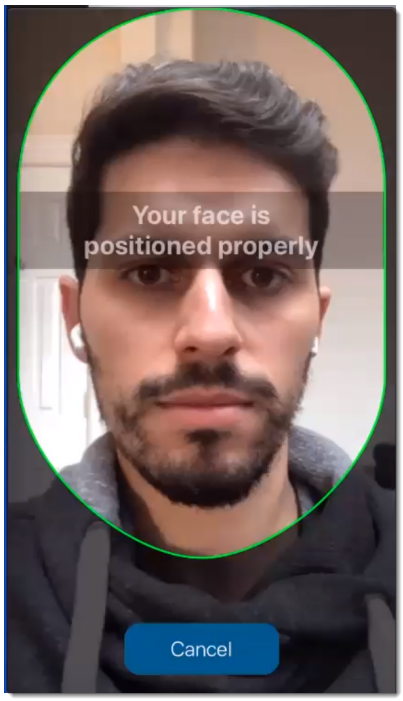
7. *On your mobile device*, tap on the notification shown:



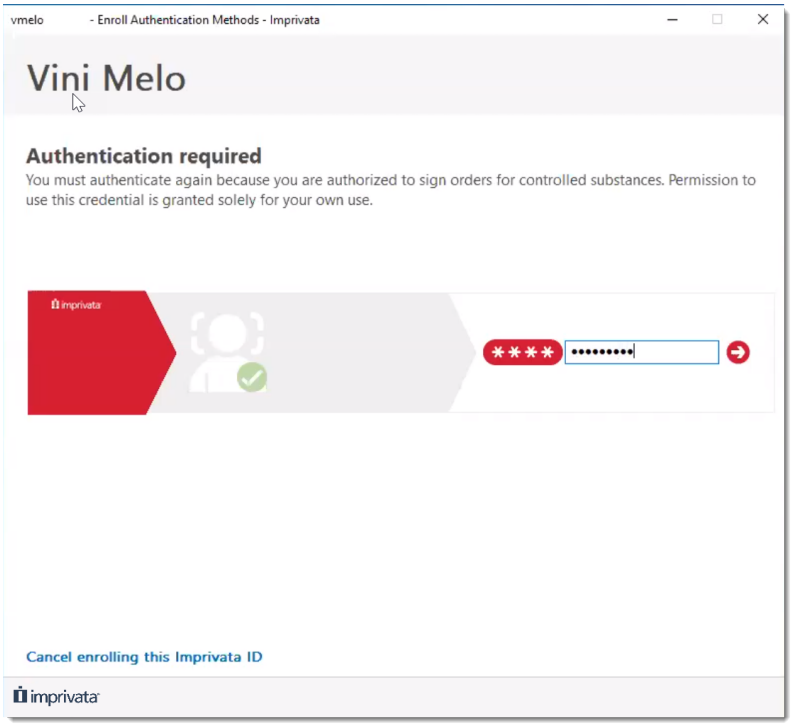
If the following display appears, click **OK**:



8. Follow the displayed instructions to properly position the device to capture an image of your face. The app then takes the picture and reports that it is processing the image:

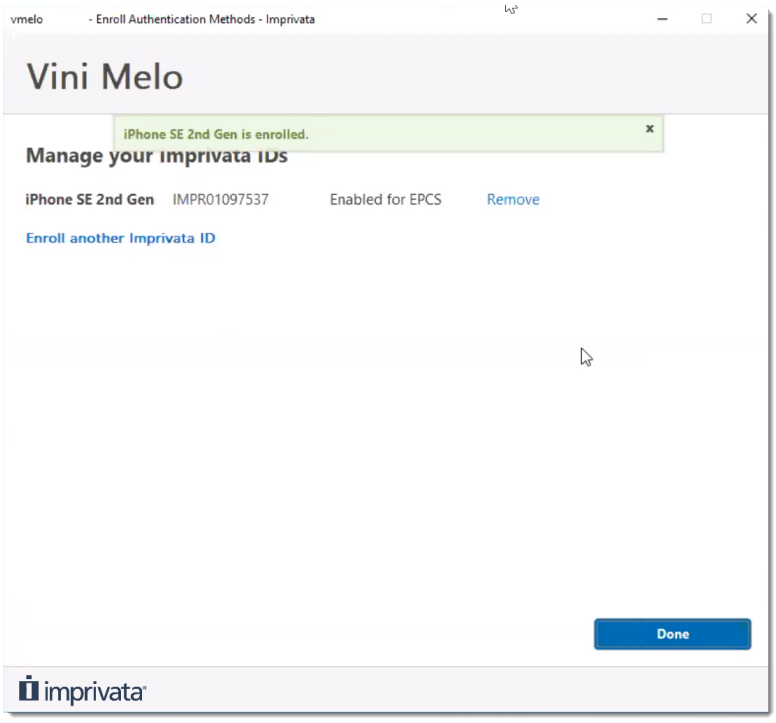


After the image is captured successfully, *your computer* shows an authentication window:



9. *On your computer*, enter your password to authenticate again.

   Your computer then shows that Imprivata ID is enrolled on your new mobile device and enabled for EPCS:



Troubleshooting

- If you cannot access the Imprivata enrollment utility and the utility pop-up **Status** area shows **Imprivata Agent connected**, ask your system administrator if the system is configured to allow

unsupervised (unwitnessed) enrollment of Imprivata ID. If the utility pop-up **Status** area shows **Imprivata Agent disconnected**, check your network connections.

- If your mobile device does not receive notifications from the Imprivata enrollment utility on your computer, check the settings of the Imprivata ID app on your mobile device to ensure that Notifications are allowed for the app. Also, in that app, select **Features** and ensure that **Fast Access** is enabled. Disabling Fast Access also disables notifications for this app.
- Check the settings of Imprivata ID on your mobile device to ensure you have release 7.4 or later.
- Check Imprivata Confirm ID Supported Components to ensure that enrolling Imprivata ID on a mobile device for EPCS using your facial biometric is supported for your mobile device and mobile operating system.
- To capture an acceptable facial biometric (facial image), good lighting is very important. If your mobile device fails repeatedly to capture an acceptable facial biometric, try improving the lighting in the room where you are taking the picture or move to an area where your face is lit evenly. You can also try to remove any facial coverings, dark-tinted eyeglasses or sunglasses, or heavy-framed eyeglasses.
- Significant changes in your facial appearance, such as growing or removing a heavy beard, may require that you delete your facial biometric and enroll a new facial biometric. To delete your facial biometric, see Deleting a Facial Biometric.

Answering Your Security Questions

To enroll security questions and answers:

1. Select **Answer security questions** on the Imprivata enrollment screen.
2. Follow the onscreen directions to choose questions that only you can answer, and provide answers to those questions.
3. Click **Done**.

   You will receive a confirmation email after the enrollment is complete. If you receive an confirmation email for an authentication method that you did not enroll, contact your Imprivata Enterprise Access Management administrator immediately.

Creating Your Imprivata PIN

To create your Imprivata PIN:

1. Select **Create your Imprivata PIN** on the enrollment screen.
2. Follow the onscreen directions to choose a PIN of the proper length and containing the specified allowed characters.
3. Click **Done**.

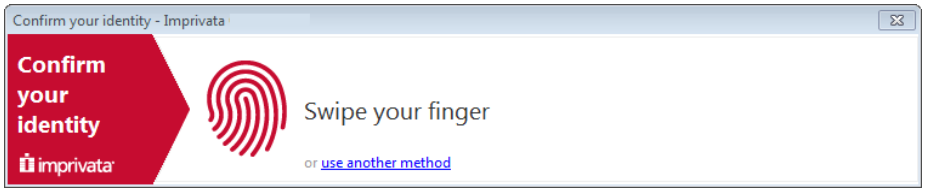
   You will receive a confirmation email after the enrollment is complete. If you receive an confirmation email for an authentication method that you did not enroll, contact your Imprivata Enterprise Access Management administrator immediately.

Signing Orders with Imprivata Enterprise Access Management MFA

When your EMR requires authentication, you are prompted to authenticate using one or two of your enrolled authentication methods. You may also be allowed to choose which authentication methods you use if multiple options are available.

Signing with One Authentication Method

The following image shows an order that requires only one authentication method. You may have the option to choose a different authentication method than the first method presented. After you successfully authenticate, order signing is complete.

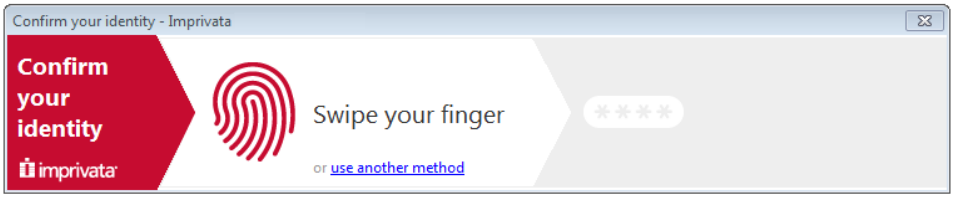


Signing with Two Authentication Methods

Some orders may require two authentication methods to successfully sign and place the order.

First Authentication Method

Enterprise Access Management prompts you to authenticate with the first authentication method. The second method (in this example, password) is not enabled until the first method is authenticated successfully. You may have the option to choose a different authentication method as the first authentication method.



Second Authentication Method

After you successfully authenticate with the first authentication method, you are prompted to use the second authentication method to successfully sign the order. In this example, only password authentication is allowed; you do not have the option to choose a different authentication method.

After the second authentication method is authenticated successfully, the order is signed and placed.