imprivata®

Product Documentation

Individual Identity Proofing

Imprivata Enterprise Access Management 26.3

© 2026 Imprivata, Inc. All Rights Reserved.

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

© 2026 Imprivata, Inc. All Rights Reserved.

This product is distributed under licenses restricting its use, copying, distribution and decompilation.

Imprivata's products may be covered in whole or in part by one or more U.S. pending or issued patents listed at http://www.imprivata.com/patents.

Trademark Information

OneSign, Imprivata, and the Imprivata logo are registered trademarks of Imprivata, Inc. ProveID and Imprivata OneSign APG are trademarks of Imprivata, Inc. in the United States and in other countries.

Legal Notices

Under international copyright laws, neither the documentation nor software may be copied, photocopied, reproduced, translated, or reduced to any electronic medium or machine-readable form, in whole or in part without the prior written consent of Imprivata, Inc., except as described in the license agreement.

The names of companies, products, people, and/or data mentioned herein are fictitious and are in no way intended to represent any real individual, company, product, or event, unless otherwise noted.

DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID.

Document revision 26.3

Identity Proofing

Identity proofing is the process for validating a provider's identity. Enterprise Access Management for MFA is configured by default for all provider identity proofing to be performed by hospital staff. A user must complete identity proofing before they can complete DEA-regulated workflows such as e-prescribing controlled substances.

IMPORTANT:
Imprivata Enterprise Access Management support for Individual identity proofing with DigiCert ends July 31, 2027. After July 31, your DigiCert license cannot be renewed.

Update to Imprivata Individual Identity Proofing before July 31. After the update, clinicians already proofed with DigiCert keep their status and don't need to be proofed again.

If your DigiCert certificate expires before updating the service, clinicians identity proofed with DigiCert cannot complete EPCS workflows.

End Of Life: Symantec NSL

As of August 1, 2019, Symantec ceased providing any and all levels of service and support for Norton Secure Login. NSL has shut down, you are no longer able to login. All customer data was purged after this date. There are no exceptions for service, support or contract extensions.

If you have any questions regarding this notice, please contact your Symantec partner or your Symantec Account Manager.

© 2026 Imprivata, Inc. All Rights Reserved.

Set Up Enterprise

Set up your enterprise for individual identity proofing.

If all of your clinicians will be identity proofed within your organization with Enrollment Supervisors, do not read this document. See "Institutional Identity Proofing" in the Imprivata Online Help.

SMTP Connection

An SMTP server must be specified to send email notifications to administrators and end users.

Configure a Connection with Basic Authentication

You can configure a connection to an SMTP server using basic (password) authentication.

> **NOTE:**
> Microsoft deprecated basic authentication in Exchange Online. While you can configure a connection using basic authentication, it is recommended that you configure the connection to your mail server over OAuth.

To configure the connection:

1. In the Imprivata Admin Console, go to the **gear icon** > **Settings**.
2. In the **Email configuration** section, click SMTP Server > **Modify**.
3. **SMTP Server** — Type the **IP address** or **FQDN** of the mail server
4. **Optional** —By default, the Imprivata appliance secures outgoing email using TLS.

   Uncheck **Use TLS** to disable this functionality. If you choose to leave TLS enabled, consider the following:

   - Imprivata supports TLS versions up to 1.2, but does not enforce any specific version. How your environment is configured determines the required version.
   - Your SMTP server must support TLS, and additional configuration may be required. For more information, see your vendor-specific documentation.
5. If required, type the **SMTP Server Account Username** and **Password** of an account that is authorized to send email through your server/mail relay.
6. **Email messages are from** — Enter the sender address.
7. Click **Save and activate**.

> **NOTE:**
> The **Test** button only confirms that the connection can be made to the SMTP server. To test that an email can be sent and received, open the **Users** page. Select a user, click **Notify**, and select the type of notification to send as a test.

When you set up the SMTP server:

- Providers receive an email when they have been successfully identity proofed.
- The Imprivata Enterprise Access Management administrator receives email notifications when users have enrolled authentication methods for Remote Access.

Configure a Connection Over OAuth

You can configure a connection to an SMTP server over OAuth.

Prerequisites

Before you begin, make sure the following prerequisites are met:

- Exchange Online is enabled for SMTP AUTH.
- You have a user account that can be used to send email. This account must be able to send email from the mailbox you specify.
- You have registered an Entra ID application that lets Imprivata connect to Exchange Online over SMTP. Configuring the connection requires that you have its:
  - Client ID
  - Tenant ID
  - Client secret
- You have registered the application's service principal in Exchange Online and granted the mailbox Send As permission.

Configure the Connection

To configure the connection:

1. In the Imprivata Admin Console, go to the **gear** icon > **Settings**.
2. In the Email configuration section, click SMTP Server **Modify**.
3. Select **Exchange Mail Server with OAuth2**.
4. Enter the following required information:
   a. **From Address**: Enter the mailbox from which email notifications should be sent.
   b. **Client ID**: Enter the registered application’s client ID.
   c. **Tenant ID**: Enter the registered application's tenant ID.
   d. **Username**: Enter the user account that can send email from the mailbox you specified.
   e. **Secret**: Enter the registered application's client secret.
5. Click **Save and Activate**.

When you set up the SMTP server:

- Providers are informed when they have been successfully identity proofed.
- The Imprivata Enterprise Access Management administrator receives email notifications when users have enrolled authentication methods for Remote Access.

© 2026 Imprivata, Inc. All Rights Reserved.

Imprivata Cloud Connection

Your Imprivata enterprise must be connected to the Imprivata cloud so Imprivata can send your users an SMS text message or voice call during Individual identity proofing.

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. Click **Test Connectivity**.
3. Services will enter your **Enterprise ID** and **cloud provisioning code**.
4. 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.

Active Directory Requirements

The following Active Directory (AD) attributes are required to enable identity proofing. Verify that the following attributes in AD are present and accurate for all providers for Individual identity proofing:

- **First Name** and **Last Name** must exactly match their government ID;
- **Email Address** — required for the clinician to receive a verification message during identity proofing;
- **Phone Number** — the clinician must be able to receive an SMS message or voice call at this number during identity proofing.

View, add, or edit these values in AD, and if necessary, re-sync with your EAM enterprise. If AD does not have these values, you can add or edit these values on the **User details** page > **Individual Identity Proofing** section in the Imprivata Admin Console.

For security reasons, your users cannot add or edit their own name, email, or phone number.

Configure Telephone Numbers in Active Directory

Configure the **homePhone** and **mobile** telephone number attributes in AD.

For complete details on synchronizing your AD users with Imprivata, see "Synchronizing the Users List" in the Imprivata Online Help.

1. Click **Synchronize** on the **Users** page. The **Synchronize** window opens.
2. Select the domain or file that holds the user records, and click **Next**.
3. Select the users to be imported.
4. Click the **Add** button in the **Extended User Attributes** section. A three-field map opens.
5. In the **Extended User Attribute Name** field, enter **homePhone**.
6. In the **Imprivata Meaning** field, enter **Phone (home)**.

   The label that will appear in the Users list is automatically filled in with the **Imprivata Meaning** value, but you can make edits.
7. Click **Add** to add another.
8. In the **Extended User Attribute Name** field, enter **mobile**.
9. In the **Imprivata Meaning** field, enter **Phone (mobile)**.

   The label that will appear in the Users list is automatically filled in with the **Imprivata Meaning** value, but you can make edits.
10. Click **Save**.

NOTE:
When a user has all three phone Extended User Attributes, when selecting a number for sending the verification code, **mobile** is the primary selection, followed by **home** and **office**.

CAUTION:
The text strings in the **Extended User Attribute Name** fields must exactly match the field names in AD or the extended user attributes will not be synchronized.

Phone Number Format

- Specify a 10-digit US telephone number in any format.
- The country code 1 is optional.
- Hyphens, periods, and parentheses are allowed.
- A phone number with any other non-digit characters will be ignored.
- Any telephone number that doesn't meet these criteria or is malformed in any other way will be ignored. The clinician will not be able to begin identity proofing until the number is corrected in AD or the Imprivata Admin Console.
- If a clinician's telephone number(s) are not present in AD, the clinician will receive an error message. You can add or edit the phone number(s) on the **User details** page of the Imprivata Admin Console.

© 2026 Imprivata, Inc. All Rights Reserved.

Set Up Users

Create User Policies

Before enrolling users, create a user policy that is assigned only to providers who must complete Individual identity proofing:

1. In the Imprivata Admin Console, go to **Users** > **User policies**. Click **Add** to create a new policy or select an existing policy to copy and rename. For example, you can create a user policy called **IndividualEPCS** and then assign it to each user who must complete Individual identity proofing.
2. Go to **Users** > **Users** to search for and select users to include in your Individual EPCS policy. See "Managing User Accounts" in the Imprivata Online Help.
3. Optional — Create user policies necessary for other workflows, for example: Institutional EPCS, Non-EPCS, medical device users, and remote access users, depending on your licensed features.

Set Up EPCS Workflow

You need to associate a user policy (or policies) with the EPCS workflow. After a user policy is associated with a signing workflow, all users in that user policy are allowed to perform that MFA workflow with the specified authentication methods. Your EMR software won't prompt a user for two-factor authentication with Enterprise Access Management (formerly Imprivata Confirm ID) until your EMR administrator enables logical access control for that user.

For complete details, see "Configuring the Enterprise Access Management Workflow Policy" in the Imprivata Online Help.

Select Authentication Methods

1. In the Imprivata Admin Console, go to the **Users** > **Workflow policy**. The **Workflow policy** page opens.
2. Select first factor and second factor authentication methods for EPCS.
3. Click **Done**.
4. Click **Save**.

NOTE:
Face recognition is supported for EPCS workflows when enrolled with heightened security. To configure clinicians for Face recognition, see Face Recognition — EPCS Desktop and Mobile EPCS Authentication.

Select Individual and/or Institutional

Associate user policies with Individual or Institutional identity proofing:

1. In the Imprivata Admin Console, go to the **Users** > **Workflow policy**. The **Workflow policy** page opens.
2. Associate your EPCS user policies with **Individual identity proofing**.
3. Click **Save**.

© 2026 Imprivata, Inc. All Rights Reserved.

Individual Identity Proofing and Enrollment

Providers configured as Individual providers (they may not prescribe using an institution's DEA number) must complete identity proofing with Imprivata and then enroll authentication methods, before e-prescribing controlled substances. Providers can enroll additional authentication methods after they are identity proofed. This identity proofing is permanent and does not expire.

This topic provides an overview of how Individual providers complete identity proofing and enroll their authentication methods.

IMPORTANT:
Imprivata Enterprise Access Management support for Individual identity proofing with DigiCert ends July 31, 2027. After July 31, your DigiCert license cannot be renewed.

Update to Imprivata Individual Identity Proofing before July 31. After the update, clinicians already proofed with DigiCert keep their status and don't need to be proofed again.

If your DigiCert certificate expires before updating the service, clinicians identity proofed with DigiCert cannot complete EPCS workflows.

Before Identity Proofing Begins

Before providers identity proof and enroll authentication methods, make sure the Imprivata Enterprise Access Management environment, users, and workflows are configured correctly before proceeding with provider enrollment.

Set Up Enterprise

Each clinician must have the following attributes present, either populated from Active Directory, or manually entered in their User Details page of the Imprivata Admin Console:

- **First Name** and **Last Name** must exactly match their government ID;
- **Email Address** — required for the clinician to receive a verification message during identity proofing;
- **Phone Number** — the clinician must be able to receive an SMS message or voice call at this number during identity proofing.

See Set Up Enterprise.

Imprivata Cloud Platform Tenant Connected

Individual identity proofing requires that you configure a connection to the Imprivata Cloud Platform. See Set Up Enterprise.

If you have already configured a connection to the Imprivata Cloud Platform, you can skip this step. To determine if a connection has already been configured, log into the Imprivata Admin Console. The **Status** panel includes connection information. A green check mark for **Access Management integration** indicates a connection has been configured.

© 2026 Imprivata, Inc. All Rights Reserved.

Integrate Your EMR Application

You need to configure the integration between Enterprise Access Management and your Electronic Medical Record (EMR) application to support MFA authentication during supported signing workflows. See Integrate Your EMR Application.

Set Up Users

Set up your clinicians for identity proofing and EPCS authentication. See Set Up Users.

Update Individual Identity Proofing Service

This section applies to enterprises who have previously integrated with DigiCert for Individual identity proofing.

IMPORTANT:
Imprivata Enterprise Access Management support for Individual identity proofing with DigiCert ends July 31, 2027. After July 31, your DigiCert license cannot be renewed.

Update to Imprivata Individual Identity Proofing before July 31. After the update, clinicians already proofed with DigiCert keep their status and don't need to be proofed again.

If your DigiCert certificate expires before updating the service, clinicians identity proofed with DigiCert cannot complete EPCS workflows.

1. In the Imprivata Admin Console, go to the **gear icon** > **Settings** > **Identity proofing**.

   This page displays the status of your enterprise in preparation for the update:

   - **ICP Tenant Connected** — If your Imprivata Cloud (ICP) tenant is not connected and reachable, complete that connection next.
   - **In-Progress DigiCert Enrollments** — You can choose to delay the service update until no clinicians are in progress, or update now, and those clinicians will need to re-enroll through the new service. A list of in-progess enrollments is available here.
   - **Imprivata Agent Version** — Individual identity proofing requires the Imprivata agent 26.3 or later. If your enterprise includes unsupported agents used in the last 90 days, a message appears here. Upgrade agents as needed. See Deploying The Imprivata Agent.

     NOTE:
     Clinicians can authenticate for EPCS at Imprivata agents pre-26.3. Only Identity proofing is unsupported.

2. When you're ready, click **Get started**.
3. Click **Update service**. This update is permanent and cannot be undone.

Individual Identity Proofing

To e-prescribe controlled substances (EPCS), you need to enroll DEA-approved authentication methods, and be identity proofed.

Before You Begin

You will need the following to complete identity proofing:

- Your smartphone
- A government-issued photo ID: U.S. driver's license, state ID card, U.S. passport, or permanent resident card.
- Access to your email and phone
- Access to your DEA-approved authentication methods

Enroll Authentication Methods

1. Begin by clicking on the Imprivata icon in the system tray > **Enroll Authentication Methods**.
2. After you log in, the enrollment utility opens.

   If you don't have at least two EPCS allowed authentication methods enrolled (Imprivata ID, password, token), you will see a notification. Enroll these first.
3. After the button is enabled, click **Start identity proofing**.

Identity Proofing Steps

This page lists the email address and phone number you must have access to. If you have access to these, plus your DEA-approved authentication methods, click **Next**.

Verify Your Email

A verification code was sent to the address listed. Enter your code and click **Submit**.

Verify Your Phone Number

1. Select to receive a text or a phone call and click **Send code**.
2. Enter your code and click **Submit**.

Confirm Your Authentication Methods

1. Authenticate with the DEA-approved authentication methods you enrolled earlier.
2. Click **Continue**.

Complete Identity Proofing

Validate your identity with a trusted identity verification provider.

1. Choose how to continue: on this computer using its webcam, or on your phone, by scanning the QR code onscreen.
2. Take a clear photo of the front and back of your government ID: U.S. driver's license, state ID card, U.S. passport, or permanent resident card.
3. Take a clear photo of your face.

© 2026 Imprivata, Inc. All Rights Reserved.

4. After the verification is complete, the process switches back to your computer.

   Your DEA-approved authentication methods will now include the message **EPCS allowed**.

Reporting

In the Imprivata Admin Console, go to **Reports**. The Individual Identity Proofing Activity Report tracks the history of identity proofing actions for clinicians.

Other relevant reports include EPCS Enrollment, EPCS Signing, User Activity, Computer Activity, and the Audit Log.

DigiCert Individual Identity Proofing and Enrollment

IMPORTANT:
Imprivata Enterprise Access Management support for Individual identity proofing with DigiCert ends July 31, 2027. After July 31, your DigiCert license cannot be renewed.

Update to Imprivata Individual Identity Proofing before July 31. After the update, clinicians already proofed with DigiCert keep their status and don't need to be proofed again.

If your DigiCert certificate expires before updating the service, clinicians identity proofed with DigiCert cannot complete EPCS workflows.

This topic provides an overview of how Individual providers complete identity proofing with DigiCert and enroll their authentication methods.

To e-prescribe controlled substances with Imprivata Enterprise Access Management, you need to complete two tasks:

- **Identity proofing**: Personal verification with DigiCert, a trusted partner.
- **Enroll** EPCS allowed authentication methods during and after successful identity proofing.

EPCS allowed authentication methods are selected by your enterprise and may include the Imprivata ID app, fingerprints, and/or OTP tokens.

BEST PRACTICE:
Online Verification is the knowledge-based process for Identity Proofing with DigiCert. It's the fastest and easiest method. For more details, see Complete Identity Proofing with DigiCert below.

Overview

1. Log into the Imprivata enrollment utility.
2. Enroll two EPCS allowed authentication methods.
3. Click **Start identity proofing**.
4. Verify your email address.
5. Verify your phone number.
6. Authenticate with an EPCS Allowed method (you enrolled this in Step 2).
7. Online Verification with DigiCert, or Declaration of Identity Verification is available as a fallback.
8. Receive Success email from Imprivata.
9. Enroll additional EPCS Allowed authentication methods.

This process is described in detail below.

© 2026 Imprivata, Inc. All Rights Reserved.

Before You Begin

To successfully complete identity proofing and enrollment with DigiCert, you need:

- If you're enrolling the Imprivata ID app, you need your iOS or Android device
- Access to the email address on file with your enterprise
- Access to the phone on file with your enterprise
- A US Social Security Number
- A government ID

List of Acceptable IDs

- U.S. passport
- U.S. passport card
- Permanent Resident card
- Alien Registration Receipt card
- Foreign passport
- CAC card
- PIV card
- U.S. military photo ID
- U.S. driver's license or ID card
- Federal, state, or local government ID
- School ID card with a photograph
- U.S. military card or draft record
- Military dependent’s ID card
- U.S. Coast Guard Merchant Mariner card
- Canada driver’s license
- Other photo ID issued by a government entity

NOTE: DigiCert cannot complete identity proofing if you use a service that blocks credit checks by Experian. Contact Experian (1-888-397-3742) to remove the hold from your credit information. Typically, the credit check hold is not removed immediately; ask Experian when the hold will be removed. After you complete identity proofing with DigiCert, contact Experian again to restore the hold to your account. If Experian is unable to assist, contact your fraud prevention service for assistance.
DigiCert does not perform a credit check. You do not need to have a credit card to complete identity proofing with DigiCert.

© 2026 Imprivata, Inc. All Rights Reserved.

Install the Imprivata ID App

To install the Imprivata ID app, go the iTunes App Store or Google Play (see links below). You must have an iOS or Android device with:

© 2026 Imprivata, Inc. All Rights Reserved.

iOS Requirements

- Imprivata supports Imprivata ID on iOS versions that Apple supports and provides updates for.

  See Apple's documentation for current supported iOS versions.
- 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.
- **Supported languages:**

  The language of the Imprivata ID app depends on the device's system settings.
  - English
  - French
- QR code for direct access to the download page on the iTunes App Store:

Android Requirements

- Imprivata supports Imprivata ID on Android versions that Google supports and provides updates for.

  See Google's documentation for current supported Android versions.
- 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.
- **Supported languages:**

  The language of the Imprivata ID app depends on the device's system settings.
  - English
  - French
- QR code for direct access to the download page on Google Play:

Log into the Enrollment Utility

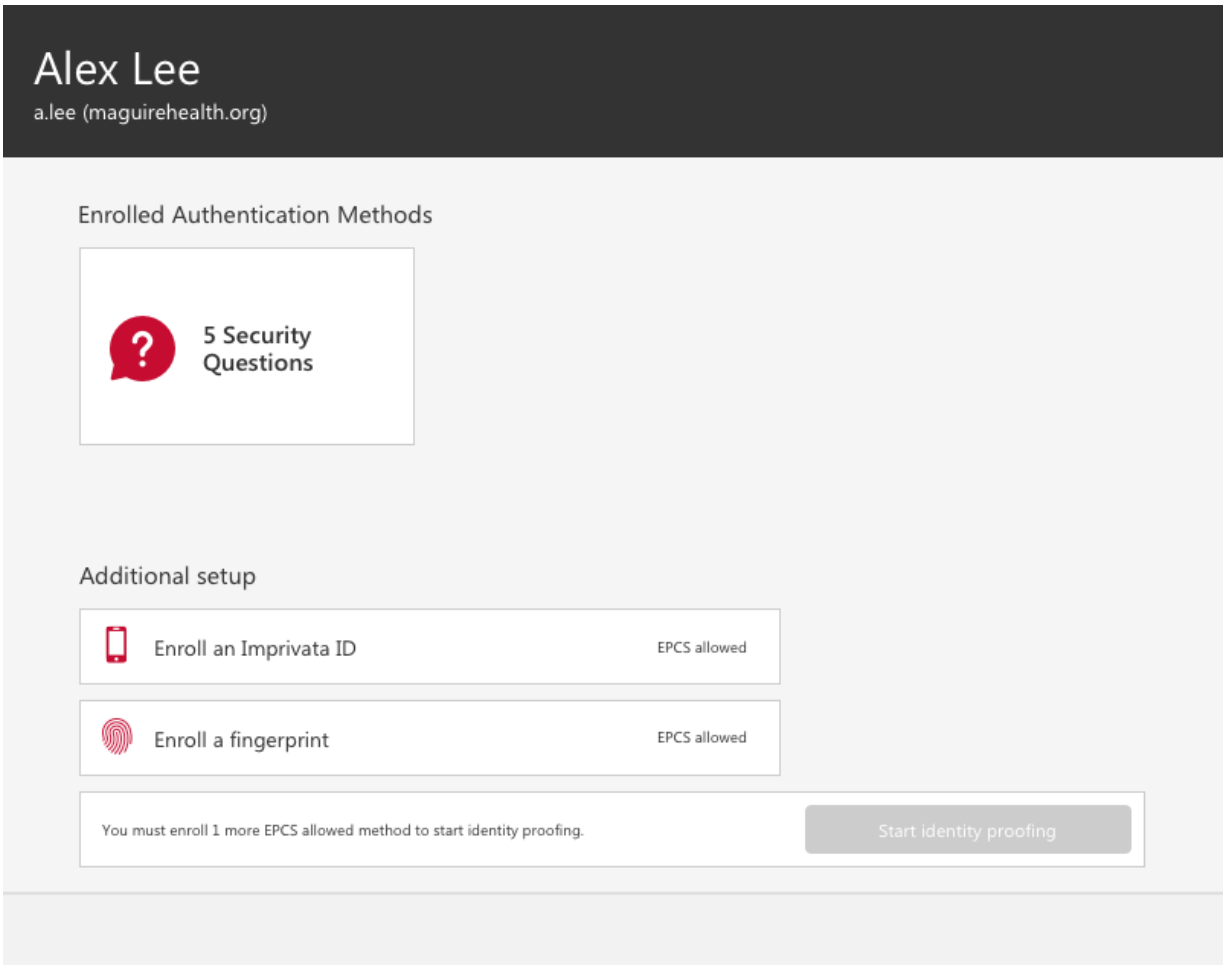
On your work computer, click the Imprivata icon in the Windows notification area, then click **Enroll Authentication Methods**.



Enroll EPCS Allowed Authentication Methods

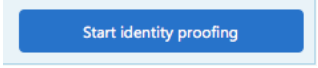
Your enterprise has selected EPCS Allowed authentication methods for EPCS. If the button **Start Identity Proofing** is not enabled yet, follow the onscreen instructions to enroll EPCS Allowed authentication methods first.

For example, this clinician must enroll Imprivata ID and one fingerprint before she can proceed:



Start Identity Proofing

After you have enrolled EPCS Allowed authentication methods, you can click **Start Identity Proofing**.



© 2026 Imprivata, Inc. All Rights Reserved.

Verify your Email Address

Imprivata Enterprise Access Management sends a verification code to your email address.

Open the message, enter the code from the email, and click **Submit**.

(Your email address is listed in your enterprise's database; typically your work email address.)

Verify your Phone Number

Verify your phone number with a verification code. Choose to receive a SMS text message or voice call.

Imprivata Enterprise Access Management uses your phone number listed in your enterprise's database.

Confirm your Identity

Confirm the methods you will use to e-prescribe controlled substances.

Only the authentication methods you use in this step are allowed for EPCS after identity proofing is complete. At the end of this process, after you have successfully completed identity proofing, return to the Imprivata enrollment utility and enroll all EPCS Allowed authentication methods.

> **NOTE on FINGERPRINT AUTHENTICATION**: If you've already enrolled more than one finger, only the finger you confirm at this step will be allowed for EPCS, and the other finger enrollment will be deleted. After you complete identity proofing, you can return to the enrollment utility and enroll more fingers for signing.

After you have confirmed the methods you will use to e-prescribe controlled substances, click **Go to DigiCert** to continue. A browser window will open.



© 2026 Imprivata, Inc. All Rights Reserved.

Complete Identity Proofing with DigiCert

Validate your identity with DigiCert, a trusted Imprivata partner. Select one of the following:

Online Verification

The online verification process will ask you a series of questions in an attempt to verify your identity. If you select this option, be prepared to answer questions pulled from your credit history. To start the process you will be required to enter your Social Security number.

Declaration of Identity Verification, "Notary option"

The Declaration of Identity verification process includes downloading a document and having it signed by a notary or trusted agent.

Online	Notary
The fastest and easiest solution. You may find it easier to complete if you review your credit history in advance. 1. On the DigiCert Personal Verification screen, click **Online Verification.** 2. Answer five personal questions based on your credit history: • Answer four out of five questions correctly in fifteen minutes. • You are given five total lifetime chances to pass Online Verification before falling back to the Notary option. 3. Log Out when you're done, and wait for an "Identity proofing confirmation" email!	The alternative to Online verification. The fallback option if you fail Online verification twice: 1. On the DigiCert Personal Verification screen, click **Declaration of Identity Verification**. 2. Download the **Declaration of Identity Verification** PDF from DigiCert. 3. Print and complete the PDF form. 4. Get the form notarized. 5. Scan the notarized form and save to your computer. 6. Log into the enrollment utility again. 7. Click **Add Document** to upload the PDF. You must upload the form within 30 days of being notarized. 8. Log Out when you're done, and 9. Wait for an "Identity proofing confirmation" email!

Identity Proofing Pending/Success

After you complete Online Verification or upload the Declaration of Identity Verification PDF, you will return to the Imprivata enrollment utility page where you will see a message **Identity proofing pending**. You will receive an email from Imprivata when you have been successfully identity proofed. After your help desk gives you access within your EMR, you can can electronically prescribe controlled substances.

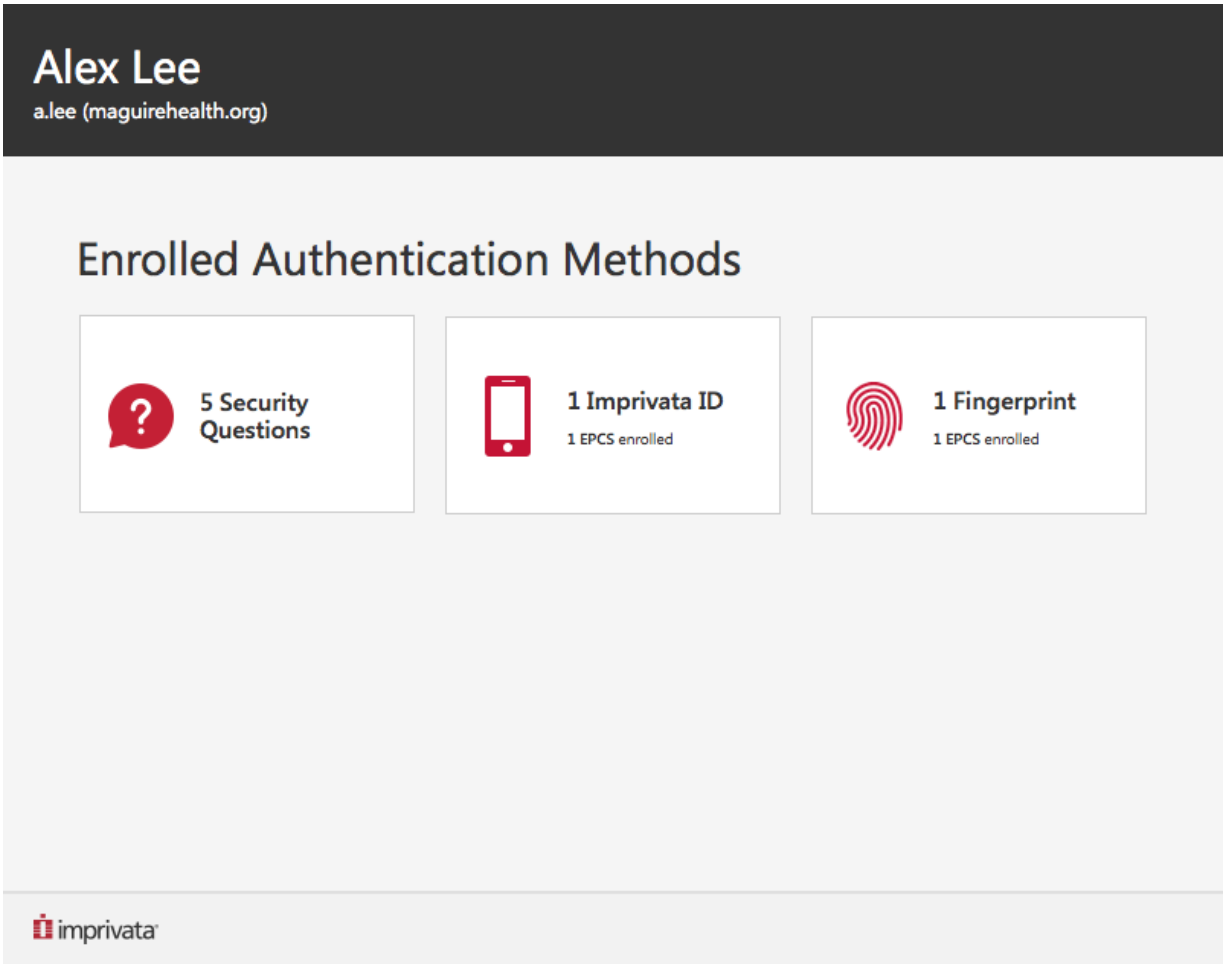
© 2026 Imprivata, Inc. All Rights Reserved.

CAUTION:
When clinicians replace their device with a new model, their EPCS Allowed Imprivata ID enrollment is not carried forward to the new device.

When these users enroll Imprivata ID on their new device, 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 again.

Afterwards: Enroll EPCS Allowed Authentication Methods

After you receive the **Identity Proofing Success** email, return to the Imprivata enrollment utility. In this example, the Enrolled Authentication Methods marked EPCS Allowed are available for signing. You can enroll more fingers and they will be available for signing too.



Identity Proofing — Clinician Enrolls Imprivata ID Again

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.

© 2026 Imprivata, Inc. All Rights Reserved.

However, 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.

Enable EPCS in EMR Software

After the provider has successfully completed identity proofing, Your EMR administrator must configure logical access control to allow the provider to authenticate for EPCS with Imprivata Enterprise Access Management.

Send Email Notifications

Configure Imprivata Enterprise Access Management to send your EMR administrator an email when each user successfully completes DigiCert identity proofing (by default, only the provider receives an automated email from Imprivata). Add the email address of the user in your enterprise responsible for logical access control for EPCS in your EMR software:

1. In the Imprivata Admin Console, go to the gear icon > **Settings** > **Notifications**.
2. On the **Notifications** page, click **Add**.
3. Select **Individual Identity proofing success email** and click **Next**.
4. Go to **Action** > **Send email** and enter the addresses for the persons who must be notified.
5. Make any additional customizations you need, then click **Save**.

Troubleshooting — DigiCert Identity Proofing

Error Message **"There is a problem. Contact your help desk."**

This message may appear when a clinician attempts to authenticate with Imprivata Enterprise Access Management. The user may encounter this error message if:

- The clinician enrolled a finger with Institutional Identity Proofing (with an enrollment supervisor), then
- Their user policy was switched to Individual Identity Proofing with DigiCert, and
- The clinician enrolled that same finger again plus another finger, then
- Their user policy is switched back to Institutional Identity Proofing.

Delete the enrolled fingers from the clinician's User page in the Imprivata Admin Console. The clinician may need to repeat identity proofing with an enrollment supervisor.

Locked Out Of Online Validation

A clinican can become locked out of online validation. They may see the DigiCert error message "**Online validation is currently unavailable. Please try another validation method or come back later**".

This message may appear if the clinician has failed online validation two times. The clinician is "locked out" from online validation for a month and must complete Declaration of Identity Verification instead. This verification method is available as an option on the DigiCert Personal Verification page.

© 2026 Imprivata, Inc. All Rights Reserved.

Troubleshooting — DigiCert User Certificates are Revoked or Renewals Fail

DigiCert Revokes Certificates for Users in a Production Enterprise After the Same Users are Deleted from a Test Enterprise

DigiCert may revoke certificates for some users in a production Imprivata enterprise in the following situation. An administrator creates a backup copy of an Imprivata production database and deploys that copy to a test enterprise. The test enterprise can communicate with DigiCert. An administrator deletes some users from the test enterprise using the administrative console for that enterprise. Imprivata Enterprise Access Management in the test enterprise tells DigiCert that those users' certificates are no longer needed, so DigiCert revokes them. The revocation affects both the test and production enterprises, preventing those users from performing EPCS (e-prescribing controlled substances).

To prevent this problem, see Block Communication with DigiCert on an Imprivata Test Appliance, in the Imprivata Online Help.

To fix this problem if it occurs, contact Imprivata Support for assistance.

DigiCert Rejects Renewing User Certificates in a Production Enterprise After Renewing the Same Users' Certificates in a Test Enterprise

DigiCert may reject certificate renewal requests for users in a production Imprivata enterprise in the following situation. An administrator creates a Imprivata test enterprise that has some or all of the same user accounts as a production enterprise. The test enterprise can communicate with DigiCert. Later, as the deadline for certificate renewal approaches, an Imprivata appliance in the test enterprise contacts DigiCert and renews certificates for user accounts in the test enterprise. Then when an appliance in the production enterprise contacts DigiCert to renew certificates for user accounts in that enterprise, DigiCert rejects renewal requests for any users whose certificates were already renewed in the test enterprise. This prevents those users from performing EPCS. It can also cause close-connection code 1006 to appear in the Imprivata Admin Console in various areas, such as in an Identity Proofing report or in the user details page for a user.

To prevent this problem, see "Block Communication with DigiCert on an Imprivata Test Appliance" in the Imprivata Online Help.

To fix this problem if it occurs, contact Imprivata Support for assistance.

SSL Inspection of Appliance Traffic Causes DigiCert User Certificate Renewal to Fail

DigiCert certificate renewal fails if you have SSL inspection enabled for all traffic to and from the Imprivata appliances. SSL inspection changes the response the appliance receives from DigiCert, so that the appliance can't parse the certificate renewal response. This can also cause close-connection

© 2026 Imprivata, Inc. All Rights Reserved.

code 1006 to appear in the Imprivata Admin Console in various areas, such as in an Identity Proofing report or in the user details page for a user.

To prevent this problem, do not enable SSL inspection for traffic to and from Imprivata appliances.

If SSL inspection is already enabled for that appliance traffic, or to fix this problem if it occurs, disable that SSL inspection until after all user certificates in the Imprivata enterprise are renewed.