imprivata®

Product Documentation

Individual Identity Proofing with DigiCert

Imprivata Enterprise Access Management 24.2

Identity Proofing

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.

Identity proofing is the process for validating a provider's identity. Imprivata Confirm ID 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.

CAUTION — Institutions with no DEA Number: For organizations with no institutional DEA number, a Certificate Authority (CA) such as DigiCert must perform identity proofing and issue certificates to your providers for DEA-regulated signing workflows. Credentials tied to a user's identity proofing must be used for DEA-regulated signing workflows.

Institutions with a DEA Number: You may perform identity proofing within your organization with Enrollment Supervisors, or you have the option to use a CA to perform identity proofing.

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.

Set Up Enterprise

Set up your enterprise for individual identity proofing with DigiCert.

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:

1. In the Imprivata Admin Console, open the **gear icon** menu, and click **Settings**.
2. In the **Email configuration** section, click **Modify**.
3. Type the **IP address** or **FQDN** of the mail server in the **SMTP Server** field.
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 you vendor specific documentation.
5. If required, type the credentials of an account that is authorized to send email through your server/mail relay in the **SMTP Server Account Username** and **SMTP Server Account Password** fields.
6. Type the sender address in the **Email messages are from** field.
7. Click **OK**.

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

Outbound Communication

To enable individual identity proofing with DigiCert, your Imprivata appliances must be able to communicate outside your firewall.

Port	Protocol	Direction	Host	Description
443	HTTPS	Outbound	api.digicert.com	DigiCert server required for Individual identity proofing
	HTTP	Outbound	http://ocsp.digicert.com	DigiCert server required for revocation checking via the online certificate status protocol
	HTTP	Outbound	http://ocsptest.digicert.com	Non-production DigiCert server for revocation checking via the online certificate status protocol. For test computers only. [1]
443	HTTPS	Outbound	www.digicert.com	DigiCert identity proofing: required to access the token URL in the enrollment utility.
443	HTTPS	Outbound	*.amazonaws.com	A connection to Amazon S3 is needed for the Imprivata appliance to update the DigiCert metadata (e.g. the client certificate). This is required for Individual identity proofing of new users.
443	HTTPS	Outbound	cloud.imprivata.com	Connection to the Imprivata Cloud, allows communication from users outside the firewall to Imprivata OneSign inside the firewall.

[1] Test computers in a non-production enterprise use a test DigiCert server for revocation checking. If communication to the test DigiCert host is blocked, the user may see an alert in the Admin Console that the DigiCert service is down. Functionality is not blocked; revocation checking will not occur.

For the complete list of remote communication sites required in an Imprivata enterprise, see "About Outbound Communications" in the Imprivata Online Help.

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. 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.

Active Directory Requirements

The following Active Directory (AD) attributes are required to be sent by Imprivata Confirm ID to enable identity proofing with DigiCert. Verify that the following attributes in AD are present and accurate for all providers who will be identity proofing with DigiCert:

- First Name
- Last Name
- Email address (the user must be able to receive a message at this address during identity proofing)
- Phone number (the user must be able to receive an SMS message or voice call at this number during identity proofing)

Verify that the provider's legal name is entered in the **First Name** and **Last Name** fields, and verify the **email address** field is accurate. Imprivata Confirm ID will automatically send these attributes to DigiCert to register the user for identity proofing.

You can also view, add, or edit these values on the User details page for each user on the Imprivata Admin Console.

For identity proofing 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**.

> ⚠ **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.
- Imprivata Confirm ID will ignore any character that is not a digit (for example: hyphens, periods, parentheses).
- Any telephone number that doesn't meet these criteria or is malformed in any way will be ignored. The provider will not be able to begin identity proofing until the number is corrected in AD or the Imprivata Admin Console.
- If a provider's telephone number(s) are not present in AD, the provider will receive an error message. You can add or edit the phone number(s) on the User details page of the Imprivata Admin Console.

Browser and PDF Requirements

The Imprivata enrollment utility launches a browser window to complete individual identity proofing with DigiCert.

When a user chooses Declaration of Identity Verification (the "notary method"), the browser must be able to download a PDF, and the user's workstation must have the ability to open and print the DigiCert form, and later, the user must be able to scan the printout so it can be uploaded to DigiCert.

Set Up Users

Set up your clinicians for DigiCert identity proofing and EPCS authentication.

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 Confirm ID workflow with the specified authentication methods. (Your EMR software won't prompt a user for two-factor authentication with Imprivata Confirm ID until your EMR administrator enables logical access control for that user.)

For complete details, see "Configuring the Imprivata Confirm ID Workflow Policy" in the Imprivata Online Help.

Select Authentication Methods

By default, Fingerprint + Imprivata ID are selected for the EPCS workflow. If you want to change this selection:

1. In the Imprivata Admin Console, go to the **Users** > **Workflow policy**. The **Confirm ID workflow policy** page opens.
2. Edit the authentication options for EPCS. EPCS Allowed authentication methods:
   - Fingerprint + network password
   - Fingerprint + Imprivata ID
   - Fingerprint + OTP token
   - Network password + Imprivata ID
   - OTP token + network password
3. Click **Save**.

Select Individual and/or Institutional

If identity proofing for any of your providers will be performed by DigiCert, then configure your enterprise as follows:

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

DigiCert Individual Identity Proofing and Enrollment

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 Confirm ID, 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 Confirm ID 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.

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.

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:

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:

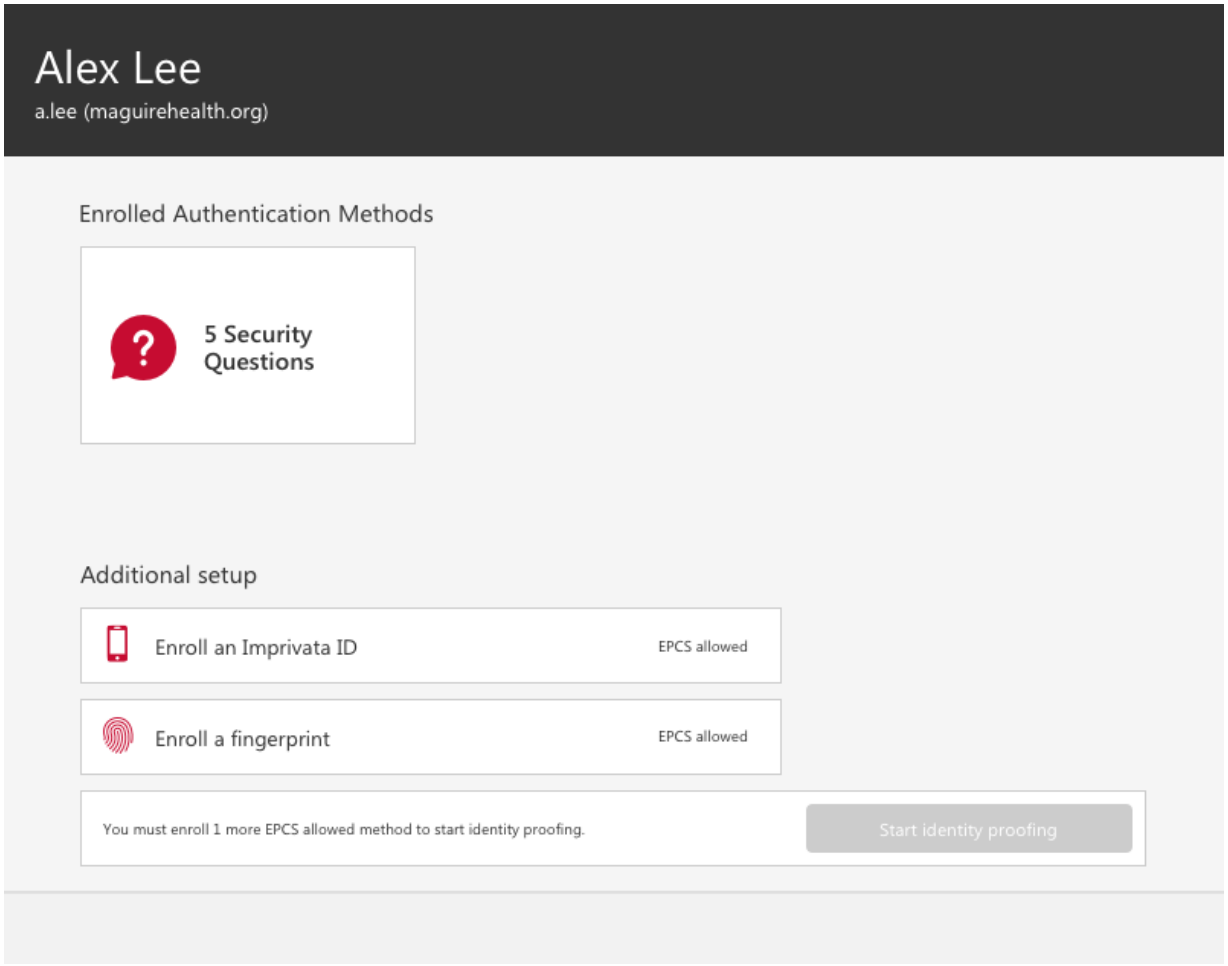
Log into the Enrollment Utility

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

Enroll EPCS Allowed Authentication Methods

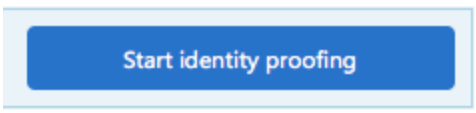
Your enterprise has selected EPCS Allowed authentication methods for EPCS. If the button **Start Identity Proofing** is not enabled yet, follow the onscreen instructions to enroll EPCS Allowed authentication methods first.

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**.



Verify your Email Address

Imprivata Confirm ID 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 Confirm ID 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.

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

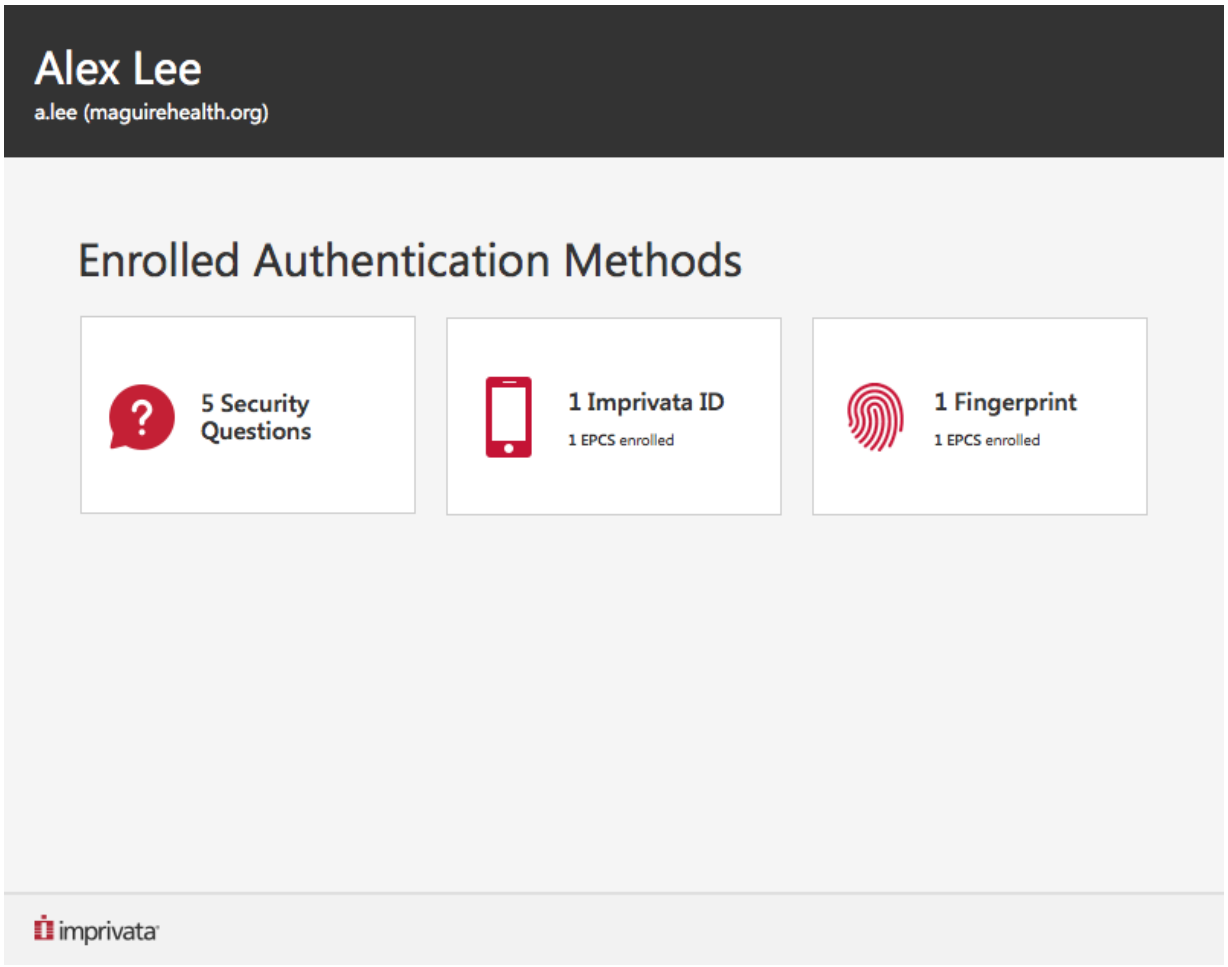
After you complete Online Verification or upload the Declaration of Identity Verification PDF, you will return to the Imprivata enrollment utility page where you will see a message **Identity proofing pending**. You will receive an email from Imprivata when you have been successfully identity proofed.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

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.

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 Confirm ID.

Send Email Notifications

Configure Imprivata Confirm ID 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 Confirm ID. 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.

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 Confirm ID enterprise in the following situation. An administrator creates a backup copy of a Confirm ID 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. Confirm ID 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 Confirm ID enterprise in the following situation. An administrator creates a Confirm ID 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 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 Confirm ID enterprise are renewed.