imprivata®

Product Documentation

Administrator Guide

Imprivata Patient Access

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

Table of Contents

System Requirements

This section includes information about the system requirements for Imprivata Patient Access. Any limitations are noted in the support details or footnotes.

Microsoft Entra ID Requirements

This section includes information about requirements for Patient Access in Microsoft Entra ID (formerly Azure Active Directory).

Imprivata IP Addresses

Add the static egress addresses for Imprivata IP addresses as trusted locations in Microsoft Entra ID:

- 44.207.16.175/32
- 44.196.189.191/32
- 34.195.47.118/32

Microsoft Entra ID Groups

Microsoft Entra ID is required to control access to the Patient Access Admin Console.

In Microsoft Entra ID, define at least one Admin group for Patient Access administrators. Move the Microsoft Entra ID Global Admin and any other admins you'd like managing Patient Access into this group.

Registration Desktop Requirements

This section includes information about the system requirements for Patient Access registration desktops. Any limitations are noted in the support details or footnotes.

If a component is not listed, then its official status is "Not Supported".

Item	Descriptions
Operating System	Windows 11 (x64) Windows 10 (x64) - all versions through Windows 10, November 2021 Update / version 21H2
Processor	**Recommended:** Intel Quad Core i5 2.5 GHz or greater with 4 GB of RAM **Minimum:** Intel Pentium Dual Core - 2.0 GHz processor or faster with at least 2 GB of RAM
Available Disk Space	**Recommended:** 6 GB **Minimum:** 1.5 GB
Microsoft Visual C++ Redistributables	Installed on the endpoint and on the Citrix server when the Imprivata Patient Access Virtual Channel component is installed there. • Microsoft Visual C++ Redistributable x64 2015-2022 version **14.40** or later • Microsoft Visual C++ Redistributable x86 2015-2022 version **14.40** or later Only needed for customers using Citrix Virtual Apps.

Item	Descriptions
Microsoft .NET Framework 4.7.2 or later	Microsoft .NET Framework 4.7.2 or later installed wherever the Imprivata Patient Access Epic Connector component is installed. • For Citrix, this will be on the Citrix server. • For a full Imprivata Patient Access client install of Epic, this will be on the endpoint.
Display and Peripherals	1400 x 900 or higher-resolution monitor Microsoft Mouse or compatible pointing device Keyboard USB 2.0 or 3.0 ports USB Web Cam (confirm model with Imprivata)

Registration Kiosk Requirements

This section includes information about the system requirements for Patient Access Epic Welcome Kiosks. Any limitations are noted in the support details or footnotes.

If a component is not listed, then its official status is "Not Supported".

Epic is a registered trademark of Epic Systems Corporation.

Item	Descriptions
Operating System	Windows 11 (x64) Windows 10 (x64) - all versions through Windows 10, November 2021 Update / version 21H2
Processor	**Recommended:** Intel Quad Core i5 2.5 GHz or greater with 4 GB of RAM **Minimum:** Intel Pentium Dual Core - 2.0 GHz processor or faster with at least 2 GB of RAM
Available Disk Space	**Recommended:** 6 GB **Minimum:** 1.5 GB
Display and Peripherals	1280 x 1024 or higher-resolution monitor Microsoft Mouse or compatible pointing device Keyboard USB 2.0 or 3.0 ports USB Web Cam (confirm model with Imprivata)

Kiosk Language Support

Language
English
Spanish

Recommended Cameras

High definition (HD) cameras perform better than standard definition (SD) cameras. Lower resolution cameras are not recommended due to outdated technology.

Virtual Desktop Infrastructure

The following table details the support status for virtual environments. If a component is not listed, then its official status is "Not Supported".

Imprivata also recommends that you check with your vendor for recommended configuration.

Citrix Virtual Apps and Desktops

Formerly known as XenDesktop and XenApp. Includes Citrix StoreFront.

Version	Notes
7 2402 LTSR	
7 2311	
7 2203 LTSR	See Known Issue below.
7 1912 LTSR	CU 7 and higher

Citrix Workspace App for Windows

Version	Notes
2402 LTSR	
2311	
2203 LTSR	See Known Issue below.
1912 LTSR	CU 7 and higher

Known Issue: Citrix has identified a memory leak in the Citrix virtual channel when a webcam is forwarded over the virtual channel. With this memory leak, the webcam stops working after roughly 10-25 uses of the camera. To resolve the memory leak issue, customers need to use 2311 or higher VDA and 2311 or higher CWA clients.

Workaround: When the webcam stops working after roughly 10-25 uses of the camera, to work around the issue, the end user must log off the Citrix Storefront session, then log back in. In some scenarios, the user may also need to unplug and plug in the USB webcam.

Patient Access Admin Console

Browsers

The following browsers are supported for accessing the Patient Access Admin Console

NOTE:
The software version and date when Imprivata will end support for a third-party product is typically when the third-party vendor (for example, Microsoft) has previously declared its end of support.

Browser	Support Information
Google Chrome	Yes
Microsoft Edge Chromium	Yes

Configure Patient Access to Microsoft Entra ID

> **NOTE:**
> Microsoft recently updated the name of Azure Active Directory to Microsoft Entra ID. Imprivata has updated as many instances as possible, but in certain instances, the older name may be used.

The following sections detail how to configure Patient Access to your Microsoft Entra ID (formerly Azure Active Directory):

1. Prepare Microsoft Entra ID for Patient Access
   - Add Enterprise Access Management Cloud IP addresses to your allowlist in Microsoft Entra ID.
2. Start the setup wizard to grant Patient Access access to your Microsoft Entra ID, finalize the configuration, and sync an Admin group to Patient Access.

After completing these steps, the user will be able to authenticate into Patient Access successfully.

Assumptions

This topic assumes the following:

- You are familiar with Microsoft Azure Portal and Microsoft Entra ID use and terminology.
- You have an Microsoft Entra ID Directory Global Administrator or Privileged Role Administrator.
- You have an active Microsoft Entra ID tenant and license.
- You have users in Active Directory that have synced to Microsoft Entra ID through Microsoft Entra Connect (formerly Azure AD Connect).

Additional References

Before configuring Patient Access, review the following documentation:

- **Microsoft Entra ID documentation**. Many configuration tasks in this topic are performed in the Azure portal.

  For more information, see the Microsoft Entra ID documentation.

  > **NOTE:**
  > Screenshots of the Microsoft Azure portal are included here as a courtesy to assist in the configuration.
  >
  > Microsoft may update their Azure portal and associated documentation at any point. It may impact the tasks documented in this guide.

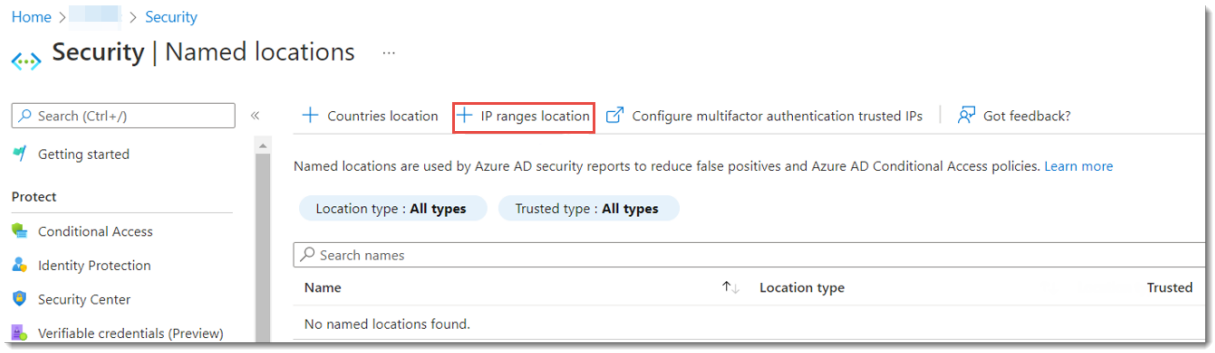
Prepare Microsoft Entra ID for Patient Access

Update Microsoft Entra ID to trust Imprivata's servers.

Step 1: Add Imprivata IP Addresses to the Microsoft Entra ID Allowlist

To add Imprivata IP addresses to your Microsoft Entra ID allowlist:

1. In your Microsoft Entra ID tenant, go to **Security > Named locations**, and select **+ IP ranges location**.

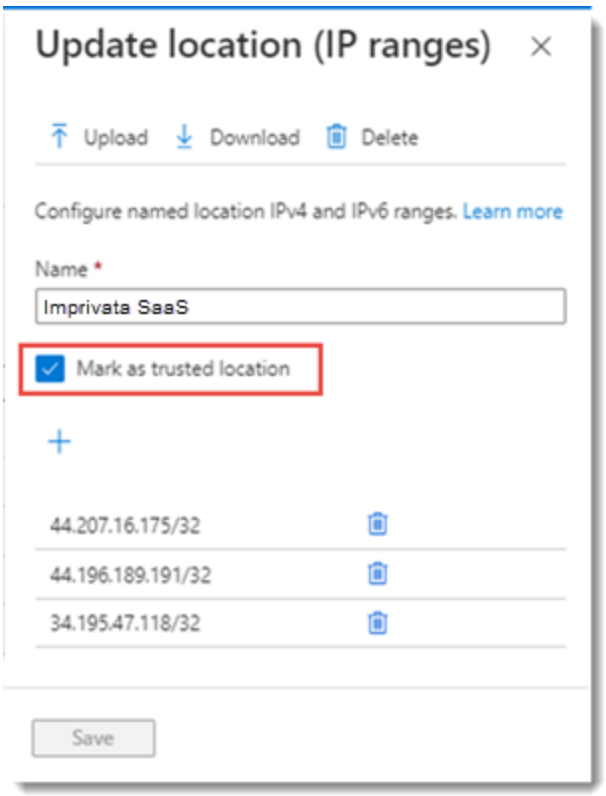


2. In the Name box, type a descriptive name for the new location and select **Mark as trusted location**.
3. Add the IP addresses:

   (Static egress IP addresses)

   - 44.207.16.175/32
   - 44.196.189.191/32

- 34.195.47.118/32

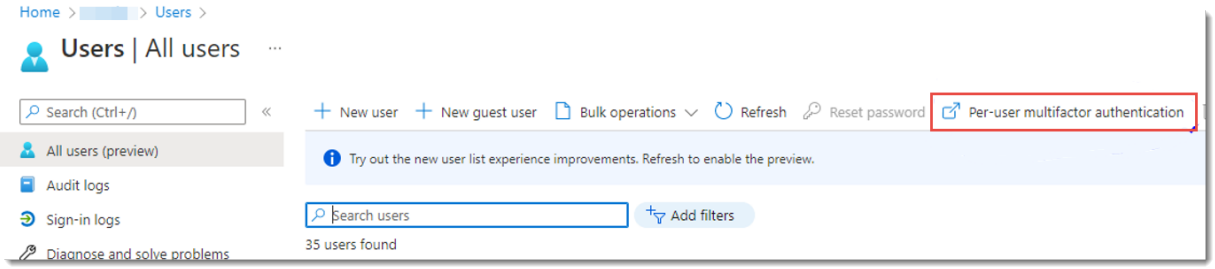


4. Click **Create**.

Step 2: Add Imprivata IP Addresses to Multifactor Authentication Trusted IPs

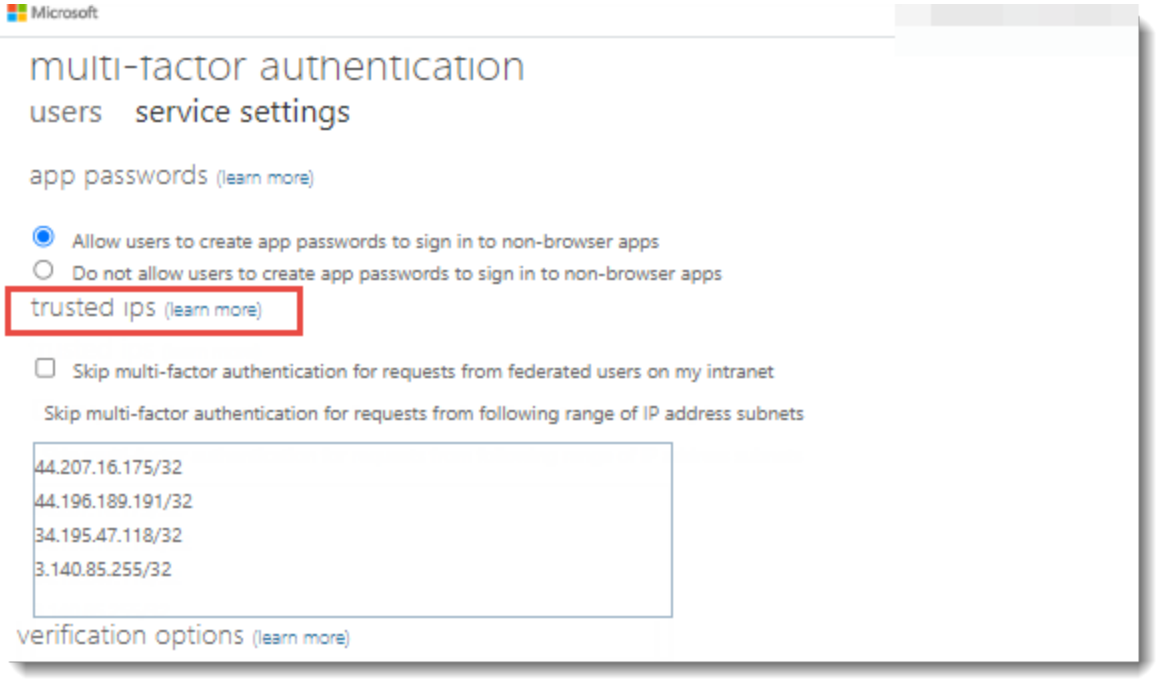
If users are in a "per-user" multifactor authentication, then add the Imprivata IP addresses to the **Multifactor authentication trusted IPs** list to successfully authenticate to Patient Access.

1. To configure multifactor authentication trusted IPs, go to **Security > Named locations**, and select **Configure multifactor authentication trusted IPs**.



2. Add the Enterprise Access Management Cloud IP addresses as trusted IPs:
   - 44.207.16.175/32
   - 44.196.189.191/32

- 34.195.47.118/32



Step 3: Create One Admin Group in Microsoft Entra ID to Sync to Patient Access

At a minimum, Patient Access user management requires one Admin group: Patient Access Admins.

This group can be created and maintained in Active Directory (AD), but will need to be synced into Patient Access during the setup wizard. After Patient Access has been set up, the admin can sync any additional Admin and user groups as needed.

1. Create the Patient Access Admin group.

   Move the Microsoft Entra ID Global Admin and any other admins you'd like managing Patient Access into this group. They will have access to the Patient Access Admin Console.

Use Patient Access Setup Wizard, Complete Configuration, and Sync Groups

This is a one-time task.

Step 1: Launch the Patient Access Setup Wizard

1. Imprivata provisions your Patient Access tenant and sends you the setup URL to your email. Launch the wizard by clicking on this link.
2. In the Patient Access setup wizard, provide information to connect to your Microsoft Entra ID:
   a. Enter or paste your Microsoft Entra ID tenant ID and click **Continue to Microsoft Authentication**.

      The system connects to your Microsoft Entra ID.

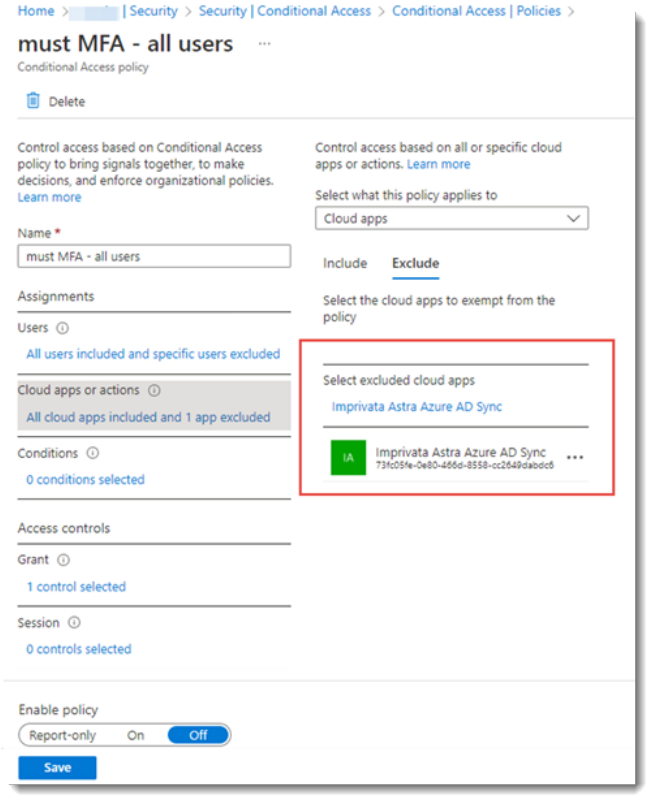
Step 2: Grant Patient Access Required Permissions to the Customer Microsoft Entra ID Tenant

1. Log in to Microsoft Entra ID with Global Administrator or Privileged Role Administrator privileges.
2. You are redirected to a page where Imprivata's verified application must be authorized for the following permissions:
   - Read directory data
   - Read all groups
   - Sign in and read user profile
   - Read all users' full profiles
3. Click **Accept** to grant Patient Access access to the AAD tenant.

Step 3: Complete Microsoft Entra ID Configs — Adjust Conditional Access Policies Requiring Multifactor Authentication

To adjust the conditional access policies requiring multifactor authentication (MFA):

1. In Microsoft Entra ID, go to **Security > Conditional Access**, and select a policy that applies to Patient Access users and requires MFA in the **Access controls** section.
2. **To exclude the Imprivata SaaS Azure AD Sync application, go to Cloud apps or actions > Cloud apps > Exclude> Select excluded cloud apps,** and select**Imprivata Astra Azure AD Sync.**



3. Exclude the **Imprivata Astra Azure AD Sync** application from all the conditional access polices that require MFA for users that will use Patient Access.

Step 4: Patient Access Setup Wizard — Create the Initial Patient Access Administrator

In the Patient Access setup wizard, you will create the first Patient Access administrator. This administrator does **not** need to be an AAD admin, it can be any Microsoft Entra ID user.

1. Enter the username (the Microsoft Entra ID UPN) for a person who will administer Patient Access. Click **Next** to continue.

   For future use, the administrator will receive an email with a URL allowing them to log in to the Patient Access Admin Console if they have an email address associated with their Microsoft Entra ID UPN.
2. The administrator logs in to the Patient Access Admin Console.

Step 5: Identify All Microsoft Entra ID Admin Groups to be Synced into Patient Access

1. Select the Microsoft Entra ID admin group created in the preparation task. Select at least one group that contains administrator users.

   You will be able to sync as many admin and user groups as needed afterwards.
   a. Start typing a group name and select it from the resulting drop-down list.

      Make sure that the admin group you select is a security group with at least one admin in it.

      Add admin groups in the same manner. Click **OK**.
   b. In the top left column, select **Add groups** to add any user groups. Click **OK**.

      The Microsoft Entra ID setup is complete. Continue exploring the Admin Console.
2. Click **Go to Patient Access Admin Console > Users tab** to view your users.

   Microsoft Entra ID setup is now complete. User sync will run in the background and display users on the users page.

Install the Patient Access Software

Assumptions

This topic assumes your knowledge in the following areas:

- Your experience installing enterprise software
- Your familiarity with MSI installation controls.

  For standard msiexec options, you may want to run "msiexec /?" on the endpoint device's operating system (these can vary by Windows Installer version). If that is not an option, you can find good references by searching for command-line switches for the Microsoft Windows Installer Tool at http://msdn2.microsoft.com.
- Your familiarity with your environment's topology and how it works.

Before You Begin

Review the Registration Desktop and Kiosk System Requirements

- Review the system requirements for registration desktop and kiosks.

Working with the Installation Key

The installation key is the privileged credentials that allow your endpoints to connect to your Patient Access tenant. It is used during installation to connect endpoints to the Imprivata cloud.

> **IMPORTANT:**
> The installation key contains data that is specific to your Imprivata tenant and therefore should not be shared with anyone outside of your organization.

Virtual Channel Prerequisites

In Citrix virtual desktop infrastructure (VDI) environments where you deliver Epic[1] as a published application to endpoints:

- A supported release of Citrix Virtual Apps must be running on the server before installing the Imprivata Patient Access software.
- A supported release of Citrix Workspace App for Windows must be installed on the endpoint before the Imprivata Patient Access software.
- The Imprivata Patient Access Virtual Channel component requires the installation of the following Microsoft Visual C++ Redistributables on the endpoint and on the Citrix server:

[1]Epic is a registered trademark of Epic Systems Corporation.

- Microsoft Visual C++ Redistributables x86 2015-2022 version **14.40** or later
- Microsoft Visual C++ Redistributables x64 2015-2022 version **14.40** or later

This only applies to customers using Citrix Virtual Apps.

- Configure the Citrix server to allow the Imprivata Patient Access Virtual Channel by creating a policy with the **Virtual channel allow list** setting that includes "IMP2266" or is **disabled**.

Imprivata Patient Access Epic Connector Prerequisites

Patient Access requires that Microsoft .NET Framework 4.7.2 or later installed wherever the Imprivata Patient Access Epic Connector component is installed.

- For Citrix, this will be on the Citrix server.
- For a full Imprivata Patient Access client install of Epic, this will be on the endpoint.

Obtain the Software and Installation Key

The Imprivata Patient Access installation program is an MSI file that can be deployed using standard MSI installation commands.

1. Log in to the Patient Access Admin Console and navigate to the **Installers** tab.
2. To obtain the endpoint installer, click **Download endpoint installer**. The endpoint installer software downloads.

   Save the endpoint installer software to your machine for later use.
3. To obtain the required installation key for use with the endpoint installer, click **Copy installation key**.

   Save the installation key for a later task.
4. (Optional) Click **Copy example command line syntax with installation key** to obtain the sample command line syntax that includes your installation key. Save the example for a later task.

Run the Installation Program

To install the endpoint on registration desktops:

1. Run the Imprivata Patient Access Installer program.
2. On the Installation key screen, paste the installation key you saved in the previous task.
3. On the Component selection page, select the components to install:
   a. Imprivata Patient Access Registrar Client.

      Install on the endpoint machine. Do not install this component on the host server in a virtual desktop environment.
   b. Imprivata Patient Access Epic Connector.

      Install on the machine where Epic is installed.

For virtual desktop environments, the Epic Connector component must be installed on the host server.

c. Imprivata Virtual Channel.

Install only in virtual desktop environments. Imprivata Virtual Channel must be installed on the host server and the endpoint machine to facilitate communication between the Imprivata Patient Access Epic Connector and Imprivata Patient Access Registrar Client.

d. Imprivata Patient Access Kiosk Client.

Install on the kiosk endpoint machine.

Requires the installation of the Imprivata Patient Access Epic Connector component on the machine where Epic is installed.

> **IMPORTANT:**
> The Patient Access Registrar Client and Kiosk Client components cannot be installed on the same endpoint.

4. Click **Next** and then **Install**.

The endpoint installs successfully.

Install the Software from the Command Line

To install the Imprivata Patient Access software using the command line, use the syntax:

Syntax

```
msiexec.exe /i "Imprivata Patient Access Installer (<build>).msi" /qn /L*V
\"<logFilePath>\" INSTALLDIR="C:\Program Files\Imprivata\PatientAccess"
INSTALLATIONKEY="<INSTALL_KEY>" INSTALL_VIRTUAL_CHANNEL="0|1" INSTALL_EPIC_
CONNECTOR="0|1" INSTALL_REGISTRAR_CLIENT="0|1" INSTALL_KIOSK_CLIENT="0|1"
```

> **IMPORTANT:**
> In your script, the command-line parameters must be a single line.

Parameters

Parameter	Required	Function
/i	Required	Specifies normal installation.
/qn	Required	Runs the embedded MSI in quiet mode with no UI.

Parameter	Required	Function
/L*V	Required	Logs all output to a file and saves log to the path specified in `<logFilePath>`. **NOTE:** The path is quoted, and the quotes are escaped. The path must already exist and be accessible. The command line will not create the path.
INSTALLDIR	Optional	The base location for installing Imprivata Patient Access. If not defined, it defaults to the following location: • `"C:\Program Files\Imprivata\PatientAccess\"` and it respects the `%programfiles%` in Windows. **NOTE:** If the path contains spaces, the INSTALLDIR value must be quoted and the quotes escaped.
INSTALLATIONKEY	Required	The installation key for the client software in your Imprivata Patient Access tenant. Required for Registrar Client installation. Required for Epic Connector installation. **Note:** Upgrades to Patient Access 2024.13 (and later) will need to pass **INSTALLATIONKEY** as a command line parameter since it may not be in the registry, if the Registrar Client was omitted on the previous installation.
INSTALL_ENDPOINT CLIENT	Required	Indicates whether the Imprivata Patient Access Registrar Client component should be installed on the endpoint. Defaults to "1", meaning it will be installed without this flag present. Valid values: 1 and 0. **NOTE:** Do not install this component on the host server in a virtual desktop environment.
INSTALL_EPIC_CONNECTOR	Optional	Indicates whether the Imprivata Patient Access Epic Connector component should be installed. Defaults to "1", meaning it will be installed without this flag present. Valid values: 1 and 0. • Install the Epic Connector on the machine where Epic is installed. • For virtual desktop environments, the Epic Connector component must be installed on the host server.

Parameter	Required	Function
INSTALL_VIRTUAL_CHANNEL	Optional	Indicates whether the Imprivata Virtual Channel component should be installed. Defaults to "0", meaning it will not be installed without this flag present. Valid values: 1 and 0. • Install only in virtual desktop environments. • Imprivata Virtual Channel must be installed on the host server and the endpoint machine to facilitate communication between the Imprivata Patient Access Epic Connector and the Imprivata Patient Access Registrar Client. **NOTE:** The Imprivata Virtual Channel component does not support a custom installation directory. Imprivata Virtual Channel will always be installed to `C:\Program Files\Imprivata\Common\Virtual Channel`, regardless of whether the Client component is installed to another drive or directory.
INSTALL_KIOSK_CLIENT	Optional	Indicates whether the Imprivata Patient Access Kiosk Client component should be installed on the kiosk endpoint. Defaults to "0", meaning it will not be installed without this flag present. Valid values: 1 and 0. By default, the Kiosk Client component will be installed to `C:\Program Files\Imprivata\PatientAccess\KioskClient`. • Requires the installation of the Imprivata Patient Access Epic Connector component on the machine where Epic is installed. **IMPORTANT:** The Patient Access Registrar Client and Kiosk Client components cannot be installed on the same endpoint.

Examples

The following examples illustrate the combinations for installing the Patient Access components.

Installation of the Patient Access software with only the Patient Access Registrar Client component selected.

```
msiexec.exe /i "Imprivata Patient Access Installer (2.10.7).msi" /qn
INSTALLDIR="C:\Program Files\Imprivata\PatientAccess"
INSTALLATIONKEY="eyJ0ZW5hbn1203015bc==" INSTALL_REGISTRAR_CLIENT="1" INSTALL_EPIC_
CONNECTOR="0" INSTALL_VIRTUAL_CHANNEL="0"
```

Installation of the Patient Access Kiosk Client and Epic Connector on the local endpoint.

```
msiexec.exe /i "Imprivata Patient Access Installer (2.10.7).msi" /qn
INSTALLDIR="C:\Program Files\Imprivata\PatientAccess"
INSTALLATIONKEY="eyJ0ZW5hbn1203015bc==" INSTALL_REGISTRAR_CLIENT="0" INSTALL_EPIC_
CONNECTOR="1" INSTALL_KIOSK_CLIENT="1" INSTALL_VIRTUAL_CHANNEL="0"
```

Installation of the Patient Access Registrar Client and Epic Connector on the local endpoint.

```
msiexec.exe /i "Imprivata Patient Access Installer (2.10.7).msi" /qn
INSTALLDIR="C:\Program Files\Imprivata\PatientAccess"
INSTALLATIONKEY="eyJ0ZW5hbn1203015bc==" INSTALL_REGISTRAR_CLIENT="0" INSTALL_EPIC_
CONNECTOR="1" INSTALL_KIOSK_CLIENT="1" INSTALL_VIRTUAL_CHANNEL="0"
```

Installation of the Patient Access Registrar Client on the endpoint in a VDI environment.

```
msiexec.exe /i "Imprivata Patient Access Installer (2.10.7).msi" /qn
INSTALLDIR="C:\Program Files\Imprivata\PatientAccess"
INSTALLATIONKEY="eyJ0ZW5hbn1203015bc==" INSTALL_REGISTRAR_CLIENT="1" INSTALL_EPIC_
CONNECTOR="0" INSTALL_KIOSK_CLIENT="0" INSTALL_VIRTUAL_CHANNEL="1"
```

Installation of the Patient Access Virtual Channel and Epic Connector on the Citrix application server.

```
msiexec.exe /i "Imprivata Patient Access Installer (2.10.7).msi" /qn
INSTALLDIR="C:\Program Files\Imprivata\PatientAccess"
INSTALLATIONKEY="eyJ0ZW5hbn1203015bc==" INSTALL_REGISTRAR_CLIENT="0" INSTALL_EPIC_
CONNECTOR="1" INSTALL_KIOSK_CLIENT="0" INSTALL_VIRTUAL_CHANNEL="1"
```

Using the Dashboard and Reports

The Dashboard and Reports are two of the most important tools at your disposal to help ensure successful adoption of Patient Access. With these tools you have insight into the overall use of Patient Access. It is important to orient your team to these, ensure everyone understands how to use them, and make sure everyone has access to them. The Dashboard and Reports are daily tools a stakeholder can use to answer questions such as: “how well is Patient Access being used across my department”.

The Patient Access is a great place to start to gain a high-level view of what is going on for your organization and gives you the ability to drill down into individual facilities or departments. Additionally, you have access to trends for your organization. Here you can quickly assess if usage is going up, or perhaps going down.

NOTE:
Make sure that all your stakeholders (executives, managers, team leads) have access to the Admin Console so they have access to the Dashboard and Reports.

Reports are helpful for when you want to drill down into the data to do further investigation.

Admin Console Dashboard

The Dashboard is the Patient Access Admin Console home page. The Dashboard displays statistics in all locations available to you.

The Dashboard displays the following information:

- Bar graphs indicating the statistics of enrollments, verifications, and identifications for the selected time period.
- A summary of total enrollments, total verifications, and total identifications. The totals include any failures.

Select a Different Time Period for Dashboard

By default, the Dashboard displays activity for the last 7 days.

To select a different time period to display Dashboard information:

1. Click the drop-down and select one of the following options: **Last 24 Hours**, **Last 7 Days**, **Last 30 Days**, **Last 12 Months**.

   The Dashboard filters the results by the selected interval.

Reports

Reports are one of the most important tools at your disposal to help ensure successful adoption of Patient Access. Reports are helpful for when you want to drill down into the data to do further investigation.

> **CAUTION**: Patient information is available in many Patient Access reports. Be sure to keep the report files secure.

1. In the Admin Console, navigate to the **Reports** tab.
2. In the Reports section, select the appropriate report.
3. Select a date range for the report:
   - Enter the start date and end date range by clicking the  and selecting the dates.
   - Select an defined interval from the **Last N days** buttons - **Last 7 Days**, **Last 14 Days**, **Last 30 Days**, or **Last 90 Days**.
4. Click **Download Report**.

   The report is exported to a .CSV format in the Downloads directory on your local drive.
5. To view the report, open the downloaded file in Microsoft Excel.

Extract Reports

Extract Reports include detailed activity information extracted into a .CSV format.

Why you may use these reports:

- These reports are useful if you leverage a third party data warehouse or business Intelligence Tool and you want to extract data from Patient Access to send to these third party tools.

Report	Description
Activity Extract	Generates a report in .CSV format for the total number of enrollments, identifications, and verifications.
Audit Extract	Generates a report in .CSV format for records of the following Patient Access Admin Console audit events: • Each user who reads a patient record. • Each user who runs a patient search. • Each user who creates a patient. • Each user who deletes a patient. **NOTE:** When enrolling a new patient, potential duplicate records are displayed to the registrar to help determine if a new enrollment is a duplicate or not, the display of these potential duplicate records is recorded in the Audit Extract. Imprivata Patient Access displays data coming from your organization's EMR, which sometimes may include blank fields.

Consent for Collecting Biometrics

> **NOTE:**
> This topic only applies to Patient Access non-production environments used for training or testing. It does not apply to production environments.

Biometric privacy regulations in certain states require the collection of consent from a person for use of their biometric data in non-production (test) environments.

During training or testing of the Patient Access system, employees must consent to the collection and use of their biometric data. Photos are deleted from the test environment after 30 days.

States Requiring Consent for Biometric Data Collection

The following states require consent for biometric data collection in non-production environments:

- Illinois (IL)
- Texas (TX)
- Washington (WA)

> **IMPORTANT:**
> Depending on state privacy regulatory requirements, this list may be updated in future.

What to Expect

When enrolling in a non-production environment, the Patient Access interface displays a page where the person whose photo is being captured must indicate whether they are a resident of IL, TX, or WA, and grant or decline consent.

Workflow

In the enrollment workflow, a Consent page is displayed.

To grant or decline consent for the collection of biometric data:

1. The person enters their name in the **First Name** and **Last name** boxes.
2. The person enters their work email address in the **Work email address** box. Personal email addresses are not supported.
3. The person selects **Yes** or **No** to the **I am currently a resident of IL or TX or WA**.
   - If **Yes**, the person reads the state-specific legal text and clicks **Grant consent** or **Decline consent**.
     - Clicking **Grant consent** allows the person to perform the enrollment and continue to the photo capture.
     - Clicking **Decline consent** prevents the enrollment from proceeding and closes Patient Access.
   - If **No**, the person continues to the photo capture.

Patient Records

Click **Patients** on the Admin Console menu to open the Patient page. Use this page to locate and manage patients' records.

Search for a Patient's Record

To search for a patient's record:

1. In the Admin Console, go to **Patients**.
2. From the Patients page, do one of the following:
   - Type a patient identifier in the **Patient Identifier** box.
   - In the **Patient Name** boxes, type the patient's full last name, and the first initial of the patient's first name. Wildcard characters are not accepted.
3. Click **Search**.

   The search results contain records matching all of your search criteria.

   Each patient record includes a photo, patient name, and enrollment details, including up to three patient identifiers.

View a Patient's Record

1. Locate the patient in the search results, and then click the row.

   The Patient Details page displays the patient's information.

   Click **View patient details** to view a larger photo.
2. Review the patient's information.
   - The Patient column displays the patient photo, name, DOB, and patient identifier.
   - The Enrollment Details column displays a summary of enrollment details for the patient.

     Click the patient record to view additional details.
   - **Activity Summary** lists the number of successful authentications and the dates when the patient was first enrolled and last authenticated.
   - **Valid ID** indicates lists whether the patient's ID was checked and indicates the user and date.
   - **Activity** displays the patients enrolled, patients found, and patients not found in the patient's record, in order by date, with the most recent activity at the top of the list.

     When the patient record has been deleted, the deletion will appear at the top of the list and no further activities will be recorded.

     When patient biometrics are deleted, the Activity History displays a "Biometric deleted" message.

- **Demographic Updates** displays the history of updates made to the patient's record.
- **Identifier History** displays the change history of updates made to the patient's identifiers.
  - For an patient identifier added by a FHIR event, click **View** to view the details.
- **HL7 Messages** displays a history of HL7 messages for photo upload for the patient.

Deleting a Patient's Record

CAUTION: Use caution when deleting a patient record. You cannot restore a patient record after it has been deleted.

To delete a patient's record:

1. Locate the patient in the search results, and then click the row.

   The Patient Details page displays the patient's information.
2. Review the patient's information.

   NOTE: If you delete the patient's record, that patient will not be identified by Patient Access on his or her next visit to your facility.

   The registrar will need to enroll the patient again by following the proper Patient Access enrollment process, including checking the patient's identification with a government-issued photo ID.
3. Click **Delete**. In the confirmation dialog, enter the following information:
   a. In the **Reason for deletion** box, enter a reason for deleting the patient record.

      IMPORTANT: You must provide a reason for the deletion.

   b. Click **Permanently delete patient biometrics** to remove all biometrics and photos from the patient record in Patient Access.
4. Click **Yes** to confirm.