



## Product Documentation

# Imprivata PatientSecure Client Installation Guide

Imprivata PatientSecure® 6.9

This document describes how to install the PatientSecure client components for release .

<b>Installing Imprivata PatientSecure Clients</b>	<b>3</b>
Setting Up Your Palm Vein Scanner	3
Epic Kiosk Support for Gen 1 and Gen 2 Scanners	3
Installing the Fujitsu Drivers	3
Install the Drivers	3
Install the Drivers from the Command Line	3
Epic Welcome or PatientWorks Kiosks	4
Installing the PatientSecure Client	4
Before You Begin	4
Install the Imprivata PatientSecure Client	4
PatientSecure Client - Command Line	6
Upgrade the Client from the Command Line	10
Parameters	11
Uninstall the Client from the Command Line	11
Mapping a Computer to a Location	11
Changing a Client Machine's Mapping	12
<b>Configuring Epic Integration</b>	<b>13</b>
Before You Begin	13
Create System Category Items	13
Create the EOA Record and Link to it from System Definition	14
Enable Palm Scanner for Specific Workstations	15
Installing the Imprivata PatientSecure Client	15
Button Placement in Epic	15
Configure Patient Identifiers in PatientSecure	16
Troubleshooting	16
Epic Integration Settings	16
<b>Epic Kiosk Configuration</b>	<b>18</b>
Before You Begin	18
Installing the Fujitsu Drivers	18
Install the Drivers	18
Install the Drivers from the Command Line	19
Epic Welcome or PatientWorks Kiosks	19
Installing the Imprivata PatientSecure Client	19
Mapping a Computer to a Location	19
Configure an Authentication Device	20
Create the Epic Configuration ProglD	21
Enabling Palm Scanner for Specific Workstations	21
Turn Off Epic Kiosk Photo Capture	21
Configure the PatientSecure Kiosk Screens	22
Troubleshooting	22
Epic Kiosk Settings	22
<b>Configure PatientSecure Virtual Channel</b>	<b>25</b>
Virtual Channel Support	25
Before You Begin	25
Review System Requirements	25
Enable PatientSecure Virtual Channel	25
Prerequisites	26
Install Software Dependencies	26
Obtain the PatientSecure Client Installation Package	26
Install Epic Integration/Toolbar and Virtual Channel on the Citrix Server	26
Install PatientSecure Client on Endpoints	27
Install from the Command Line	28

# Installing Imprivata PatientSecure Clients

---

Imprivata PatientSecure runs the biometric scanner on each client machine in your installation.

## Setting Up Your Palm Vein Scanner

Registrars work with Imprivata PatientSecure to match patients with their medical records in your electronic medical record system (EMS).

For installations that use palm scans, Imprivata PatientSecure supports Fujitsu palm vein scanners.

## Epic Kiosk Support for Gen 1 and Gen 2 Scanners

In PatientSecure 6.9, Epic kiosks only support Gen 2 palm scanners, not the Gen 1 palm scanners.

To use a Gen 1 palm scanner on an Epic kiosk using a PatientSecure environment, you will need to use the 4.x or 5.x Epic Kiosk, Hub and Gateway components.

## Installing the Fujitsu Drivers

### Install the Drivers

To install Fujitsu F-Pro extended drivers with InstallShield:

1. Disconnect the palm scanner from the computer.
2. Download the PatientSecure software .zip file from the Imprivata PatientSecure downloads page.
3. Extract the .zip and navigate to the F-Pro Sensor drivers directory.
4. Run PSSD\_32.msi or PSSD\_64.msi, according to your kiosk's platform.
5. Follow the instructions in the installer.
6. When the installation is completed, click **Finish**.
7. Click **Yes** to restart the computer.

Repeat this procedure for each kiosk using a scanner.

### Install the Drivers from the Command Line

To install the Fujitsu F-Pro drivers from the command line:

1. In the extracted .zip directory, navigate to the directory F-Pro Sensor drivers.
2. From the command line, run the commands, according to your kiosk's platform:

```
msiexec /i <pathToFujitsuDrivers>\PSSD_64.msi /qn /forcerestart
```

```
msiexec /i <pathToFujitsuDrivers>\PSSD_32.msi /qn /forcerestart
```

where <pathToFujitsuDrivers> is the path to the Fujitsu F-Pro drivers.

# Epic Welcome or PatientWorks Kiosks

If you are installing Imprivata PatientSecure on Epic Welcome or PatientWorks kiosks:

1. Uninstall the drivers from the kiosk.
2. Install the Fujitsu F-Pro drivers.
3. Install the Imprivata PatientSecure client software with the kiosk.

## Installing the PatientSecure Client

Use the Imprivata PatientSecure Install Wizard to install pre-defined combinations of PatientSecure features, based on your implementation.

### Before You Begin

Before you begin, have the following information ready:

- **PatientSecure environment.** PatientSecure server components are installed and Admin Console is configured.
  - Take note of the fully qualified domain name (FQDN) and the port number of the PatientSecure Web Services (PSWS) server. You will use it during client installation.
- **Review the [system requirements](#)** for the Imprivata PatientSecure client.
  - Install the required software dependencies on the client computer.
  - Ensure that the required client communication ports are open.
- For Epic Integration clients, see [Epic Integration requirements](#).
- For Epic Kiosk clients, see [Epic Kiosk requirements](#).
- For Citrix environments where you want to use Imprivata Virtual channel communications for PatientSecure Toolbar or Epic Integration as published applications on endpoints, see [Configure PatientSecure Virtual Channel](#).

## Install the Imprivata PatientSecure Client

To install the PatientSecure client:

1. Download the client installation package provided by your Imprivata PatientSecure representative or from the PatientSecure software download package available on the [Imprivata Customer Experience Center](#).
2. Extract the software package and run `ImprivataPatientSecureWebClient.exe`.
3. Click **Next**.
4. Complete the wizard, including the following steps:
  - a. If there are missing software prerequisites, such as Microsoft Visual C++ redistributables, the wizard prompts for you to install them. In this case, the PatientSecure client installation will require a reboot of the endpoint.

- b. Accept the default destination folder for the installation files, or click **Change** to navigate to and select a different folder. Click **Next**.
- c. Enter the fully qualified domain name (FQDN) for the PatientSecure Web Services (PSWS) application server.
- d. Enter the port to use. The default is **7002**.
- e. To verify the connection to the PSWS, click **Test Connection**.
- f. Click **Next**.
- g. On the Setup Type page, do the following:
  - To install only the default components (PatientSecure Client, PatientSecure Client Hub and PatientSecure Client Gateway), click **Typical** and **Next**.
  - To choose from groups of features to install, click **Custom** and **Next**. The Custom Setup page presents you with pre-defined groups of features to be installed.

Select the group of features to be installed, based on your integration.

Integration	Select the group of features
PatientSecure and Imprivata OneSign APG integrations, or other custom integrations	<ul style="list-style-type: none"> <li>◦ Client, Hub, Gateway, Toolbar</li> </ul> <p><b>NOTE:</b> This group of features will not display the Virtual Channel dialog, even when installed on a Citrix server.</p>
Epic Integration	<ul style="list-style-type: none"> <li>◦ Client, Hub, Gateway, Epic integration</li> </ul>
Epic Integration as a published application on the endpoint.	<ul style="list-style-type: none"> <li>◦ On the server - install Epic integration.</li> <li>◦ On the endpoint - install Client, Hub, Gateway.</li> </ul>
Epic Kiosks	<ul style="list-style-type: none"> <li>◦ Epic Kiosk, Hub</li> </ul>
Toolbar as a published application on the endpoint	<ul style="list-style-type: none"> <li>◦ On the server - install Toolbar.</li> <li>◦ On the endpoint - install Client, Hub, Gateway.</li> </ul>
Windows Kiosk API v.2 integration	<ul style="list-style-type: none"> <li>◦ Hub, Gateway</li> </ul>
Epic Integration or Toolbar as a Citrix published application on the endpoint with PatientSecure Virtual Channel communication.  For more information on integrating with Imprivata Virtual Channel, see <a href="#">Configure PatientSecure Virtual Channel</a> .	<ul style="list-style-type: none"> <li>◦ On the server - install either Epic Integration or Toolbar.</li> <li>◦ On the endpoint - install Client, Hub, Gateway</li> </ul>

5. Click **Next**.
6. If you selected a group of features that includes the PatientSecure Toolbar, on the Toolbar Theme page, select the **Toolbar is running as a published application** checkbox to allow the Toolbar

application to run as a published application. Click **Next**.

- a. On the Toolbar Buttons page, select the toolbar settings that will be available:
  - Show Authenticate Button on Toolbar
  - Show Enroll Button on Toolbar
  - or both

7. *For PatientSecure Virtual Channel communication support on Citrix only.* For more information on this integration, see [Configure PatientSecure Virtual Channel](#).

If your PatientSecure endpoints will integrate with Imprivata Virtual Channel communication in Citrix, and you selected the group of features for PatientSecure Toolbar, or Epic Integration, set the following:

- a. On the Toolbar Theme page, select the **Toolbar is running as a published application** checkbox to allow the Toolbar application to run as a published application. Click **Next**.
- b. On the Toolbar Buttons page, select the toolbar settings that will be available:
  - i. Show Authenticate Button on Toolbar
  - ii. Show Enroll Button on Toolbar
  - iii. or both

Click **Next**.

- c. On the Virtual Channel page, the PatientSecure installer detects Citrix on the server. To use Virtual Channel communication, select the **Use Virtual Channel** checkbox.

The default is not selected. If Citrix is not detected on the server, this page is not displayed.

Click **Next**.

8. To review log entries for the installation when you exit the Installer, select **Show the Windows Installer log**.

You can also install the Imprivata PatientSecure Client from the [command line](#) in silent mode.

## PatientSecure Client - Command Line

You can also install the Imprivata PatientSecure client from the command line



**NOTE:**

The command line installation does not check for software prerequisites.

For more information on software prerequisites, see the [Imprivata Environment Reference portal](#).

# Syntax

```
ImprivataPatientSecureWebClient.exe /s /v"/QN [/L*V \"<logFilePath>\"] PSWS_
ADDRESS=<pwsFQDN> [PSWS_PORT=<pwsServerPort>]
[INSTALLDIR=<InstallationDirectory>] [COMBO=<1-8>]] [TOOLBAR_UI_THEME=
[XenApp|Default]] [SHOWAUTHENTICATE=[True|False]] [SHOWENROLL=[True|False]]
[TOOLBARMODE=[OneSign|D11]] [TOOLBAR_CUSTOM_DLL=[BJS|MMS|SMH|Wise]] [USE_VIRTUAL_
CHANNEL=[True|False]] [VIRTUAL_CHANNEL_PROTOCOL=[Unknown|Citrix|VMware]]"
```





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

Installation may take up to 30 seconds to begin.


## Parameters

The following table describes the command-line parameters:

Parameter	Required	Function
/s	Yes	Runs the installer in silent mode.
/v	Yes	Passes command-line options through to Msiexec.exe, which installs the embedded .MSI file. <div> <b>NOTE:</b> There is no space between /v and the first double quote, and the parameters being passed by /v that need to be quoted also need to have their double quotes escaped.</div>
/QN	No	Runs the embedded MSI in quiet mode with no UI. <div> <b>TIP:</b> If /s is used, you must use /QN to run the embedded MSI in silent mode.</div>
/L*V	Yes	Logs all output to a file and saves the log to the path specified in <logFilePath>. <div> <b>NOTE:</b> 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.</div>

Parameter	Required	Function
PSWS_ADDRESS	Yes	<p>The fully qualified domain name (FQDN) of the Imprivata PatientSecure Web Services application server in your environment.</p> <div>  <b>NOTE:</b> The PSWS_ADDRESS variable should not include an https:// prefix. </div>
PSWS_PORT	No	<p>The communication port for the Imprivata PatientSecure Web Services server.</p> <p>The default port is 7002.</p>
INSTALLDIR	No	<p>The base location for installing PatientSecure Client, PatientSecure Client Hub, PatientSecure Client Gateway, and PatientSecure Toolbar. If not defined, defaults to the following location:</p> <ul style="list-style-type: none"> <li>• <b>32-bit:</b> "C:\Program Files\Imprivata\PatientSecure\"</li> <li>• <b>64-bit:</b> "C:\Program Files (x86)\Imprivata\PatientSecure\"</li> </ul> <div>  <b>NOTE:</b> If the path contains spaces, the INSTALLDIR value may need to be quoted and the quotes escaped. </div>
<COMBO=<1-8>>	No	<p>Specifies one of the following pre-defined combinations of PatientSecure features to install, based on your integration. Specify an integer between 1 and 7 for the groups of features.</p> <p><b>Valid values:</b></p> <p>1 - Client, Hub, Gateway</p> <p>2 - Client, Hub, Gateway, Toolbar</p> <p><b>NOTE:</b> COMBO=2 includes the Toolbar, but should not be used if you are installing the group of features that support Citrix virtual channel communication. Use COMBO=5 or COMBO=6 for Epic Integration or Toolbar on the Citrix server in combination with USE_VIRTUAL_CHANNEL. For more information, see <a href="#">Configure PatientSecure Virtual Channel</a>.</p> <p>3 - Client, Hub, Gateway, Epic Integration (for <a href="#">Epic Integration installations</a>)</p> <p>4 - Epic Integration (for Epic Integration installations)</p> <p>5 - Epic Integration, Toolbar (for Epic Integration installations)</p> <p>6 - Toolbar</p> <p>7 - Epic Kiosk, Hub (for <a href="#">Epic Kiosk installations</a>).</p> <p>8 - Hub, Gateway (for Windows Kiosk API v.2 integration)</p>



Parameter	Required	Function
Optional Arguments		Use the following arguments for PatientSecure toolbar or Epic Integration:
SHOWAUTHENTICATE		Indicates that the Authenticate toolbar button should be visible. The default is False. Valid values: True or False.
SHOWENROLL		Indicates that the Enroll toolbar button should be visible. The default is True. Valid values: True or False.
TOOLBAR_UI_THEME		Indicates that the toolbar is being installed in a Windows (Default) or Citrix environment (XenApp). Valid values: XenApp and Default.
TOOLBARMODE		Indicates that the toolbar is being installed in a mode for integration with Imprivata OneSign Application Profile Generator (APG) or for an integration using a custom DLL. The default is OneSign. Valid values: OneSign and D11.
TOOLBAR_CUSTOM_DLL		<div>  <p><b>IMPORTANT:</b> Before using this parameter, contact your Imprivata Professional Services representative for assistance.</p> </div> <p>Sets the Custom DLL the Toolbar references, when TOOLBARMODE is set to D11.</p> <p>Only valid if the Toolbar is being installed <b>and</b> TOOLBARMODE is set to 'D11'</p> <p>The default is BJS.</p> <p>Valid values: BJS, MMS, SMH, and Wise.</p>
USE_VIRTUAL_CHANNEL		Causes the Toolbar and Epic Integration components to use Imprivata Virtual Channel as the means of communication. Only valid if Citrix is detected on the server. For more information, see <a href="#">Configure PatientSecure Virtual Channel</a> The default is False. Valid values: True, False.

Parameter	Required	Function
VIRTUAL_CHANNEL_PROTOCOL		<ul style="list-style-type: none"> <li>Indicates to the Toolbar which Virtual Channel protocol to use.</li> <li>Has no effect when used with other PatientSecure features.</li> <li>This parameter is set automatically by the installer. <ul style="list-style-type: none"> <li>The default is Unknown.</li> <li>If Citrix is detected on the target machine, this parameter is set to Citrix.</li> <li>If VMware is detected on the target machine, this parameter is set to VMware.</li> <li>If both Citrix and VMware are detected on the target machine, the installer will favor VMware.</li> </ul> </li> </ul> <p>The only scenario where VIRTUAL_CHANNEL_PROTOCOL is required is when both Citrix and VMware exist on the machine, and you prefer to use Virtual Channel for Citrix instead of VMware.</p> <ul style="list-style-type: none"> <li>Valid values: Unknown, Citrix, VMware</li> </ul>

## Examples



### IMPORTANT:

In your script, the command-line parameters must be typed in a single line.

### *Epic 2018 Integration on 64-bit*

```
ImprivataPatientSecureWebClient.exe /s /v"/QN /L*V
"C:\myInstallerLogs\PsiInstallLog.txt\" PSWS_ADDRESS=myserver.example.com PSWS_
PORT=7002 INSTALLDIR="C:\Program Files (x86)\Imprivata\" COMBO=3"
```

### *Epic Kiosk 2018 on 64-bit endpoint*

```
ImprivataPatientSecureWebClient.exe /s /v"/QN /L*V
"C:\myInstallerLogs\PsiInstallLog.txt\" PSWS_ADDRESS=myserver.example.com PSWS_
PORT=7002 INSTALLDIR="C:\Program Files (x86)\Imprivata\" COMBO=7"
```

## Upgrade the Client from the Command Line

To upgrade the PatientSecure clients from the command line:

```
ImprivataPatientSecureWebClient.exe /s /v"/QN /L*V "<logFilePath>"
```

**IMPORTANT:**

In your script, the command-line parameters must be typed in a single line.

## Parameters

The following table describes the command-line parameters for upgrade:

Parameter	Function
/s	Runs the installer in silent mode.
/v	Passes command-line options through to Msiexec.exe (which installs the embedded .MSI file). <div> <b>NOTE:</b> There is no space between /v and the first double quote, and the parameters being passed by /v that need to be quoted also need to have their double quotes escaped.</div>
/QN	Runs the embedded MSI in quiet mode with no UI. <div> <b>TIP:</b> To run PatientSecureClientSetup.exe in silent mode, you must run the embedded MSI in silent mode as well, so /QN must always be present if /s is present.</div>
/L*v	Logs all output to the log and saves the log to the path specified in <logFilePath>.
<logFilePath>	The path for the installer log file. <div> <b>NOTE:</b> The path is quoted, and the quotes are escaped.</div>

## Uninstall the Client from the Command Line

The PatientSecure client installer supports standard msixexec options. For more information on these commands, run `msiexec /?`.

```
ImprivataPatientSecureWebClient.exe /s /v"/QN [/L*v \"<LogFilePath>\"] REMOVE=ALL "
```

## Mapping a Computer to a Location

Before you begin, make sure that all facilities and departments have been configured in Admin Console.

To map your computer to a facility and department using the Admin Console, use one of the following methods:

### From the Locations page:

1. In the Admin Console, go to **Settings > Locations**.
2. Select the correct **Organization**, **Facility** and **Department** for your needs.
3. In the right pane, select **Map a Machine** from the **Options** drop-down list.
4. In the dialog box, enter the machine name and click **Map Machine**.

The computer is added to the facility and department you specified.

### From the Machine Mappings page:

1. In the Admin Console, go to **Settings > Machine Mappings**.
2. To add a new machine, click **Add new machine**.
  - a. In the dialog box, click **Add names manually**.
  - b. Type a machine name.
  - c. Click **Add**.

The new machine is added to the list of machines. Unmapped machines are indicated by a flag and the status of "no location".

To add additional machines, select **Add another** and type the additional machine name.

3. To map an unmapped machine, select the unmapped machine and click **Map selected**.
  - a. In the dialog box, select the Organization, Facility and Department from the drop-down lists and click **OK**.

## Changing a Client Machine's Mapping

You can switch a machine mapping from one department in your location to another.



**NOTE:** A machine can be mapped to only one department. Adding a machine to a new location removes it from its former department.

To change a client machine's mapping:

1. From the Admin Console menu, select **Settings > Locations**.

The Locations page opens.

2. Select the organization, facility, and department where you will map the machine.
3. From the Options drop-down list, click **Map a Machine**.
4. Enter the machine name in the field.
5. Click **Map Machine**.

You see a message that the machine is already mapped to another department.

6. To map the machine to a new department, click **Continue Machine Mapping**.

You see a message that the machine was mapped successfully.

7. Restart the client machine's Gateway, Hub, and Client services for the new location to take effect. Alternately, reboot the client machine.

# Configuring Epic Integration

This document describes how to install the Imprivata PatientSecure® client-side components for Epic Integration.

## Before You Begin

Before you begin, have the following information ready:

- **PatientSecure:**

- 



**NOTE:** Check with your Imprivata PatientSecure representative to make sure that the server components are installed and that Admin Console is installed and configured.

- **Epic environment.** Ensure that the Epic environment is already configured.

- **Identifier.** Take note of the identifier passed in the HL7 message. You will use this later when configuring patient identifiers in the Admin Console.
- [Create System Category Items](#)
- [Create EOA Record and Link to it from System Definition](#)
- **Epic LWS records.** Ensure that the local workstation (LWS) records for the kiosks already exist in the Epic database.
- **Epic Configuration ProglID.** Take note of the ProglIDs in the Epic database. For more information, see [Enabling Palm Scanner for Specific Workstations](#).
- **External Authentication Setting ID Type.** Confirm that the External Authentication Setting ID Type is set to **MRN**. This is the **ID type used** field in Epic.  
When Epic passes the identifiers to PatientSecure, they must be in the correct order. The **MRN** must be the first part passed to PatientSecure.
- Set up the Authentication buttons on the Epic screens.

## Create System Category Items

To add the Imprivata Login Devices as Category Items in the EOA database:

1. Log in to Hyperspace as an administrator.
2. Go to the **Epic** menu and select **Admin > General Admin > Item Editor**.
3. On the Item Editor, select the **Service Configurations [EOA]** database.
4. Type **700** in the **Item** field.
5. Click **Edit Categories**. The Category List Maintenance page for EOA 700 opens.
6. Type a **Category ID** in the **Edit Category** section.  
The number must be greater than 10,000 and not already in use by another Login Device.

For example, type 10006. The Release Range shown (0 to 10000) is reserved for Epic use only.

7. Select **PalmScanner** in the **Title** field.
8. Type **PSEpicIntegration.EpicIntegrator** in the **Login Device ProgID** field.

This allows the Epic enroll and authentication buttons to reference the PatientSecure Integration component on the Citrix server and local machine (in a thick client installation) in order to directly communicate with the local machine.



**NOTE:** The ProgID is not case-sensitive.

9. Click **Accept**.

The new login devices is shown in the **Category List**.

## Create the EOA Record and Link to it from System Definition

You only need to complete this task once for your Epic and Imprivata integration for all Patient Authentication.

To create the EOA record and create a link to it from the system definition:

1. Type **d ^E** at the **Cache** prompt for the Epic environment you want to configure, then press **Enter**.  
Note the space after the "d".
2. On the **Chronicles** screen, type **EOA** for the **Database Initials** to edit the External Servers database.
3. On the **Chronicles** Main Menu, select **Enter Data**, then select **Create Configuration**.
4. On the **Open Configuration** page, tpe a **Configuration ID**, then press **Enter**.  
The Configuration ID number must be greater than 99,999 and not already used for another EOA record. This Configuration ID is not the same one you created for the Category ID in the previous section. The range shown (1 to 99999) is the range reserved for Epic use only.
5. Type **Imprivata** for the **CONFIG NAME**, then click **Enter**.
6. Type **t** (today) for the **CONTACT DATE**, then click **Enter**.
7. On the **Service Configuration** page, type **Authentication** for **Config Type**, then press **Enter**.  
Chronicles completes the Authentication Device Settings.
8. Press the **Page Down** key to return to the page that requests the Config ID.
9. Return to a Cache prompt, then type **d ^%ZeUSTBL**. (Note the space after the "d".) The system definition utility opens.
10. Select **Hyperspace**.
11. On the **Hyperspace Settings** page, select **Miscellaneous Security Settings**.
12. On the **Miscellaneous Security Settings** page, select **Authentication Configuration Record**.
13. On the **Authentication Configuration Record** page for Configuration, type **Palm Scanner**.

# Enable Palm Scanner for Specific Workstations

To enable the Palm Scanner at the Workstation level:



**NOTE:** The following instructions assume that the local workstation (LWS) records already exist in the Epic database.

1. Log in to Hyperspace as an administrator.
2. Click **Epic**, then select **Admin > Access Management > Authentication Administration**.
3. Do one of the following:
  - If Imprivata is the Active authentication record, click **Accept**.
  - If Imprivata is not the Active authentication record, select **Other** and then select **Imprivata**.The Authentication Administration page opens.
4. Click **Add/Edit Workstation** and search for the specific workstation for which you want to enable the Connector, and then select it from the list.
5. Click **Add/Edit Context** for the selected workstation, and set the **Context** to '**Kiosk Identification (1010)**'.
6. Set the **Primary Device** to **Palm Scanner Welcome**.

For more information, search your Epic documentation for "external patient authentication."

## Installing the Imprivata PatientSecure Client

Install the Imprivata PatientSecure client with the appropriate pre-defined group of PatientSecure features for your Epic environment:

- During setup, select the **Client, Hub, Gateway, Epic integration** group of features.

For Epic Integration as a published application on the endpoint:

- On the server, install the **Epic Integration** group of features.
- On the endpoint, install the **Client, Hub, Gateway** group of features.

For more information on the pre-defined groups of features, see [Install the Imprivata PatientSecure Client](#).

## Button Placement in Epic

This section provides recommendations for placing buttons in Epic.

- **Look up window.** Authenticate button in lower left corner. Used in multiple workflows.
- **Patient station.** Enroll and Authentication buttons on the toolbar.
- **Appointment desk.** Enroll and Authentication buttons on the toolbar.
- **ED arrival.** Enroll and Authentication buttons on the toolbar.

- **DAR.**
  - Enroll and Authentication buttons on the toolbar.
  - Include Enroll and Authentication options from the right-click context menu that appears when you select the patient from the DAR.

## Configure Patient Identifiers in PatientSecure

Configure the external system and patient identifiers with the appropriate information for your Epic Integration system.

For more information, see "Adding a System" and "Adding Patient Identifiers" in the PatientSecure Admin Console online help.

## Troubleshooting

### User Can Only Authenticate Once

#### Symptom

A User can only authenticate one time in Epic; on the second attempt, nothing happens.

#### Reason

This is a known issue in Epic.

#### Solution

- Back out of the patient record, re-enter the record and authenticate.

### Epic Attempts to Authenticate Patients Below the Minimum Age

#### Symptom

Epic attempts to authenticate a patient that is younger than the minimum age specified in the PatientSecure Minimum Age Limit setting.

#### Solution


- Manually cancel the Authentication window.

## Epic Integration Settings

The Epic integration settings configure your Epic installation. If you have Epic Kiosk installed on your client machines, see [Epic Kiosk](#).

1. Scroll down the page and click the **Epic Integration** heading to expand it.
2. Review the Epic Integration settings and make changes, as needed.



Item	Description
<b>Force Request DOB</b>	Specify whether or not Epic should prompt the registrar to enter a patient Date of Birth (DOB) during authentication. The default setting is <b>OFF</b> .
<b>Force Request ID</b>	The default setting is <b>ON</b> . For Epic Integration: Epic 2012 installations, select <b>OFF</b> ; Epic 2014 and later installations, select <b>ON</b> .
<b>Patient Identifier Name</b>	Specify the name for the patient identifier used with Epic Integration and Epic Kiosk. The default setting is <b>EPICMRN</b> . <div>  <b>NOTE:</b> Epic Integration and Epic Kiosk support only a single patient identifier. A department or facility set up with multiple patient identifiers would not work with Epic. </div>

3. To clear all the changes and start over with the latest saved settings, click **Reset**.
4. Click **Save**.
5. To change an individual setting to its default, click **Reset to default** next to the setting name. The setting will be reset and saved.

# Epic Kiosk Configuration

This document describes how to install the Imprivata PatientSecure® client-side components for Epic Kiosk.

## Before You Begin

Before you begin, have the following information ready:

- **PatientSecure:**
  - **Directory path(s)** where you will install the pre-defined group of features for Epic Kiosk.



**NOTE:** Check with your Imprivata PatientSecure representative to make sure that the server components are installed and that Admin Console is installed and configured.

- ◦ **Epic environment.** Ensure that the Epic environment is already configured.
  - **Epic LWS records.** Ensure that the local workstation (LWS) records for the kiosks and registrar endpoints already exist in the Epic database.
  - **Epic Configuration ProglID.** Take note of the ProglIDs for the kiosks in the Epic database. For more information, see [Enabling Palm Scanner for Specific Workstations](#).



**BEST PRACTICE:**

Take note of the machine names where the Imprivata PatientSecure client is installed, so you can map each machine to your location settings.

## Installing the Fujitsu Drivers

### Install the Drivers

To install Fujitsu F-Pro extended drivers with InstallShield:

1. Disconnect the palm scanner from the computer.
2. Download the PatientSecure software .zip file from the Imprivata PatientSecure downloads page.
3. Extract the .zip and navigate to the F-Pro Sensor drivers directory.
4. Run PSSD\_32.msi or PSSD\_64.msi, according to your kiosk's platform.
5. Follow the instructions in the installer.
6. When the installation is completed, click **Finish**.
7. Click **Yes** to restart the computer.

Repeat this procedure for each kiosk using a scanner.

# Install the Drivers from the Command Line

To install the Fujitsu F-Pro drivers from the command line:

1. In the extracted .zip directory, navigate to the directory `F-Pro Sensor drivers`.
2. From the command line, run the commands, according to your kiosk's platform:

```
msiexec /i <pathToFujitsuDrivers>\PSSD_64.msi /qn /forcerestart
```

```
msiexec /i <pathToFujitsuDrivers>\PSSD_32.msi /qn /forcerestart
```

where `<pathToFujitsuDrivers>` is the path to the Fujitsu F-Pro drivers.

## Epic Welcome or PatientWorks Kiosks

If you are installing Imprivata PatientSecure on Epic Welcome or PatientWorks kiosks:

1. Uninstall the drivers from the kiosk.
2. Install the Fujitsu F-Pro drivers.
3. Install the Imprivata PatientSecure client software with the kiosk.

## Installing the Imprivata PatientSecure Client

Install the Imprivata PatientSecure client with the appropriate pre-defined group of features for your Epic Kiosk environment.

- During setup, select the **Epic Kiosk, Hub** group of features.

For more information, see [Install the Imprivata PatientSecure Client](#).

## Mapping a Computer to a Location

Before you begin, make sure that all facilities and departments have been configured in Admin Console.

To map your computer to a facility and department using the Admin Console, use one of the following methods:

### From the Locations page:

1. In the Admin Console, go to **Settings > Locations**.
2. Select the correct **Organization**, **Facility** and **Department** for your needs.
3. In the right pane, select **Map a Machine** from the **Options** drop-down list.
4. In the dialog box, enter the machine name and click **Map Machine**.

The computer is added to the facility and department you specified.

### From the Machine Mappings page:

1. In the Admin Console, go to **Settings > Machine Mappings**.
2. To add a new machine, click **Add new machine**.
  - a. In the dialog box, click **Add names manually**.
  - b. Type a machine name.
  - c. Click **Add**.

The new machine is added to the list of machines. Unmapped machines are indicated by a flag and the status of "no location".

To add additional machines, select **Add another** and type the additional machine name.
3. To map an unmapped machine, select the unmapped machine and click **Map selected**.
  - a. In the dialog box, select the Organization, Facility and Department from the drop-down lists and click **OK**.

## Configure an Authentication Device For Epic 2017 and Epic 2018

To configure an authentication device in Epic 2017 or Epic 2018:

1. In Chronicles, access the EOG master file.
2. Go to **Enter Data > Create/Edit Device**.
3. Type a new ID of **10000** or greater. You can also enter an asterisk (\*) to select the next available open ID.

Chronicles prompts you to create a new device.
4. Type **y**. The **RECORD ID** field displays the ID.
5. (Optional) If necessary, you can edit the ID value.
6. In the **RECORD NAME** field, type **Palm Scanner Welcome**.
7. On the General Settings screen, complete the following fields:
  - **Description**: This is an optional value.
  - **Platform**: Select the **Desktop platform**.
  - **ProgID**: Type **PSEpicWelcomeIntegration.EpicWelcomeIntegrator**
  - **Device icon path**: This is an optional value.
8. Enter the record and exit Chronicle.

## For Epic 2015 IU2

To configure an authentication device in Epic 2015 IU2:

1. In Chronicles, access the EOG master file.
2. Go to **Enter Data > Create/Edit Device**.

3. Type a new ID of **10000** or greater. You can also enter an asterisk (\*) to select the next available open ID.
4. On the General Settings screen, fill out the following fields:
  - **Description:** Type **Palm Scanner Welcome**.
  - **Platform:** Select the **Desktop platform**.
5. On the Desktop Settings screen, type the following Progid:  
**PSEpicWelcomeIntegration.EpicWelcomeIntegrator**
6. Exit the record and exit Chronicles.

## Create the Epic Configuration Progid

Take note of the Epic Configuration Progid that corresponds to this kiosk.

**For example:**

A second Login Device will need to be created, with a progid of 'PSEpicWelcomeIntegration.EpicWelcomeIntegrator'. Depending on what the login device for palm scanning was named, you will want to add 'Welcome' to the title. 'PalmScannerWelcome'. Once that is completed the login device will need to be added to the kiosk at the LWS level. Set the Context 'Kiosk Identification(1010)'.

## Enabling Palm Scanner for Specific Workstations



**NOTE:** The following instructions assume that the local workstation (LWS) records already exist in the Epic database.

To enable the Palm Scanner at the Workstation level:

1. Log in to Hyperspace as an administrator.
2. Click **Epic**, then select **Admin > Access Management > Authentication Administration**.
3. Do one of the following:
  - If Imprivata is the Active authentication record, click **Accept**.
  - If Imprivata is not the Active authentication record, select **Other** and then select **Imprivata**.The Authentication Administration page opens.
4. Click **Add/Edit Workstation** and search for the specific workstation for which you want to enable the Connector, and then select it from the list.
5. Click **Add/Edit Context** for the selected workstation and set the **Context** to '**Kiosk Identification (1010)**'.
6. Set the **Primary Device** to **Palm Scanner Welcome**.

## Turn Off Epic Kiosk Photo Capture

To turn off photo capture for Epic Kiosk:

1. Log in to the Admin Console.
2. From the **Settings** menu, select **Client Settings**.  
The Client Settings page opens.
3. Expand the **Epic Kiosk** section.
4. Set the **Capture Picture** setting to **OFF**.
5. Click **Save**.

## Configure the PatientSecure Kiosk Screens

You may need to modify the PatientSecure authentication and verification windows to better resemble the current kiosk screens in use by the client.

For more information, see Epic Kiosk settings in the Admin Console online help.

## Troubleshooting

### Error Connecting to Device Hub

#### Symptom

The kiosk displays an error: "Error Connecting to Device Hub".


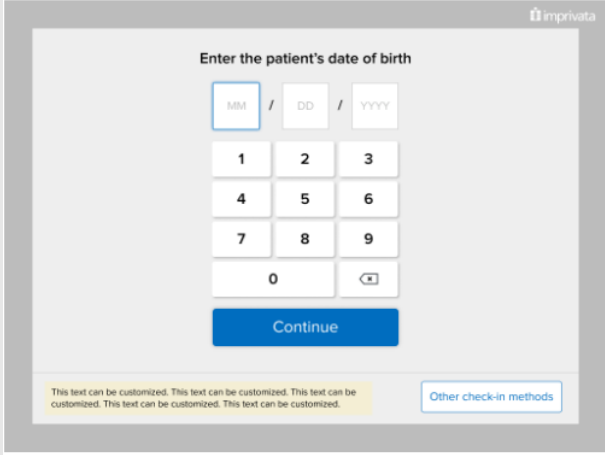
#### Solution


1. Verify the following items:
  - You installed the extended Fujitsu drivers on the device.
  - The machine is mapped correctly in Admin Console for the Production environment.
  - PatientSecure was not installed on this machine before installing the PatientSecure Kiosk.  
If the Control Panel displays PatientSecure as installed, uninstall all components and start from the beginning.
2. On the device, navigate to Services and restart the **PatientSecure Hub Service**.

## Epic Kiosk Settings

The Kiosk settings configure your clients that are installed on kiosks, for example, Epic Kiosk. For other Epic settings, see [Epic Integration Settings](#).

1. Scroll down the page and click the **Epic Kiosk** heading to expand it.
2. Review the Kiosk settings and make changes, as needed.

Item	Description
<b>Capture Picture</b>	<p>Enables patient photos to be taken during enrollment or authentication. The default setting is <b>OFF</b>.</p> <div>  <p><b>NOTE:</b> Photo captures include the date when the photo was taken. This date reflects the client system date, which may not conform to the Time Zone setting.</p> </div>
<b>Allow patients to close out of PatientSecure from the Kiosk</b>	<p>Enables the ability to display a customized message on the kiosk to guide patients to use another check-in method.</p> <p>This message can be displayed in all languages currently supported by the kiosk and will be displayed next to the <b>Other check-in methods</b> button.</p> <p>The default setting is <b>OFF</b>. Enabling the setting displays the language text entry fields below.</p> 
<b>English</b>	<p>Enter the English text of the message to be displayed next to the <b>Other check-in methods</b> button.</p> <p>200 character limit.</p>
<b>Spanish</b>	<p>Enter the Spanish text of the message to be displayed next to the <b>Other check-in methods</b> button.</p> <p>200 character limit.</p>
<b>Polish</b>	<p>Enter the Polish text of the message to be displayed next to the <b>Other check-in methods</b> button.</p> <p>200 character limit.</p>
<b>Russian</b>	<p>Enter the Russian text of the message to be displayed next to the <b>Other check-in methods</b> button.</p> <p>170 character limit.</p>

Item	Description
<b>Chinese (Traditional)</b>	Enter the Chinese text of the message to be displayed next to the <b>Other check-in methods</b> button. 100 character limit.
<b>Help Palm Image File Name</b>	Upload a PNG image file with correct hand placement for patients using the kiosk. The default setting is <b>HelpPalmImage.png</b> .
<b>Maximum Age for Kiosk</b>	Set the maximum age at which a patient may use the kiosk to enroll or authenticate in PatientSecure. The default maximum age is <b>120</b> . <div> <b>TIP:</b> This setting also helps to prevent user input errors.</div>
<b>Minimum Age for Kiosk</b>	Set the minimum age at which a patient may use the kiosk to enroll or authenticate in PatientSecure. This limit should be set according to the individual hospital policies for the minimum age for enrolling a child's biometric information. If the child's age is below the minimum age limit, the ongoing workflow will be prevented. The default minimum age is <b>7</b> . Valid values: <b>5</b> through <b>18</b> .
<b>Request ID</b>	The default setting is <b>OFF</b> . For Epic 2014 and later installations, select <b>ON</b> . For Epic 2012 installations, select <b>OFF</b> .
<b>Seconds Before Timeout</b>	Set the number of seconds that a patient interaction on the kiosk can be idle before timing out (without warning). The default setting is <b>60</b> .
<b>Seconds Between Warning and Timeout</b>	Set the number of seconds that a patient interaction on the kiosk can be idle before the kiosk actually times out after the timeout warning is displayed. The default setting is <b>30</b> .

3. To clear all the changes and start over with the latest saved settings, click **Reset**.
4. Click **Save**.



# Configure PatientSecure Virtual Channel

---

Imprivata PatientSecure uses Virtual Channels to communicate between the Virtual Channel Driver (VCD) module residing on the client machine and the modules residing within the remote session on the server machine. After the initial connection is established both client and server sides can utilize request/response and one-way communication messages.

PatientSecure uses virtual channel communication to allow remote session PatientSecure Toolbar or Epic Integration applications to communicate to the PatientSecure Gateway on the client desktop.

## Virtual Channel Support

- Supports Citrix environments where you want to use Imprivata Virtual channel communications for PatientSecure Toolbar or Epic Integration as published applications on endpoints.
- PatientSecure supports virtual channels over the ICA protocol on the Windows platform.
- PatientSecure does not support launching the published Epic app multiple times from the same user on the same Citrix session.

## Before You Begin

Before you begin, consider the following items:

### Review System Requirements

Review the PatientSecure system requirements and Citrix supported components on the [Imprivata Environment Reference](#) portal.

## Enable PatientSecure Virtual Channel

**Applies to Citrix Virtual Apps and Desktops 7 2109 or later.**

In Citrix Virtual Apps and Desktops 7 2109 and later, the Virtual channel allow list policy setting is enabled by default. This causes the PatientSecure virtual channel to fail. For more information, see the [Citrix documentation](#).

The Virtual channel allow list policy setting enables the use of an allow list that specifies which virtual channels are allowed to be opened in an ICA session. There are two ways to allow the Imprivata virtual channel to run in Citrix 7 2109 or later:

- When disabled:
  - All virtual channels (including PatientSecure virtual channel) are allowed.
  - This is not recommended
- When enabled:
  - Only Citrix virtual channels are allowed
  - The PatientSecure virtual channel must be added to this allow list.

To add a virtual channel to the list:

- Enter the virtual channel name followed by a comma, and then the path to the process that accesses the virtual channel.
- You can add additional executable paths, separating the paths by commas.
- **For Toolbar, add:**

IMP3388,C:\Program Files  
(x86)\Imprivata\PatientSecure\Toolbar\ImprivataPatientSecureToolbar.exe

- **For Epic Integration, add:**

IMP3388,*pathToEpicInstallation*

where

*pathToEpicInstallation* is the installation path to Epic, including the Epic executable (.exe).

## Prerequisites

- A supported release of Citrix Virtual Apps and Desktops must be running on the Citrix server before installing the PatientSecure client software.
- A supported release of Citrix Workspace App must be installed on the endpoint before the PatientSecure client.

## Install Software Dependencies

- Install the required software dependencies on the Citrix server and endpoints.
- Ensure that the necessary client communication ports are open.

## Obtain the PatientSecure Client Installation Package

Download the client installation package provided by your Imprivata PatientSecure representative or from the PatientSecure software download package available on the [Imprivata Support and Learning Center](#).

## Install Epic Integration/Toolbar and Virtual Channel on the Citrix Server

On the Citrix server, install either the Epic Integration or Toolbar group of features and select Virtual Channel:

1. Extract the software package and run `ImprivataPatientSecureWebClient.exe`.
2. Click **Next**.
3. Complete the wizard, including the following steps:
  - a. If there are missing software prerequisites, such as Microsoft Visual C++ redistributables, the wizard prompts for you to install them.

- b. Accept the default destination folder for the installation files, or click **Change** to navigate to and select a different folder. Click **Next**.
- c. Enter the fully qualified domain name (FQDN) for the PatientSecure Web Services (PSWS) application server.
- d. Enter the port to use. The default is **7002**.
- e. To verify the connection to the PSWS, click **Test Connection**. Click **Next**.
- f. On the Setup Type page, to choose from groups of features to install, click **Custom** and **Next**. The Custom Setup page presents you with pre-defined groups of features to be installed. install either the **Epic Integration** or **Toolbar** group of features.
- g. If you selected a group of features that includes the PatientSecure Toolbar, on the Toolbar Theme page, select the **Toolbar is running as a published application** checkbox to allow the Toolbar application to run as a published application. Click **Next**.
  - i. On the Toolbar Buttons page, select the toolbar settings that will be available:
    - Show Authenticate Button on Toolbar
    - Show Enroll Button on Toolbar
    - or both
- h. On the Virtual Channel page, the PatientSecure installer detects Citrix on the server. To use Virtual Channel communication, select the **Use Virtual Channel** checkbox.
- i. The default is not selected. If Citrix is not detected on the server, this page is not displayed. Click **Next**.
- j. To review log entries for the installation when you exit the Installer, select **Show the Windows Installer log**.

## Install PatientSecure Client on Endpoints

On the endpoints, install the Client, Hub, Gateway group of features:

1. Extract the software package and run `ImprivataPatientSecureWebClient.exe`.
2. Click **Next**.
3. Complete the wizard, including the following steps:
  - a. If there are missing software prerequisites, such as Microsoft Visual C++ redistributables, the wizard prompts for you to install them. In this case, the PatientSecure client installation will require a reboot of the endpoint.
  - b. Accept the default destination folder for the installation files, or click **Change** to navigate to and select a different folder. Click **Next**.
  - c. Enter the fully qualified domain name (FQDN) for the PatientSecure Web Services (PSWS) application server.
  - d. Enter the port to use. The default is **7002**.
  - e. To verify the connection to the PSWS, click **Test Connection**.

- f. Click **Next**.
- g. On the Setup Type page, to install only the default components (PatientSecure Client, PatientSecure Client Hub and PatientSecure Client Gateway), click **Typical** and **Next**.
- h. Click **Next**.
- i. To review log entries for the installation when you exit the Installer, select **Show the Windows Installer log**.

## Install from the Command Line

Alternately, you can install the PatientSecure Client from the command line with specific switches for Virtual Channel. For more information, see [PatientSecure Client - Command Line](#).