

imprivata® Product Documentation

Imprivata PatientSecure Server Installation Guide

Imprivata PatientSecure® 6.5

Table of Contents

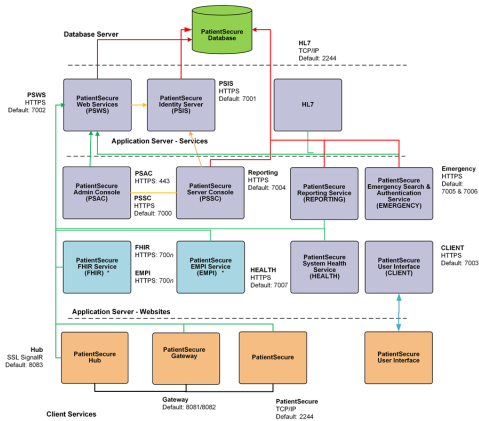
Services and Communications	3
Server Components	3
Install the Imprivata PatientSecure Server Console	4
Before You Begin	4
Review the PatientSecure Server Requirements	4
Install Software Dependencies	4
Install the Roles and Features on Application Servers	4
Set Up a Certificate Authority for Generated Certificates	4
Set Up Active Directory Groups for PatientSecure	4
Installation Tasks	4
Install the PatientSecure Server Console	5
Create an Empty Database by SQL Script	6
Install PatientSecure Server Console from the Command Line	7
Syntax	7
Parameters	7
Set Up a New Installation	9
Adding a Server	14
PatientSecure Services Installation Order	14
Adding a Server	15
Viewing a server	18
Editing a Server	18
Server Info	18
SSL Info	18
Add a Certificate to the Local Certificate Store	18
Change the Server Certificate	19
Services	19
Change Source Settings	19
View Installation Logs for Services	20
Uninstall an Installed Service	20
Reinstall an Installed Service	20
Adding an Active Directory Group	21
Editing the Active Directory Account Settings	22
Deleting a Server	22
Delete the Server from the PatientSecure Server Console	22
Delete Remnant Files on Uninstalled Servers	23
Replace the Server Certificate	23
Before You Begin	23
Replacing the server certificate using a .PFX certificate (recommended)	23
Replacing the server certificate using a .CER certificate	24
Deleting the Active Directory Account Settings	24
PatientSecure Server Console	26

Services and Communications

Server Components

The following diagram illustrates the data flow between the various Imprivata PatientSecure server components, including communication protocols and default port information.

For more information, see the [system requirements](#).



* Denotes optional service. Port number depends on next available in 7000 range.

Install the Imprivata PatientSecure Server Console

Your Imprivata PatientSecure installation begins with the PatientSecure Server Console, which installs and manages the service components that support Imprivata PatientSecure.

Before You Begin

Review the PatientSecure Server Requirements

Review the system requirements for the PatientSecure database server and application servers.

For more information, see the PatientSecure system requirements on the [Imprivata Environment Reference portal](#).

Install Software Dependencies

Install the required software on the PatientSecure database server and application servers.

For more information, see the PatientSecure system requirements on the [Imprivata Environment Reference portal](#).

Install the Roles and Features on Application Servers

Enable the appropriate server Roles and Features on the PatientSecure application servers.

For more information, see the PatientSecure system requirements on the [Imprivata Environment Reference portal](#).

Set Up a Certificate Authority for Generated Certificates

If you plan to use a certificate that you supply, set up a certificate authority (CA) for the generated certificates.

For more information, see the Microsoft TechNet Group Policy instructions for your Windows Server version.

Set Up Active Directory Groups for PatientSecure

Identify the Active Directory server for your environment, and set up Active Directory groups for PatientSecure Owners, Administrators, and Users.

Installation Tasks

To install the PatientSecure software, perform the following tasks, in order:

1. Install the [PatientSecure Server Console](#).
2. Determine the PatientSecure database installation method for your environment:
 - **Create an empty database.** As a user with sysadmin privileges, run a SQL script that creates an empty database for PatientSecure and populates the database with the PatientSecure service account.
For more information, see [Create an Empty Database by SQL Script](#).

- **Installation program creates the database.** Create the database with the PatientSecure installation program.

This scenario allows the PatientSecure installation program to create the PatientSecure database and service account.

For more information, see Step 6 of [Set Up a New Installation](#).

3. Use the PatientSecure Server Console to set up the rest of the PatientSecure application services. See [Set Up a New Installation](#).

Install the PatientSecure Server Console

Install the PatientSecure Server Console on the Imprivata PatientSecure server.



NOTE: You can also install the Imprivata PatientSecure Server Console [from the command line](#).

To install the PatientSecure Server Console:

1. Download the PSI package provided by your Imprivata PatientSecure representative.
2. Click `PatientSecureServerSetup.exe`, and then click **Run**.

The InstallShield Wizard opens.

3. Follow the wizard prompts to install the PatientSecure Server Console.
4. The wizard prompts to select the environment.
 - a. To set up the environment as a Production environment, select **Production**.
 - b. To set up the environment as a test or other non-production environment, select **Non-Production**.

This setting is used in coordination with the PatientSecure Site Monitoring (PSSM) component to collect data as either a production or test environment.

5. When the installation is complete, you see a success or failure message.
 - The **Launch Imprivata PatientSecure Server Console** checkbox is selected by default, so you can continue installing Imprivata PatientSecure components when you exit the Installer.
 - To launch the Server Console later, clear the **Launch Imprivata PatientSecure Server Console** checkbox and make a note of the address provided on the screen.
 - To review log entries for the installation when you exit the Installer, select the **Show the Windows Installer log** checkbox.
6. Click **Finish**.



TIP: If you selected the **Launch Imprivata PatientSecure Server Console** checkbox and the Server Console does not launch successfully, refresh your browser.

Create an Empty Database by SQL Script



IMPORTANT:

This task only applies to the scenario where you decided to separately create an empty database for PatientSecure data in SQL Server Management Console first.

If you want the PatientSecure installation program to handle the PatientSecure database creation as part of PatientSecure component installation and setup, skip to [Set Up a New Installation](#).

The PatientSecure software provides the SQL script that creates an empty PatientSecure database with the necessary PatientSecure service user account:

- `DatabaseInstall.sql`. This file is in the following location:

```
C:\Program Files\Imprivata\PatientSecure\PatientSecure.ServiceInstaller\AppData\InstallPackages\nDb_6.3.0.zip\BlankDatabaseInstall.
```

You must unzip the package to get the SQL script.

To configure the PatientSecure database, run the SQL script:

1. Log onto the database server.
2. Log in to SQL Server Management Studio with an account that has **sysadmin** or equivalent privileges.
3. Navigate to the location where you unzipped `DatabaseInstall.sql` and open it.
4. Replace the following variables with the desired values:
 - **'@dbName'** - the database name for the PatientSecure database.
 - **'@dbUserName'** - a user name for a new service account for the PatientSecure database.



NOTE:

We recommend that you follow the naming convention of **'ImprivataPatientSecureServices_[databasename]'** for the **'@dbUserName'** variable. This allows you to have an easily-identifiable name for the PatientSecure service account.

- **'@password'** - Password for the new service account.



IMPORTANT:

- Do not modify other portions of the SQL script than the variables listed above.
- Take note of the database name, user account and password for later use.

5. Run the script.

The script creates an empty PatientSecure database with a user and login with permissions suitable for PatientSecure to run.

Install PatientSecure Server Console from the Command Line

Install the PatientSecure Server Console from the command line

Syntax

```
PatientSecureServerSetup.exe /s /v"/QN /L*V \"<path-to-log-file>\"  
INSTALLDIR=<directory-to-install-to> ISPROD=true|false"
```



IMPORTANT:

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

Parameters

The following table describes the command-line parameters:

Parameter	Function
/s	Runs the installer in silent mode.
/v	Passes command-line options through to Msiexe.exe (which installs the embedded .MSI file). <div> NOTE: There is no space between /v and the first double quote, and the parameters being passed via /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> TIP: If you want to run PatientSecureServerSetup.exe in silent mode, you'll need to run the embedded MSI in silent mode as well, so /QN should always be present if /s is present.</div>
/L*V	Logs all output to the log and saves the log to the path given. <div> NOTE: The path is quoted, and the quotes are escaped.</div>
INSTALLDIR	Identifies the location where PSI will be installed. If this is not set, it defaults to "C:\Program Files\Imprivata\PatientSecure\". <div> NOTE: If the path contains spaces, the INSTALLDIR value may need to be quoted and the quotes escaped.</div>

Parameter	Function
ISPROD	<p>Optional.</p> <p>Designates the PatientSecure environment as a production environment or a test environment, with respect to data collected by the PatientSecure Site Monitoring (PSSM) component.</p> <p>Valid values: <code>True</code> or <code>False</code>.</p>

Set Up a New Installation

The PatientSecure Server Console runs on the server over a secure SSL connection using HTTPS.

For a full list of supported browser versions, see the [supported configurations](#) or your Imprivata PatientSecure representative.



NOTE: If you plan to use a certificate that you supply, set up a certificate authority for the generated certificates. For more information, see the Microsoft TechNet Group Policy instructions for your Windows Server version. The certificate will secure only the name you enter when you create it.

To set up the new PatientSecure installation:

1. Start the PatientSecure Server Console.

The PatientSecure Server Console may start automatically after installing PatientSecure. If you chose to set up your installation at a later date, open your browser and type the URL in the address line.

- a. Select the server domain from the drop-down list.
- b. Type your user name and password and click **Log In**.

You may have a limited number of attempts to enter valid credentials. If you are locked out, contact your system administrator.


The Imprivata PatientSecure Server page displays the setup options.

2. Click **+ Set up new installation**. The Download Passphrase page opens.
3. Click **Download** to download the passphrase file to the `Downloads` directory on the local drive.
4. Copy the passphrase file (in `.PS` format) to a secure location for future use.



IMPORTANT: This passphrase allows you to restore the installation process, in case you ever need to recover or move this installation. Make sure you save this file in a safe place.

5. Click **Next**. The Set Up Database page opens.
6. Identify the server where the Imprivata PatientSecure database will reside:

Item	Description
Server Name	Enter the name (up to 50 characters) or the IP address of the database server.
Database Name	<p>Enter the name assigned to the database.</p> <p>If you created the database by SQL script, this is the database name you took note of in step 4 of Create an Empty Database by SQL Script.</p>
Database User	<p>Enter the name of the database user account with which the database will be installed.</p> <ul style="list-style-type: none"> • If you created the database by SQL script, this is the database user you took note of in step 4 of Create an Empty Database by SQL Script. • If you are creating the database now, this database user account must have the appropriate permissions to create and set up the database. <div>  <p>NOTE: Take note of the username and password for the database service user account.</p> </div>

Item	Description
Database service account	<p>The two database user accounts have the following permissions:</p> <ul style="list-style-type: none"> • SQL Database server Database user account <ul style="list-style-type: none"> ◦ Alter any DB ◦ Alter any login ◦ Connect any DB ◦ Connect SQL ◦ Create any DB ◦ Create server role ◦ Create availability group ◦ Select all user securables ◦ View any database ◦ View server state • Service user account created by PatientSecure during installation User name: ImprivataPatientSecureServices_[DB_NAME] Permissions granted to the service user at the SQL Server level: <ul style="list-style-type: none"> ◦ Connect SQL ◦ View Database State ◦ View Server State Role membership granted to the service user for the PatientSecure database: <ul style="list-style-type: none"> ◦ datareader ◦ datawriter ◦ ddladmin ◦ executor with permission to execute stored procedures against the PatientSecure database ◦ owner ◦ public For more information, see "Permissions of Fixed Database Roles (Database Engine)" on the Microsoft TechNet website.
Database Password	Type the password for the database user account.
Import Settings	(Optional) Navigate to the location where the PatientSecure export file (in .ZIP format) is stored. Click Open to upload the file.

7. Click **Next**.

The Configure Active Directory page opens.

8. Enter the Active Directory server information and specify the Active Directory groups with access permissions for PatientSecure:



NOTE: The Active Directory groups must already exist on the Active Directory server. You cannot assign a group to more than one role.

TIP: You can add individual users to your Active Directory groups through the [Location Access](#) settings in the Admin Console at any time.

Item	Description
Display Name	Enter the name (up to 50 characters) that will reference Active Directory.
Domain	Enter the domain name assigned to the Active Directory server, and then specify the port: <ul style="list-style-type: none">• If SSL is enabled, type 636.• If SSL is not enabled, type 389.
Container	Enter the container name for organization units (OU), if any.
AD Account Name	Enter the name of the user who is a domain administrator on the Active Directory.
AD Account Password	Enter the password for the user who is a domain administrator on the Active Directory.
Owners	Specify the Active Directory group(s) with users who will be assigned Owner access to Imprivata PatientSecure.
Administrators	Specify the Active Directory group(s) with users who will be assigned Administrator access to Imprivata PatientSecure.
Users	Specify the Active Directory group(s) with users who will be assigned User access to Imprivata PatientSecure.

9. Click **Next**. The Installation Type page opens.
10. Select the option that best models how you will install [Imprivata PatientSecure services](#):

Item	Description
Basic	<p>Installs the minimum set of services required for PatientSecure to run on a single application server, using an automatically generated certificate.</p> <p>The minimum set of PatientSecure services include:</p> <ul style="list-style-type: none"> • Generate Certificate/Cert Authority • Identity Server • Web Services • Admin Console • Client UI • Reporting Service • Job Scheduler • HL7 • Emergency Search & Authentication Service • System Health Service
Complete	<p>Installs the complete set of Imprivata PatientSecure services on a single application server, using an automatically generated certificate.</p> <p>Installs the set of services from the Basic option, plus PatientSecure EMPI Service and FHIR Service.</p>
Advanced	<p>Customize how PatientSecure services are installed on multiple application servers. or using an existing certificate that you select.</p>

11. Click **Next**.

- For a **Basic** or **Complete** environment:
 - a. Enter the hostname (up to 50 characters) for the Imprivata PatientSecure application server, and then click **Next**.
 - b. Enter the Windows administrator credentials (user name and password) for the Imprivata PatientSecure application server, and then click **Confirm**.

When your installation is complete, the [Imprivata PatientSecure Server Dashboard](#) opens.

The Imprivata PatientSecure services are installed on the application server.
- For an **Advanced** environment, the Imprivata PatientSecure Server Dashboard opens. You will set up the Imprivata PatientSecure services manually on one or more servers.



NOTE: Your Server Console session times out after 30 minutes of inactivity.

Adding a Server

**NOTE:**

Use the following topic as reference if you selected the [Complete](#) or [Advanced](#) option during installation. If you selected the [Basic](#) installation option, skip this topic.

Imprivata PatientSecure application servers run the following Imprivata PatientSecure services:

- PatientSecure Identity Server (PSIS)
- PatientSecure Web Services (PSWS)
- PatientSecure Admin Console (ADMIN)
- PatientSecure User Interface (CLIENT)
- PatientSecure Reporting Services (REPORT)
- PatientSecure Job Services (JOB)
- PatientSecure HL7 (HL7)
- PatientSecure System Health Service (HEALTH)
- PatientSecure EMPI Service (EMPI) - optional. Allows PatientSecure to integrate with EMPIs such as Verato MPI or IBM Initiate.
- Emergency Search & Authentication Service (EMERGENCY)
- FHIR Service (FHIR) - optional. The FHIR Service is a server component that allows PatientSecure to integrate with the FHIR APIs to allow you to search for and add a patient into the Cerner EMR.

PatientSecure Services Installation Order

You can install one or more services on a single Imprivata PatientSecure application server or on separate servers.

Services must be installed in the following order:

1. PatientSecure Identity Server (PSIS)



IMPORTANT: PatientSecure Identity Server (PSIS) must be installed and active before you install PatientSecure Web Services (PSWS).

2. PatientSecure Web Services (PSWS)



IMPORTANT: PatientSecure Identity Server (PSIS) and PatientSecure Web Services (PSWS) must be installed before you install the remaining services.

3. The remaining services, in any order:
 - PatientSecure Admin Console (ADMIN)
 - PatientSecure User Interface (CLIENT)
 - PatientSecure Reporting Services (REPORT).

**IMPORTANT:**

Reporting Services is required for the Admin Console to display the dashboard and to run reports. While you can install Admin Console and Reporting in any order, they both must be installed in the environment.

PatientSecure Job Services (JOB)

PatientSecure HL7 (HL7)

PatientSecure Emergency Search & Authentication Service (EMERGENCY)

PatientSecure System Health Service

PatientSecure EMPI Service, optional

PatientSecure FHIR Service (FHIR), optional

**NOTE:**

If you plan to use a certificate that you supply, set up a certificate authority (CA) for the generated certificates.

For more information, see the Microsoft TechNet Group Policy instructions for your Windows Server version. The certificate will secure only the name you enter when you create it.

Adding a Server

To add a server:

1. In the Server Status section, click **Add a Server**.
2. Enter the fully qualified domain name (FQDN) for the server (up to 50 characters) in the **Hostname** box, and then click **Next**.
3. Enter the Windows administrator credentials for the application server, and then click **Confirm**.
4. To configure the SSL Certificate, select one of the following:
 - Click **Select an existing certificate** to select a certificate from the Trusted Certificate directory on the server.



NOTE: The certificate must be unique to each server.



- Click **Generate a new certificate** and type the fully qualified domain name (FQDN).
 - Click **Save** to save the `PatientecureCertAuth.pfx` file.
5. In the Services section, select one or more services to run on the server.


If a service is grayed and unavailable, it has already been installed and cannot be installed on additional servers, or the dependencies for the service have not been installed.

For example, Emergency Search services may be installed on one server only.



NOTE: The port setting must be unique to each service.

Abbreviation	Server Component	Notes
PSIS	PatientSecure Identity Server	<ol style="list-style-type: none">1. Select the drive and port, and then click Install.2. Enter the Windows administrator credentials for the server, and then click Confirm.
PSWS	PatientSecure Web Services	<ol style="list-style-type: none">1. Select the drive and port, and then click Install.2. Enter the Windows administrator credentials for the server, and then click Confirm. <div>NOTE: Scanning services (palm) are installed with the PSWS service.</div>
ADMIN	PatientSecure Admin Console	<ol style="list-style-type: none">1. Select the drive, and then click Install.2. Enter the Windows administrator credentials for the server, and then click Confirm. <div>NOTE: The PatientSecure Admin Console uses port 80 (and redirected to port 443) or port 443. You cannot configure a port for the Admin Console.</div>
CLIENT	PatientSecure User Interface	<ol style="list-style-type: none">1. Select the drive and port, and then click Install. By default, the port is 7003.2. Enter the Windows administrator credentials for the server, and then click Confirm.
HL7	PatientSecure HL7	<ol style="list-style-type: none">1. Select the drive and port, and then click Install.2. Enter the Windows administrator credentials for the server, and then click Confirm.
REPORT	PatientSecure Reporting Service	<ol style="list-style-type: none">1. Select the drive and port, and then click Install. By default, the port is 7004.2. Enter the Windows administrator credentials for the server, and then click Confirm.

Abbreviation	Server Component	Notes
JOB	PatientSecure Job Scheduler Service	<ol style="list-style-type: none"> 1. Select the drive and port, and then click Install. By default, the port is 7005. 2. Enter the Windows administrator credentials for the server, and then click Confirm.
EMERGENCY	Emergency Search (one)	<ol style="list-style-type: none"> 1. Select the drive and port, and then click Install. By default, the port is 7006. 2. Enter the Windows administrator credentials for the server, and then click Confirm. <div>  <p>NOTE: PatientSecure Site Monitoring (PSSM) is installed on the same server with Emergency Search. It is not listed as a separate service on the server.</p> <p>To implement the Site Monitoring website, work with your Imprivata PatientSecure representative.</p> </div>
HEALTH	System Health Service	<ol style="list-style-type: none"> 1. Select the drive and port, and then click Install. By default, the port is 7007. 2. Enter the Windows administrator credentials for the server, and then click Confirm.
FHIR	FHIR Service (optional)	<ol style="list-style-type: none"> 1. Select the drive and port, and then click Install. By default, the port is the next available port in the 7000 range. 2. Enter the Windows administrator credentials for the server, and then click Confirm.
EMPI	EMPI Service (optional)	<ol style="list-style-type: none"> 1. Select the drive and port, and then click Install. By default, the port is the next available port in the 7000 range. 2. Enter the Windows administrator credentials for the server, and then click Confirm.

The Server Details page displays the installed services.

6. When you have installed all of the services for the server, click **Dashboard** at the top of the page to return to the Server Dashboard.


Viewing a server

The PatientSecure Server Console Dashboard lists all of the servers that are available for your PatientSecure installation.

In the Server Status section:

1. Locate a server, and then click the row.

The Server Details page is divided into three sections:

Item	Description
Server Info	<div>Displays the system details for the server.</div> <div> TIP: To refresh the server information, click Reload Details.</div>
SSL Info	Displays the SSL certificate thumbprint, which ensures secure access to Imprivata PatientSecure data on the server.
Services	<div>Lists the Imprivata PatientSecure services available on the server. If a service section is blank, it is not installed on this server.</div> <div>For each installed service, review the installation information and Install Status indicator:</div> <ul style="list-style-type: none">• Successful (green): The service is running and communicating with Imprivata PatientSecure.• Error (red): The service is not communicating with Imprivata PatientSecure. <div>If the status indicator is red, click an Install Logs button on the left to investigate.</div>

2. To return to the Server Console Dashboard, click **Dashboard**.

Editing a Server

To edit a server in the Server Dashboard, locate the server in the Server Status list, and then click the server row. The Server Details page opens.

Server Info

The Server Info section displays the system details for the server.

1. To uninstall all services on this server, click **Uninstall All**. Enter your Windows credentials for the server.
2. To update the connection strings for all services installed on this application server, click **Update Service Connection Strings**. Enter your Windows credentials for the server.
3. To refresh the server information, click **Reload Details**.

SSL Info

The SSL Info section displays the certificate thumbprint.

Add a Certificate to the Local Certificate Store

To add a server certificate to the local certificate store:

1. Click **Download Certificate Authority**.

The server certificate .pfx file is downloaded to the local Downloads directory.

2. When you open the certificate, the **Certificate Import Wizard** opens.
3. Follow the instructions in the wizard to copy the certificate to a local store.

Change the Server Certificate

To change the server certificate:

1. Click **Edit SSL Info**. The Configure SSL Certificate page opens.
2. You can supply a certificate from a trusted source or generate a new certificate:
 - Click **Use an existing certificate**.
 - Click **Generate a new certificate**.
3. Click **Save**.
4. Enter your Windows credentials for the server.

The certificate is updated. For more information, see [Replace the Server Certificate](#)

Services

The Services section lists the Imprivata PatientSecure services available for the server.

For an installed service, review the installation information and **Install Status** indicator:

- **Successful** (green): The service is running and communicating with Imprivata PatientSecure.
- **Error** (red): The service is not communicating with Imprivata PatientSecure.

Change Source Settings

To change source settings:

Click **Advanced Settings**. The Advanced Settings page displays the installed Imprivata PatientSecure components, including:

- PatientSecure Server Console
- PatientSecure Database
- PatientSecure Identity Server
- PatientSecure Web Services
- PatientSecure User Interface
- PatientSecure Reporting Service
- PatientSecure System Health Service
- PatientSecure FHIR Service (optional)
- PatientSecure EMPI Service (optional)



NOTE: If you make changes to the source settings for any of the Imprivata PatientSecure components, you may need to reinstall services on the server.

View Installation Logs for Services

To view the installation logs for an installed service:

1. Click the **Install Logs** button. The Log Viewer opens.
2. To return to the Server Details page, click outside the log viewer.

Uninstall an Installed Service

To uninstall an installed service:

1. Click **Uninstall**.
2. Enter your Windows credentials for the server. Uninstalling a PatientSecure service removes the service and its associated files from the database.
3. Click **Yes** to confirm.



NOTE: If the uninstall process is incomplete, or the application server is unavailable, select **Force Uninstall** from the **Uninstall** drop-down list. This removes the service from the database, but it may not remove all of the associated files. This allows you to reinstall a service on an available server.

For more information on removing the associated files, see [Delete Remnant Files on Uninstalled Servers](#)

Reinstall an Installed Service

To reinstall an installed service:

1. Click **Reinstall**.



NOTE: If more than one build is available for reinstallation, select the build number from the **Reinstall** drop-down list.

2. Enter your Windows credentials for the server. The service is reinstalled.
3. Check the **Installed Status** indicator to ensure that the re-installation was successful.



IMPORTANT: Use caution when reinstalling a Imprivata PatientSecure service, as you may lose saved data.

Adding an Active Directory Group

User access is determined by Active Directory groups on the Active Directory server.

To add an Active Directory group:

1. Make sure that the Active Directory group is set up on the Active Directory server.



NOTE: The Active Directory groups must already exist on the Active Directory server. You cannot assign a group to more than one role.

TIP: You can add individual users to your Active Directory groups through the [Location Access](#) settings in the Admin Console at any time.

2. In the Active Directory Status section, click **Add an Active Directory**.

The Configure Active Directory page opens.

The Active Directory information at the top of the page is grayed and unavailable. To update it, [edit the Active Directory](#) entry.

3. Identify the Active Directory server:

Item	Description
Display Name	Enter the name (up to 50 characters) that will reference Active Directory.
Domain	Enter the domain name assigned to the Active Directory server, if any.
Container	Enter the container name for organization units (OU), if any.
AD Account Name	Enter the name of the user who is a domain administrator on the Active Directory.
AC Account Password	Enter the password for the user who is a domain administrator on the Active Directory.

4. Add one or more Active Directory groups:

Item	Description
Owners	Specify the Active Directory group(s) with users who will be assigned Owner access to Imprivata PatientSecure.
Administrators	Specify the Active Directory group(s) with users who will be assigned Administrator access to Imprivata PatientSecure.
Users	Specify the Active Directory group(s) with users who will be assigned User access to Imprivata PatientSecure.

5. When you are done, click **Next**.

The Active Directory settings are updated and you return to the Server Dashboard.

Editing the Active Directory Account Settings

To edit the Active Directory account settings in the Server Dashboard:

1. Make sure that your changes have been made to the Active Directory group on the server where Imprivata PatientSecure is installed.
2. In the Active Directory Status section, click the server row.
The Configure Active Directory page opens.
3. Update the fields in the Active Directory form:

Field	Description
Display Name	Enter the name (up to 50 characters) that will reference Active Directory.
Domain	Enter the domain name assigned to the Active Directory server, if any.
Container	Enter the container name for organization units (OU), if any.
AD Account Name	Enter the name of the user who is a domain administrator on the Active Directory.
AC Account Password	Enter the password of the user who is a domain administrator on the Active Directory.
Owners	Specify the Active Directory group(s) with users who will be assigned Owner access to Imprivata PatientSecure.
Administrators	Specify the Active Directory group(s) with users who will be assigned Administrator access to Imprivata PatientSecure.
Users	Specify the Active Directory group(s) with users who will be assigned User access to Imprivata PatientSecure.

4. Click **Next**.

The Active Directory settings are updated and you return to the Server Dashboard.

Deleting a Server

Before you can delete a server from the Server Dashboard, you must first uninstall all of the services installed on the server.

Delete the Server from the PatientSecure Server Console

To delete a server from the Server Dashboard:

1. Locate the server in the Server Status list, and then click the server row.
The Server Details page opens.
2. The Services section lists all of the Imprivata PatientSecure services installed on the server. For each installed service:

- a. Click **Uninstall**.
- b. Enter your Windows credentials for the server.
- c. Click **Yes**.

The Server Info section displays the system details for the server.

3. To remove the server from your installation, click **Delete Server**.
4. Click **Delete**.

Delete Remnant Files on Uninstalled Servers

After you delete a server from the Server Dashboard, you must manually delete some Imprivata PatientSecure keys and files that remain on the uninstalled server. These files reside in the `C:\ProgramData\Imprivata` directory and contain Imprivata PatientSecure state information.



NOTE: Deleting the `ProgramData\Imprivata` directory and its contents is especially important if you plan on re-installing Imprivata PatientSecure in a clean state in the future.

Replace the Server Certificate

If you encounter a certificate error after installing the Imprivata PatientSecure server for release 6.5, you can replace the server certificate without reinstalling the PatientSecure server:

- Replacing the server certificate using a .PFX certificate (recommended)
- Replacing the server certificate using a .CER certificate



NOTE:

Replacing a server certificate is performed in the Internet Information Services (IIS) Manager on your Windows Server. The steps may vary depending on your version of Windows Server and IIS.

For more information on server certificates, see the IIS documentation for your Windows Server version.

Before You Begin

Consider the following items before you replace the server certificates:

- Ensure that you have successfully installed Admin Console
- Ensure that users can access Admin Console over SSL (<https://<server>/AdminConsole> through remote desktop or by logging in directly to the server where Imprivata PatientSecure is installed.

Replacing the server certificate using a .PFX certificate (recommended)

To replace a .PFX server certificate:

1. Start the **Computer Management** tool, navigate to the **Internet Information Services (IIS) Manager**. In **Connections**, select your server, and then double-click **Server Certificates**. The Actions panel includes options for your server certificate.
2. From the Actions panel, select **Import**.
3. In the Import Certificate dialog box:
 - a. Enter the full path to your certificate .pfx file.
 - b. Enter the associated password.
 - c. Select **Allow this certificate to be exported**.
 - d. Click **OK**.Your certificate is added under Server Certificates.
4. In the **Connections** panel, click **Default Web Site**.
5. In the Actions panel, click **Bindings**.
6. In the Site Bindings dialog box, select the **https** entry for port 443, and then click **Edit**.
7. In the Edit Site Bindings dialog box, click **Select**, and then select the new SSL certificate. Click **OK** twice to exit.
8. Restart your site.

Replacing the server certificate using a .CER certificate

To replace a .CER server certificate:

1. Start the **Computer Management** tool, navigate to the **Internet Information Services (IIS) Manager**.
2. In **Connections**, select your server, and then double-click **Server Certificates**. The Actions panel includes options for your server certificate.
3. Select the certificate you want to replace.
4. In the Actions panel, click **Enable Automatic Rebind of Renewed Certificate**.
The link changes to **Disable Automatic Rebind of Renewed Certificate**.
5. While your Server Certificate is still selected, click **Renew**.
6. In the Renew an Existing Certificate dialog box, select the **Complete certificate renewal request** and click **Next**.
7. Click the ellipsis [...], select your certificate .cer file, and then click **Finish**.
8. Restart your site.

If binding does not happen automatically for some configurations:

- a. Select **Default Web Site > Bindings**, and then select the https entry for port 443 and click **Edit**.
- b. In the Edit Site Binding dialog box, click **Select**, and then select **CertCreatedWithCertGen**.
- c. Click **OK**.

Deleting the Active Directory Account Settings

User access is determined by Active Directory groups on the server where Imprivata PatientSecure is installed.

To remove the Active Directory account settings:

1. In the Active Directory Status section, click the server row.
The Configure Active Directory page opens.
2. Review the Active Directory settings.
3. To remove the Active Directory account from Imprivata PatientSecure, click **Delete**.






IMPORTANT: Use caution when removing Active Directory settings, which control access to Imprivata PatientSecure components. Users will not be able to work with Imprivata PatientSecure tools until you replace the Active Directory configuration.

4. Click **Delete**.

PatientSecure Server Console

In the PatientSecure Server Console, the **Dashboard** page displays the current state of the servers running Imprivata PatientSecure components:

Element	Description
SQL Database Status	<p>Displays information (source, name, user) about the server running the PatientSecure database, which communicates with your EMR system and provides patient data for your installation.</p> <div> NOTE: The user account listed on the Dashboard is a new service user account created by Imprivata PatientSecure during installation. For more information, see Database user accounts.</div> <p>Color-coded status indicators describe the server and database:</p> <ul style="list-style-type: none">• The server status indicator is green when the server is running and communicating with Imprivata PatientSecure and red when the server is running but has a problem communicating with Imprivata PatientSecure.• The database indicator is green when the database is available and known to exist and red when the database is not found. <p>There is only one SQL Database server.</p> <div> TIP: After you install the database server, be sure to review the database maintenance time. The default setting is 1:00 AM, according to the Time Zone setting for your installation. For more information, see "Set up a database maintenance schedule in the <i>PatientSecure online help</i>.</div>
Server Status	<p>Displays information about the server and each Imprivata PatientSecure service running on the server.</p> <p>Color-coded status indicators describe each installed service:</p> <ul style="list-style-type: none">• The status indicators are green when the service is running and communicating with Imprivata PatientSecure and red when the service is not communicating with Imprivata PatientSecure. <p>You can add any number of application servers.</p>
Active Directory Status	<p>Displays information about the server where the Active Directory groups are located. You can adjust user permissions by adding, editing, or deleting Active Directory groups on this server.</p> <div> TIP: You can later add individual users to your Active Directory groups through the Location Access settings in the Admin Console.</div>

For more information, hover your cursor over a status indicator.



NOTE: When a server running a Imprivata PatientSecure component stops communicating with Imprivata PatientSecure, the status indicator turns **red**.

Users with Owner access can view, add, edit, or delete a server from the Imprivata PatientSecure Server Dashboard, and add individuals to Active Directory groups.

Database user accounts

The two database user accounts have the following permissions:

- **SQL Database server Database user account**

- Alter any DB
- Alter any login
- Connect any DB
- Connect SQL
- Create any DB
- Create server role
- Create availability group
- Select all user securables
- View any database
- View server state

- **Service user account created by PatientSecure during installation**

User name: `ImprivataPatientSecureServices_[DB_NAME]`

Permissions granted to the service user at the SQL Server level:

- Connect SQL
- View Database State
- View Server State

Role membership granted to the service user for the PatientSecure database:

- datareader
- datawriter
- ddladmin
- executor with permission to execute stored procedures against the PatientSecure database
- owner
- public

For more information, see "Permissions of Fixed Database Roles (Database Engine)" on the Microsoft TechNet website.