imprivata®

Product Documentation

Imprivata PatientSecure Admin Console User Guide

Imprivata PatientSecure® 6.11

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

© 2024 Imprivata, Inc. All Rights Reserved.

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

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

Trademark Information

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

Legal Notices

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

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

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

Document revision 6.11

This document describes the features of the Imprivata PatientSecure Admin Console release 6.11 for Administrators and Users.

Contents:

Getting Started with the Admin Console

The Imprivata PatientSecure Admin Console is a hosted web application that provides authorized users access to configuration settings and Imprivata PatientSecure data for your installation.

Logging in to the Admin Console

The Admin Console is available over a secure SSL connection using HTTPS.

The URL for accessing the Admin Console is unique to each installation. Before you begin, ask your system administrator for the correct address.

For a full list of supported browser versions, see the *Imprivata PatientSecure Supported Configurations* in the Imprivata Customer Experience Center or your Imprivata PatientSecure representative.

To log in to the Admin Console:

1. Open your browser and type the URL in the address line.

> (i) **NOTE**: The URL must include the server name and Fully Qualified Domain Name (FQDN), if a domain or an IP address is used. Login addresses using HTTP are automatically redirected to HTTPS.

   The Log In page opens.

2. Select your server domain from the drop-down list.

3. Enter your user name in the **Username** field.

4. Enter your password in the **Password** field.

> (i) **NOTE**: Passwords are case sensitive; user names are not.

5. 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 Admin Console home page displays the Dashboard for your installation.

> (i) **IMPORTANT**: Your Admin Console session will time out automatically after 30 minutes of inactivity.

Managing Your Imprivata PatientSecure License

The License page displays the details of your active license for all hospitals, clinics, and other entities associated with your company in Imprivata PatientSecure. If you have an implementation without an existing license or if your license is near or past its expiration date, you can upload a new license.

> **IMPORTANT**: If your Imprivata PatientSecure license has expired, registrars will still be able to authenticate existing patients, but they will not be able to enroll new patients until you update your license.
>
> **NOTE**: If your license is still valid when you upgrade to a newer version of Imprivata PatientSecure in the future, you will not need to reapply the license file.

For information on how to obtain a new or updated license, contact your Imprivata PatientSecure representative.

To open the License page:

• From the Admin Console menu, select **Settings > License**.

Reviewing the Active License

The active license is valid until its expiration date, if one exists. To prevent an interruption in service, be sure to review your active license regularly.

> **NOTE**: If you have not yet loaded a license or your license has expired or needs updating, **Settings > License** is the only option available on the Admin Console menu until you upload a new license. For assistance, contact your Imprivata PatientSecure representative.

To review your active license:

1. In the Admin Console, go to **Settings > License**.

2. Review the following information for your active license:

   • License version

   • Name of your company

   • Names of hospitals associated with your company in Imprivata PatientSecure that are contractually permitted to use Imprivata PatientSecure

   • Number of clinics or other entities associated with your company in Imprivata PatientSecure that are contractually permitted to use Imprivata PatientSecure

   • Date when the license expires (if any)

   • Date when the license file was created

   • Date when the license file was uploaded to the Admin Console

Uploading a License

Users with Owner access should work with your Imprivata PatientSecure representative to obtain a new or updated license:

• If you have an existing implementation without a license.

• If you are adding hospitals and/or clinics to your license.

• If you are nearing the license expiration date.

When you receive a new license, download the license file to a directory accessible from the machine running Imprivata PatientSecure Admin Console.

To upload the license:

1. From the Admin Console menu, select **Settings > License**.
2. Click **Upload License**.
3. In the Upload License dialog box, click **Browse**, navigate to the location of the license file (in .LIC format), and then click **Open**.
4. Click **Upload**.

   The license uploads successfully. The message displays the number of clinics added to or removed from your license (if applicable).

The following information is updated on the License page:

- License version
- Named hospitals l Number of clinics l Expiration date
- License file creation date
- License file upload date

Admin Console Menu

Your access level determines the Admin Console menu items available to you.

> **NOTE**: If **Settings – License** is the only option on the Admin Console menu, then your license is not active and you cannot access Admin Console data. Users with Owner access may upload a license. For assistance, contact your Imprivata PatientSecure representative.

Element	Description
	Displays statistics on activities in all locations available to you. You can also access dashboards on activities by facility or by department.
Patient Search	Provides access to records for individual patients.
Reports	Lists the Imprivata PatientSecure report types and provides access to scheduled reports that have been run.
Settings	Set up your installation and configure your location settings, limit user access to facility data, and review and upload your Imprivata PatientSecure license.
Troubleshooting	Provides access to the tools for investigating issues in service operations.
Help	Links to the online Help system, Imprivata Customer Experience Center site, and provides information about the Imprivata PatientSecure release.

Element	Description
Notifications	Indicates that there are system messages that require attention. Click 🔔 to toggle the list of notifications. Notifications are color coded: • Danger (red) • Warning (orange) • Success (green) • Information (blue) ⓘ **IMPORTANT**: Super Administrators should contact their Imprivata PatientSecure system administrator when notifications require attention.
Log out	Exit the Imprivata PatientSecure Admin Console.

PatientSecure User Groups

Permission to access Imprivata PatientSecure data in the Admin Console is determined by the user group to which you are assigned in the Active Directory settings on the server.

There are three levels of access to Imprivata PatientSecure:

- **Owner** has full access to all features on the site.
- **Administrator** has access to system notifications, patient records, and report data; can configure location permissions; can edit all scheduled reports; and can view the Imprivata PatientSecure license.
  - View system notifications.
  - Limit user access to facility data.
  - Edit and delete scheduled reports created by other users.
- **User** has access to the Dashboard and report data.
  - View statistics on activities in all facilities available to you.
  - Generate reports using Imprivata PatientSecure data.

ⓘ **NOTE**: If you encounter a problem accessing Imprivata PatientSecure, or you cannot access data in the Admin Console for a facility in your purview, contact your system administrator.

Working with Imprivata PatientSecure Data

The Admin Console provides statistics on activities, access to patient records, and a variety of reports for your installation.

The location access settings restrict the range of data available to users, according to their Active Directory group or individual setting.

Setting Up Location Access

Users have access to all locations in your installation, unless their access permissions have been restricted.

- In the Admin Console, go to **Settings > Location Access**.

  The Location Access page lists the roles whose access is limited to one or more locations, based on Active Directory groups and individuals. All other users can see data from all locations.

Only Administrators and Owners can add, edit, and delete user access roles.

> **(i)** **NOTE:**
> Changes to the Location Access settings take effect the next time the user logs in to the Imprivata PatientSecure Admin Console.

Adding a Role with Access Restrictions

To add a role with access restrictions:

1. In the Admin Console, go to **Settings > Location Access**.

   The Location Access page lists the roles whose access is limited to one or more locations, based on Active Directory groups and individuals.

2. Click **Add new role** in the upper-right corner of the page.

3. In the Role Name field, enter a unique name.

   Imprivata PatientSecure verifies that the role name does not match one already in use.

4. Specify the Active Directory groups and users to add to the restricted access list.

Domain	Select the Active Directory domain from the drop-down list.
Groups	Enter the full name of one or more Active Directory groups to add to the restricted access list. Separate multiple entries with a **,** (comma).
Users	Enter the user name of one or more Active Directory users to add to the restricted access list. Separate multiple entries with a **,** (comma).

Be sure to enter the names exactly. Imprivata PatientSecure checks the Active Directory entries when you click **Save.**

5. Specify the locations that will be accessible by this role, starting with the highest, organization, level. A lower-level location is not available until you select its parent level.

> ⓘ **IMPORTANT:**
> Be specific. The users in this role will have access to the locations you specify but not to any other locations at this level, any upper levels, or any other organizations in your installation.

Organizations	Select one or more organizations; users in this role will not have access to any other organizations.
Facilities	Select one or more available facilities; users in this role will not have access to organization-level data for the facilities you select or to any other facilities in the organization.
Departments	Select one or more available departments; users in this role will not have access to facility-level or organization-level data for the departments you select or to any other departments in the facility.

> ⓘ **TIP:**
> Start typing the location name: a list of matching names pops up and you can select a name from the list. You can add more than one available organization, facility, and department. To remove a location from the list, click **x** next to the name.
>
> **NOTE**: If a location is later deleted, then it will no longer appear in location access roles and users will no longer have access to data for that location. If all locations assigned to a user are deleted, then the user will have no access to view Imprivata PatientSecure data.

6. Click **Save**.

    Imprivata PatientSecure validates your Active Directory entries before creating the new role, and then returns to the Location Access page.

Editing the Location Access for a Role

To edit the location access for a role:

1. In the Admin Console, go to **Settings > Location Access**.

    The Location Access page lists the roles whose access is limited to one or more locations, based on Active Directory groups and individuals.

2. Locate the role in the Location Access list, and then click the row.

    The Edit Role page displays the settings for the role.

3. Review the role settings and make changes, as needed:

Role Name	Enter a unique name. Imprivata PatientSecure verifies that the role name does not match one already in use.
Domain	Select the Active Directory domain from the drop-down list.
Groups	Enter the full name of one or more Active Directory groups to add to the restricted access list. Separate multiple entries with a **,** (comma).
Users	Enter the user name of one or more Active Directory users to add to the restricted access list. Separate multiple entries with a **,** (comma).
Organizations	Select one or more organizations; users in this role will not have access to any other organizations.
Facilities	Select one or more available facilities; users in this role will not have access to organization-level data for the facilities you select or to any other facilities in the organization.
Departments	Select one or more available departments; users in this role will not have access to facility-level or organization-level data for the departments you select or to any other departments in the facility.

> **(i)** **TIP:**
> Start typing the location name: a list of matching names pops up and you can select a name from the list. You can add more than one available organization, facility, and department. To remove a location from the list, click **x** next to the name.

4. Click **Save**.

   Imprivata PatientSecure validates any changes to your Active Directory entries, and then returns to the Location Access page.

Deleting a Location Access Role

If you remove a location access role, then the groups and users in that role will have access to all locations in your installation, until you add them to a new or existing location access role.

To delete a location access role:

1. In the Admin Console, go to **Settings > Location Access**.

   The Location Access page lists the roles whose access is limited to one or more locations, based on Active Directory groups and individuals.

2. Locate the role in the Location Access list, and then click the row.

   The Edit Role page displays the settings for the role.

3. Review the role settings to make sure that you want to delete this role.

4. To remove the location access restrictions from the groups and users listed in this role, click **Delete**.

5. Click **Confirm Delete**.

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 PatientSecure. With these tools you have insight into the overall use of PatientSecure. 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 PatientSecure being used across my department".

The Admin Console 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. You may be able to see outliers compared to other organizations, facilities, or departments. With this information you can take proactive measure to investigate why usage looks to be trending down compared to other areas. Or, perhaps one department is doing really well, and you can learn what has made them so successful and then share those best-practices to help other areas.

> ⓘ **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. There are many reports, but to start the most important report will probably be the Activities Summary report and/or the Utilization Summary report (see setting up utilization reporting). This report will show you activity data from the highest level (e.g. Organization) down to the most detailed level (e.g. user or machine).

If, for example, a depart manager wanted to see the usage of PatientSecure across her staff this would be a great place to start by running this report. Using the Dashboard and Reports will help ensure you and your teams have the information they need at hand to ensure success.

For more information, see The PatientSecure Dashboard and Reports.

The PatientSecure Dashboard

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

Scanner Activity

The Scanner Activity section displays a summary of the client machines in your PatientSecure environment.

- **Activity (green icon)** - indicates that the client machine has recent activity.
- **Moderate inactivity (blue timer icon)** - indicates that the client machine has been active in the past, but has experienced some period of inactivity.
- **Extended inactivity (red timer icon)** - indicates that the client machine has been active in the past, but has experienced an extended period of inactivity.
- **Information unavailable (gray icon)** - indicates that the client machine's activity is unknown.

Activity thresholds are configured in General Settings.

System Health

The System Health section displays a summary of the health of your PatientSecure environment, including a summary of event alerts and service alerts.

For additional details, see the System Health Dashboard.

Maintenance Schedule

The Maintenance Schedule section displays a summary of the scheduled maintenance tasks performed in your PatientSecure environment, including their scheduled start times.

- Database maintenance
- Site Monitoring data collection
- Biometric Auto-deletion
- Scheduled Reports
- Patient Privacy Intelligence (formerly Imprivata FairWarning)

Utilization

The Utilization section contains two charts that display interactions (Utilization, Patients Found, Patients Not Found, Patients Enrolled, Opt-outs, and Registrar Declines) for all organizations, facilities and departments available to you. The default setting is **Monthly** for the year to date.

- The **All interactions** bar chart displays color-coded activities, by day, week, month, quarter, or year, for the selected date range.

  The legend below the chart displays total counts for each activity type.

  If Utilization Reporting is enabled, a line chart displays the utilization of PatientSecure in registrations. For more information, see About Utilization Reporting.

- The **Interactions by Organization** or **Interactions by Facility** or **Interactions by Department** line chart displays totals for all interactions (default), by month, quarter, or year, for the selected date range, color-coded by the top five organizations, facilities or departments.

  The legend below the chart identifies the organization.

If Utilization Reporting is enabled, the **Utilizations (%) by** line chart displays percentages for all interactions in the organization, facility or department by month, quarter or year, for the selected date range. The line chart displays the items by color code; only the top five are displayed in the legend.

> **(i)** **TIP:**
> Hover the cursor over a label in the legend to highlight the points on the matching graph line; click a label in the legend to toggle (remove/add) the line on the chart.

For each chart, click **Download** to generate an image of the chart. The image is exported as a .PNG file in the Downloads folder on your local drive.

> **(i)** **TIP:**
> If you clicked a label in the legend and removed one or more lines from the **Interactions by** chart, the downloads will match the modified chart data.

Changing the Charts Options

To change the options for the Trends charts:

1. Click the **Trends ⌄** drop-down.
2. Select the **Group By** filter: **daily**, **weekly**, **monthly**, **quarterly**, or **yearly**.
   - When you select the daily view:
     - The default date range displays the past 8 days, including today.
     - Data is collected beginning at 12:00:00 AM on the start date until 11:59:59 PM on the end date.
     - The minimum number of days you can select is 1.
     - When using the daily filter, selecting more than 120 days is not recommended.
   - When you select the weekly view:
     - The default date range displays the past 8 weeks, including this week.
     - A week starts on Sunday and ends on Saturday. If you do not select a Sunday for the start date, the system determines the date of the Sunday immediately before the date you select.
     - Data is collected beginning at 12:00:00 AM on the start date until 11:59:59 PM on the end date.
     - The minimum number of weeks you can select is 1.
3. To select a range of time, click the calendar icon 📅 and set the start and end dates.
4. To filter the chart by type of interaction, select the interaction from the **Interaction to Include** checkboxes:

- **Patients Found**
- **Patients Not Found**
- **Patients Enrolled**
- **Opt-outs** (if Opt-out Tracking is enabled).
- **Registrar Declines** (if enabled).
- **Utilization** (if enabled).

5. Click **Save**.

Machine Mappings

The Machine Mappings section displays a summary of the number of machines running the PatientSecure client software that are unmapped and mapped:

- **Unmapped** indicates the number of machines not yet mapped to a location in your organization.
- **Mapped** indicates the number of machines mapped to a location in your organization.

For more information, see Machine Mappings.

Duplicate Records Detection

The **Duplicate Patient Records** section of the Dashboard displays information representing duplicate patient record handling.

- **Active duplicates**. The active number of duplicates detected.
- **Duplicates detected**. The total number of duplicates detected.
- **Duplicates resolved**. The total number of duplicates investigated and resolved.

PatientSecure detects when a patient with the same palm is attempting to enroll with a different patient identifier. When a duplicate is detected, it should be reviewed to determine the action to take.

Duplicates are marked as **Resolved** when they are merged in the EMR or when the record is deleted from PatientSecure.

For more information, see Duplicate Records Detection.

Reports

The Reports section displays a summary of the last six scheduled reports that ran.

- For a successful report, click the download icon to download the report in its specified format (.XLSX or .CSV).
- For a report that encountered errors, hover your mouse over the report name to view a tooltip with the error message.

For more information, see Scheduling a Report.

PatientSecure Activities

Admin Console dashboards and reports display PatientSecure data for the interactions of registrars (users) working with palm scanners (machines) in the locations available to you:

- Patients Found
- Patients Not Found
- Patients Enrolled

For more information on how PatientSecure calculates enrollment and authentication interactions, see Calculating PatientSecure Interactions.

Terminology

Additional terms for PatientSecure interactions may be used in this topic:

Term	Definition	Notes
Enrollment	A biometric enrollment for a patient	
Opt-out enrollment	An opt-out that occurred during an enrollment.	
Identification	A one-to-many authentication of a patient	Used during non-scheduled visit workflows, such as urgent care. Also used during kiosk checkins.
Failed identification	An attempted identification that did not result in a successful authentication	
Opt-out identification	An opt-out that occurred during an identification.	
Verification	A one-to-one authentication of a patient	Used during scheduled visit workflows.
Failed verification	An attempted verification that did not results in a successful authentication	
Opt-out verification	An opt-out that occurred during a verification.	
Deletion	A deletion of a patient and their associated biometric enrollment.	
Biometric Addition	The addition of a different format of biometric to an existing enrollment.	

Registration Workflow

The recommended registration workflow includes the following steps:

1. The registrar asks the patient for his or her date of birth, and then assists the patient with hand placement for an authentication scan.
   - If the patient is found in the Imprivata PatientSecure system, the registrar sees a **Match Found** message and the result is a **Patient Found**.

     The patient's medical record is accessed and no other steps are needed.
   - If the patient is not found in the Imprivata PatientSecure system, the registrar sees a **No Match Found** message.

     In this case, the registrar searches for the patient in the EMR and either finds a result, or creates a new registration.
2. The registrar adds the patient to the system with an **Enrollment** scan.

- A **Patient Enrolled** message indicates that the patient's medical record, demographic information, and scan are now linked in Imprivata PatientSecure.

> **ⓘ** **NOTE:**
> If the patient's demographic information matches a record but the scan cannot be matched, perhaps due to a poor-quality original scan, the registrar has the option of re-enrolling the patient.
>
> In most charts and reports, re-enrollments are counted as enrollments, but are counted separately in the Patients Enrolled Details and Patients Enrolled Expanded Details reports.

  For palm installations, a Patient Found requires one scan and a Patient Enrolled requires two scans.

- In some cases, the registrar scans the patient's palm one or more times and sees a **No Match Found** message each time.

  This may be because of improper hand placement on the palm scanner.

- If the registrar is unable to complete a Patient Found or Patient Enrolled for a patient, the registration workflow ends as a **Patient Not Found**.

- If Photo Only workflows are allowed, the patient may opt out of having their palm scanned. In this case, the registration workflow ends with a photo-only enrollment or photo-only verify.

Calculating PatientSecure Interactions

PatientSecure keeps track of every patient enrollment and every patient authentication scan as discrete events. While each individual scan is tracked and stored, the final outcome of the interaction with the patient is the key data point. There are common situations where multiple scans occur, but they represent only one interaction with PatientSecure.

The purpose of PatientSecure interactions is to determine the final outcome of the interaction with the patient and report on that as opposed to reporting on each individual scan. The reason for looking at the final outcome is so that when compared to a total registration count from the EMR, the utilization equation (below) accurately reflects whether or not PatientSecure was used for each registration. Counting each individual scan in this equation would incorrectly inflate the value.

Example

A registrar attempts to authenticate a patient in PatientSecure with a result of **Biometric Didn't Match**.

The registrar then enrolls the patient in PatientSecure.

In this situation, there were two scans (a **Biometric Didn't Match** scan and a **Biometric Enrolled** scan), but the final outcome of the interaction with the patient is a successful Enrollment.

Definitions

The following terms and definitions are used in this topic:

- Individual scans will be classified as **Biometric Matched**, **Biometric Didn't Match** or **Biometric Enrolled**.
- The final outcome of the interaction with the patient (PatientSecure Interactions) will be classified as **Patient Not Found**, **Patient Found** or **Patient Enrolled**.
- An authentication attempt is a single attempt to identify or verify a patient using a biometric.

  A single authentication attempt will result in either a **Biometric Matched** or a **Biometric Didn't Match**.
- **Opt-outs** are activities without a biometric. For more information on opt-outs, see Patient Opt-Out Tracking.

Scenarios and Results

Scenario	Results	Description
Zero to many **Biometric Didn't Match** scans followed by a **Biometric Matched**	Patient Found	Multiple authentication attempts with the same search criteria, are performed on the same machine by the same user, that result in zero to many **No Match Found** scans and end with a **Biometric Matched** scan. Each attempt must occur with 5 minutes of the prior authentication attempt in order to be grouped together. When viewing Interaction-based reporting, this is reflected as a single **Patient Found**. Child re-enrollments and LinkIDs count as authentications.
Zero to many **Biometric Didn't Match** scans followed by a **Biometric Matched** Scan	Patient Enrolled	Multiple failed authentications with the same search criteria, are performed on the same machine by the same user, followed by an enrollment with demographics that match the search criteria. The **Biometric Enrolled** scan must occur within 15 minutes of the last **Biometric Didn't Match** scan in order to be grouped together.
One to many **Biometric Didn't Match** scans, without a subsequent **Biometric Enrolled** scan	Patient Not Found	Multiple failed authentications with the same search criteria, are performed on the same machine by the same user, without being followed by a **Biometric Enrolled** or **Biometric Matched** scan. Each authentication attempt must occur with 5 minutes of the prior authentication attempt in order to be grouped together.
One to many **Biometric Didn't Match** scans followed by an opt-out	Opt-Out	Multiple failed authentications with the same search criteria, are performed on the same machine by the same user, followed by an **opt-out** with demographics that match the search criteria. The opt-out must occur within 15 minutes of the last **Biometric Didn't Match** scan in order to be grouped together.

> **NOTE:** Any change to the search criteria (date of birth), or a change in the machine or user, will begin a new PatientSecure Activity.

Interactions and Opt-outs

For the File Upload method of calculating utilization, Imprivata PatientSecure includes the ability to decide whether photo-only opt-outs and patient opt-outs will be counted as part of the above equation.

The ability to count patient opt-outs as part of PatientSecure interactions relies on the **Opt-out Tracking** setting being enabled.

Opt-out Tracking enabled	Opt-out Tracking disabled
Adds Total opt-outs to the equation above: where **Total opt-outs**= Photo-Only + Patient Opt-outs So that the equation is now: $$\frac{(\text{Patients Found} + \text{Patients Not Found} + \text{Patients Enrolled} + \textbf{Total Opt-outs})}{\text{Registrations}}$$	The equation remains the same as above: $$\frac{(\text{Patients Found} + \text{Patients Not Found} + \text{Patients Enrolled} + \text{Photo-Only})}{\text{Registrations}}$$

Patient Records

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

Searching for a Patient's Record

To search for a patient's record:

1. In the Admin Console, go to **Patient Search**.

2. From the Patient Search page, do one of the following:

   - Select a Patient Identifier from the drop-down list and enter a value in the adjacent field.

   - Click **Advanced Search**, and enter one or more search criteria:

Patient Name	Enter the first initial of the patient's first name or preferred first name, and the patient's full last name or preferred last name. Wildcard characters are not accepted.
Date of Birth	Enter the patient's date of birth in the format provided. You can also click and select a date from the calendar. ⓘ **NOTE**: When you search by date of birth only, Imprivata PatientSecure searches the first 200 patients whose date of birth falls within one day of the date provided.
Sex	Select one of the following options: ◦ All ◦ Female ◦ Male ◦ Other Each Sex option includes records marked "Unknown."

Include deleted records	Select the **Include deleted records** checkbox to search all patient records, including deleted records and records marked **Inactive** in the HL7 feed; clear this checkbox to limit your search to active patient records only. ⓘ **NOTE**: You cannot search by patient identifier for inactive patients.

3. Click **Search**.

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

    Each patient record includes a photo (if available), palm silhouette (if a palm scan is used), patient name, and details, including up to three patient identifiers. The patient record indicates whether or not a valid ID was presented.

    The Search options are available in the left pane.

    > ⓘ **NOTE:**
    > If the number of patients in the search results list exceeds the maximum allowed, you see a message indicating the maximum number of results that Imprivata PatientSecure will display.

Refining Your Search

To refine your search:

1. To narrow your search, refine the search criteria in the left pane.
2. To search all records in the database, select the **Include deleted records** checkbox.
3. Click **Search**.

Viewing 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.

   > **(i) NOTE:**
   > If a palm scan is used, the patient's hand silhouette shown here is not the image of the patient palm vein pattern. The hand silhouette is included in the record to confirm that the patient's hand was placed correctly when the enrollment scan was taken.

2. Review the patient's information:
   - **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 History** 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. For PatientSecure environments where there is a mix of biometric scanners, also displays the biometric format type for each activity.

     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.
   - **Demographics History** 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.
3. To close the Patient Details page, click **Back to Patient Search**.

Editing a Patient's Record

To edit a patient's record:

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

   The Patient Details displays the patient's information.

2. Click **Edit** in the left pane to open the Edit page.

3. Make changes to one of more of the following fields:

   - **First Name**
   - **Preferred First Name**
   - **Last Name**
   - **Preferred Last Name**
   - **Date of Birth**
   - **Sex**
   - **Patient identifier** - The patient identifier number must be unique; you cannot specify a patient identifier number that is already in use.

     The PVID is displayed first in the list. You cannot edit or delete the PVID.

     ◦ Click **Add New** to add a new patient identifier.
     ◦ To edit a patient identifier, click the edit icon (✏️).
     ◦ To delete a patient identifier (other than PVID), click the delete icon (🗑️).
   - **Valid ID checked** - select **Yes** or **No** to indicate whether you checked the patient's identification.

4. Click **Save**. The Confirm Changes page lists the original values and the new values for the patient's information.

5. Review your changes carefully.

6. Enter a reason for the change you are making.

> ℹ️ **IMPORTANT:**
> You must provide a reason for the change.

7. Click **Confirm**.

Changes made to enrollment records are available in the Enrollment Record Updates report.

Deleting a Patient Photo

The patient may request that their photo be removed from their PatientSecure enrollment. Removing the photo still allows the patient to be successfully authenticated.

To delete a patient's photo:

1. Locate the patient in the search results, and then click the row. The Patient Details displays the patient's information.

2. To delete the patient's photo, click the delete icon (🗑️).

   The deletion creates an HL7 Photo Deletion outbound message.

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. Click **Edit** in the left pane to open the Edit page.

3. Review the patient's information.

> ℹ️ **NOTE:**
> When you delete the patient's record, that patient will not be identified by Imprivata PatientSecure on his or her next visit to your facility.
>
> The registrar will need to enroll the patient again by following the proper Imprivata PatientSecure enrollment process, including checking the patient's identification with a government-issued photo ID.

4. Click **Delete**. On the confirmation page, enter the following information:

   a. In the **Reason for deletion** box, enter a reason for deleting the patient record.

   > ℹ️ **IMPORTANT**: You must provide a reason for the deletion.

   b. Click **Permanently delete patient biometrics** to remove all palm vein biometrics and photos from the patient record in PatientSecure.

1. Click **Yes** to confirm.

The deleted record will be grayed in the search results list. You can view a deleted record, but you cannot edit it. If you selected the **Permanently delete patient biometrics** option, all biometrics are permanently removed from the patient record. As a visual indicator, the photo and palm scan icons are replaced with icons indicating that the photo and palm were deleted.

Changes made to enrollment records, including deletions, are available in the **Enrollment Record Updates** report.

Reports

To open the Reports page:

1. In the Admin Console, go to **Reports > Run or schedule a report**. The Reports page lists the reports available in Imprivata PatientSecure, along with a brief description of each report type.

2. Select a report to run immediately or schedule to run at an interval you specify.

Reports are saved in either an Excel (.XLSX) file or a .CSV file in the `Downloads` folder on your local drive or (for scheduled reports) in the scheduled reports output folder or subfolder that you specify.

- For reports with multiple worksheets, when you select the CSV format, each worksheet is created as a separate CSV file with the worksheet name appended to the filename.
  - For reports that are run immediately, the CSV files are bundled into a .ZIP file, available for download.
  - For scheduled reports, the CSV files are bundled into a .ZIP file that is saved to the scheduled reports output folder on the fileshare.
  - For emailed reports, the CSV files are attached to the email as separate attachments. The total size of all attachments will not exceed 20 MB.

> **(i) IMPORTANT:**
> Patient information is available in many Imprivata PatientSecure reports. Be sure to keep the report files secure.

Data Types in PatientSecure

There are several classes of data used in PatientSecure reports:

- **Interactions Data**

  The best way to think of interactions data is in the context of the end result - a certain set of PatientSecure activities between the registrar and patient that result in an outcome. The goal of a registrar using PatientSecure is to either enroll or authenticate a patient.

  For more information, see Calculating PatientSecure Interactions.

- **Scan Data**

  Scan-based data are the activities with a biometric, generated by the actual palm scanner device.

- **Opt-outs Data**

  Opt-outs are activities without a biometric. For more information on opt-outs, see Patient Opt-Out Tracking.

For more information on how PatientSecure calculates enrollment and authentication activities, see PatientSecure Activities.

Terminology

The following terms are used in this topic:

- **Gen 2 palm scanner** - the Keyo hand guide with the Fujitsu F-Pro Palm Vein Sensor, which supported touchless authentication for patients. Also referred to as the Fujitsu F-Pro sensors or the M5 sensors.
- **Gen 1 palm scanner** - the Fujitsu hand guide with the M3 palm vein sensor. The older generation of palm scanner hand guides that requires patients to place their hand on the scanner for all enrollment and authentication workflows. Also referred to as "Fujitsu V2 sensors".

- **Fujitsu V1 sensors** - a Fujitsu sensor version no longer supported by PatientSecure 4.x and later. This version should only be referenced when running the `Findscanners` Windows Powershell tool, as the tool may find PatientSecure clients with very old palm scanners attached.
- **I-Format biometrics** - the biometric type captured by the Gen 1 palm scanner.
- **R-Format biometrics** - the biometric type captured by the Gen 2 touchless authentication palm scanner.

Report Types

There are two kinds of reports in Imprivata PatientSecure:

- **Summary reports** contain statistics or a count of records.

  For example, the Enrollments Summary report contains counts of total enrollments for the selected date range.

- **Detail reports** contain patient records of an activity.

  For example, the Patients Found Details report contains patient records of successful authentications by a specific registrar (user) and client (machine).

The following report types are available in Imprivata PatientSecure:

Management Reports

Management Reports include summary reports with a global overview of interactions and other areas of interest for all locations available to you.

Why you may use these reports:

- You want to understand the usage of PatientSecure for your organization and how well PatientSecure is being adopted.
- You want to view the usage of PatientSecure for a particular department and its staff.
- You would like to see what departments are using PatientSecure the most relative to all other departments.

Report	Description
Expanded Interactions Summary	Displays daily counts of interactions, total scans per interaction type, client version, and scanner type for the selected date range. The report file contains separate tabs for data by organization, facility, department, machine, machine type, client version, scanner type. For the machine type: • **Kiosk** indicates that the scan occurred on a Windows based kiosk, an Epic Kiosk or a Linux kiosk. • **PC** indicates that the scan occurred on a registrar machine. For scanner type: • If scanner format is **I**, then Scanner Type is Gen 1 palm scanner • If the scanner format is **R** or **Dual**, then the Scanner Type is Gen 2 palm scanner All mapped machines on the date displayed with or without activity are reported; this includes deleted machines with activity on the activity date. ⓘ **NOTE:** This report may take a long time to run on large databases when more than one day is selected.
Interactions Summary	Displays counts of one or more interactions — patients found, patients not found, patients enrolled, opt-outs and registrar declines (depending on your settings) for the selected date range, grouped by day, week, month (default), quarter, or year. The report file contains separate tabs for data by organization, facility, department, user, and machine. For the machine type: • **Kiosk** indicates that the scan occurred on a Windows based kiosk, an Epic Kiosk or a Linux kiosk. • **PC** indicates that the scan occurred on a registrar machine. Access the Interactions Summary report directly from the **Reports > Quick Links** menu.

Report	Description
Interactions Metrics Summary	Displays the average number of scans for each interaction, in the locations you select. • Ideally, with the palm biometric, each successful authentication requires one scan (Match Found) and each enrollment requires two scans (No Match Found and Patient Enrolled). In practice, though, the registration workflow requires additional scans or reverts to a manual process. This report illustrates the efficiency of scanner use in the selected locations and gives managers insight into individual users who may need assistance or additional training with workflow steps and patient communication.
Merged Records Summary	Compares the number of records that are protected from duplication with records that remain unprotected in your source hospital system. When duplicate records are merged in your hospital information system (HIS), the resulting record may be a Imprivata PatientSecure record, with a biometric scan attached, or it may be a record for a patient who is not enrolled in Imprivata PatientSecure. There can be only one Imprivata PatientSecure record for each patient, so when a patient is enrolled in Imprivata PatientSecure, their medical record is protected from duplication.
Utilization Summary	Counts of records where PatientSecure was utilized as part of registration interactions by organization, facility, department and/or user. • Includes information on patients found, patients not found, patients enrolled, opt-outs and registrar declines (depending on your settings). • The inclusion of opt-outs in the utilization summary report is dependent on whether the **Count Opt-outs Towards Utilization %** setting is enabled. • For utilization reporting determined by file upload, the tabs included in the report depend on the data type you upload for utilization reporting. For more information, see Registration Data Files Types.

Lookup Reports

Lookup Reports provide quick access to records for a selected user or machine.

Why you may use these reports:

- You want to understand how well a particular user is using PatientSecure.
- You want to dig into the details of a machine at a location to see if it is having any issues relative to other scanners.
- You want to understand which machines have no PatientSecure scans so that you can troubleshoot scanner issues.

Report	Description
Machine Scans	Displays the total number of scans, by scan type and machine type, for one or more selected machines: • **Match Found** scan results in a Biometric Matched. • **Match Not Found** results in a Biometric Didn't Match. • **Patient Enrolled** results in Biometric Added. For machine type: • **Kiosk** indicates that the scan occurred on a Windows based kiosk, an Epic Kiosk, or a Linux kiosk. • **PC** indicates that the scan occurred on a registrar machine. For more information, see PatientSecure Activities. Access the Machine Scan report form directly from the **Reports > Quick Links** menu. To display the machine scan report for the total number of machines with no PatientSecure scans, select **Only Include Machines With No Scans** when running or scheduling the report.
User Scans	Displays the total number of scans, by scan type, for one or more selected users: • **Match Found** scan results in a Biometric Matched. • **Patient Enrolled** results in a Biometric Added. • **Match Not Found** results in a Biometric Didn't Match. For more information, see PatientSecure Activities. Access the User Scans report form directly from the **Reports > Quick Links** menu.

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 PatientSecure to send to these third party tools.

Report	Description
Activity Extract	Generates a report in .CSV format for the total number of: • authentication scans, including multiple appointment checkins, if the location is configured for it. • enrollment scans • photo-only enrollments • photo-only verifications • deletions • biometric deletions • opt-out enrollments • opt-out identifications • opt-out verifications For machine type: • **Kiosk** indicates that the scan occurred on a Windows based kiosk, an Epic Kiosk or a Linux kiosk. • **PC** indicates that the scan occurred on a registrar machine.
Enrollments Extract	Generates a report in .CSV format for the total number of active biometric enrollments and their associated identifiers.

Opt-out Reports

Opt-out Reports include statistics for Photo-Only interactions for enrollments and verifications.

Why you may use these reports:

• You want to understand the how often patients are opting out of using PatientSecure and why they are choosing not to use PatientSecure.

Report	Description
Opt-Out Summary	Displays the counts of total activities (enrollments, verifications and identifications) without a biometric identification, including: • photo-only enrollments • photo-only verifications • opt-out enrollments • opt-out identifications • opt-out verifications • total opt-outs. Organized by organization, facility, department, user, and machine. If Opt-Out Tracking is disabled, registrar declines are counted as opt-out enrollments/verifications/identifications on this report. If the Allow Photo-Only Workflows setting is disabled, the report does not include the counts for photo-only enrollments or verifications. The report file contains separate tabs for data by organization, facility, department, user, and machine.
Opt-Out Details	Displays records of activities without a biometric identification (enrollments, verifications and identifications). Includes photo-only enrollments and verifications. • photo-only enrollments • photo-only verifications • opt-out enrollments • opt-out identifications • opt-out verifications Displays the reason text selected or entered by the registrar for the opt-out activity. • If Opt-Out Tracking is disabled, or no opt-out reasons are configured, this report still records the opt-out reason as 'Registrar Declined'. The report file contains separate tabs for data by user and machine.

Authentication Reports

Authentication Reports include statistics for and individual records of successful authentications and emergency authentication attempts for all locations available to you.

Why you may use these reports:

- You want to understand the usage of PatientSecure, specific to authentications, for your organization and how well PatientSecure is being adopted.
- You want to view the usage of PatientSecure for Emergency Search in the ED.

Report	Description
Patients Found Summary	Displays counts of total patients found for the selected date range. The report file contains separate tabs for data by organization, facility, department, user, and machine.
Patients Found Details	Displays records of patients found. The report file contains separate tabs for data by user and machine.
Emergency Search Details	Displays records of all attempts to identify an unknown patient in an emergency. The report file contains separate tabs for data by user and machine.

Patients Enrolled Reports

Patients Enrolled Reports include statistics for and individual records of patients being enrolled and re-enrolled for all facilities available to you.

Why you may use these reports:

- You want to understand the usage of PatientSecure, specific to patient enrollments, for your organization and how well PatientSecure is being adopted.
- For auditing purposes, you want to view what patients have been deleted in PatientSecure.

Report	Description
Patients Enrolled Summary	Displays counts of total patients enrolled and biometric re-enrolled for the selected date range. The report file contains separate tabs for data by organization, facility, department, user, and machine.
Patients Enrolled Details	Displays records of patient enrollments and biometric re-enrollments, including demographic details. The report file contains separate tabs for data by user and machine.

Report	Description
Patients Enrolled Expanded Details	Displays records of patients enrolled, including biometric re-enrollments and deletions.
Patients Enrolled Deletion Details	Displays records of patient enrollment deletions, including demographic details and whether biometrics were deleted when the patient was deleted. For a previously deleted patient whose biometric data is subsequently removed, due to inactivity or biometric deletions made through the Delete Patients page, the report will show an additional row for that patient indicating the biometric data deletion date.
Patient ID Validation Summary	Displays counts of total enrollments with or without a valid ID, by organization, facility, department, user and machine.
Re-enrollment Details	Displays records of patient re-enrollments. Patient re-enrollments are typically performed to replace the original poor-quality enrollment scan, primarily due to improper hand placement (palm scan).
Enrollment Record Updates	Lists changes made to patient records by admin users, Link ID, or HL7 feed, and includes the reason for the change. To include changes made by HL7 feed in the report, select **Include Updates Made By HL7**. For more information, see Editing a Patient's Record and Deleting a Patient's Record.

Biometric Reports

Biometric reports include statistics for biometrics being re-enrolled and the biometric formats.

Why you may use these reports:

• You want to understand how many biometrics were re-enrolled to replace original scans.

• You want to understand where R-format biometrics were added to PatientSecure machines, in environments where Gen 1 and Gen 2 scanners are in use.

Report	Description
Biometric Re-enrollment Details	Displays records of biometric re-enrollments, including demographic details. Biometric re-enrollments are typically performed to replace the original poor-quality enrollment scan, primarily due to improper hand placement (palm scan).

Report	Description
Biometric Enrollment Format Summary	Displays counts of biometric enrollments, distributed by biometric format.
	Includes the total counts of active patients with one or more biometrics: I-Format, R-Format, Both Formats.
	This report is made available by enabling the **Use old (I-Format) biometric scan to identify patients** in client Desktop settings.
Biometric Addition Details	Displays records containing multiple formats of biometric types, where an additional biometric scan was added. Includes machine type, the biometric format added (ex. R-format), and demographic details.
	This report is made available by enabling the **Use old (I-Format) biometric scan to identify patients** in client Desktop settings.
	This report is helpful for PatientSecure environments being migrated from the Gen 1 palm scanners to Gen 2 touchless authentication palm scanners, as it reports on patient uptake of the touchless palm scanner on PCs and Kiosks machines.
Skipped Biometric Addition Summary	Displays counts of skipped biometric additions.
	Includes the total counts of times that the biometric enrollment is skipped by the user.
	The report file contains separate tabs for data by organization, facility, department, user, and machine.
	This report is helpful for PatientSecure environments being migrated from the Gen 1 palm scanners to Gen 2 touchless authentication palm scanners, as it reports on the number of times users authenticate using a dual format authentication, but then skip the addition of an R-format scan.

Audit Reports

Why you may use these reports:

You want to understand which PatientSecure administrators and users have access to certain reports.

Report	Description
Recipient List of Scheduled Reports	Displays records of the email addresses that scheduled reports were sent to.

Custom Reports

The following custom reports may be available for your installation. For more information, see your Imprivata PatientSecure representative.

Enrollment Reports	
Enrollment Expanded Details	Displays records of patient enrollments, including re-enrollments and deletions.

Configuring Report Options

Report settings determine the display of PatientSecure data in reports.

To configure report options:

1. In the Admin Console, go to **Settings > Report Options**.
2. In the **Reports** section, review the settings and make changes, as needed:

Item	Description
Report Scheduling Execution Time	Set the time of day, according to the Time Zone setting, when scheduled reports will be run. The default setting is **4:00 AM**.
Show the 'patients enrolled expanded details' report	Enable the Patients Enrolled Expanded Detailsreport, which displays displays records of patients enrolled, including biometric re-enrollments and deletions. The default setting is **OFF**.

3. *(Optional)* Configure PatientSecure utilization reporting.
   a. In the Utilization Reporting section, click **ON** to enable utilization reporting.
   b. Click **Utilization Reporting** to expand the panel and configure the remaining settings for utilization reporting.

      For more information on utilization reporting, see About Utilization Reporting.
4. In the **Email Configuration** section, configure the SMTP server connections and the handling of PatientSecure reports distributed by email.

Item	Description
SMTP server address	Type the name or IP address of the outgoing SMTP email server. For example: smtp.gmail.com. For Office365, type smtp.office365.com.
User name	Type the email address or user name, if the outgoing SMTP server requires authentication. For example: PatientSecureReports@yourOrganization.com.
Password	Type the password for the SMTP server.

Item	Description
Domain	Type the domain required for connecting to the SMTP server. Typically, only required for Microsoft Exchange Server.
SMTP port	Type the SMTP port number. This port is usually 25 or 587. The default is **587**.
Enable SSL	Set Enable SSL to **ON** if the email server requires TLS or SSL encryption. The default setting is **ON**.
Reply email address	Type an email address where emailed replies will be sent.
Reply email display name	Type the name that will be displayed for reply emails. This is the user-friendly alias for the From address. For example: PatientSecureReports.
Scheduled report subject template	Type the string to customize the Subject field of the emails. By default, the Subject template displays the following strings: `PatientSecure {ReportName} for {ReportName}` where • The {**ReportName**} value will be replaced by the name of the report. • The **{Date}** value will be replaced by the date the report was run.

Scheduled report message template	Type the string to customize the message text of the emails.
	
	 By default, the Message template displays the following strings:
	
	 `PatientSecure {ReportName} for {Date} {ReportDescription}.`
	`Warning: This email may contain PHI.`
	
	 where
	
	 • The **{ReportName}** value will be replaced by the name of the report.
	 • The **{Date}** value will be replaced by the date the report was run.
	 • The **{ReportDescription}** is the description of the report.

Scheduled report success confirmation subject template	Notification email only, the report is not included. Enter the subject template to be used for scheduled report success confirmation emails. By default, this template displays the following strings: `PatientSecure {ReportName} for {Date} Success Confirmation` where • The **{ReportName}** value will be replaced by the name of the report. • The **{Date}** value will be replaced by the date the report was run.

Item	Description
Scheduled report success confirmation message template	Enter the scheduled report message template to be used for emails. By default, this template displays the following strings: `PatientSecure {ReportName} for {Date} ran successfully. {ReportDescription}` where • The **{ReportName}** value will be replaced by the name of the report. • The **{Date}** value will be replaced by the date the report was run. • The **{ReportDescription}** is the description of the report.
Scheduled report failure alert subject template	Enter the subject template to be used for scheduled report emails. By default, this template displays the following strings: `PatientSecure {ReportName} for {Date} Failure Alert` where • The **{ReportName}** value will be replaced by the name of the report. • The **{Date}** value will be replaced by the date the report was run.
Scheduled report failure alert message template	Enter the scheduled report message template to be used for emails. By default, this template displays the following strings: `PatientSecure {ReportName} for {Date} failed to run properly. {ReportDescription}` where • The **{ReportName}** value will be replaced by the name of the report. • The **{Date}** value will be replaced by the date the report was run. • The **{ReportDescription}** is the description of the report.
Send test email	To send a test email through the configured SMTP server to verify the configuration: Type an email address in the box, and click **Test**. The email address entered will not be saved to the system, it is simply used to verify the configuration.

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

Running or Scheduling a Report

You can run a report on a one-time basis or schedule a report to run at an interval you specify.

Imprivata PatientSecure reports are exported to an Excel (.XLSX) file or a .CSV file in the Downloads folder on your local drive or, for scheduled reports, to a file share location.

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

Running a Report

To run a report on a one-time basis:

1. In the Admin Console, go to **Reports > Run or schedule a report** .

   The Reports page lists the available [report types](#).

2. Select the report type. The report form opens.

   > **ⓘ TIP:**
   > You can also access the Interactions Summary, Machine Activity, and User Activity report forms directly from the **Reports > Quick Links** submenu.

3. Select **One-time** (default) to run the report when you complete the report form and click **Go**. The report will run once and will not run again.

4. In the Data Parameters sections, specify how you wish the data to be handled:

   a. For Interactions Summary reports, select the time interval to group the data by: **daily**, **weekly**, **monthly**, **quarterly**, or **yearly**.

   a. In the Time Filters section, enter the start date and end date range, or click 🗓 and select the dates.

5. In the Locations / Machines section, select the location data to include in the report: **Organizations**, **Facilities**, **Departments**.

   - For Machine Scans report:

     ○ Select one or more machines from the **Machines** box.

     ○ Select **Only include machines with no scans** to limit the report to those machines with no PatientSecure scans.

   - For User Scans report, select one or more users from the **Users** box.

     > **ⓘ TIP:**
     > Start typing the location name: the type-ahead control displays matching names for you to select. You can add more than one available organization, facility, and department.
     >
     > To remove a location from the list, click **x** next to the name.

   - For Interactions Summary reports, select the interactions to include in the report:

- In the Include Interactions section, select **Authentications**, **Failed Authentications**, **Enrollments**, or **Opt-outs** to include in the report.
- In the Include Totals section, the **Yes** option is selected by default. This option controls whether or not to include the totals in the Interactions Summary report.

6. In the Output Format section, for **File Type**, select either **Excel** or **CSV**.

7. When you are done, click **Go**.

The report is exported to an Excel (.XLSX) file or .CSV file in the Downloads folder on your local drive. The report type and date run comprise the report file name. If this name is in use, then Imprivata PatientSecure appends a number (1, 2, 3, etc.) to the report name.

For reports with multiple worksheets, when you select the CSV format, each worksheet is created as a separate CSV file with the worksheet name appended to the filename.

For reports that are run immediately, the CSV files are bundled into a .ZIP file, available for download.

> **NOTE**: A one-time report can display up to 100,000 records.

Scheduling a Report

To schedule a report to run daily, weekly, or monthly schedule:

1. In the Admin Console, go to **Reports > Run or Schedule a Report**.

   The Reports page lists the available report types. A list of recently run scheduled reports, if any, appears on the right.

2. Select the report type. The report page opens.

3. Select the schedule frequency:
   - **Daily** runs the report every day.
   - **Weekly** runs the report once a week, starting on the day you select.
   - **Monthly** runs the reports once a month, starting on the first of next month.

4. Specify the date range for the data: **last day** (the day before the report is run) or **current year** (to date).

5. In the Output Format section, for **File Type**, select either **Excel** or **CSV**.
   - For reports with multiple worksheets, when you select the CSV format, each worksheet is created as a separate CSV file with the worksheet name appended to the filename.
     - For scheduled reports, the CSV files are bundled into a .ZIP file that is saved to the scheduled reports output folder on the fileshare.
     - For emailed reports, the CSV files are attached to the email as separate attachments. The total size of all attachments will not exceed 20 MB.

6. Enter a unique, descriptive report name in the **Report Name** box.

To avoid overwriting scheduled reports, the date when the report is run will be appended to the file name.

7. Select an export file share from the **File Share** list. Optionally enter a subfolder name in the subfolder box.

8. To add a new file share for this report, click **Add a new file share.**

9. Optionally, specify email parameters for sending this scheduled report to the configured reports email addresses.

    Requires that an SMTP server connection is configured in Report Options.

    a. To enable the setting, click **Send email using the configured settings on the Report Options page.**

    b. In the **To address** box, enter the email address of the recipient. For multiple recipients, separate the addresses by a semicolon.

10. When you are done, click **Save**.

The report is added to the Scheduled Reports page. When the report is run at the default run time of 08:00 UTC, it is stored in an Excel (.XLSX) file in the export file share (or subfolder) that you specified.

The report continues to run at the specified interval until you edit or delete it.

> ⓘ **NOTE:**
> Scheduled reports can display up to 500,000 records.

Working with Scheduled Reports

- To schedule a report, click **Create or schedule a report**. For more information, see Scheduling a Report.

- To filter the reports, select **Show only my reports**.

- To view a report, locate the report in the list.
    - The **Output File** column indicates the file share location where the report exists. The report is saved to the scheduled reports output folder or subfolder. Click **Download** to download a copy of the report.
    - The **email status** column indicates the status of emailed reports; whether the email was successful, there were errors, or no information.

- To view a history of the scheduled report, click **History**. The run history of the selected report is displayed on the **Report history** page.

- To edit a report, click **Edit** for the selected report. Make your changes to the report options and save.

- To re-run a failed scheduled report with the same parameters, click **Re-run**. The report will be added to the queue, but may take some time to run.

- To delete a report, click **Edit** for the selected report. On the Edit Report dialog, click **Delete.**

- All users can view the full list of scheduled reports, but cannot view the actual data contained within each report.
- Only Administrators and Owners may edit or delete a report created by another user.

Report History

The Report History page displays the history of a scheduled report, including the owner, date, output file, email status, and any errors.

- Narrow your search by filtering by **Errors only** or **Only my reports**.
- For reports with output files, click **Download** to download a copy of the report.
- For reports that failed, click **Re-run** to run the scheduled report again with the same parameters. The report will be added to the queue, but may take some time to run.

About Utilization Reporting

Utilization reporting allows you to gain an accurate insight into the utilization of Imprivata PatientSecure at the registration workstations.

With this insight, customers can make more informed decisions regarding the adoption of Imprivata PatientSecure and take proactive measures to address any concerns with usage below acceptable standards.

When enabled, Utilization Reporting displays utilization metrics in the Dashboard charts, including a utilization goal line. Enabling Utilization Reporting also makes the Utilization report available.

The Dashboard displays utilization data for the File Upload method only if locations are included. If the file upload is performed by user only, the utilization data will not be displayed on the Dashboard.

Calculating the Denominator for Utilization

Utilization Determined by Registrar Declines

This method of Utilization Reporting depends on the number of times registrars decline to use PatientSecure.

When **Registrar Declines** is selected:

Utilization % =	$\dfrac{\text{Patients Found + Patients Not Found + Patients Enrolled}}{\text{Patients Found + Patients Not Found + Patients Enrolled + Registrar Declines}}$

> **(i) NOTE:**
> Photo-only is not included in the numerator or the denominator.

Utilization Determined by Patient Opt-Outs

This method of Utilization Reporting depends on using data from the Patient Opt-out tracking feature and photo-only workflows, if enabled.

When **Patient Opt-Outs** is selected:

Utilization % =	$\dfrac{\text{Patients Found} + \text{Patients Not Found} + \text{Patients Enrolled}}{\text{Patients Found} + \text{Patients Not Found} + \text{Patients Enrolled} + \text{Patient Opt-Outs} + \text{Photo-only}}$

> **(i) NOTE:**
> Photo-only is not included in the numerator, but is in the denominator.

Utilization Determined by File Upload

This method of Utilization Reporting depends on information from outside of PatientSecure. In this case, PatientSecure is reliant on registration data from your EMR or ADT system to generate a number (the denominator) which is used to calculate the utilization percentage.

For more information, see Calculating PatientSecure Interactions.

You create the registration data to be used for calculating the denominator from your EMR/ADT system and upload it to PatientSecure through a file share location. You can create the file by various means, such as EMR reporting tools, or third party reporting tools and reports on registration data from your source EMR/ADT system.

For more information, see Registration Data Files Types.

> **(i) IMPORTANT:**
> You must create the file containing registration data from your EMR or ADT system; it cannot be created by PatientSecure.

Count Opt-Outs towards Utilization Percentages

PatientSecure includes the ability to decide whether patient opt-outs and photo-only opt-outs are counted as part of the utilization equation.

The ability to count patient opt-outs as part of PatientSecure utilization percentages relies on two settings being enabled:

- the **Opt-out Tracking** setting.
- the **Count Opt-outs Toward Utilization %** setting.

Opt-out Tracking disabled and Count Opt-outs towards Utilization % enabled	Opt-out Tracking and Count Opt-outs towards Utilization % enabled
$$\frac{(Patients\ Found + Patients\ Not\ Found + Patients\ Enrolled + Photo\text{-}Only)}{Registrations}$$	Adds Total opt-outs to the equation: where **Total opt-outs**= Photo-Only + Patient Opt-outs So that the equation is now: $$\frac{(Patients\ Found + Patients\ Not\ Found + Patients\ Enrolled + \textbf{Total Opt-outs})}{Registrations}$$

> **NOTE:**
> There may be a discrepancy between the counts displayed in the Dashboard for activities versus the counts reported by utilization reporting, depending on whether the **Count Opt-outs toward Utilization %** is enabled.

Configuring File Shares

Configure file share locations for PatientSecure for the following purposes:

- to monitor for new periodic admissions data as part of the Utilization Reporting feature.
- as an output location for scheduled reports.

Before You Begin

Before you begin, consider the following information:

- The file share locations must exist in your application server environment before you configure it in the Admin Console.
- You must configure separate files share locations for use with Utilization Reporting and Scheduled Reports. You cannot reuse a file share location used by Utilization Reports for the scheduled reports.
- Ensure that the user account has appropriate read and write access for the file share location.

  For FTP file shares, the user account must have write access to the FTP location and create directory access for saving reports to a subfolder on the FTP share.
- The file share location does not support SFTP types that require the PatientSecure client to accept a host key.

Add a File Share

To add a file share:

1. In the Admin Console, go to **Settings > File Shares**.
2. Click **Add a new file share** and enter the following information:
   a. **Protocol Type** Select a file share protocol from the drop-down list.
   b. **Server.** Enter the information that corresponds to the file share protocol selected:
      - For an FTP site, enter the FTP address and port number.

        For example:

        ftp://myServer.myDomain and port 21
      - For a Network share, enter the Uniform Naming Convention (UNC) path to a file share in the **Server** box.

        For example:

        \\myServer.myDomain\myShare

        \\myServer.myDomain\C$\myShare
      - For a SSH File Transfer Protocol (SFTP) site, enter the SFTP address and port number.

        For example:

        sftp://myServer.myDomain and port 22.
      - For an Imprivata FairWarning SFTP site, enter the SFTP address and port number supplied by the Imprivata FairWarning customer support team.

        Only applies to a [PatientSecure integration with Imprivata FairWarning.](#)
   c. **Account Username:** Enter the domain and username for an account with read and write access to the file share.

      For example:

      myDomain\myUserName

      For an Imprivata FairWarning SFTP site, enter the username supplied by the Imprivata FairWarning customer support team.
   d. **Account Password:** Enter the password for the account to access the file share.
3. Click **Save.**

Edit a File Share

To edit a file share:

1. From the Admin Console menu, select **Settings > File Shares**.
2. Select a file share from the list and click its row. The Edit File Share dialog opens.
3. Edit the settings as needed and click **Save.**

Registration Data Files Types

> **NOTE:**
> This topic applies to the File Upload method of calculating utilization only. For more information, see File Upload

At a high level, the File Upload method of Utilization Reporting can process two different types of file upload: Summary Uploads and Detailed Uploads.

Depending on the reporting capabilities of your EMR/ADT system, you may choose one file type to generate over the other.

Registrations are patient admissions or check-ins.

Plan for Gathering Registration Data for File Upload

Registration Data Considerations

There are some important points to consider as you create this registration data file:

- Compare the location hierarchy in PatientSecure to the location hierarchy in your source EMR/ADT system.

  For example:

  - Is the PatientSecure location of "Primary Care" named the same in your EMR/ADT hierarchy?

  - Or is it named differently, such as "Dept-Primary Care"?

    If they are different, you could ensure that the file you generate lists the department name as it exists in PatientSecure, or you can ensure the department is mapped correctly.

- Keep location names across multiple facilities and organizations in mind.

  Scenario:

  If you have three facilities with the same location of Emergency Dept, make sure they are mapped correctly to your PatientSecure locations for accurate reporting.

- Consider the visit types for a department and determine whether you want all of them, or a subset, to be counted towards the registrations.

  Scenario:

  In a department you may have three different visit types such as Adult, Pediatric and Other. You may decide that only the visit type of Adult should be summed up for the department.

- The Dashboard displays utilization data for the File Upload method only if locations are included. If the file upload is performed by user only, the utilization data will not be displayed on the Dashboard.

Examples

Different EMR/ADT systems can have different reporting capabilities. Utilization Reporting is flexible so that you have some options when generating the data source file from your EMR/ADT system.

Example 1 - Summary Level Report for a Department

Your source system may only be able to report data at a summary level for a department. In this case, an example report may look similar to the following:

Column 1	Column 2	Column 3
7/31/19	Emergency Dept	550
7/31/19	Primary Care	210

In this example, each row is the total count of registrations for a particular department for the month of July 2019.

See Summary Uploads.

Example 2 - Detail Level Report for a Department

By comparison, if your source system generates a data file at a detailed level for a department, then your example report may look similar to the following:

Column 1	Column 2
7/11/19 09:30	Emergency Dept
7/11/19 10:15	Emergency Dept
7/15/19 19:30	Emergency Dept

In this example, each row represents a registration event. If the Emergency Dept had 600 registrations for the month of July 2019, the file would have 600 rows.

See Detailed Uploads

You have the option to either create a new report, or you can leverage an existing report. When leveraging an existing report, you can designate the columns that PatientSecure should use.

For more information, see Configuring Utilization Reporting.

Quick Start for File Upload

To get started quickly with Utilization Reporting using the File Upload method, we recommend that you create a new report from your EMR/ADT system at a summary level for your departments.

This will give you a good insight into the utilization of PatientSecure at a department level, and should be a relatively easy report to generate.

Before You Begin

Before you begin, review the following requirements:

- **Configure a file share location for uploading registration data files.** PatientSecure monitors the file share for the periodic registration data files. See Configuring File Shares.
- **Periodic registration data files from your EMR system**. Create or obtain the data files according to the following requirements:

- **File formats:** CSV, XLS, XLSX.
- **File Size limit:** 500 MB.
- **Unique file and contents:** Ensure that the file name is unique and that you do not append new data to an already-processed file.
- **File contents:** For information on the registration data types, see Registration Data Files Types

> 💡 **BEST PRACTICE:** We recommend that you upload registration data files on a daily or weekly basis.

Date and Time Considerations

Consider the following items with respect to date and time stamp data in the registration data files you upload to utilization reporting:

- **Date and time stamps are supported for summary and detailed uploads.** Detailed uploads require a date and time stamp. For more information, see Registration Data Files Types.

  For summary uploads, time stamps are not required, but if you do not supply a time stamp column in the data file, PatientSecure sets the time of each registration to 12 noon.

- **Time Zone of Admin Console.** Utilization Reporting captures the time stamp according to the Admin Console's time zone. Changing the time zone of the Admin Console component will not change past utilization data.

Summary Uploads

Summary User

Contains summary registration counts by user.

PatientSecure ties the user from the user field to the PatientSecure user to derive the department and then uses the associated date and registrations to fill in reporting data to the appropriate utilization metric.

Summary data files may be less accurate, especially when the user moves between multiple departments.

The uploaded file must contain the following columns:

- Date
- User
- Registrations count

  Extra columns in the file are ignored.

Summary - Location

Contains summary registration counts by location.

PatientSecure needs to create a mapping from the supplied location to a PatientSecure department and then uses the associated date and registrations columns to fill in reporting data to the appropriate utilization metric.

To define your location by Department only, the file must contain the following columns:

- Date
- Department
- Registrations count.

To define your location by Facility and Department, the file must contain the following columns:

- Date
- Facility
- Department
- Registrations count

To define your location by Organization, Facility and Department, the file must contain the following columns:

- Date
- Department
- Facility
- Organization
- Registrations count

Summary - User and Location

Summary - User and Location

Contains summary registration counts by user and location.

PatientSecure needs to create a mapping from the supplied user and department to a PatientSecure department and then uses the associated date and registrations columns to fill in reporting data to the appropriate utilization metric.

To define your user and location by Department only, the file must contain the following columns:

- Date
- User
- Department
- Registrations count

  Extra columns in the file are ignored.

To define your user and location by Facility and Department, the file must contain the following columns:

- Date
- User
- Facility

- Department
- Registrations count

    Extra columns in the file are ignored.

To define your user and location by Facility, Department and Organization, the file must contain the following columns:

- Date
- User
- Facility
- Department
- Organization
- Registrations count

    Extra columns in the file are ignored.

Detailed Uploads

Detail - User

Contains detailed data about each registration. Each row represents a patient registration by a particular user.

PatientSecure ties the user from the user field to the PatientSecure user to derive the location and then uses the associated date and registration to fill in reporting data to the appropriate utilization metric.

> (i) **NOTE:** A data file containing detailed data must contain a row with the date and time stamp, not just a date stamp

The file must contain the following columns:

- Date and time stamp
- User

    Extra columns in the file are ignored.

Detail - Location

Each row represents a patient registration at a particular location.

PatientSecure ties the user from the user field to the PatientSecure user to derive the location and then uses the associated date/time and registration to fill in reporting data to the appropriate utilization metric.

> (i) **NOTE:** A data file containing detailed data must contain a row with the date and time stamp, not just a date stamp.

To define your location by Department only, the file must contain the following columns:

- Date and time stamp

- Department

To define your location by Facility and Department, the file must contain the following columns:

- Data and time stamp

- Facility

- Department

To define your location by Organization, Facility and Department, the file must contain the following columns.

- Data and time stamp

- Facility

- Department

- Organization

Detail - User and Location

Contains detailed data about each registration by user and department.

The department is the main criterion from which utilization is measured and the user is matched to the PatientSecure user in the same manner as the other data file types.

> **ⓘ** **NOTE:** A data file containing detailed data must contain a row with the date and time stamp, not just a date stamp.

To define your user and location by Department only, the file must contain the following columns:

- Date and time stamp

- User

- Department

  Extra columns in the file are ignored.

To define your user and location by Department and Facility only, the file must contain the following columns:

- Date and time stamp

- User

- Department

- Facility

  Extra columns in the file are ignored.

To define your user and location by Department, Facility, and Organization, the file must contain the following columns:

- Date and time stamp

- User

- Department
- Facility
- Organization

    Extra columns in the file are ignored.

Configuring Utilization Reporting

Enable utilization reporting, specify the method by which PatientSecure will calculate the utilization, and configure user and location mapping options.

Enable Utilization Reporting

To enable utilization reporting:

1. In the Admin Console, go to **Settings > Report Options**.
2. In the Utilization Reporting section, click **ON** to enable utilization reporting.
3. Click **Utilization Reporting** to expand the panel and configure the remaining settings for utilization reporting.
4. Select one of the three following methods for calculating the utilization percentage - **Registrar Declines**, **Patient Opt-Outs** or **File Upload**.

Registrar Declines

By using the **Registrar Declines** method, PatientSecure calculates the utilization percentage by the number of times registrars decline to use PatientSecure. This is the simplest method for utilization but gives less insight into why PatientSecure was not utilized.

For more information on how PatientSecure calculates utilization with this method, see Utilization Determined by Registrar Declines

To calculate utilization percentage by the Registrar Declines method:

1. In the Admin Console, go to **Settings > Patient Opt-Outs** and disable the Patient Opt-Out Tracking setting.
2. Go to **Settings > Report Options** and select **Registrar Declines**.

Patient Opt-Outs

By using the **Patient Opt-Outs** method, PatientSecure calculates the utilization percentage by using data from the Patient Opt-out tracking feature and photo-only workflows, if enabled.

This method delivers detailed insight into the reasons for why PatientSecure was not utilized. For more information on how PatientSecure calculates utilization with this method, see Utilization Determined by Patient Opt-Outs.

To calculate utilization percentage by the Patient Opt-Outs method:

1. In the Admin Console, go to **Settings > Patient Opt-Outs** and enable the Patient Opt-Out Tracking setting.

2. Go to **Settings > Report Options** and select **Patient Opt-Outs**.

File Upload

PatientSecure calculates the utilization percentage by leveraging information from your EMR or registration system. The files you upload from your EMR or registration system enable you to map PatientSecure usage to individual visits.

The File Upload method of calculating utilization percentages requires several additional prerequisites and considerations, and several additional configuration tasks than the other methods. For more information on how PatientSecure calculates utilization with this method, see Utilization Determined by File Upload

Before You Begin

Before you begin, review the following requirements:

- **Configure a file share location for uploading registration data files.** PatientSecure monitors the file share for the periodic registration data files. See Configuring File Shares.
- **Periodic registration data files from your EMR system**. Create or obtain the data files according to the following requirements:
  - **File formats:** CSV, XLS, XLSX.
  - **File Size limit:** 500 MB.
  - **Unique file and contents:** Ensure that the file name is unique and that you do not append new data to an already-processed file.
  - **File contents:** For information on the registration data types, see Configuring Utilization Reporting

> 💡 **BEST PRACTICE:** We recommend that you upload registration data files on a daily or weekly basis.

Date and Time Considerations

Consider the following items with respect to date and time stamp data in the registration data files you upload to utilization reporting:

- **Date and time stamps are supported for summary and detailed uploads.** Detailed uploads require a date and time stamp. For more information, see Registration Data Files Types.

  For summary uploads, time stamps are not required, but if you do not supply a time stamp column in the data file, PatientSecure sets the time of each registration to 12 noon.
- **Time Zone of Admin Console.** Utilization Reporting captures the time stamp according to the Admin Console's time zone. Changing the time zone of the Admin Console component will not change past utilization data.

Specify a File Share Location

To specify a file share location for uploading registration date files:

- Select an existing file share location from the **Data Source File** drop-down list.
  - (Optional) Enter a subfolder name in the **Subfolder** box.
- Click **Add a new file share** to add a file share location. See Configuring File Shares.

Define the Data Format

In the Data Format area, define how your registration data files are structured: by detailed events or by a summary count.

1. In the **Each row represents** section, specify **detailed event** or **summary count**.
2. In the **Data is listed by section**, specify whether the data is listed by **user**, **location** or by **user and location**.

   For more information on registration data file types you can upload to PatientSecure, see Registration Data Files Types.
3. If your registration data file contains a header row, select **File includes header row**.
4. In the **Date Format** box, specify the date format used in your registration date file.

   For example:

   MM/dd/yyyy

   MM/dd/yyyy HH:mm

> (i) **NOTE:** Registration data files with detailed events must include a date and time stamp.

Define the Data Columns

With your registration data file as a guide, define the column numbers where the data resides.

Enter the column number representing the type of data, as it appears your registration data file.

- If you selected the **location** option for **Data is listed by**, the **Department** column is required.
- If you specify a column for **Organization**, the **Facility** and **Department** columns are also required.

Example 1

For a summary count by user:

Column 1 is the Date

Column 2 is the User

Column 4 is the registration count

Example 2

For a detailed report by user:

Column 3 is the User

Column 1 is the Date/Time

Example 3

For a detailed event report by user and location, where the Organization, Facility and Department are included in the registration data file:

Column 4 is the User

Column 3 is the Department

Column 2 is the Facility

Column 1 is the Organization

Column 5 is the Date/Time

User Mapping

Map the users specified in your registration data files to PatientSecure users.

The **User in File** list displays any unknown users that occur in the registration data file.

> **BEST PRACTICE:**
> To maintain the most accurate registration data, you should map as many unknown users as possible to PatientSecure users. If you are unable to map certain unknown users to PatientSecure users, it is a best practice to map them to an easily-identifiable test or junk user.

- To display only unmapped users, select **Show only unmapped users.**
- To map the unknown user to a PatientSecure user, select a user name from the **PatientSecure User** drop-down list.
- To filter the results, click the filter icon, select **Contains** or **Starts With** and enter a string in the field. Click **Filter**.
- To remove a specific user mapping, click **Clear Selection**.

Location Mapping

The **Location in File** list displays any unknown departments that occur in the registration data file.

> **BEST PRACTICE:**
> To maintain the most accurate registration data, you should map as many unknown locations as possible to PatientSecure departments. If you are unable to map certain unknown locations to PatientSecure departments, it is a best practice to map them to an easily-identifiable test or junk department.

- To display only unmapped departments, select **Show only unmapped locations.**
- To map the unknown location to a PatientSecure location, select a department name from the **PatientSecureLocation** drop-down list.
- To filter the results, click the filter icon, select **Contains** or **Starts With** and enter a string in the field. Click **Filter**.
- To remove a specific location mapping, click **Clear Selection**.

User Mapping Upload

Export or import a CSV file containing the mapping of your EMR's user names to PatientSecure user names.

Download the current PatientSecure user name mapping to use it as a template when comparing user names from your EMR to those in PatientSecure.

File Upload Requirements

Before you begin, review the following requirements of the upload file:

- **File formats:** CSV.
- **File Size limit:** 500 MB.

Download the current user name mappings file

To download a the current PatientSecure user name mapping file:

1. Click **Download**.

   The current user name mapping file is saved to your computer's download directory.

   The file contains rows of the current mappings of EMR to PatientSecure user names.

   Unmapped users in PatientSecure are indicated by a blank cell in the **PatientSecure User** column.

2. Edit the file as needed to map the unmapped user names to PatientSecure users and save the file.

Upload a user name mappings file

After downloading and editing the user mappings file as needed (see above), upload the file.

To upload a user name mapping file:

- Click **Upload**. In the File Upload dialog, enter the path or browse to the file location and click **Upload**.

Troubleshooting

If there are errors from the import, view the error logs for more details.

Specify a Utilization Goal

- In the **Utilization Goal** box, specify a utilization goal (in percent) for PatientSecure utilization.

  The Dashboard charts will display a utilization goal line as one of the chart elements.

Count Opt-outs toward Utilization %

> **ⓘ NOTE:**
> This option is displayed when you select **File Uploads** as the utilization calculation method. It does not apply to the **Registrar Declines** or **Patient Opt-Outs** methods of calculating utilization.

When enabled, opt-outs will be counted towards the utilization percentage.

Opt-outs include:

- photo-only enrollments and verifications
- patient opt-outs (when Opt-Out Tracking is enabled).

Click the **ON/OFF** slider to toggle the setting.

The default setting is **OFF**.

Include Patients Not Found in Utilization Reporting

> **ⓘ NOTE:**
> This option is displayed when you select **File Uploads** as the utilization calculation method. It does not apply to the **Registrar Declines** or **Patient Opt-Outs** methods of calculating utilization.

When enabled, **Patients not found** will be counted towards the utilization percentage.

Patients not found include:

- failed verifications
- failed identifications
- failed emergency searches

Click the **ON/OFF** slider to toggle the setting.

The default setting is **ON**.

This setting affects the PatientSecure dashboard and reports in the following ways:

When enabled:

- The Utilization Summary report displays:
  Total PatientSecure Interactions = Patients Found + Patients Not Found + Patients Enrolled + Total Opt-outs
- The PatientSecure dashboard, Interactions Summary report, and Utilization Summary report display:
  Utilization = (Patients Found + Patients Not Found + Patients Enrolled + Total Opt-outs*) / Registrations
  - Patients Not Found counts continue to appear

When disabled:

- Utilization Summary report displays:

  Total PatientSecure Interactions = Patients Found + Patients Enrolled + Total Opt-outs*

  Patients Not Found counts do not appear

- The PatientSecure dashboard and Interactions Summary report display:

  Patients Not Found counts continue to appear

- The PatientSecure dashboard, Interactions Summary report, and Utilization Summary report display:

  Utilization = (Patients Found + Patients Enrolled + Total Opt-outs*) / Registrations