imprivata®

Product Documentation

Imprivata Digital Identity Reference Architectures for Epic Customers

Imprivata Enterprise Access Management

Last Updated: January 2025

Contacting Imprivata

20 CityPoint, 480 Totten Pond Road, 6th Floor

Waltham, MA 02451 USA

Phone: 781-674-2700

Toll-Free: 1-877-OneSign

Fax: 1 781 674 2760

Support: 1 800 935 5958 (North America)

Support: 001 408-987-6072 (Outside North America)

https://www.imprivata.com

support@imprivata.com

Copyright and Legal Information

Trademark Information

Legal Notices

Document revision

Table of Contents

Chapter 1: Introduction

This resource provides common clinical workflows and recommended reference architectures for implementing Imprivata Enterprise Access Management (formerly Imprivata OneSign and Imprivata Confirm ID). Reference architectures represent proven configurations that:

- Have been designed around the clinician experience.
- Have been successfully implemented by many Imprivata customers.
- Provide a cornerstone of technical guidance that has been developed by delivery teams at Imprivata and are foundational to the testing and development methodologies at Imprivata.

By following these recommendations, you can expect to minimize the time spent with and reduce the operational risks involved in the planning, design, and implementation of Imprivata Enterprise Access Management and Imprivata Mobile Access Management (formerly GroundControl) solutions with Epic.

1.1 Intended Audience

This resource is intended for:

- Decision makers who are involved in selecting the end user computing and mobile workflows to integrate with Epic in a particular clinical setting.

  This includes CMIOs, CIOs, application analysts, and IT and end user computing architects.
- Technical stakeholders that are responsible for ensuring that existing or to–be–purchased technical infrastructures and components are compatible with the recommended options.

  This includes IT architects, Imprivata implementation partners, and Imprivata's customer-facing resources.

Readers should have a thorough understanding of:

- Common end user computing and mobile clinical workflows including, but not limited to, those that are used with Epic EHR and Epic Rover in exam rooms, nursing stations, physician loungers, and emergency departments.
- Imprivata Enterprise Access Management and its capabilities for delivering single sign-on (SSO), advanced authentication and application and virtual desktop access.
- Imprivata Enterprise Access Management and its capabilities for delivering multifactor authentication workflows including support for Electronic Prescribing of Controlled Substances (EPCS) and Epic Code Narrator.
- Imprivata Mobile Access Management for mobile device provisioning and delivering check-in / check-out and application credential autofill workflows for shared mobile devices.
- Application and desktop virtualization technologies like Citrix DaaS (formerly Citrix XenApp, XenDesktop, and Virtual Apps and Desktops) and Omnissa Horizon (formerly VMware Horizon).
- The differences between Microsoft Windows-based "thick clients" and non-Windows-based "thin or zero clients".

- MDM solutions such as Omnissa Workspace ONE (VMware Workspace ONE), Microsoft Intune, and Jamf Pro.

1.2 How to Use This Guide

It is recommended that thisguide should be used in conjunction with architectural design assistance from an Imprivata pre or post–sales consultant.

The purpose of this information is to help you:

Goal	Where to Begin
Select a clinical workflow for your environment.	If you are involved in the design of the end user computing clinical workflow experience, begin with common clinical workstation workflows. Each workflow includes a list of common clinical settings, such as use in exam rooms or private offices, as well as considerations for each setting.
Understand the Imprivata enterprise architecture	If you are tasked with implementing Imprivata begin with the Imprivata Digital Identity Solutions Overview and Architecture. This chapter describes the various components of the Imprivata digital identity solution and how they can be configured to scale and support thousands of clinical workstations and end users.
Select a technical reference architecture for implementation	If you have selected a clinical workstation workflow, review the respective reference architecture for implementation. Workflows typically include several reference architectures in support of a variety of end-user computing and mobile technologies, including: • Application virtualization • VDI • Thin and zero clients

Additional Resources

See the following Imprivata documentation when designing and implementing the digital identity reference architectures:

- Imprivata Supported Components Guide - for maintained releases of Imprivata Enterprise Access Management for SSO and MFA.
- Imprivata Mobile Access Management online documentation - for supported Mobile Device Management (MDM) solutions, as well as configuration documentation for implementing shared mobile device workflows.
- Imprivata Documentation portal - for detailed information on configuring EAM to build the workflows listed in this guide.
- Imprivata Connector for Epic Hyperdrive Configuration Guide - for detailed information on configuring the Imprivata Connector for Epic Hyperdrive.

Chapter 2: Common Clinical Workstation and Mobile Workflows

Clinical workstations refer to desktop computing platforms running Microsoft Windows or lightweight operating systems used to remotely connect to virtualized applications and desktops. They can generally be grouped into two main categories:

- Shared workstations

  Shared workstations, often called kiosks or public workstations, are commonly used in areas where many different users require fast access to clinical applications for a limited period of time. Electronic prescribing and approval workflows may also be commonly encountered on these workstations. ,These workstations are typically found in patient rooms, exam rooms, nursing stations, and physician documentation areas.

- Private workstations

  Private workstations are commonly used by a single user who requires access to one or more applications for a prolonged period of time. These workstations are typically found in a private location, administration area, or specialty areas such as radiology.

The following table provides a summary of workstation configurations and the common clinical setting for which they are suited. Additional information about each clinical workflow and the recommended reference architectures is available is this chapter.

Workstation Configuration	Common Clinical Setting
Shared with Epic EHR	Used in settings where there is direct interaction between the patient and the provider. For example – exam rooms or inpatient rooms. Detailed Architecture
Shared with roaming applications	• Used in most clinical settings. • Not recommended for settings where the patient record must remain persistent on the workstation for different users to access, such as in an exam room setting. Shared workstation with roaming applications
Shared with roaming virtual desktop	• Used in most clinical settings. • Not recommended for settings where the patient record must remain persistent on the workstation for different users to access, such as in an exam room setting. Shared workstation with roaming virtual desktop

Workstation Configuration	Common Clinical Setting
Private workstation	Used in a private location, administration area, or specialty areas (such as radiology) where a limited number of users require access. For example – a physician office or loung , or an administration area that is only used by unit coordinators. Private workstation

Clinical mobility can generally be grouped into three main categories:

- Shared mobile devices

  Devices owned and managed by the institution using Mobile Device Management that are commonly used in areas where many different users, primarily nurses, EVS, and ancillary services, utilize a common supply of mobile devices for set periods of time, often shift based. These devices are typically checked out of a central location on each unit or floor, but then utilized across the entire facility including but not limited to patient rooms, exam rooms, nursing stations, and physician documentation areas. The devices are managed by Mobile Device Management.
- Single user mobile devices

  Devices are owned and managed by the institution using Mobile Device Management and used perpetually by a single user both inside and outside the hospital, most commonly by physicians.
- Clinician owned devices (BYOD)

  Privately owned devices, often purchased by the individual and used by a single user both inside and outside the hospital.

The following table provides a summary of mobile device configurations and the common clinical setting for which they are suited. Additional information about each clinical workflow and the recommended reference architectures is available is this chapter.

Workflow	Common Clinical Setting
Shared mobile devices	Used throughout every major venue of the hospital from EVS staff to laboratory to bedside patient care environments

2.1 Shared Workstation with Epic EHR

The shared workstation with Epic EHR configuration gives users fast access to the workstation and the EHR:

- The EHR is not closed on user switch.
- Other applications, such as web browsers and email, are closed on user switch.
- Typically used in locations where there is direct patient-provider interaction, such as in exam rooms and inpatient rooms.

2.1.1 Clinical Workflow

The following describes the workflow:

	User 1 (nurse) taps their proximity card to authenticate to a shared workstation that is secured by Imprivata Enterprise Access Management. • The Epic EHR is already running (persistent), and the nurse is automatically signed in. • The nurse may choose to open additional applications, which can be configured for SSO, if required.
	When the nurse is finished, they tap their proximity card to secure the workstation. All of the applications that were in use by the nurse remain running, including the Epic EHR, but are now secured behind the Imprivata lock screen.
	User 2 (physician) taps their proximity card to authenticate to the shared workstation. • All of the nurse's applications are closed and the Epic EHR is automatically signed in as the physician. • The physician may choose to open additional applications, which can be configured for SSO, if required.
	The physician may need to electronically prescribe medications or sign off on attestation workflows with the EHR using single- or multifactor authentications. Using Imprivata Enterprise Access Management, the most efficient authentication options are presented to the physician, depending on the specific workflow requirements, the physician's enrolled authentication methods, and the authentication methods available at that workstation.
	When the physician is finished, they tap their proximity card to secure the workstation. All of the applications that were in use remain running, including the Epic EHR, but are secured behind the Imprivata lock screen.
	The physician returns to the same workstation, during a period of time in no other users have authenticated to that workstation, and taps their badge. The physician has immediate access to all of the applications that were previously being used, including the Epic EHR.

2.1.2 Reference Architectures

You can implement this workflow on Windows workstations, as well as thin and zero client endpoints.

- Windows

  In environments with Windows–based workstations, Epic is typically delivered to the desktop via an application virtualization technology.

  For example – Citrix DaaS.

- Thin or zero client

In environments with thin or zero clients, there are three options for delivering Epic to the desktop.

- Option 1 — With this option, the Epic client is installed to a virtual desktop, and the endpoint is configured to maintain a persistent connection with the desktop. This is also known as a single hop.
- Option 2 — With this option, there is a persistent VDI connection. However, Epic is delivered to the virtual desktop via an application virtualization technology.

  For example — Citrix DaaS. This is also known as a double hop.
- Option 3 — With this option, there is a virtual application connection where Epic is delivered directly to the thin or zero client via an application virtualization technology.

> **NOTE**: For information about the technology and a summary of the configurations, see Shared workstation with Epic EHR.

2.2 Shared Workstation with Roaming Applications

The shared workstation with roaming applications configuration lets users move from workstation to workstation and automatically connect to one or more applications, including the Epic EHR:

- The applications are delivered via application virtualization technology.
- As a clinician authenticates to different shared workstations, they reconnect to their application virtualization session.

  This makes it appear as if the applications are "roaming" with them.
- The Epic EHR will either have closed all non-roaming enabled activities or completely restarted.
- Can be used in most clinical settings. It is not recommended for settings where the patient's medical record needs to remain persistent on the workstation for different users to access, such as in an exam room.

2.2.1 Clinical Workflow

The following describes the workflow:

	User 1 (physician) taps their proximity card to authenticate to a shared workstation that is secured by Imprivata Enterprise Access Management. • The roaming applications, including the Epic EHR, are automatically launched for the physician. • The physician is automatically signed in to the applications.
	When the physician is finished, they tap their proximity card to secure the workstation. Securing the workstation disconnects the roaming applications from the workstation.

	The physician continues their rotation, moving to a new floor. They tap their proximity card to authenticate to a different shared workstation. • The roaming applications, including the Epic EHR, are automatically reconnected to the workstation. • The non-Epic applications are in the same state as they were when the physician last used them at the previous shared workstation. • The Epic EHR will either have closed all non-roamin enabled activities or will have completely restarted (depending on whether Roaming is enabled within Epic Hyperdrive).
	The physician may need to electronically prescribe medications or sign off on attestation workflows with the EHR using single- or multifactor authentications. Using Imprivata Enterprise Access Management, the most efficient authentication options are presented to the physician, depending on the specific workflow requirements, the physician's enrolled authentication methods, and the authentication methods available at that workstation.
	When the physician is finished, they tap their proximity card to secure the workstation. Securing the workstation disconnects the roaming applications from the workstation.
	User 2 (nurse) taps their proximity card to authenticate to the same shared workstation that the physician was using. • The nurse's roaming applications, including the Epic EHR, are automatically launched. • The nurse is automatically signed in to the applications.

2.2.2 Reference Architectures

You can implement this workflow on Windows workstations, as well as thin and zero client endpoints.

- Windows

  In environments with Windows-based workstations, Epic is typically delivered to the desktop via an application virtualization technology.

  For example – Citrix DaaS. Citrix can be configured to support application auto launching and roaming.

- Thin or zero client

  Some non–Windows based thin or zero clients support application auto launching and roaming without first requiring a connection to a full Windows desktop.

> **NOTE**: For more information about the technology and a summary of the configurations, see Shared Workstations with Roaming Applications.

2.3 Shared Workstation with Roaming Virtual Desktop

The shared workstation with roaming virtual desktop configuration lets users move from workstation to workstation and automatically connect to a full Windows desktop, which is is delivered via VDI technology. As a clinician authenticates to different shared workstations, they reconnect to their desktop virtualization session.

- This makes it appear as if the desktop, and all the applications that are running within it, are “roaming” with them.
- Can be used in most clinical settings. It is not recommended for settings where the patient's medical record needs to remain persistent on the workstation for different users to access, such as in an exam room.

2.3.1 Clinical Workflow

The following describes the workflow:

	User 1 (physician) taps their proximity card to authenticate to a shared workstation that is secured by Imprivata Enterprise Access Management. • The roaming virtual desktop is automatically launched for the physician. • The physician is automatically signed in to the desktop and any applications that are enabled for SSO, including the Epic EHR.
	When the physician is finished, they tap their proximity card to secure the workstation. Securing the workstation disconnects the roaming desktop from the workstation.
	The physician continues their rotation, moving to a new floor. They tap their proximity card to authenticate to a different shared workstation. • The roaming virtual desktop is automatically reconnected to the workstation. • The desktop and the applications are running are in the same state as they were when the physician last used them at the previous shared workstation. • The Epic EHR will either have closed all non-roamin enabled activities or will have completely restarted.
	The physician may need to electronically prescribe medications or sign off on attestation workflows with the EHR using single- or multifactor authentications. Using Imprivata Enterprise Access Management, the most efficient authentication options are presented to the physician, depending on the specific workflow requirements, the physician's enrolled authentication methods, and the authentication methods available at that workstation.
	When the physician is finished, they tap their proximity card to secure the workstation. Securing the workstation disconnects the roaming desktop from the workstation.

	User 2 (a nurse) taps their proximity card to authenticate to the same shared workstation that the physician was using. • The roaming virtual desktop is automatically launched for the nurse. • The nurse is automatically signed in to the desktop and any applications that are enabled for SSO, including the Epic EHR.

2.3.2 Reference Architectures

Although Windows-based workstations can support virtual desktop roaming workflows, non–Windows-based thin or zero clients are becoming more commonly used for full desktop roaming. There are two options for delivering Epic to the virtual desktop:

- Option 1 — With this option, the Epic client is installed directly on the virtual desktop image.
- Option 2 — With this option, Epic is delivered to the virtual desktop via an application virtualization technology.

  For example — Citrix DaaS. This is also known as a double hop.

> **NOTE**: For more information about the technology and a summary of the configurations, see Shared Workstation with Roaming Desktop.

2.4 Private Workstation

The private workstation configuration is typically dedicated to a single user throughout an entire shift. The user accesses a full Windows desktop and uses locally installed applications, as well as applications that are delivered via application virtualization technology.

This configuration is commonly used in private/physician offices, shared offices with limited repeat users, for unit coordinators, and in specialty areas such as radiology.

2.4.1 Clinical Workflow

The following describes the workflow:

	A user taps their proximity card to authenticate to a private workstation that is secured by Imprivata Enterprise Access Management. • The Windows logon process completes, and the user can open one or more applications, including the Epic EHR. • Any of these applications can be configured for SSO.
	When the user is finished, they tap their proximity card to secure the workstation. Unlike shared workstation configurations, only the user who locked the workstation can unlock it.

	The user returns to the private workstation, and taps their proximity card to authenticate. • The workstation is unlocked. • The desktop and the applications that are running are in the same state as they were when the physician last used them.
	The physician may need to electronically prescribe medications or sign off on attestation workflows with the EHR using single- or multifactor authentications. Using Imprivata Enterprise Access Management, the most efficient authentication options are presented to the physician, depending on the specific workflow requirements, the physician's enrolled authentication methods, and the authentication methods available at that workstation.
	When the user is finished using that workstation for the day, they should shut down all applications and log off.

2.4.2 Reference Architectures

In environments with Windows–based workstations, Epic is typically delivered to the desktop via an application virtualization technology. For example — Citrix DaaS.

> **NOTE**: For information about the technology and a summary of the configurations, see Private Workstation.

2.5 Electronic Prescribing of Controlled Substances (EPCS)

To complete an order for controlled substances, physicians must use two factor authentication as required by the United States Drug Enforcement Agency (DEA). This task is often completed within the health system on a clinical workstation, however there are a certain subset of physicians where it makes sense to allow EPCS on a mobile device.

The allowed factors for authentication include a combination of two of the three categories:

Something you are	Something you have				Something you know
Fingerprint Biometrics	Hands Free Authentication	Push Notification	Soft Token	Hardware Token	Password
					

2.5.1 Clinical Workflow - EPCS on a Clinical Workstation

	The physician navigates to the Order Entry section of Epic and places their controlled substance order.
	The physician is prompted to complete two factors of authentication to confirm the order is appropriate. Imprivata Enterprise Access Management prompts the user for two factors of authentication based on enrollment status and the most convenient options that are available on the clinical workstation. **NOTE:** A proximity card is not recognized by the DEA as an acceptable form of authentication for EPCS.
	After the order is complete, it is sent electronically to the appropriate pharmacy for fulfillment.

For information on the technology and high level configurations required to support EPCS workflows using Imprivata Enterprise Access Management, refer to the reference architectures for clinical workstations section for more information.

2.5.2 Clinical Workflow - EPCS on Epic Haiku or Canto

For a subset of physicians, it makes sense to complete controlled substance ordering from their mobile devices.

Controlled substance orders can be sent from Epic Haiku or Canto on a physician's personal Android or iOS device.

The Mobile EPCS license also allows providers who sign off on EPCS orders from their workstations to leverage facial biometrics to avoid another supervised enrollment and self-enroll a new Imprivata ID app on a new or replacement iOS device.

	The physician navigates to the Epic application Haiku on their mobile Android or iOS device, or Canto from their iOS tablet.
	An order for a controlled substance is placed. The physician is prompted to enter their password as the first form of authentication.

	The physician is prompted to enter their one-time password (OTP) from their hard token. After the order is completed, it will electronically be sent to the appropriate pharmacy for fulfillment.

2.6 Reauthentication Workflows

For security and safety, Epic has enabled multiple workflows that require a user to reauthenticate with their credentials to complete a task. Without Imprivata, this is completed by entering their Epic password. This causes end-user frustration and takes time away from their patients. Imprivata enables users to tap their badge or use their fingerprint (as well as many of the authentication methods) to reauthenticate to more than sixty signing workflows in Epic.

2.6.1 Clinical Workflow

	The clinician accesses a workflow in Epic that requires reauthentication. This could be for break the glass, attestation, or a med dispense.
	After completing the details of the workflow, they click the Accept button in Epic. Imprivata Enterprise Access Management prompts the user for authentication based on enrollment status and the most convenient options that are available on the clinical workstation. Typically, the user would tap their enrolled proximity card to complete the authentication request.

For information on the technology and high-level configurations required to support reauthentication workflows using Imprivata Enterprise Access Management, see the reference architectures for clinical workflows section for more information.

2.7 Witnessing Workflows

For security and safety, Epic has enabled multiple workflows that require a second user to witness a transaction initiated by a first user already authenticated to Epic. Without Imprivata, this is completed by the witnessing user entering their Epic password. This causes end-user frustration and takes time away from their patients. Imprivata allows both users to tap their proximity badge or use their fingerprint to reauthenticate.

Imprivata recommends an Imprivata OneSign Fingerprint Identification (FBID) license if using a fingerprint for witnessing workflows (not needed for reauthentication workflows).

2.7.1 Clinical Workflow

	• The clinician accesses a workflow in Epic that requires a witnessing user to authenticate. This could be for a medication administration, blood administration, or cosign of an order. • The user that is authenticated to Epic completes the workflow in Epic and clicks **Accept**.
	• A second user checks the first user's work and clicks **Sign Off** in Epic. • The second user — who is the witness to the first user's work — is prompted by Imprivata Enterprise Access Management for authentication based on enrollment status and the most convenient options available on the clinical workstation. Typically, the user would tap their enrolled proximity card to complete the authentication request.

For information on the technology and high-level configurations required to support witnessing workflows using Imprivata Enterprise Access Management, see the reference architectures for clinical workstations section for more information.

2.8 Epic Specialty Narrator

The Specialty Narrator in Epic is a tool used to capture attendance during critical events. The most common events are Trauma, Code, and Sedation.

By using Imprivata in the Specialty Narrator, the burden of capturing attendance is removed from the nurse orscribe in the room, allowing person to concentrate on capturing all the other critical details of the event. Imprivata allows for a badge tap to passively capture both the arrival and departure of an individual in the Narrator as they enter and exit the event respectively.

There are two common ways to configure the Specialty Narrator: Integrated and Standalone.

2.8.1 Clinical Workflow - Integrated Specialty Narrator

With Standalone Specialty Narrator, a dedicated workstation for clinicians registers their attendance on a pre-login screen of Epic. Clinicians approach the workstation and tap their proximity card on a reader to mark themselves as arrived or departed. This dedicated workstation can act as a hub for a group of care rooms in a department.

A standalone badge scanning workstation might be more suitable for trauma events, while integrated badge scanning might be more suitable for code or sedation events where having a separate workstation is not always feasible.

	• A user starts the Specialty Narrator event in Epic.

	• Upon arriving to the event, each attendee taps their proximity card on a dedicated workstation. • If there is only one event tied to the dedicated workstation, the user continues to the event. Imprivata Enterprise Access Management marks them as arrived automatically in the Specialty Narrator. • If there are multiple events tied to the same dedicated workstation, the user selects which event they are attending. This action will then automatically mark them as arrived. Multiple users may tap their badge in rapid succession, not creating a delay.
	• When the attendee leaves the narrator event, they tap their proximity card on the dedicated workstation, and Imprivata Enterprise Access Management automatically marks them as departed.

2.8.2 Clinical Workflow - Standalone Specialty Narrator

When the Staff toolbox group is used in Epic specialty Narrators, staff use a proximity card scanner to mark themselves as arrived or departed during a specialty event.

Using integrated proximity card scanning allows clinical staff to mark themselves as arrived or departed with a tap of their proximity card, so they do not have to interrupt documenting important patient care assessments and medications.

This workflow is performed on the same workstation that clinicians are already using to document patient care.

	• User 1, commonly a nurse or scribe, starts the Special Narrator event in Epic. • After the event has started, the user can actively document events as they occur (LDA, Medication, Vitals, etc.).
	• Each attending member of the event taps their proximity card on the reader of the scribe's clinical workstation as they enter the area/room where the event is occurring. • Imprivata Enterprise Access Management seamlessly marks the attendee as arrived, without disrupting the workflow of the scribe.
	• As attendees leave the area/room where the event is occurring, they again tap their proximity cards on the reader of the scribe's clinical workstation. • Imprivata Enterprise Access Management automatically marks them as departed from the event. • If an attendee fails to tap their proximity card, they are automatically marked as departed from the event when the scribe ends the Specialty Narrator event in Epic.

For information on the technology and high-level configurations required to support Specialty Narrator workflows using Imprivata Enterprise Access Management, see the reference architectures for clinical workstations section for more information.

2.9 Shared Mobile Devices

Shared mobile Apple iOS and Android devices are often allocated to units or departments and stored in a shared space for daily/shift-based assignment. These devices allow clinicians to have fast and secure access to mobile applications including Epic Rover and clinical messaging systems. With Rover, clinicians can record documentation in a patient's chart and perform other tasks, including medication administration, at the point of care from a handheld device.

- A clinician typically obtains a shared mobile device at the beginning of their shift, and they are required to authenticate to installed mobile applications, including Rover, using usernames and passwords.
- The applications need to remain logged in and active for the duration of the clinician's shift, or for as long as the clinician requires access to the mobile device.
- When the clinician is finished using the mobile device, they need to log out of all the mobile applications and return the device to a charging station where it can be available for the next user.

Using Imprivata Mobile Access Management (formerly GroundControl) with Imprivata Enterprise Access Management integration, the retrieval from inventory, the use, and return to inventory processes for shared mobile devices is streamlined.

Clinicians tap their proximity card on a reader connected to a mobile device smart hub to rapidly provision a device for their use. Integration with Imprivata Enterprise Access Management provides credential autofill for mobile applications running on the device, including Rover. At the end of their shift, the clinician returns the mobile device to the smart hub, which automatically closes Rover and other applications and removes any personalization settings and recharges the device for the next user.

This configuration is typically used in locations where there is direct patient-provider interaction such as in exam rooms and inpatient rooms.

2.9.1 Clinical Workflow

	• The user taps their proximity card on a reader that is connected to a mobile device smart hub managed by Imprivata Mobile Access Management. Smart hubs are used to centrally charge and manage 8to 24 shared mobile devices. • The mobile device is personalized within a few seconds and is configured with the appropriate applications. • The user retrieves the device from the smart hub and is prompted to set a device-level PIN (facility operational dependency). • The user launches one or more mobile applications, including Epic Rover, and they click the iOS keychain icon to allow MAM to autofill application-specific usernames and passwords.
	• The user secures the mobile device by enabling the iOS lock screen. • If the device is left inactive for a specified amount of time, the device will secure automatically. When secured, all the applications that were in use by the nurse remain logged in, including Epic Rover.
	• The nurse unlocks the device using the PIN set during device provisioning and resumes use of the applications that are already running.

	• At the end of their shift, or when the mobile device is no longer needed, the user returns the device to the smart hub.
	  ◦ This automatically closes Rover and other applications.
	  ◦ Any personalization settings are removed from the device, and it is recharged and made available for the next user.

For information on the technology and high-level configurations required to support shared mobile device workflows, see the reference architecture for Shared Mobile iOS device with Epic Rover.

Chapter 3: Imprivata Digital Identity Solutions Overview and Architecture

The Imprivata Digital Identity Framework (DIF) provides an organized structure to help healthcare delivery organizations holistically manage, secure, and monitor their organization's digital identities. The framework is designed around the key categories required for a robust digital identity strategy that meets the unique demands of healthcare. These categories, which align with H-ISAC's identity framework for healthcare, include the following: governance and administration, identity management, authorization, and authentication and access.

The Imprivata DIF is represented in the diagram and includes a color-coded legend that describes how Imprivata's digital identity solutions map to each of the capabilities defined in the framework. This guide will focus on reference architectures for implementing Imprivata Enterprise Access Management single sign-on, multifactor and advanced authentication using Imprivata Confirm ID , and mobile solutions using Imprivata Mobile Access Management (GroundControl) to support workflows with Epic EHR and Epic Rover.

The Imprivata Digital Identity Framework.

3.1 Imprivata Enterprise Access Management SSO and MFA Overview

Imprivata Enterprise Access Management for SSO is the enterprise single sign-on (SSO), authentication management (AM), virtual desktop access (VDA), and self-service password reset (SSPR) solution specifically designed for healthcare. Enterprise Access Management provides simple and secure access to both cloud and on-premises clinical and administrative applications enabling providers to instantly log into their desktop and sign into their applications with just a tap of a badge or swipe of a finger.

Enterprise Access Management security also helps to protect patient data, empowering organizations to meet HIPAA compliance requirements, preventing credential-sharing, securing PHI on unattended workstations, and enabling easier and more thorough auditing and reporting of workstation and application access.

Imprivata Enterprise Access Management for MFA is a comprehensive identity and multifactor authentication solution designed for healthcare. Enterprise Access Management centralizes identity and multifactor authentication across all enterprise workflows, including remote access, cloud applications, Electronic Prescribing of Controlled Substances (EPCS), medical devices, and clinical workflows such as medical ordering, witness signing, user verification, and procedure attestation. Enterprise Access Management also supports a variety of authentication methods, including hands-free authentication, push token, fingerprint, badge, SMS, and more. Users are only prompted for those authentication methods for which they are enrolled and that are available and allowed for the specific workflow.

The sections below describe the Imprivata appliance and Imprivata agent — the key components of the Imprivata architecture — as well as design considerations for implementing SSO and MFA with the Epic EHR.

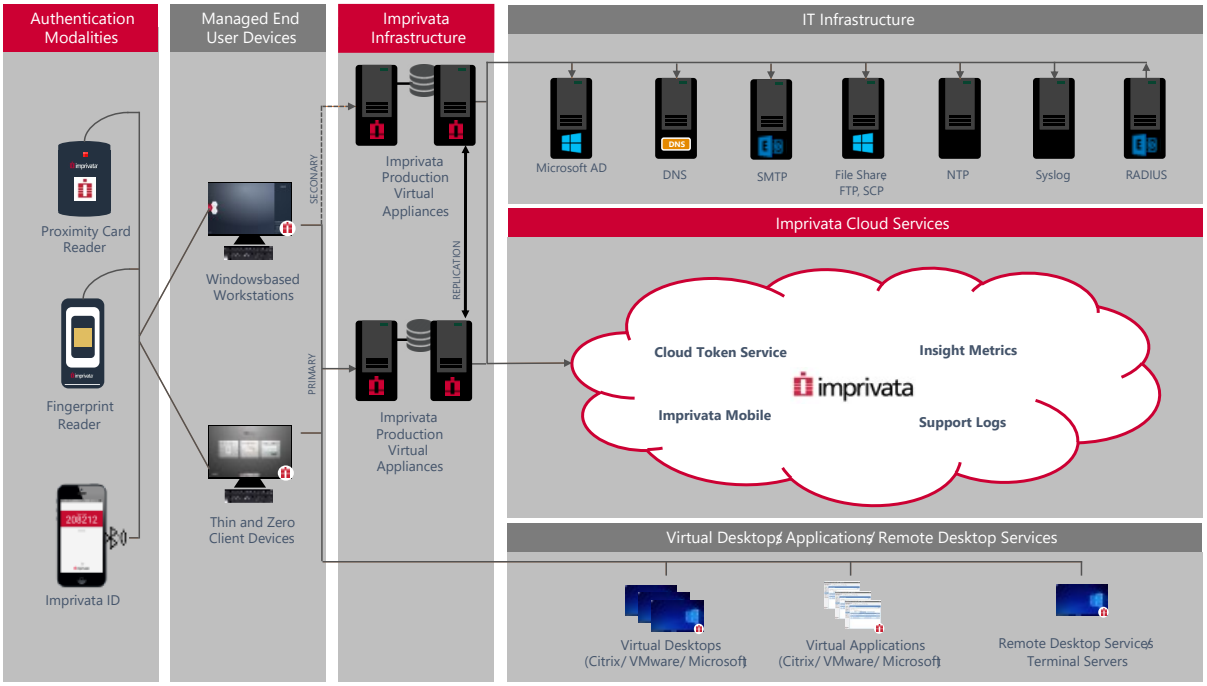
3.1.1 Imprivata Appliance

The Imprivata appliance is the foundation of the Imprivata Enterprise Access Management solutions. It is delivered as an Open Virtualization Format (OVF) image that can be hosted on the premises using VMware ESX, Microsoft Hyper-V, and Nutanix virtual environments, or within the organization's Microsoft Azure tenant. The appliance is configured to synchronize with Microsoft Active Directory (AD) to import user identities into Imprivata Enterprise Access Management.

User identities can be imported based on either organizational units (OUs), security groups, or individual users; and enabled for single sign-on and other EAM capabilities. During a user authentication event, the Imprivata appliance performs an LDAP bind to Active Directory to verify a user's status. A single appliance can handle thousands of simultaneous authentication events from Imprivata-enabled workstations.

The following diagram shows Imprivata appliances as they would commonly be deployed and depicts other network services and infrastructure to support the appliance's operations, management, and interfaces to supporting systems. Some of the network services are customer systems hosted on-premises or in the customer's cloud infrastructure. Imprivata appliances also communicate with Imprivata cloud services to integrate and support other Imprivata solutions.

Imprivata appliances and Imprivata agent high level communications architecture



The Imprivata appliance uses a SUSE Linux-based operating system and is hardened to ensure the highest level of security. Access to the Appliance is restricted to HTTPS (SSL) on port 443 for the Imprivata users and Administrators and HTTPS (SSL) on port 81 for managing the appliance device settings. Data is stored on the appliance in an encrypted database. Only signed software from Imprivata can be uploaded and installed on the appliance. The Imprivata enterprise appliance infrastructure should be deployed behind boundary firewalls alongside other core infrastructure servers and should never be installed in a DMZ.

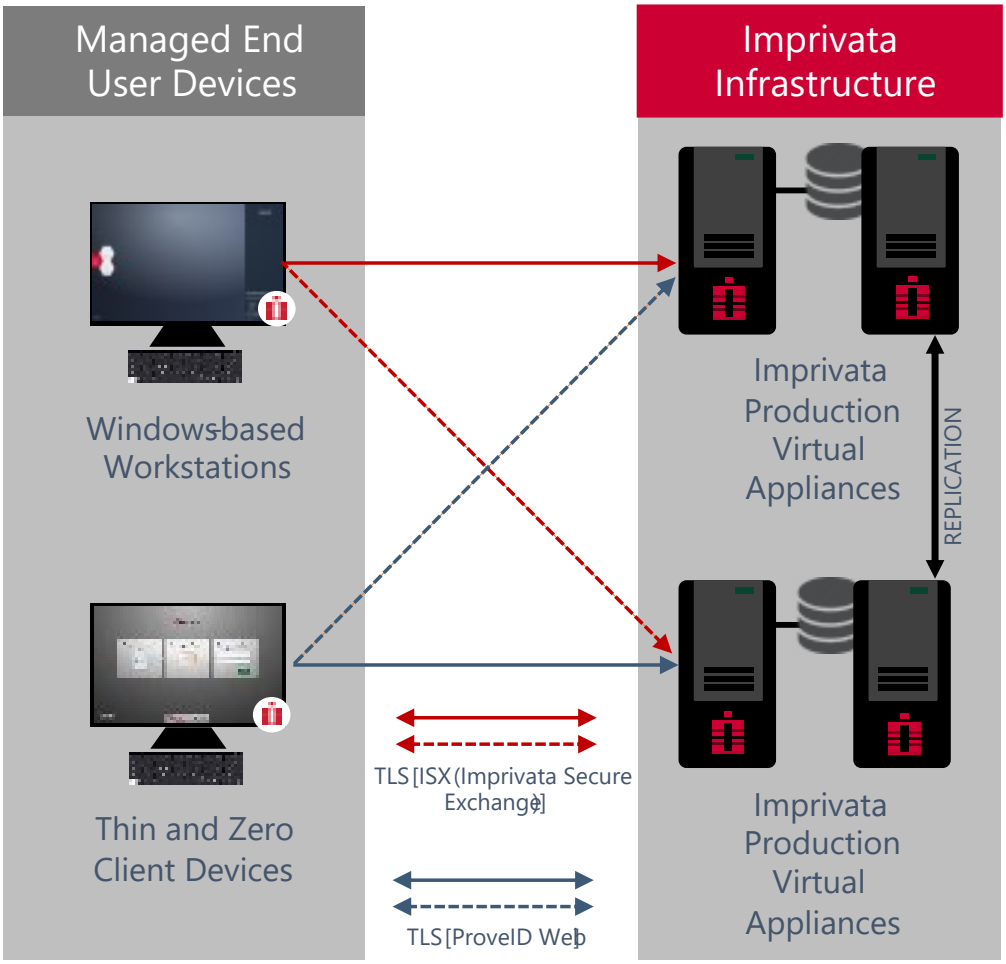
3.1.2 Imprivata Agent

The Imprivata agent is installed on devices where Imprivata Enterprise Access Management authentication and SSO services are required. This includes Windows-based workstations, thin/zero-client devices (embedded), virtual desktop images, and shared servers (such as Citrix and VMware Virtual Application servers). It is a lightweight client that

- Is delivered as an MSI.
- Enforces user authentication, authorization, and user workflow management.
- Provides SSO for enabled applications.

Imprivata agents on Microsoft-based Windows operating systems communicate with an Imprivata appliance using Imprivata Secure Exchange (ISX) — a proprietary Imprivata protocol that uses AES 256-bit encryption, which is then encapsulated in TLS for securing user data while it is in transit. Thin and zero-client devices communicate with the Imprivata appliance using Imprivata's ProveID Web protocol — a proprietary Imprivata protocol that encapsulates in TLS for secure communication.

Imprivata appliances and Imprivata agent secure communication



Imprivata agents have intelligence to detect a communications failure to an appliance and automatically switch to other appliances within the system. To achieve this higher availability, the Imprivata agent maintains a network topology map of all Imprivata appliances along with defined failover rules that instruct the agent where to go next if it cannot communicate with an appliance.

The Imprivata agent can be configured to support a variety of workstation configurations that are frequently used in a healthcare setting:

- **Shared workstations** – Windows-based shared workstations are typically configured to automatically logon to Windows using workstation-specific credentials configured and secured within the Windows registry (e.g., <Sharedkiosk10N35user>/<Sharedkiosk10N35password>) during the boot process. The Imprivata agent then secures the workstation with a customizable lock screen.

  The Imprivata shared workstation lock screen

In this model, a full Windows logon process does not occur when a user authenticates to the workstation; rather, the user's credentials are verified against Active Directory and then the workstation is unlocked. This allows for a fast logon process and switching between users. This is referred to as Imprivata Enterprise Access Management Fast User Switching (FUS).

- **Private workstations** – With Windows-based private workstations, Enterprise Access Management integrates with the standard Windows logon process. Private workstations are typically dedicated to a single user throughout an entire shift, and when they are locked, only the currently authenticated user or an administrator can unlock the session or logout the current user.
- **Shared workstations with Multi-User Desktop** – The Multi-User Desktop (MUD) feature of Windows can support multiple concurrent Windows sessions on the same workstation, and when enabled using Imprivata policy, this configuration can provide another form of a shared workstation. The number of concurrent sessions and maximum lifetime of those sessions can be limited using Imprivata policy. When the number of concurrent sessions is set to one (1), the limitation of the private workstation experience described above is removed, and any user can log out the current user when authenticating to the workstation.

Imprivata agents are also installed on virtual desktop images managed within a VDI infrastructure and on Citrix and VMware Virtual Application servers hosting virtualized applications and desktops. In these scenarios, the Imprivata agent provides single sign-on and advanced authentication functionality in the virtualized environment on behalf of the authenticated user. It can also interoperate with the Imprivata agent installed on the remote workstation to provide "tap and go" access to virtualized resources using Imprivata Virtual Desktop Access.

Supported Authentication Methods

The Imprivata agent supports a variety of authentication methods that can be used for primary authentication, multifactor authentication, and secondary or re-authentication with Epic Hyperdrive clinical workflows.

Supported authentication methods

Many of these authentication methods can be combined to support multifactor authentication (MFA) for desktop access using Imprivata Enterprise Access Management or to support various authentication workflows using MFA . For example, an Enterprise Access Management desktop authentication policy can be created to require MFA using a passive proximity card and domain password. This policy can be enabled for all authentication attempts, or it can be configured to require MFA only at the start of a shift while providing users with a grace period where they are only required to use a single factor (passive proximity card, in this example) during the remainder of their shift. Additionally, a workflow policy can be created to require MFA for Electronic Prescribing of Controlled Substances (EPCS).

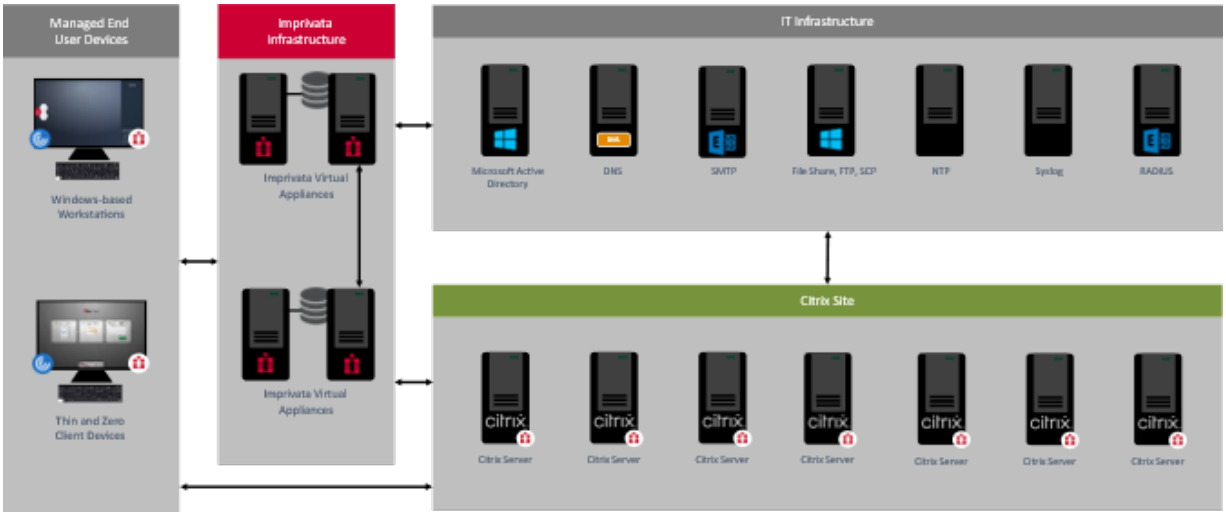
3.1.3 Imprivata Enterprise Access Management and Application and Desktop Virtualization

Imprivata Enterprise Access Management supports a variety of desktop and application virtualization delivery solutions including Citrix DaaS and Omnissa Horizon.

3.1.4 Application Virtualization

In an environment that includes applications delivered via application virtualization technology, like Citrix DaaS, the Imprivata agent is installed on user workstations and on each server in the Citrix site. The Imprivata agent on the user workstation interacts with the locally installed Citrix Workspace app to authenticate to the Citrix session and launch applications and achieve single sign-on. Optionally, Citrix applications can be launched automatically using Imprivata Virtual Desktop Access. The Imprivata agent on the Citrix server provides single sign-on and advanced authentication to applications hosted in the site.

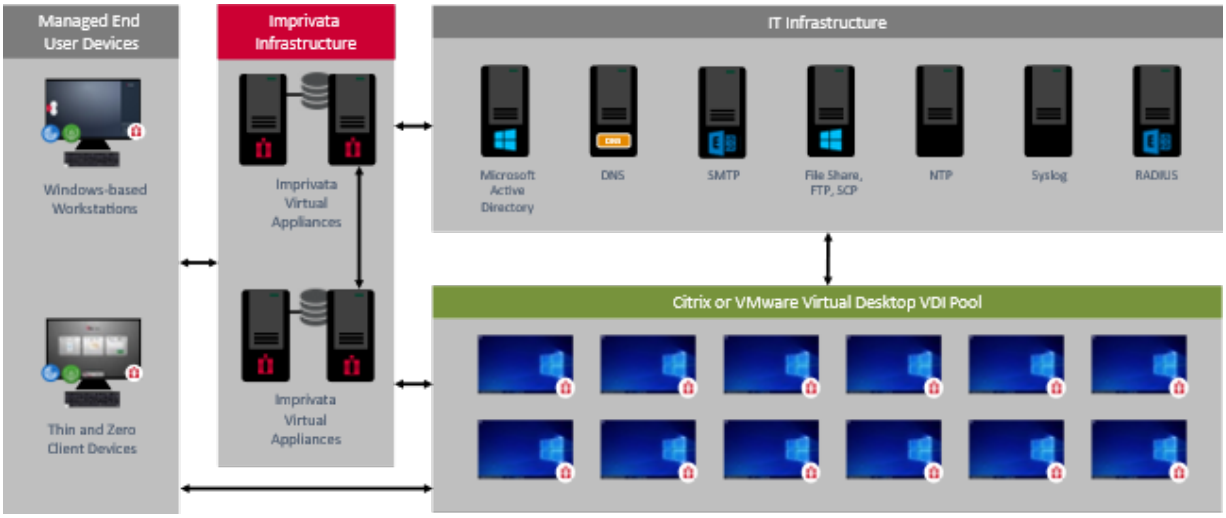
Imprivata Enterprise Access Management architecture with Citrix DaaS



3.1.5 Desktop Virtualization

In an environment that includes virtualized desktops that are delivered via Citrix DaaS or Omnissa Horizon, the Imprivata agent is installed on each user workstation and on each virtual desktop instance in the desktop pools that require application single sign-on and advanced authentication. The Imprivata agent on the user workstation interacts with the locally installed Citrix Workspace app or Omnissa Horizon Client to authenticate to and automatically launch virtualized desktops using Imprivata Virtual Desktop Access. The Imprivata agent on the virtualized desktop provides single sign-on and advanced authentication to applications installed on the virtualized desktops.

The Imprivata Enterprise Access Management architecture with Omnissa Horizon or Citrix DaaS VDI



3.1.6 Thin and Zero Client Workstations

"Thin or zero" client workstations are an alternative to using Windows-based workstations when delivering virtualized applications and desktops. All applications are delivered to the user via application and/or desktop virtualization technologies.

These devices:

- Can be used to deliver the same – or very similar – end user computing experience.
- Use a lightweight operating system, which is typically Linux-based.

  The authentication functionality of the Imprivata agent is built into the operating system (firmware) of most of these devices. They connect to the Imprivata Enterprise using a secure, RESTful API to retrieve configuration information and to handle user authentication requests.
- Are generally less expensive to own and operate than Windows-based workstations.

Imprivata Enterprise Access Management supports a growing list of thin and zero client devices from vendors such as HP, IGEL, and Dell ThinOS. For a full list of supported application and desktop virtualization technologies, and thin and zero client devices, see the Imprivata Enterprise Access Management Supported Components Guide.

3.1.7 Integration with Epic Hyperdrive EHR

For more than a decade, Imprivata has worked with Epic Systems to develop the Imprivata Connector for Epic Hyperspace and now Hyperdrive. The Connector leverages Epic's authentication API to provide single sign-on, single sign-off, and fast user switching for Epic Hyperdrive.

Imprivata Enterprise Access Management offers two different configuration options for Epic that can be enabled on a per-workstation basis:

- **SSO for Multiple Applications including Epic** – With this workflow, the Windows desktop is secured by the Imprivata agent between user sessions. Users authenticate to EAM using any of the Imprivata supported authentication methods — typically fingerprint or proximity card. This workflow is optimized for workstations on which EAM SSO is required for multiple applications, including Epic.
- **SSO for Epic Only workflow** – With this workflow, the Windows desktop is always unlocked. Users authenticate to Epic using most of the Imprivata Enterprise Access Management supported authentication methods — typically fingerprint or proximity card. This workflow is optimized for workstations on which Epic is the most frequently accessed and typically the only application. Single sign-on /sign-off for applications other than Epic is not supported. Standard desktop security mechanisms can be used to make the desktop more secure to protect against accidental PHI exposure from other non-Epic applications. This configuration should be configured to not allow other applications to be launched as the desktop is not locked between user sessions.

Imprivata Enterprise Access Management can be configured to secure Epic and maintain the current patient context or log the user out of Epic with either of these workflows. Secure is typically used in clinical settings where a patient is provided care by multiple care providers and maintaining patient context between user sessions provides for smoother workflows. This is often seen in ambulatory settings such as exam rooms. Logout is used in other areas where maintaining the patient in context is not advantageous.

Imprivata Enterprise Access Management for Electronic Prescribing of Controlled Substances (EPCS) is an end-to-end solution for meeting the DEA requirements for EPCS, including provider identity proofing, supervised enrollment of credentials, two-factor authentication, and auditing and reporting. The Imprivata Confirm ID for EPCS license also includes the Imprivata Enterprise Access Management for Clinical Workflows license.

Imprivata Enterprise Access Management for Clinical Workflows offers advanced multifactor authentication support for more than sixty signing workflows in Epic. A few of the more common workflows enabled with Imprivata Enterprise Access Management include:

- **Anesthesia attestation** – Anesthesiologists tap their proximity badge when attestation signing instead of entering their password. This saves time and improves efficiency as anesthesiologists move from room to room.
- **Medication administration record (MAR)** – Some patient care procedures require a re-verification that the user logged into Epic is the one who is administering a medical. Some facilities and even states within the United States require that a user re-authenticate to ensure it is them that recorded that a medication was administered. The user taps a badge or swipes a finger to re-authenticate versus enter username and password or answering security questions.
- **Dual MAR/Med wasting/Witnessing** – In patient care, frequent situations occur where a care provider must ensure there is a witness to a specific procedure. These are common to the administration of high-risk medications and blood transfusions and for wasting of controlled medications. In these situations, authorized care providers quickly and efficiently authenticate to witness that the correct medication and dosage or the correct blood type was administered, or that residual medication that was not administered to the patient was safely and properly destroyed. Instead of manually entering their username and password or answering security questions, authorized witness care providers tap a badge or swipe a fingerprint.
- **Break-the-glass** – In code situations or other emergencies, Imprivata Enterprise Access Management for Clinical Workflows gives providers a fast, efficient authentication option when they need to override their assigned privileges to access patient records, order emergency medications, or complete different transactions. Instead of having to remember and manually enter a password while under duress, providers simply tap a badge to break the glass.
- **Specialty narrator** – During critical events, including Trauma, Code, and Sedation, Epic Specialty Narrator is used to capture the attendance of clinical staff responding to the event. With Imprivata Enterprise Access Management, staff tap a badge to record their arrival and departure in the narrator as they enter and exit the event. There are two common ways to configure the Specialty Narrator: Integrated and Standalone.
    - **Integrated specialty narrator** – Using the Staff toolbox group in Epic specialty Narrators, staff can use a badge scanner to mark themselves as arrived or departed during a specialty event. Using Integrated Badge Scanning allows clinical staff to mark themselves as arrived or departed with just a scan of their badge so they do not have to interrupt documenting important patient care assessments and medications. This workflow is performed on the same workstation that clinicians are already utilizing to document patient care.
    - **Standalone specialty narrator** – With standalone narrator, a dedicated workstation can be configured for staff to scan in on a pre-login screen of Epic. Staff can approach the workstation and tap their badge to mark themselves as arrived or departed. This dedicated workstation can act as a hub for a group of care rooms in a department. A standalone badge scanning workstation might be more suitable for trauma events, while integrated badge scanning might be more suitable for code or sedation events where having a separate workstation isn't always feasible.

3.1.8 Integration with Epic Community Connect

Imprivata has worked with Epic Systems to develop the Imprivata Connector for Epic so that it integrates with Hyperdrive when accessed via Epic Community Connect (where Hyperdrive is hosted by another health organization). The Connector leverages Epic's Slingshot authentication API to provide single sign-on, single sign-off, fast user switching, and advanced multifactor authentication workflows for Epic Hyperdrive.

Imprivata Enterprise Access Management currently offers SSO for the Multiple Application configuration option for Epic Community Connect, which can be enabled on a per-workstation basis:

- **SSO for multiple applications including Epic** – With this workflow, the Windows desktop is secured by the Imprivata agent. Users authenticate to Enterprise Access Management using any of the supported authentication methods — typically fingerprint or proximity card. This workflow is optimized for workstations on which Imprivata SSO is required for multiple applications, including Epic.

Enterprise Access Management can be configured to secure Epic and maintain the patient context or log the user out of Epic with this workflow.

Enterprise Access Management for Electronic Prescribing of Controlled Substances (EPCS) is an end-to-end solution for meeting the DEA requirements for EPCS, including provider identity proofing, supervised enrollment of credentials, two-factor authentication, and auditing and reporting. The Enterprise Access Management for EPCS license also includes the Imprivata Confirm ID for Clinical Workflows license.

Enterprise Access Management for Clinical Workflows offers advanced multifactor authentication support for more than sixty signing workflows in Epic, including, but not limited to:

- **Anesthesia attestation** – Anesthesiologists can tap their proximity badge when attestation signing instead of entering their password. This saves time and improves efficiency as anesthesiologists move from room to room.
- **Medication administration record (MAR)** – Some patient care procedures require a re-verification that the user logged into Epic is the one who is administering a medical. Some facilities and even states within the United States require that a user re-authenticate to ensure it is them that recorded that a medication was administered. The user taps a badge or swipes a finger to re-authenticate versus enter username and password or answering security questions.
- **Dual MAR/Med wasting/Witnessing** – In patient care, frequent situations occur where a care provider must ensure there is a witness to a specific procedure. These are common to the administration of high-risk medications and blood transfusions, and for wasting of controlled medications. In these situations, authorized care providers can quickly and efficiently authenticate to witness that the correct medication and dosage or the correct blood type was administered, or that residual medication that was not administered to the patient was safely and properly destroyed. Instead of manually entering their username and password or answering security questions, authorized witness care providers taps a badge or swipes a fingerprint.

- **Break-the-glass** – In code situations or other emergencies, Enterprise Access Management for Clinical Workflows gives providers a fast, efficient authentication option when they need to override their assigned privileges to access patient records, order emergency medications, or complete different transactions. Instead of having to remember and manually enter a password while under duress, providers can simply tap a badge to break the glass.
- **Specialty Narrator and Willow Ambulatory** are currently not supported with Enterprise Access Management with Epic Community Connect.

If the instance of Epic that the Community Connect host is providing to their Community Connect sites is hosted on the same Citrix/VMware server image that the host uses internally, there are additional steps required by both the host and site to configure Enterprise Access Management for EPCS and Clinical Workflows. Contact your Imprivata Enterprise Managed Services or Professional Services team for configuration details.

3.2 Imprivata Enterprise Design

An Imprivata enterprise consists of at least two Imprivata appliances that service authentication requests from a collection of Imprivata agents. The appliances are configured to connect to existing IT infrastructure including:

- AD domain controllers
- DNS servers, NTP servers, SMTP servers for alerts
- FTP servers or file shares for storing backups, offloading archived audit data, and storing reports

The connections between the Imprivata agents and the Imprivata appliances use the secure ISX protocol.

Imprivata recommends deploying at minimum a single appliance in each of two data centers to provide data center-level redundancy. In this configuration, the data stored within each appliance in the two data centers is replicated to the peer appliance in the alternate data center. Imprivata agent connect to the appropriate appliance based on site configuration and appliance availability.

3.2.1 Database and Service Appliances

Two or more appliances are configured to create an Imprivata enterprise. Appliances are designated as either a *database appliance* or a *service appliance*.

Database Appliances

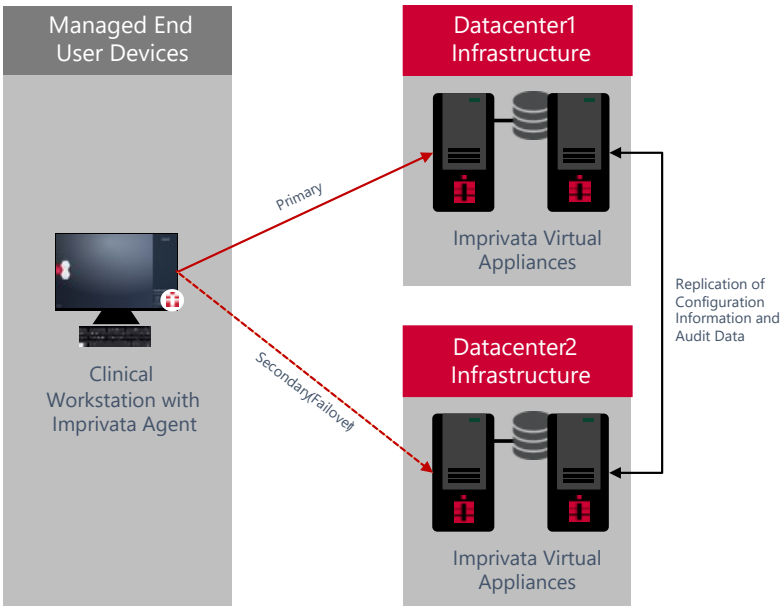
Database appliances host replicas of all enterprise data comprising a collection of user and computer policies, application profiles, user and computer objects, and the defined interrelationship between each of these elements. Changes to any data item is replicated in real time to the peer database appliance.

There are a maximum of two database appliances typically deployed to separate data centers that can be configured as active-active or active-passive for high availability purposes. An Imprivata enterprise should always have two database appliances to ensure database and audit continuity if one database appliance becomes unavailable. Data replication consumes network bandwidth, so one database

appliance per site is enough for most enterprise needs. Database replication occurs only between the database appliances, not to service appliances.

A minimum configuration of an Imprivata enterprise would be two (2) database appliances that should ideally reside in different datacenters. The first two appliances created for an enterprise are database appliances. Thereafter, any additional appliances created are service appliances. For a multisite enterprise as shown below, the first site will be created as the enterprise is created. The second site should be created as the second database appliance is added. If not, the second database appliance will be added to the first site. As the first two appliances created within an enterprise are always database appliances, they should be added to the appropriate desired site before any service appliances are added.

Imprivata enterprise fault-tolerant architecture



Service Appliances

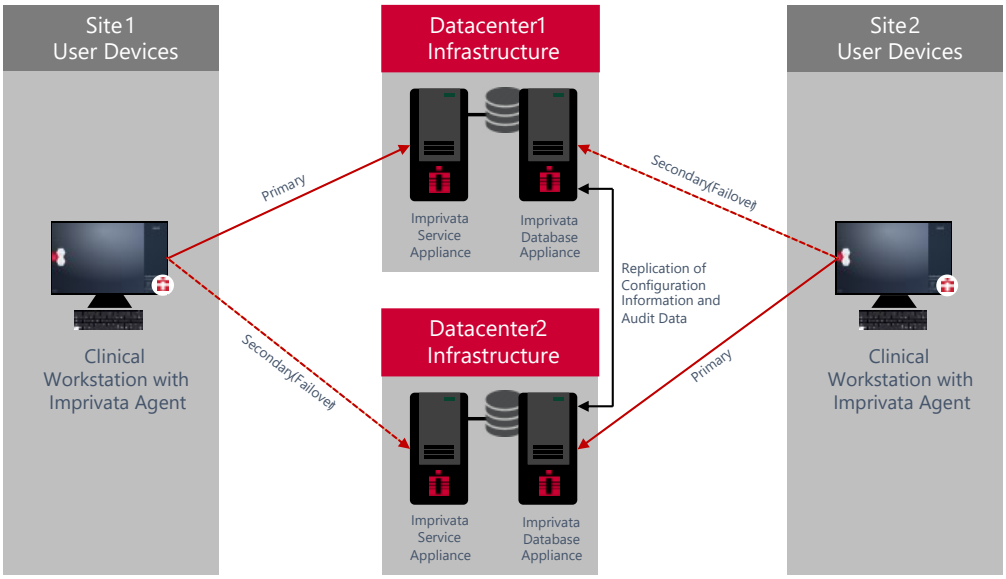
Service appliances are added to increase capacity by sharing authentication events and offloading that workload from the database appliance. These appliances differ from database appliances in that they do not host replicated database tables containing Imprivata configuration, user information, and audit data. A service appliance should reside in the same data center as its corresponding database appliance to reduce the time needed for the service appliances to service requests from endpoint Imprivata agents.

After the first two (2) appliances (database appliances) are added, any additional appliances created will be service appliances. For a multisite enterprise as shown above, both sites should be created as the first and second database appliance is added. This must be completed before a service appliance is added to a site. A new service appliance can then be added to either site. Typically, sites have an equivalent number of database and service appliances.

3.2.2 Scaling for Session Loading

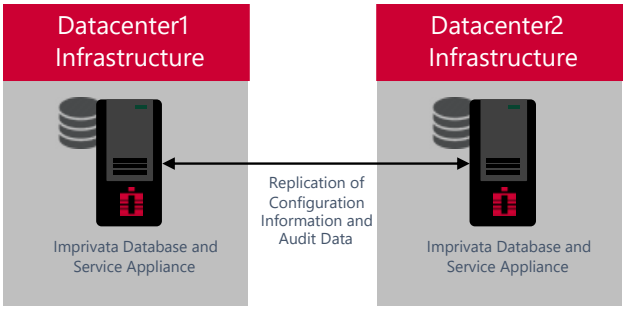
Imprivata conducted exhaustive performance testing to allow individual appliances to increase throughput by increasing CPU resources. In general, up to four (4) appliances within the enterprise could scale linearly by adding more vCPU resources to each appliance. This meant that an appliance could double the throughput of its primary job of authenticating sessions simply by increasing the vCPUs for the appliance virtual machine from two (2) vCPUs to four (4) vCPUs. With four (4) or fewer appliances within the enterprise, this linear scaling was found to be very accurate. In fact, each appliance could attain a four-fold increase in throughput over the default two (2) vCPUs by increasing the vCPUs to a total of eight (8) for each appliance. This provided additional options for organizations that needed to increase enterprise capacity but did not want to add additional appliances.

Imprivata Enterprise Active-Active Architecture with Service Appliances



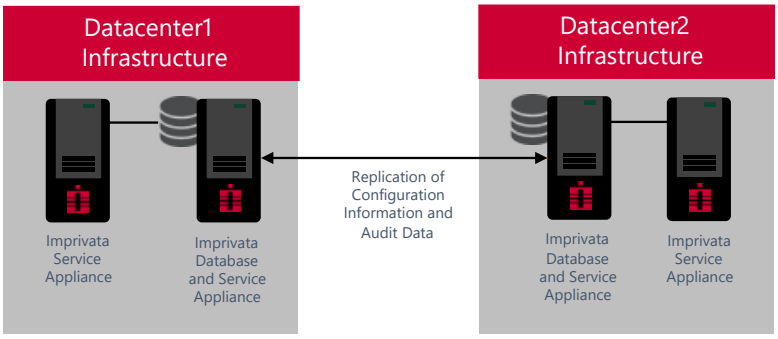
Using the new testing parameters, Imprivata developed new standards for enterprise sizing and scaling. With the new architecture, two appliances will host and support the full database. For fourth generation 4 (G4) and later Imprivata enterprises, Imprivata recommends three standard architecture options: two-, four-, and six-appliance enterprises. The two-appliance enterprise offers three different CPU and RAM configuration options for scale.

Two-appliance Imprivata enterprise

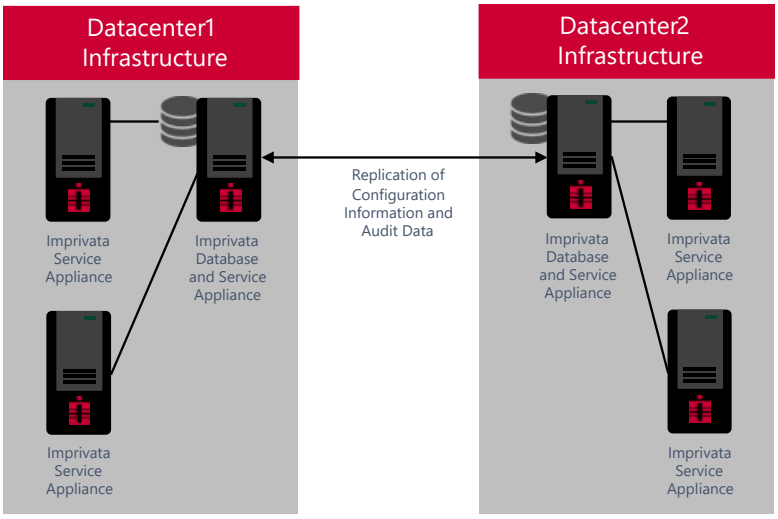


Sites with the database appliances and service appliances should typically be balanced such that there is an equal number of service appliances for each database appliance.

Four-appliance Imprivata enterprise



Six-appliance Imprivata enterprise



At this time, Imprivata does not provide recommendations beyond the six-appliance enterprise. Load testing does not indicate that an appreciable increase in concurrent user-session capacity is achieved by adding more than two service appliances to each site or database appliance.

Recommended options for appliances based on numbers of concurrent user sessions

Recommended Options	2 Appliance Enterprise			4 Appliance Enterprise	6 Appliance Enterprise
Database appliances	2	2	2	2	2
CPUs per appliance	4	8	8	8	8
RAM (GB) per appliance	8	16	32	16	16
Service appliances				2	4
CPUs per appliance				2	2
RAM (GB) per appliance				8	8
Total appliance CPUs in enterprise	**8**	**16**	**16**	**20**	**24**

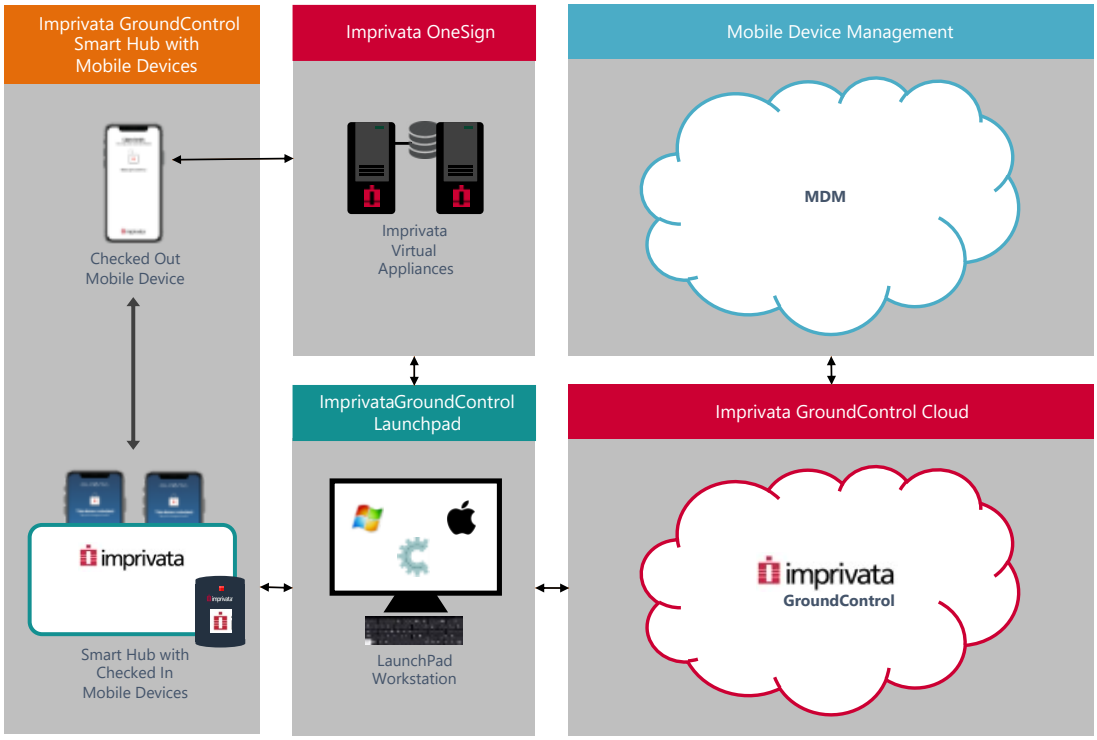
Recommended Options	2 Appliance Enterprise			4 Appliance Enterprise	6 Appliance Enterprise
Total appliance RAM in enterprise	16	32	64	48	64
Number of user sessions supported (in optimal conditions)	22,000 to 28,000	28,000 to 36,500	36,500 to 47,500	47,500 to 62,000	62,000 to 80,000+

3.3 Imprivata Mobile Access Management Overview

Imprivata Mobile Access Management (formerly GroundControl) delivers automated setup and check-in / check-out workflows for shared mobile devices. The solution helps optimize the workflows for users of mobile devices while improving security and auditability. When used in conjunction with Imprivata Enterprise Access Management, MAM provides proximity card-based device check out and credential autofill for mobile applications, which further streamlines mobile workflows.

The sections below describe the key components of Imprivata Mobile Access Management including the cloud tenant and associated management console, the Launchpad, smart hubs, mobile devices, mobile device management (MDM), and the Locker mobile application. Design considerations for implementing MAM with Epic Rover are also provided.

Imprivata Mobile Access Management logical architecture



3.3.1 Imprivata Mobile Access Management Cloud Tenant and Management Console

Imprivata Mobile Access Management is a hybrid solution that consists of on premises and cloud components. Administrators can manage the solution using a cloud-delivered, web-based management console. The console allows MAM administrators to configure mobile device workflows and automations and manage Launchpads and devices.

Most customers are deployed on MAM's multi-tenant cloud; however, some prefer a dedicated cloud environment. A dedicated cloud is physically isolated from other customers and is still managed by Imprivata, however, it allows an organization to receive GroundControl software updates on a delayed and controlled release cadence. Dedicated clouds have the same high-availability infrastructure as the shared cloud environment.

3.3.2 Imprivata Mobile Access Management Launchpad

The Imprivata Mobile Access Management Launchpad software is installed on dedicated Apple Mac or Microsoft Windows workstations that are co-located with mobile device smart hubs. The Launchpads receive instructions from the Imprivata Mobile Access Management cloud environment and interact with attached smart hubs and connected mobile devices to support various shared device workflows.

BEST PRACTICE:
When the Launchpad software is used with Windows-based hardware, it is highly recommended that the hardware be thoroughly tested with large quantities of connected mobile devices (20+). Windows-based hardware capabilities vary between different manufacturers, and testing is required to ensure reliability and scalability of the Imprivata Mobile Access Management solution.

- The Launchpad workstations must be configured for unattended use, and since the software runs as a foreground service, the workstations must automatically log in as a user that should not have administrator privileges.
- Headless workstations without displays are preferred, and the workstations must be configured to automatically restart in case of unexpected shutdowns.
- Protected power outlets are recommended whenever possible.
- The workstations should also have reliable connectivity to the Imprivata Mobile Access Management cloud environment; therefore, a hardwired network connection is required.
- When using the check-in / check-out capabilities of Imprivata Mobile Access Management with Imprivata Enterprise Access Management, a USB-connected proximity card reader is required, however, the Imprivata agent is not required and should not be installed on these workstations.
- Workstation management policies and security software that limit USB functionality may need to be removed or altered to allow the use of smart hubs and proximity card readers.

3.3.3 Imprivata Mobile Access Management Smart Hubs

Smart hubs are used to store, recharge and sometimes secure shared mobile devices. They are connected via USB to workstations that have the Imprivata Mobile Access Management Launchpad software installed. The Launchpad software is used to configure the devices that are connected to the

smart hubs during device setup and check-in / check-out workflows.

Smart hubs come in a variety of different models and sizes and can accommodate shared mobile phones as well as shared tablets. They are offered in two form factors including device trays and docks. Imprivata Mobile Access Management only supports smart hubs that are qualified and sold by Imprivata.

Imprivata Mobile Access Management Smart Hub Options

Smart hubs charge mobile devices to their maximum power faster than ordinary hubs. They support a variety of different cabling options including USB-C and Apple Lightning. Imprivata Mobile Access Management uses special integrations with the smart hubs to report the port number of each connected device and communicate status to users via integrated LEDs. Up to two smart hubs may be connected to a single Mac or Windows workstation when used with the Launchpad software.

3.3.4 Mobile Devices

The Imprivata Mobile Access Management solution supports managing a fleet of shared mobile devices. Apple devices enrolled in the Apple Device Enrollment Program (DEP) are supported as well as non-DEP devices. Devices must be managed by a Mobile Device Management (MDM) solution (see section on mobile device management) and used with smart hubs connected to workstations running the Launchpad software.

When using protective cases on shared mobile devices, their size must be considered when selecting smart hubs as they may require different smart hub slot sizes versus using the devices without cases. Cases with batteries are not supported, as the batteries interfere with power and data. The mobile devices should also have reliable Wi-Fi network connectivity to the Imprivata Mobile Access Management cloud environment and to the Imprivata enterprise.

3.3.5 Mobile Device Management

Imprivata Mobile Access Management requires devices that are managed using a supported Mobile Device Management (MDM) solution. Imprivata Mobile Access Management does not replace the functionality of an MDM, rather, it works alongside industry leading MDMs to trigger actions that are typically performed manually such as clearing device passcodes using API-based integrations.

There are several required items that must be configured in the MDM to support Imprivata Mobile Access Management. For more information, see the Imprivata Mobile Access Management Implementation Guide.

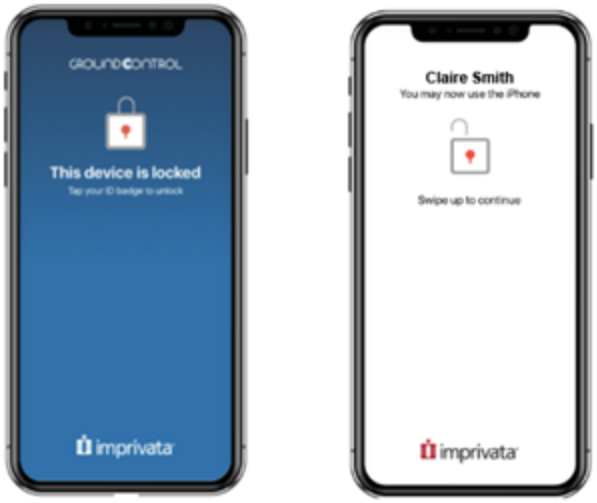
3.3.6 Imprivata Locker Application

The Imprivata Locker application is used to manage mobile device authentication (sign in and out) and credential autofill when used in conjunction with Imprivata Enterprise Access Management.

> **IMPORTANT:**
> Credential autofill is not fully equivalent to single sign-on/sign-off (SSO). Users still need to sign into multiple apps, but the sign in process is dramatically easier. Autofill by itself does not alter the application logout process.

Imprivata distributes the Locker app through Apple's Custom App feature within Apple Business Manager. The application requires support for notifications that can be configured via the MDM. The Locker application supports using a PIN or the user's domain password as a second factor for credential autofill.

Imprivata locker application: locked device (left) and unlocked device (right)



For more information, see the Imprivata Mobile Access Management Implementation Guide.

3.3.7 Using Imprivata Mobile Access Management with Epic Rover

Imprivata Mobile Access Management fully supports shared mobile workflows with Epic's Rover application on iOS devices. When used in conjunction with Imprivata Enterprise Access Management, proximity card-based device check out and credential autofill is also supported.

The following design considerations are recommended when implementing MAM to support workflows with Epic Rover:

- **Smart hubs** – Users are required to retrieve shared mobile devices at the beginning of their shift (or when needed during their shift) using the MAM check out process from smart hubs connected to Launchpad-enabled workstations. The Launchpad-enabled workstations and the attached smart hubs should be installed in locations that are easily accessible by clinical users but not in patient pathways. Physical space requirements for the smart hubs and the associated Launchpad-enabled workstation should also be considered in locations where they are needed. The number of mobile

devices required for a shift in a given department will dictate the size and number of smart hubs that are required. Sizing should also consider mobile devices being returned at the end of a shift with depleted batteries and the need for fully charged devices for users associated with the next shift.

- **Check out process** – It is highly recommended to use Imprivata Enterprise Access Management in conjunction with Imprivata Mobile Access Management to support device check out workflows using proximity cards. With EAM integration, users simply tap their proximity cards on the readers attached to MAM smart hubs and Launchpad-enabled workstations to initiate the device check out process. The process is similar to authenticating to Imprivata OneSign-enabled workstations using proximity cards. If users have already enrolled their proximity cards with EAM, the badges will work with MAM without further enrollment. Since the smart hubs and associated Launchpad-enabled workstations typically do not include monitors, audible and LED cues are provided to users to indicate check out status. Users should be informed of these cues during the training process for MAM.

  It is also recommended to configure MAM to display the user's name on the Locker application when checking out a device so the user associated with the device is easily identifiable. For more information on implementing device check out, see the Imprivata Mobile Access Management documentation.
- **Mobile applications** – Applications including Epic Rover and clinical communications tools are installed on the mobile devices using the MDM solution. The list of applications required by each department or clinical function may vary, and most will require some form of authentication. When used in conjunction with EAM, application profiles are created and deployed from EAM to provide credential autofill for mobile applications. For more information, see the Imprivata Mobile Access Management documentation.

  As previously mentioned, users may need to log out of autofill-enabled applications manually before returning a device to a smart hub. The list of applications that have been validated for autofill and auto-logout are listed on the application support portal for Imprivata Mobile Access Management.
- **Network** – Launchpad-enabled workstations and shared mobile devices must be able to reliably communicate with the Imprivata Mobile Access Management cloud and with the Imprivata enterprise. A hardwired network connection is required for all Launchpad-enabled workstations, and robust and reliable wireless coverage is recommended for the mobile devices in all locations where they will be used.
- **Check-in process** – Before returning a device to a smart hub, users will need to manually log out of most mobile applications. Applications that support auto-logout are listed on the application support portal for MAM. To check in a device, a user simply returns and re-connects it to a smart hub. The user should wait to confirm the associated smart hub LED illuminates before walking away. The application logout and check-in processes should be reviewed during end-user training.
- **Overdue devices** – Checked out devices that aren't returned after a specified number of hours can become overdue, and individuals such as IT administrators can be notified accordingly via e-mail. If desired, MAM can trigger Apple's "Lost Mode" (if using a supported MDM) to lock down the device over the air. MAM automatically removes lost mode when the device is returned to any smart hub connected to a Launchpad-enabled workstation.

Chapter 4: Digital Identity Reference Architectures

The digital identity reference architectures for clinical workstations and shared mobile devices in the following sections are well-proven configurations that have been thoroughly tested by Imprivata and successfully implemented by many of Imprivata's customers.

Readers should request architectural design assistance from an Imprivata pre- or post-sales consultant or certified Imprivata Partner when deviating from these designs.

4.1 Reference Architectures for Clinical Workstation Workflows

The following reference architectures are proven configurations that have been used to implement Imprivata Enterprise Access Management and Epic EHR on shared and private workstations.

Each reference architecture includes:

- A description of the environment, including a logical architecture
- Details of how each component in the environment is configured

> **NOTE:**
> In addition to the following information, Imprivata recommends that you review the Enterprise Access Management Supported Components.
>
> This resources include the currently supported component versions, as well as the policies associated with the addition and retirement of specific component versions. For reference architectures that use thin an zero clients, this resource contains detailed information about the functionality supported by these devices in the Imprivata endpoint ecosystem.

4.1.1 Shared Workstation with Epic EHR Delivered via Citrix to Windows Workstations

Detailed Architecture

This workflow is used in settings where there is direct interaction between the patient and the provider. For example – exam rooms and inpatient rooms.

You can deliver the EHR via application virtualization to Windows, VDI to thin clients, and VDI and application virtualization to thin clients.

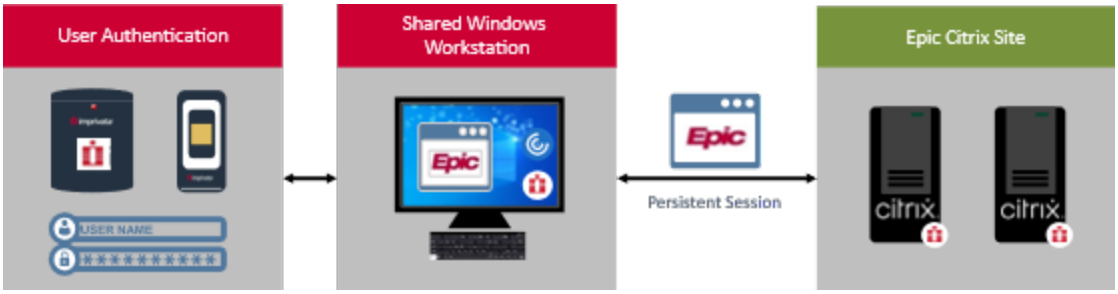
As illustrated in the following, the Epic EHR is delivered to a shared Windows workstation via Citrix DaaS virtual application.

Required Imprivata licenses:

- Imprivata OneSign Single Sign–On with the Imprivata Connector for Epic Hyperdrive.
- Imprivata OneSign Authentication Management

Optional Imprivata licenses:

- Imprivata Confirm ID for EPCS
- Imprivata Confirm ID for Clinical Workflows, bundled with the EPCS license
- Imprivata Virtual Desktop Access



The following table summarizes how Imprivata Enterprise Access Management and the other technologies in your environment are configured:

Technology	Configuration
Epic EHR	• The Epic login device is configured to use the Imprivata Connector for Epic Hyperdrive. • E-Prescribing Controlled Medications (and other Epic signing contexts) are configured to programmatically re-authenticate using the correct Imprivata Connector API calls for the respective MFA workflow policies
EAM SSO	• Imprivata computer policies for the workstations and Citrix servers are configured for Fast User Switching • Imprivata computer policies can be configured for Epic Secure or Epic Logout • Imprivata Virtual Desktop Access should be configured to launch Hyperdrive if users also need access to personal Citrix applications • Both Epic Multi-App and Epic Only modes are supported
EAM MFA	• Relevant user policies are added to the correct Imprivata Clinical and EPCS workflows, for the purposes of enrollment, licensing, and re-authentication
Citrix	• Epic is delivered via Citrix DaaS application virtualization • The Imprivata Citrix or Terminal Server agent (type 3) is installed on all Citrix servers delivering Epic. • The Imprivata Connector for Epic Hyperdrive is installed on all Citrix servers delivering Epic.
Windows workstation	• The workstation is configured to automatically boot and authenticate to Windows using generic workstation-based credentials. • The Imprivata shared–kiosk workstation agent (type 2) is installed. • Citrix Workspace app is installed and configured to connect to Citrix using workstation–based credentials, for example: kioskuser/kioskpassword.

4.1.2 Epic EHR Delivered via VDI to Thin Clients

Detailed Architecture

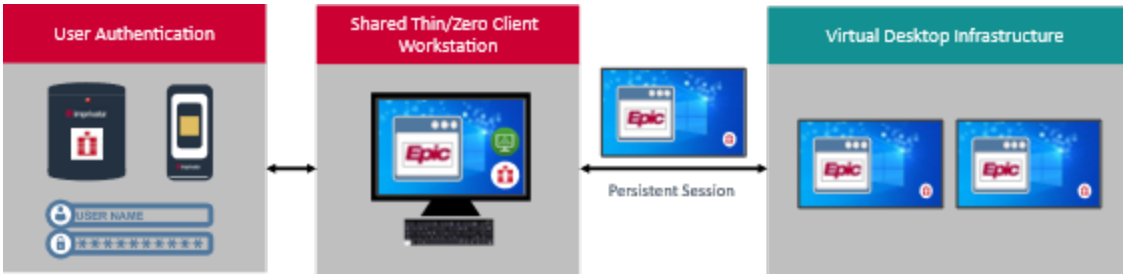
As illustrated in the following, the Epic EHR is delivered to a shared thin or zero client endpoint via a virtual desktop. The Epic EHR thick client is installed locally on Omnissa Horizon or Citrix DaaS VDI image.

Required Imprivata licenses:

- Imprivata OneSign Single Sign–On with the Imprivata Connector for Epic Hyperdrive
- Imprivata OneSign Authentication Management

Optional Imprivata licenses:

- Imprivata Confirm ID for EPCS
- Imprivata Confirm ID for Clinical Workflows, bundled with EPCS license
- Imprivata Virtual Desktop Access



The following table summarizes how Imprivata Enterprise Access Management and the other technologies in your environment are configured:

Technology	Configuration
Epic EHR	• Epic login device is configured to use the Imprivata Connector for Epic Hyperdrive • E-Prescribing Controlled Medications (and other Epic signing contexts) are configured to programmatically re-authenticate using the correct Imprivata Connector API calls for the respective Imprivata Confirm ID workflow policies
EAM SSO	• Imprivata computer policies for the VDI images are configured for fast user switching • Imprivata computer policies for the thin/zero clients can be configured for Epic Secure or Epic Logout • Imprivata Virtual Desktop Access should be configured to launch Hyperdrive if users also need access to personal Citrix applications • Both Epic Multi-App and Epic Only modes are supported
EAM MFA	• Relevant user policies are added to the correct Imprivata Clinical and EPCS workflows, for the purposes of enrollment, licensing, and re-authentication
VDI	• Epic is locally installed on the Omnissa Horizon or Citrix DaaS virtual desktop images. • Imprivata shared–kiosk workstation agent (type 2) is installed on all virtual desktop images. • The Imprivata Connector for Epic Hyperdrive is installed on all virtual desktop images.
Thin client	• Thin clients are configured to automatically boot and connect to a persistent VDI Windows desktop using device-based credentials (i.e. kioskuser/kioskpassword)

4.1.3 Epic EHR Delivered via VDI and Citrix to Thin Clients (Double Hop)

Detailed Architecture

As illustrated in the following, the Epic EHR is delivered via Citrix Virtual Apps to an Omnissa Horizon or Citrix DaaS VDI image. This type of configuration is also known as a double hop.

Required Imprivata licenses:

- Imprivata OneSign Single Sign–On with the Imprivata Connector for Epic Hyperdrive
- Imprivata OneSign Authentication Management
- Imprivata Virtual Desktop Access

Optional Imprivata licenses:

- Imprivata Confirm ID for EPCS
- Imprivata Confirm ID for Clinical Workflows, bundled with EPCS license

The following table summarizes how Imprivata Enterprise Access Management and the other technologies in your environment are configured:

Technology	Configuration
Epic EHR	• Epic login device is configured to use the Imprivata Connector for Epic Hyperdrive • E-Prescribing Controlled Medications (and other Epic signing contexts) are configured to programmatically re-authenticate using the correct Imprivata Connector API calls for the respective Imprivata Confirm ID workflow policies
EAM SSO	• Imprivata computer and user policies are configured to support automated access to VDI desktop using Imprivata Virtual Desktop Access • Imprivata computer policies for the thin/zero clients can be configured for Epic Secure or Epic Logout • Both Epic Multi-App and Epic Only modes are supported
EAM MFA	• Relevant user policies are added to the correct Imprivata Clinical and EPCS workflows, for the purposes of enrollment, licensing, and re-authentication
Citrix	• Epic is delivered via Citrix DaaS application virtualization to the VDI images. • The Imprivata Citrix or Terminal Server agent (type 3) is installed on all Citrix servers delivering Epic. • The Imprivata Connector for Epic Hyperdrive is installed on all Citrix servers delivering Epic.
VDI	• Imprivata shared–kiosk workstation agent (type 2) is installed on all virtual desktop images. • Citrix Workspace app is installed on all virtual desktop images and configured to connect to Citrix using workstation-based credentials • Epic Hyperdrive in Slingshot Mode is installed and configured to connect to Citrix with the Windows user's credentials
Thin client	• Thin clients are configured to connect to Imprivata using ProveID Embedded or ProveID Web **NOTE:** For more information on thin or zero clients supporting this workflow, see the Imprivata Enterprise Access Management Supported Components.

4.1.4 Shared Workstations with Roaming Epic EHR

This workflow can be used in most clinical settings. However, it is not recommended for settings where the patient record must remain persistent on the workstation for different users to access.

You can deliver the EHR via application virtualization to Windows and application virtualization to thin clients.

Detailed Architecture

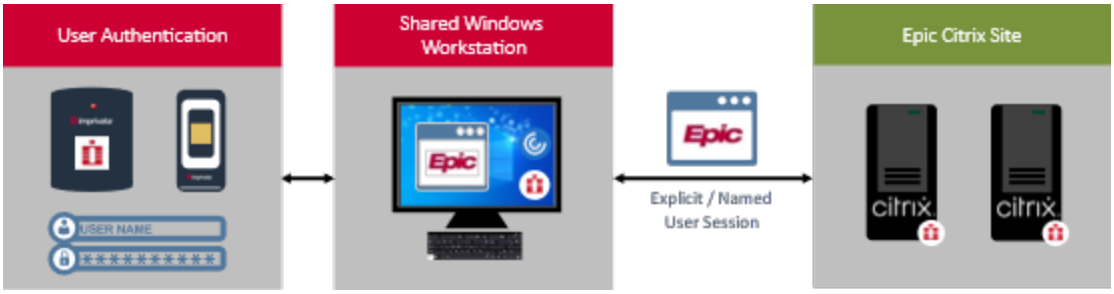
As illustrated in the following, the Epic EHR is delivered to a shared Windows workstation via Citrix DaaS application virtualization.

Required Imprivata licenses:

- Imprivata OneSign Single Sign-On with the Imprivata Connector for Epic Hyperdrive
- Imprivata OneSign Authentication Management
- Imprivata Virtual Desktop Access

Optional Imprivata licenses:

- Imprivata Confirm ID for EPCS
- Imprivata Confirm ID for Clinical Workflows, bundled with EPCS license



The following table summarizes how Imprivata Enterprise Access Management and the other technologies in your environment are configured:

Technology	Configuration
Epic EHR	• The Epic login device is configured to use the Imprivata Connector for Epic Hyperdrive. • Epic system definitions configured to support roaming. • E-Prescribing Controlled Medications (and other Epic signing contexts) are configured to programmatically re-authenticate using the correct Imprivata Connector API calls for the respective Imprivata Confirm ID workflow policies
EAM SSO	• Imprivata computer and user policies are configured to support automated access to Citrix using Imprivata Virtual Desktop Access • Imprivata computer policies can be configured for Epic Secure or Epic Logout • Epic Multi-App mode is supported
EAM MFA	• Relevant user policies are added to the correct Imprivata Clinical and EPCS workflows, for the purposes of enrollment, licensing, and re-authentication
Citrix	• Epic is delivered via Citrix DaaS application virtualization. • The Imprivata Citrix or Terminal Server agent (type 3) is installed on all Citrix servers delivering Epic. • The Imprivata Connector for Epic Hyperdrive is installed on all Citrix servers delivering Epic. • Citrix workspace control settings are configured to support a single session per user for session roaming.
Windows workstation	• The workstation is configured to automatically boot and authenticate to Windows using generic workstation-based credentials. • The Imprivata shared–kiosk workstation agent (type 2) is installed. • Citrix Workspace app is installed.

4.1.5 Roaming Epic EHR Delivered via Citrix to Thin Clients

Detailed Architecture

As illustrated in the following, the Epic EHR is delivered to a shared thin or zero client endpoint via Citrix DaaS application virtualization.

Required Imprivata licenses:

- Imprivata OneSign Single Sign-On with the Imprivata Connector for Epic Hyperdrive.
- Imprivata OneSign Authentication Management
- Imprivata Virtual Desktop Access

Optional Imprivata licenses:

- Imprivata Confirm ID for EPCS
- Imprivata Confirm ID for Clinical Workflows, bundled with EPCS license

The following table summarizes how Imprivata Enterprise Access Management and the other technologies in your environment are configured:

Technology	Configuration
Epic EHR	• The Epic login device is configured to use the Imprivata Connector for Epic Hyperdrive for Epic login. • Epic system definitions configured to support roaming. • E-Prescribing Controlled Medications (and other Epic signing contexts) are configured to programmatically re-authenticate using the correct Imprivata Connector API calls for the respective Imprivata workflow policies
EAM SSO	• Imprivata computer and user policies are configured to support automated access to Citrix using Imprivata Virtual Desktop Access. • Imprivata computer policies on thin/zero clients can be configured for Epic Secure or Epic Logout • Epic Multi-App mode is supported
EAM MFA	• Relevant user policies are added to the correct Imprivata Clinical and EPCS workflows, for the purposes of enrollment, licensing, and re-authentication
Citrix	• Epic is delivered via Citrix DaaS application virtualization. • The Imprivata Citrix or Terminal Server agent (type 3) is installed on all Citrix servers delivering Epic. • The Imprivata Connector for Epic Hyperdrive is installed on all Citrix servers delivering Epic. • Citrix workspace control settings are configured to support a single session per user for session roaming.
Thin client	• Thin clients are configured to connect to Imprivata using ProveID Web or ProveID Embedded. **NOTE:** See the Imprivata Enterprise Access Management Supported Components Guide to determine which thin or zero clients support this workflow. • Citrix Workspace app is installed on the thin client or is embedded into the firmware or operating system.

4.1.6 Shared Workstation with Roaming Epic EHR Delivered via VDI to Thin Clients

This workflow can be used in most clinical settings. However, it is not recommended for settings where the patient record must remain persistent on the workstation for different users to access.

You can deliver the EHR to thin or zero clients via:

- A virtual desktop
- VDI and application virtualization

Detailed Architecture

As illustrated in the following, the Epic EHR is delivered to a shared thin or zero client endpoint via a virtual desktop.

Required Imprivata licenses:

- Imprivata OneSign Single Sign-On with the Imprivata Connector for Epic Hyperdrive
- Imprivata OneSign Authentication Management
- Imprivata Virtual Desktop Access

Optional Imprivata licenses:

- Imprivata Confirm ID for EPCS
- Imprivata Confirm ID for Clinical Workflows (bundled with EPCS license)

The following table summarizes how Imprivata Enterprise Access Management and the other technologies in your environment are configured:

Technology	Configuration
Epic EHR	• Epic login device is configured to use the Imprivata Connector for Epic Hyperdrive • Epic system definitions configured to support roaming • E-Prescribing Controlled Medications (and other Epic signing contexts) are configured to programmatically re-authenticate using the correct Imprivata Connector API calls for the respective Imprivata workflow policies
EAM SSO	• Imprivata computer and user policies are configured to support automated access to Citrix DaaS or Omnissa Horizon Virtual Desktop VDI using Imprivata Virtual Desktop Access • Imprivata computer policies on thin/zero clients can be configured for Epic Secure or Epic Logout • Epic Multi-App mode is supported
EAM MFA	• Relevant user policies are added to the correct Imprivata Clinical and EPCS workflows, for the purposes of enrollment, licensing, and re-authentication

Technology	Configuration
VDI	• Epic is locally installed on the Omnissa Horizon or Citrix Virtual Desktop virtual desktop images. • The Imprivata single user computer agent (type 1) is installed on all virtual desktop images. • The Imprivata Connector for Epic Hyperdrive is installed on all desktop images.
Thin client	• Thin clients are configured to connect to Imprivata using ProveID Web or ProveID Embedded. **NOTE:** See the Imprivata Enterprise Access Management Supported Components Guide to determine which thin or zero clients support this workflow. • Omnissa Horizon or Citrix Workspace app is installed on the thin client or is embedded into the firmware or operating system.

4.1.7 Shared Workstation with Roaming Epic EHR delivered via VDI and Citrix to Thin Clients (Double Hop)

Detailed Architecture

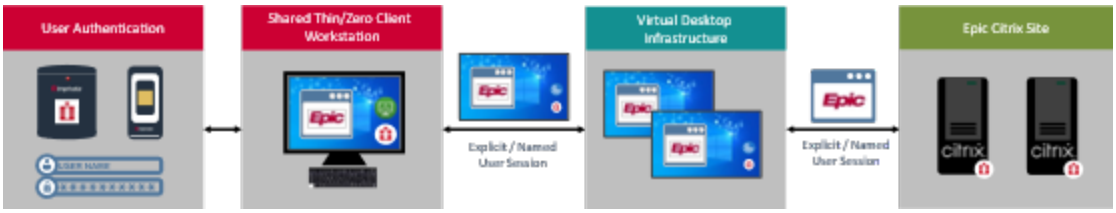
As illustrated in the following, the Epic EHR is delivered via Citrix DaaS to an Omnissa Horizon or Citrix DaaS VDI image. This type of configuration is also known as a double hop.

Required Imprivata licenses:

- Imprivata OneSign Single Sign-On with the Imprivata Connector for Epic Hyperdrive
- Imprivata OneSign Authentication Management
- Imprivata Virtual Desktop Access

Optional Imprivata licenses:

- Imprivata Confirm ID for EPCS
- Imprivata Confirm ID for Clinical Workflows (bundled with EPCS license)



The following table summarizes how Imprivata Enterprise Access Management and the other technologies in your environment are configured:

Technology	Configuration
Epic EHR	• Epic login device is configured to use the Imprivata Connector for Epic Hyperdrive • Epic system definitions configured to support roaming • E-Prescribing Controlled Medications (and other Epic signing contexts) are configured to programmatically re-authenticate using the correct Imprivata Connector API calls for the respective Imprivata workflow policies

Technology	Configuration
EAM SSO	• Imprivata computer and user policies are configured to support automated access to Citrix DaaS or Omnissa Horizon Virtual Desktop VDI using Imprivata Virtual Desktop Access • Imprivata computer policies for the thin/zero clients can be configured for Epic Secure or Epic Logout • Epic Multi-App mode is supported
EAM MFA	• Relevant user policies are added to the correct Imprivata Clinical and EPCS workflows, for the purposes of enrollment, licensing, and re-authentication
Citrix	• Epic is delivered via Citrix Virtual Apps application virtualization to the VDI images. • The Imprivata Citrix or Terminal Server agent (type 3) is installed on all Citrix servers delivering Epic. • The Imprivata Connector for Epic Hyperdrive is installed on all Citrix servers delivering Epic.
VDI	• Imprivata single user agent (type 1) is installed on all virtual desktop images. • Citrix Workspace app is installed. • Epic Hyperdrive in Slingshot Mode is installed and configured to connect to Citrix with the Windows user's credentials
Thin client	• Thin clients are configured to connect to Imprivata using ProveID Web or ProveID Embedded. **NOTE:** See the Imprivata Enterprise Access Management Supported Components Guide to determine which thin or zero clients support this workflow. • Omnissa Horizon Client or Citrix Workspace app is installed on the thin client or is embedded into the firmware or operating system

4.1.8 Shared Workstation with Epic EHR Locally Installed

Detailed Architecture

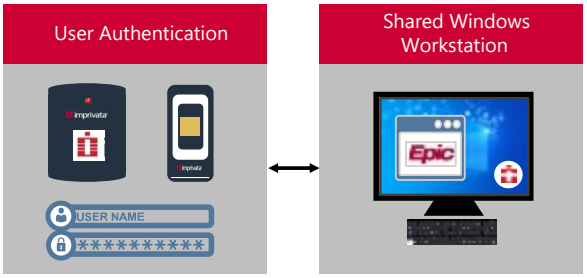
As illustrated in the following, the Epic EHR is locally installed on shared workstations.

Required Imprivata licenses:

- Imprivata OneSign Single Sign–On with the Imprivata Connector for Epic Hyperdrive
- Imprivata OneSign Authentication Management

Optional Imprivata licenses:

- Imprivata Confirm ID for EPCS
- Imprivata Confirm ID for Clinical Workflows (bundled with EPCS license)



The following table summarizes how Imprivata Enterprise Access Management and the other technologies in your environment are configured:

Technology	Configuration
Epic EHR	• Epic login device is configured to use the Imprivata Connector for Epic Hyperdrive • E-Prescribing Controlled Medications (and other Epic signing contexts) are configured to programmatically re-authenticate using the correct Imprivata Connector API calls for the respective Imprivata workflow policies
EAM SSO	• Imprivata computer policies for the workstations are configured to not close Epic on user switch • Imprivata computer policies can be configured for Epic Secure or Epic Logout • Both Epic Multi-App and Epic Only modes are supported
EAM MFA	• Relevant user policies are added to the correct Imprivata Clinical and EPCS workflows, for the purposes of enrollment, licensing, and re-authentication
Windows workstation	• Workstations are configured to automatically boot and authenticate to Windows using workstation-based credentials (i.e., kioskuser/kioskpassword) • Imprivata Shared Workstation Agent (Type 2) is installed • Imprivata Connector for Epic Hyperdrive is installed

4.1.9 Private Workstation with Epic EHR Delivered via Citrix to Windows Workstations

This workflow is used in a in a private location, administration area, or specialty areas where a limited number of users require access.

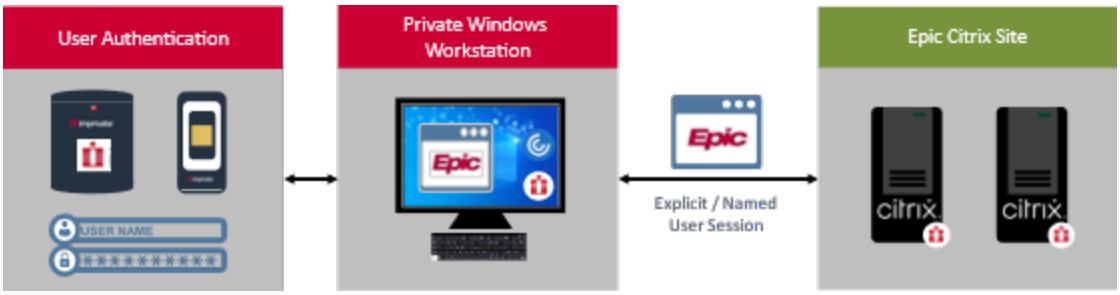
For example – a physician office or an administration area that is only used by unit coordinators.

Epic is typically delivered to the Windows–based workstation via application virtualization technology, such as Citrix DaaS.

Detailed Architecture

As illustrated in the following, the Epic EHR is delivered to a private Windows workstation via Citrix Virtual Apps application virtualization. The following licenses are required:

- Imprivata OneSign Single Sign-On with the Imprivata Connector for Epic Hyperdrive
- Imprivata OneSign Authentication Management



The following table summarizes how Imprivata Enterprise Access Management and the other technologies in your environment are configured:

Technology	Configuration
Epic EHR	• The Epic login device is configured to use the Imprivata Connector for Epic Hyperdrive for Epic login.
EAM SSO	• The Imprivata computer policies can be configured for Epic Secure or Epic Logout.

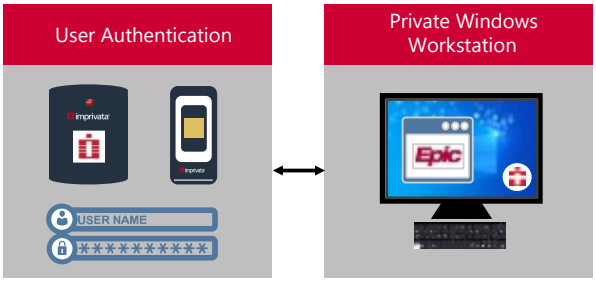
Technology	Configuration
Citrix	• Epic is delivered via Citrix Virtual Apps application virtualization. • The Imprivata Citrix or Terminal Server agent (type 3) is installed on all Citrix servers delivering Epic. • The Imprivata Connector for Epic Hyperdrive is installed on all Citrix servers delivering Epic.
Windows workstation	• The Imprivata single user agent (type 1) is installed. • Citrix Workspace app is installed.

4.1.10 Private Workstation with Epic EHR Locally Installed

Detailed Architecture

As illustrated in the following, the Epic EHR is locally installed on a private workstation.

- Required Imprivata licenses:
  - Imprivata OneSign Single Sign-On with the Imprivata Connector for Epic Hyperdrive
  - Imprivata OneSign Authentication Management
- Optional Imprivata licenses:
  - Imprivata Confirm ID for EPCS
  - Imprivata Confirm ID for Clinical Workflows, bundled with EPCS license



The following table summarizes how Imprivata Enterprise Access Management and the other technologies in your environment are configured:

Technology	Configuration
Epic EHR	• Epic login device is configured to use the Imprivata Connector for Epic Hyperdrive • E-Prescribing Controlled Medications (and other Epic signing contexts) are configured to programmatically re-authenticate using the correct Imprivata Connector API calls for the respective Imprivata workflow policies
EAM SSO	• Imprivata computer policies can be configured for Epic Secure or Epic Logout • Imprivata computer policies can be configured for Multi-User Desktop (MUD) with the number of concurrent sessions limited to one (1) to allow any user to logout the authenticated user • Epic Multi-App mode is supported
EAM MFA	• Relevant user policies are added to the correct Imprivata Clinical and EPCS workflows, for the purposes of enrollment, licensing, and re-authentication
Windows workstation	• The Imprivata single user agent (type 1) is installed. • Imprivata Connector for Epic Hyperdrive is installed

4.1.11 Shared Workstation with Epic EHR Delivered via Citrix to Windows for Community Connect

Detailed Architecture

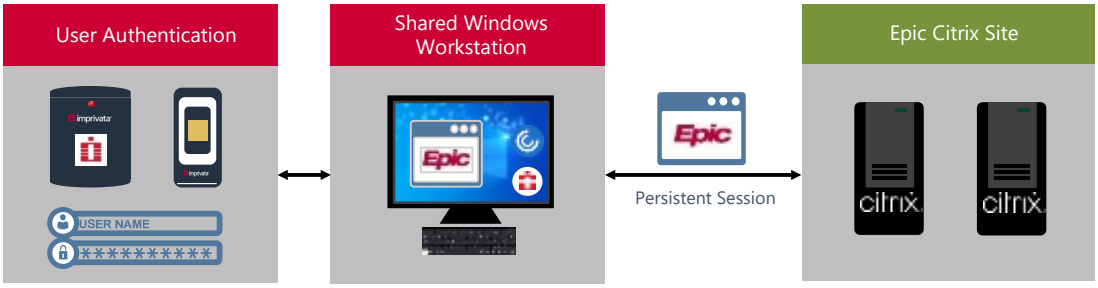
As illustrated in the following, the Epic EHR is delivered via Citrix DaaS to a Windows workstations.

Required Imprivata licenses:

- Imprivata OneSign Single Sign–On with the Imprivata Connector for Epic Hyperdrive
- Imprivata OneSign Authentication Management

Optional Imprivata licenses:

- Imprivata Confirm ID for EPCS
- Imprivata Confirm ID for Clinical Workflows, bundles with EPCS license



The following table summarizes how Imprivata Enterprise Access Management and the other technologies in your environment are configured:

Technology	Configuration
Epic EHR	• E-Prescribing Controlled Medications (and other Epic signing contexts) are configured to programmatically re-authenticate using the correct Imprivata Connector API calls for the respective Imprivata workflow policies
EAM SSO	• Imprivata computer policies for the workstations are configured for Fast User Switching • Imprivata computer policies can be configured for Epic Secure or Epic Logout • Epic Multi-App mode is supported
EAM MFA	• Relevant user policies are added to the correct Imprivata Clinical and EPCS workflows, for the purposes of enrollment, licensing, and re-authentication
Citrix	• Epic is delivered via Citrix DaaS application virtualization
Windows workstation	• Workstations are configured to automatically boot and authenticate to Windows using workstation-based credentials (i.e., kioskuser/kioskpassword) • Imprivata Shared Workstation Agent (Type 2) is installed • Imprivata Connector for Epic Hyperdrive is installed • Citrix Workspace app is installed • Epic Hyperdrive in Slingshot Mode is installed and configured to connect to Citrix with Workstation-based credentials

4.1.12 Shared Workstation with Epic EHR Delivered via VDI and Citrix to Thin Clients for Community Connect

Detailed Architecture

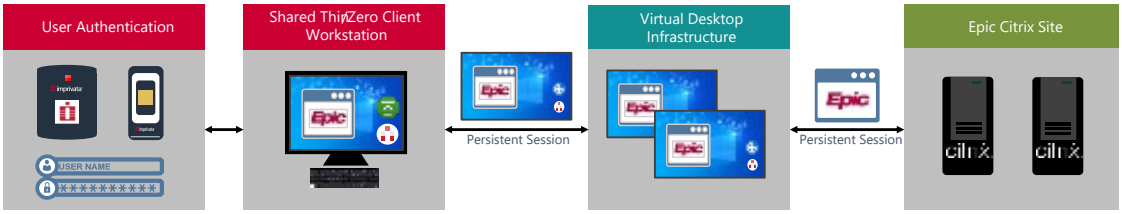
As illustrated in the following, the Epic EHR is delivered via Citrix DaaS to an Omnissa Horizon or Citrix Virtual Desktop VDI image. This type of configuration is also known as a double hop.

Required Imprivata licenses:

- Imprivata OneSign Single Sign–On with the Imprivata Connector for Epic Hyperdrive
- Imprivata OneSign Authentication Management

Optional Imprivata licenses:

- Imprivata Confirm ID for EPCS
- Imprivata Confirm ID for Clinical Workflows, bundles with EPCS license



The following table summarizes how Imprivata Enterprise Access Management and the other technologies in your environment are configured:

Technology	Configuration
Epic EHR	• E-Prescribing Controlled Medications (and other Epic signing contexts) are configured to programmatically re-authenticate using the correct Imprivata Connector API calls for the respective Imprivata workflow policies
EAM SSO	• Imprivata computer and user policies are configured to support automated access to a Citrix DaaS or Omnissa Horizon Virtual Desktop VDI using Imprivata Virtual Desktop Access • Imprivata computer policies for the VDI images can be configured for Epic Secure or Epic Logout • Epic Multi-App mode is supported
EAM MFA	• Relevant user policies are added to the correct Imprivata Clinical and EPCS workflows, for the purposes of enrollment, licensing, and re-authentication
Citrix	• Epic is delivered via Citrix DaaS application virtualization to the VDI images
VDI	• Imprivata Shared Workstation Agent (Type 2) is installed on all virtual desktop images • Imprivata Connector for Epic Hyperdrive is installed • Citrix Workspace app is installed. • Epic Hyperdrive in Slingshot Mode is installed and configured to connect to Citrix with the Windows user's credentials
Thin client	• Thin clients are configured to automatically boot and connect to a persistent VDI Windows desktop using device-based credentials (i.e., kioskuser/kioskpassword)

4.1.13 Shared Workstation with Roaming Epic EHR Delivered via VDI and Citrix to Thin Clients for Community Connect

Detailed Architecture

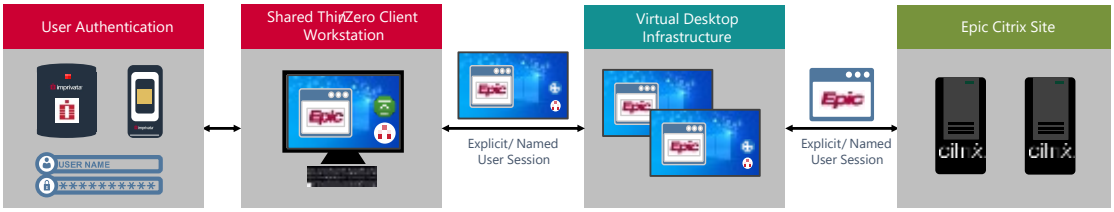
As illustrated in the following, the Epic EHR is delivered via Citrix DaaS to an Omnissa Horizon or Citrix Virtual Desktop VDI image. This type of configuration is also known as a double hop.

Required Imprivata licenses:

- Imprivata OneSign Single Sign–On with the Imprivata Connector for Epic Hyperdrive
- Imprivata OneSign Authentication Management
- Imprivata Virtual Desktop Access

Optional Imprivata licenses:

- Imprivata Confirm ID for EPCS
- Imprivata Confirm ID for Clinical Workflows, bundles with EPCS license



The following table summarizes how Imprivata Enterprise Access Management and the other technologies in your environment are configured:

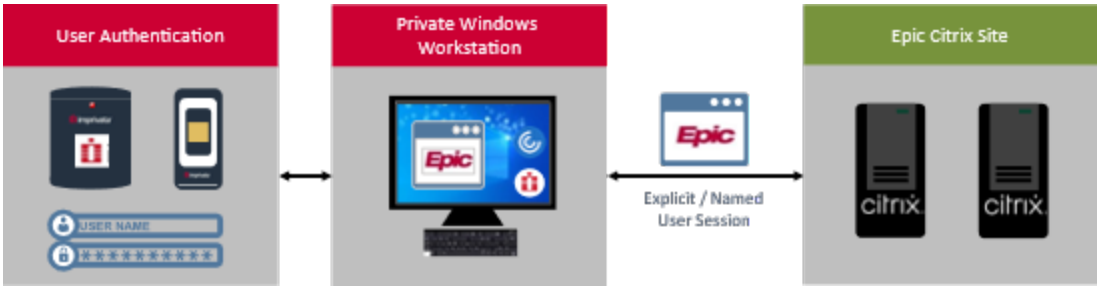
Technology	Configuration
Epic EHR	• Epic system definitions configured to support roaming • E-Prescribing Controlled Medications (and other Epic signing contexts) are configured to programmatically re-authenticate using the correct Imprivata Connector API calls for the respective Imprivata workflow policies
EAM SSO	• Imprivata computer and user policies are configured to support automated access to a Citrix DaaS or Omnissa Horizon Virtual Desktop VDI using Imprivata Virtual Desktop Access • Imprivata computer policies for the VDI images can be configured for Epic Secure or Epic Logout • Epic Multi-App mode is supported
EAM MFA	• Relevant user policies are added to the correct Imprivata Clinical and EPCS workflows, for the purposes of enrollment, licensing, and re-authentication
Citrix	• Epic is delivered via Citrix DaaS application virtualization to the VDI images
VDI	• Imprivata single user agent (type 1) is installed on all virtual desktop images. • Imprivata Connector for Epic Hyperdrive is installed • Citrix Workspace app is installed. • Epic Hyperdrive in Slingshot Mode is installed and configured to connect to Citrix with the Windows user's credentials
Thin client	• Thin clients are configured to connect to Imprivata using ProveID Web or ProveID Embedded. **NOTE:** See the Imprivata Enterprise Access Management Supported Components Guide to determine which thin or zero clients support this workflow. • Omnissa Horizon Client or Citrix Workspace app is installed on the thin client or is embedded into the firmware or operating system

4.1.14 Private Workstation with Epic EHR Delivered via Citrix to Windows Workstations for Community Connect

Detailed Architecture

As illustrated in the following, the Epic EHR is delivered to a private Windows workstation via Citrix DaaS application virtualization.

- Required Imprivata licenses:
  - Imprivata OneSign Single Sign-On with the Imprivata Connector for Epic Hyperdrive
  - Imprivata OneSign Authentication Management
- Optional Imprivata licenses:
  - Imprivata Confirm ID for EPCS
  - Imprivata Confirm ID for Clinical Workflows, bundled with EPCS license



The following table summarizes how Imprivata Enterprise Access Management and the other technologies in your environment are configured:

Technology	Configuration
Epic EHR	• E-Prescribing Controlled Medications (and other Epic signing contexts) are configured to programmatically re-authenticate using the correct Imprivata Connector API calls for the respective Imprivata Confirm ID workflow policies
EAM SSO	• Imprivata computer policies can be configured for Epic Secure or Epic Logout • Epic Multi-App mode is supported
EAM MFA	• Relevant user policies are added to the correct Imprivata Clinical and EPCS workflows, for the purposes of enrollment, licensing, and re-authentication
Citrix	• Epic is delivered via Citrix DaaS application virtualization
Windows workstation	• The Imprivata single user agent (type 1) is installed. • Imprivata Connector for Epic Hyperdrive is installed • Citrix Workspace app is installed. • Epic Hyperdrive in Slingshot Mode is installed and configured to connect to Citrix with the Windows user's credentials

4.2 Reference Architecture for Shared Mobile Devices

The following reference architecture is intended for shared mobile devices. See the Imprivata Mobile Access Management (formerly GroundControl) Online Documentation for supported component versions as well as policies around the addition and retirement of specific component versions.

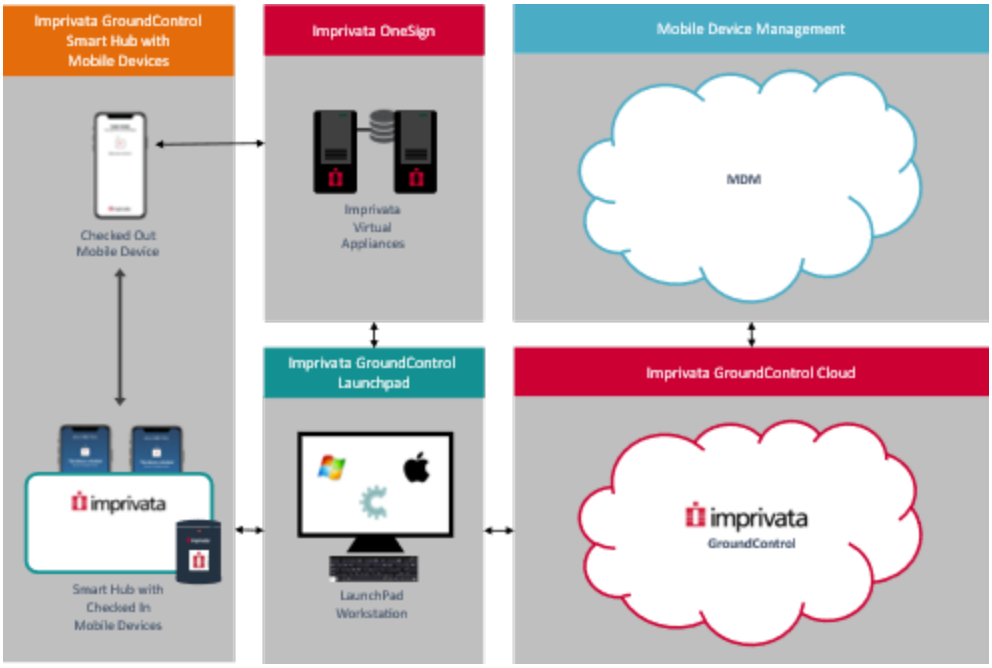
4.2.1 Shared Mobile iOS Device with Epic Rover

Detailed Architecture

As illustrated in the following, Epic Rover is delivered to shared mobile devices via Mobile Device Management (MDM).

Required Imprivata licenses:

- o Imprivata GroundControl Mobile Device Provisioning
- o Imprivata GroundControl Mobile Device Check Out
- o Imprivata OneSign Single Sign-On, may be shared with workstation licensing
- o Imprivata OneSign Authentication Management, may be shared with workstation licensing



The following table summarizes how Imprivata Mobile Access Management, Imprivata Enterprise Access Management and the other technologies in your environment are configured:

Technology	Configuration
Network configuration	• Launchpad workstations should have reliable, hardwired network connectivity to the MAM cloud environment and to the Imprivata enterprise • The shared mobile devices should have reliable, wireless network connectivity to the MAM cloud environment, the MDM and the Imprivata enterprise for Imprivata Enterprise Access Management
Epic Rover configuration	• Epic Rover can be configured with an extended application-level timeout if device-based passcodes are used.
MAM configuration	• MAM is configured for device check out and credential AutoFill using EAM integration • MAM is configured to integrate with the Mobile Device Management solution that is used to manage the shared devices
EAM configuration	• The Imprivata ProveID API is enabled to support integration with MAM • Mobile application profiles are created and deployed to shared device users for applications requiring credential autofill including Epic Rover
Mobile Device Management (MDM) configuration	• Install Epic Rover and Locker apps • Enable notifications for both Imprivata Locker (com.imprivata.b2b.locker) and Epic Rover (com.epic.rover) • Require passcode policy with appropriate complexity

Glossary of Terms

Citrix DaaS	Citrix DaaS (formerly Citrix Virtual Apps and Desktops service) provides virtualization solutions that give IT control of virtual machines, applications, and security while providing anywhere access for any device. End users can use applications and desktops independently of the device's operating system and interface. (Source: Citrix)
Citrix Site	Farms were the top-level objects in XenApp 6.5 and previous versions. In later versions, the Site is the highest-level item. Sites offer applications and desktops to groups of users. (Source: Citrix)
Double hop	A configuration in which applications are delivered to a virtual desktop image using application virtualization technology like Citrix DaaS. Applications are therefore two virtual "hops" away from the workstation with the first "hop" consisting of the virtual desktop and the second "hop" consisting of the virtualized applications that are delivered to the desktop.
Fast user switching (FUS)	Imprivata Enterprise Access Management fast user switching (FUS) is used in shared workstation workflows to allow rapid switching between user identities at the desktop level and at the application level. For desktop-level FUS, the Windows-based shared workstation or virtual desktop kiosk is configured to automatically authenticate to Windows using generic credentials (i.e. kioskuser/kioskpassword). Users authenticate to Imprivata (versus having to authenticate to Windows) to access the shared Windows desktop which greatly reduces the time to logon. For application-level FUS, an application, such as the EHR, is configured to remain persistent (or "hot") on a shared workstation. During a desktop-level fast user switch, EAM logs the previous user out of the application and logs the new user in which greatly reduces the time to access the application since it is not restarted during the user change event. Application-level FUS can be configured to support virtualized applications delivered via technologies like Citrix DaaS.
Imprivata Citrix Server / Terminal Server Agent (Type 3)	A method of installing and configuring the Imprivata agent to support shared Citrix (Citrix XenApp) servers or Microsoft Terminal Server servers.
Imprivata Private Workstation Agent (Type 1)	A method of installing and configuring the Imprivata agent to support private workstation workflows. Also see private workstations.
Imprivata Shared Workstation Agent (Type 2)	A method of installing and configuring the Imprivata agent to support shared workstation workflows. Also see shared workstations.

Mobile Device Management	Mobile Device Management (MDM) solutions allow an organization to control and secure mobile devices through centralized policy management. MDMs are often used to track device inventory, distribute, and manage mobile applications, and enforce security and data encryption policies.
Multi-User Desktop	Multi-User Desktop (MUD) is a feature of Windows that can allow multiple concurrent Windows sessions on a workstation.
Private workstations	Private workstations are commonly used by a single user who requires access to one or more applications for a prolonged period of time. These workstations are typically found in private/physician offices, administration areas and in specialty areas such as radiology.
Shared workstations	Often called kiosks or public workstations, shared workstations are commonly used in areas where many different users require fast access to clinical applications for a limited period of time. These workstations are typically found in patient rooms, exam rooms, nursing stations and physician documentation areas.
Single hop	A configuration in which applications are installed directly on the virtual desktop image. Applications are therefore one virtual “hop” away from the workstation with the single “hop” consisting of the virtual desktop.
Smart hub	Smart hubs or docking stations are used to store, recharge, and sometimes secure shared mobile devices. Smart hubs come in a variety of models and sizes and can accommodate shared mobile phones as well as shared tablets. They are offered in several form factors including device trays as well as locking cabinets and carts.
Thin or zero client	A thin or zero client is an end user computing device that uses a lightweight version of Windows or a non-Windows operating system such as Linux to access virtualized applications and/or desktops.
Virtual desktop infrastructure (VDI)	Virtual desktop infrastructure is a desktop virtualization approach in which a desktop operating system, typically Microsoft Windows, runs and is managed in a data center. The desktop image is delivered over a network to an endpoint device, which allows the user to interact with the OS and its applications as if they were running locally. (Source: techtarget.com)
Omnissa Horizon	Omnissa Horizon (formerly VMware Horizon) is a desktop virtualization software platform that allows multiple users to access and run Microsoft Windows desktops that are installed at a centralized location separate from the devices from which they are being accessed. Earlier versions were referred to as VMware View. (Source: Wikipedia)