imprivata®

Product Documentation

Epic Community Connect Reference Architecture

Imprivata Enterprise Access Management

Last Updated: March 2026

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

1. Introduction

1.1 Purpose

This document defines the reference architectures for Epic Community Connect[1] (ECC) hosts integrating Epic Hyperdrive with Imprivata Enterprise Access Management for SSO and MFA, including Electronic Prescribing for Controlled Substances (EPCS). Use it to select a directory and trust model, a Hyperdrive delivery model, and decide whether the host or each ECC site controls EPCS.

1.2 Audience

This guide is written for ECC host architects and implementation teams, plus ECC site IT teams and Imprivata teams supporting the deployment. Readers should be familiar with EAM (appliances, agents, connectors, Confirm ID), Epic concepts (Hyperdrive, Slingshot, ECC, EPCS), and basic application virtualization (Citrix/VDI).

1.3 Scope

The scope includes authentication directory strategy, Hyperdrive delivery models, EPCS authority models, protocol and identity configurations (LDAP, non-LDAP, OIDC, SAML, Entra ID/ROPC), shared enterprise designs, cross-site user considerations, and thin-client/VDI scenarios in ECC environments. Epic build details, customer-specific legal advice, and detailed commercial terms are out of scope.

1.4 How to Use This Document

Use this guide as a design framework rather than a strict blueprint.

1. Start with **Section 2** to choose the identity source, protocol, and trust model.
2. Use **Section 3** to select the closest "most likely" configuration.
3. Use **Sections 4-6** to confirm directory design, delivery details, and EPCS ownership.

1.5 Outcomes

When you're done with this document, you should be able to answer each of the following questions:

1. Which directories will ECC users authenticate against for endpoint access, Epic Hyperdrive and EPCS authentication (host directory, ECC site directory, or both)?
2. How does the Imprivata Connector is configured to retrieve user credentials (LDAP and non-LDAP)?
3. How does the Imprivata Connector authenticate into Epic Hyperdrive (password or SAML)?
4. How is Epic Hyperdrive launched (local install vs published via application virtualization)?

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

5. Where must the Imprivata agent and Imprivata Connector be installed (endpoint, virtual session host, or both)?
6. Which EAM instance (host-provided vs ECC site-provided) will provide EPCS authentication?
7. Is Slingshot required for the chosen Epic Hyperdrive delivery model, and which Slingshot access method is used (calculated password, pass-through, interactive)?
8. What directory trust model is required between host and ECC site directories (one-way, two-way or none), and why?
9. What endpoint types are required (Type 1 vs Type 2) to support shared workstations and cross-site users?
10. How will cross-site users authenticate at both host and ECC sites (accounts and EPCS enrollment)?

1.6 Glossary

Active Directory (AD): Microsoft directory used for user accounts, groups, and Windows logon.

Application virtualization: Delivering Hyperdrive through a published remote session (for example, Citrix) instead of installing it locally.
Used when: Hyperdrive runs on a session host, not the endpoint.

Authentication: The first identity check that grants access (endpoint logon, virtualization logon, or Epic login).

Citrix: A common application virtualization platform used to publish Hyperdrive.

Clinical workflows: In-Epic actions that require identity confirmation beyond login (step-up or witness).

Confirm ID: Imprivata's authentication factor service used for MFA and step-up workflows (including EPCS).

Cross-site user: A user who works at more than one org boundary (host and one or more ECC sites).
Used when: deciding identity source, trust needs, and whether EPCS enrollment must work in more than one place.

Directory: The identity store for users and groups, typically AD and/or Entra ID.

Domain: The identity realm being referenced. It can mean an AD domain or an Entra ID tenant. For trusts, it means an AD domain.
Used when: describing where an identity is valid and whether trust is required.

Double hop: Two remote hops (endpoint → published desktop → published application)

EAM (Enterprise Access Management): Imprivata platform used for endpoint SSO, MFA, workflow reauthentication, and Epic integrations.

EAM instance: A specific EAM deployment (appliances, policies, directory integration, agents, connectors).

ECC (Epic Community Connect): Epic model where a host shares its Epic instance with other organizations.

ECC site: An organization that accesses the host's Epic through ECC.

ECC-dedicated application virtualization: Hyperdrive is published from a host-managed virtualization environment dedicated to one ECC site. (separate from the host's virtualization environment).
ECC-shared application virtualization: Hyperdrive is published from a host-managed managed

virtualization environment shared by multiple ECC sites (separate from the host's virtualization environment).

Electronic Prescribing for Controlled Substances (EPCS): Requires higher assurance and authentication at signing.

Endpoint: The workstation or device the user interacts with (shared or assigned).

Endpoint type (Type 1 / Type 2):

- Type 1 endpoint: private or assigned device, usually tied to a single primary user.
- Type 2 endpoint: shared workstation used by many users. Allows for fast-user switching through EAM.

Entra ID: Microsoft cloud identity directory (formerly Azure AD). Used for SSO as an Identity Provider.

EPCS provider: A prescriber who needs EPCS authentication.

Host: The organization that runs the Epic instance.

Host-shared application virtualization: Hyperdrive is published from the host-managed virtualization environment shared by host and ECC site users.
Used when: the host centralizes virtualization operations and standardizes delivery.

Hosted Infrastructure as a Service (IaaS): Systems running in cloud (not on local hardware).

Hyperdrive (Epic Hyperdrive): Epic's client application used to access Epic Hyperspace Web.

Identity Provider (IdP): System that authenticates the user and issues SAML and OIDC assertions.

Local install (Hyperdrive): Hyperdrive runs on the endpoint, not in a published session.

LDAP: Method for Imprivata Connector to authenticate user into Epic Hyperdrive.

Multifactor Authentication (MFA): Requires at least two or more distinct credentials (e.g. password, biometric, one-time password, PIN)

Named user: Person-specific account used for access and audit (not a shared/generic account).

Non-LDAP (Epic non-LDAP in EAM): Method for Imprivata Connector to authenticate user into Epic Hyperdrive when Epic username is different than the EAM username. Epic credentials must be captured from the user.

OpenID Connect (OIDC): Token-based authentication on OAuth 2.0. Typically used for EPCS workflows.
Published application: Hyperdrive is delivered through application virtualization and runs on a session host.

Published application: Application installed on a centralized remote server.

Reauthentication: Security process of requiring a user to authenticate again during an active session for higher-risk actions (e.g. Imprivata Clinical Workflows).

Resource Owner Password Credentials (ROPC): OAuth 2.0 flow where an application collects a username/password and exchanges it for an access token.

SAML: Method for the Imprivata Connector to authenticate user into Epic Hyperdrive through Generic Authentication API.

Service Provider (SP): The application that relies on the Identity Provider. For SAML-based Epic login, Epic is the service provider.

Session host: The server that runs published applications or desktops and hosts the user session.

Single sign-on (SSO): Using an existing authentication event to log into desktops or Epic without retyping credentials.

Slingshot: Locally installed Hyperdrive running in "Slingshot" mode for published Hyperdrive that launches the virtual session and supports SSO configurations.
Used when: Hyperdrive is published through application virtualization, when there are multiple hops and session persistence is needed.

- **Calculated password:** a generic account and password value is derived or provided to support launching Hyperdrive in a published session.

  Used when: enabling launch configurations where the published session needs a credential to start.
- **Interactive:** the user completes an interactive authentication step during launch.
  Used when: pass-through or calculated options do not fit the security model.
- **Pass-through:** an upstream authentication is reused to launch the published session and Hyperdrive.
  Used when: aiming for tap-and-go behavior into published Hyperdrive.

Slingshot Launcher: Imprivata application installed by the Imprivata Connector for Epic Hyperdrive to launch Slingshot passing named credentials for single sign-on.
Used when: Slingshot is not configured for pass-through or calculated password.

Standard user: A user who needs SSO to endpoints and Epic Hyperdrive, but does not need EPCS authentication.

Trust (AD trust): Relationship between AD domains that allows one domain to accept identities from the other. One-way or two-way.
Used when: cross-site users must log into endpoints or session hosts joined to the other domain.

Virtual Desktop Infrastructure (VDI): A virtualized desktop session that users connect to remotely. Often used alongside published application delivery configurations.

2. Identity, Authentication Protocols and Cross-site Access

This section defines the core decision categories and technical identity configurations that underpin all ECC reference architectures. It covers authentication directory choices, Hyperdrive delivery models, EPCS authority, protocol options (LDAP, non-LDAP, OIDC, SAML, Entra ID/ROPC), domain trust configurations, endpoint types, and cross-site users scenarios.

2.1 Core Decision Categories

Every ECC architecture can be decomposed into three primary decision axes:

- **A: Authentication Directory** – how does a user authenticate into an endpoint and application virtualization, if required, how does a user authenticate into Epic Hyperdrive (Host directory vs ECC directory).
- **B: Hyperdrive Delivery Model** – how Hyperdrive is launched (Local Install, Host-shared application virtualization, ECC-shared application virtualization, ECC-dedicated application virtualization).
- **C: EPCS Authentication** – which organization's EAM instance controls EPCS authentication.

2.2 Epic Login Identity and Protocol

The source of identity/directories used to authenticate users into Epic will dictate the protocol used. This has a major impact on ECC design. The source of identity will dictate the configuration within EAM and within Epic for AD authentication using. The supported configuration options within EAM for authentication to Epic are: LDAP and non-LDAP.

OIDC is used for EPCS workflows and does not replace the Epic login configuration. Entra ID ROPC is not supported in this reference architecture.

2.2.1 ECC LDAP vs Non-LDAP Epic Authentication

LDAP configuration: Epic authenticates identities from the directory used by the ECC site's EAM instance.

Non-LDAP configuration: Epic is not bound to ECC site's directory as the authentication source and Epic Hyperdrive credentials must be captured by the EAM instance.

2.2.2 SAML Authentication with Epic (LDAP and Non-LDAP Configuration)

SAML can be used for Epic authentication in both LDAP and non-LDAP Imprivata enterprises.

- In **LDAP-configured** scenarios, EAM still synchronizes identities from the directory and SAML token is used to authenticate the user into Epic.

- In **non-LDAP-configured** scenarios, Imprivata uses Epic Identity Provider to capture Epic username that will be used in SAML token to authenticate into Epic session.

Each Hyperdrive login device must be configured to reference the SAML certificate, downloaded from the ECC Imprivata appliance.

Each Hyperdrive login device must be configured at each ECC site.

2.2.3 Entra ID (Azure AD) ROPC with Epic and Imprivata Connector

The Imprivata Connector for Epic Hyperdriveonly interacts with Generic Authentication Epic APIs for Single Sign-On. The connector does not interact with Entra ID.

Imprivata does not officially support Entra ID ROPC configurations.

2.2.4 When Slingshot is Required

Use Slingshot when Hyperdrive is delivered as a published application (host-shared, ECC-shared, or ECC-dedicated) and you need SSO or tap-and-go into the published session. Slingshot is also required for multi-hop launch patterns. Slingshot is usually not required for locally installed Hyperdrive (except optional auto-launch behavior).

2.3 OIDC-based EPCS

OIDC-based EPCS changes how EPCS authentication is performed but it does not change how users log into endpoints or how Epic sessions are created. The Imprivata agent is used to complete the supervised enrollment of the EPCS provider. The Imprivata agent and Imprivata Connector do not need to be installed to perform OIDC-based EPCS authentication.

Use this section to determine when OIDC-based EPCS applies, what endpoint and session requirements exist and how the design impacts cross-site EPCS providers (host-provided EPCS: single enrollment. ECC-site provided EPCS: per-site enrollment).

2.3.1 OIDC-based EPCS for Windows Endpoints

As EPCS moves toward OIDC-based authentication, Windows endpoints use the Imprivata agent and Imprivata Connector for workstation logon and Hyperdrive SSO, but EPCS authentications are executed via OIDC instead of legacy Confirm ID integration.

- For **host-provided EPCS**, Hyperdrive is configured to authenticate against the host's EPCS OIDC environment.
- For **ECC-provided EPCS**, Hyperdrive is configured to authenticate against the ECC site's OIDC EPCS environment.

The Hyperdrive delivery model (local install vs application virtualization) does not change; only the protocol used for EPCS does.

When using host-provided EPCS and locally installed Hyperdrive, EPCS authentication must be performed via OIDC (See Section 6).

2.3.2 OIDC for Mac and Agentless Endpoints

For Mac or other agentless endpoints where a native Imprivata agent cannot be installed, Hyperdrive or Epic access may occur via a browser or a light client container. In this case, workstation logon is not Imprivata-controlled. EPCS authentications rely on OIDC through Epic's web layer and upstream identity providers.

An Epic username can only be captured through the Imprivata agent and Imprivata Connector. An Epic username cannot be captured via OIDC.

Design sessions should explicitly identify which endpoints are truly agentless and whether clinical users will instead access Hyperdrive via a Windows VDI or application virtualization session where Imprivata components are present.

2.4 Cross-site Users (Standard Users and EPCS Providers)

A cross-site user is any user who works across an organization boundary between a host and one or more ECC sites.

User Types

- Standard User: needs SSO to endpoints and Epic Hyperdrive
- EPCS Provider: Standard user plus EPCS

What cross-site access changes

- Epic login identity: Use one Epic identity model across locations (host directory vs ECC site directory).
- SSO mapping: The endpoint or session-host identity must map to the correct Epic user (LDAP vs non-LDAP).
- EPCS enrollment scope (EPCS providers): Host-owned EPCS supports one enrollment across sites. ECC site-owned EPCS requires supervised enrollment in each EAM instance where the provider will prescribe.
- OIDC-based EPCS: Route the OIDC flow to the EAM instance that owns the provider's EPCS enrollment.

2.5 Domain Trust Configurations and Endpoint Types (Type 1, Type 2)

Active Directory trust direction between the host and ECC site domains determines who can sign in to which endpoints and session hosts. It also drives whether Type 1 (private) or Type 2 (shared) endpoints are practical for cross-site users.

2.5.1 Trust Configurations (AD)

- **One-way trust (Host trusts ECC site):** host accepts ECC site accounts; ECC site does not accept host accounts.
- **One-way trust (ECC site trusts Host):** ECC site accepts host accounts; host does not accept ECC site accounts.
- **Two-way trust:** both domains accept each other's accounts.
- **No trust:** host and ECC site domains do not trust each other. Users can authenticate only within their own domain. ECC site endpoints accept only ECC site accounts, and host users cannot sign in to ECC site domain-joined endpoints (and vice versa).

2.5.2 Endpoint Type Implications

- **Type 1 (private)** endpoints are suited to users who primarily use a single device and domain identity.
- **Type 2 (shared)** endpoints are preferred for shared clinical workstations where multiple providers from different domains log on to the same device. In cross-organization settings, Type 2 endpoints help support cross-site users and reduce friction at the workstation.

For cross-site user scenarios, favor Type 2 shared endpoints in locations where multiple organizations' providers will be working. Confirm that the direction of the AD trust matches the expected roam direction; otherwise clinicians may not be able to log into the workstations where they need to provide care.

3. Most Likely Configurations

This section summarizes the ECC reference configurations most commonly deployed. Each configuration is defined by two choices:

1. **Hyperdrive delivery model** (local install or published application virtualization), and
2. **EPCS ownership** (host-provided or ECC site-provided).

Before selecting a configuration, confirm:

- Which identity Epic will accept for login (host directory or ECC directory).
- Where users authenticate at each step: endpoint, virtualization (if used), Epic login, and EPCS authentication.
- Whether any users work at “alternate” (host and ECC) sites, and whether any roamers are EPCS providers. See **Section 2.4 Cross-site User**s.

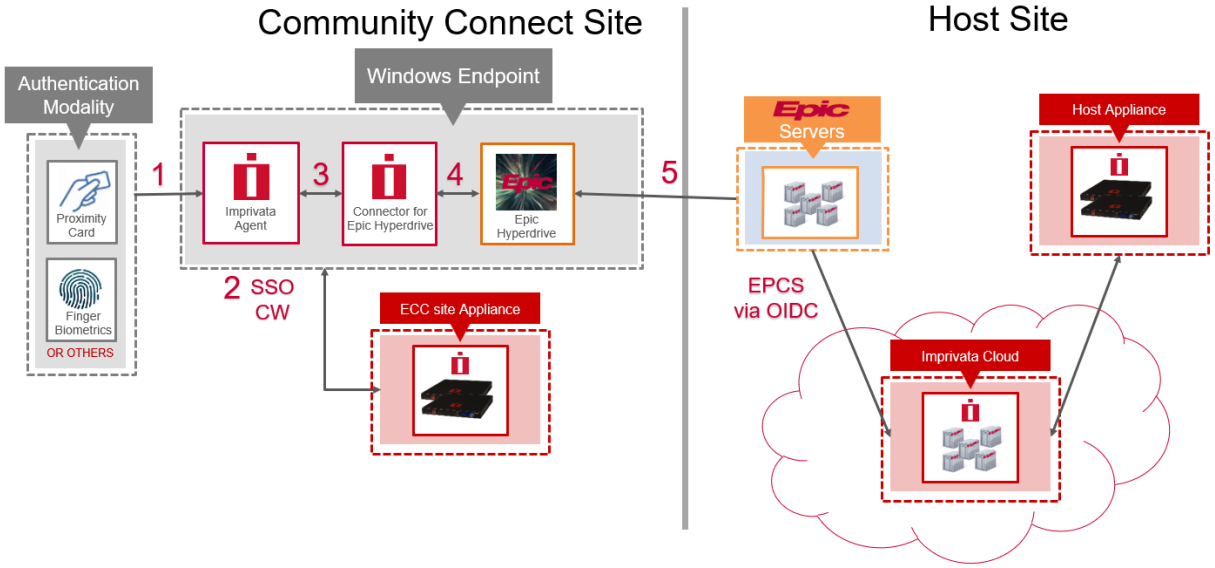
Imprivata currently supports numerous application virtualizations vendors. See the Virtual Desktop Infrastructure section of the Imprivata Enterprise Access Management - SSO Supported Components document.

> **NOTE:**
> The below configurations represent the most common scenarios for configuring EAM for ECC site implementations. If none of the configurations match your scenario, consult your Imprivata account team for further guidance.

3.1 – Local Install / Host EPCS

Local Install compared to host-delivered Hyperdrive in (3.2).
Locally installed Hyperdrive performance and simplicity while host retains EPCS authentication for all prescribers.

Host-managed EPCS provides most flexibility for cross-site EPCS users.



3.2 – Host-delivered Hyperdrive via Application Virtualization / Host EPCS

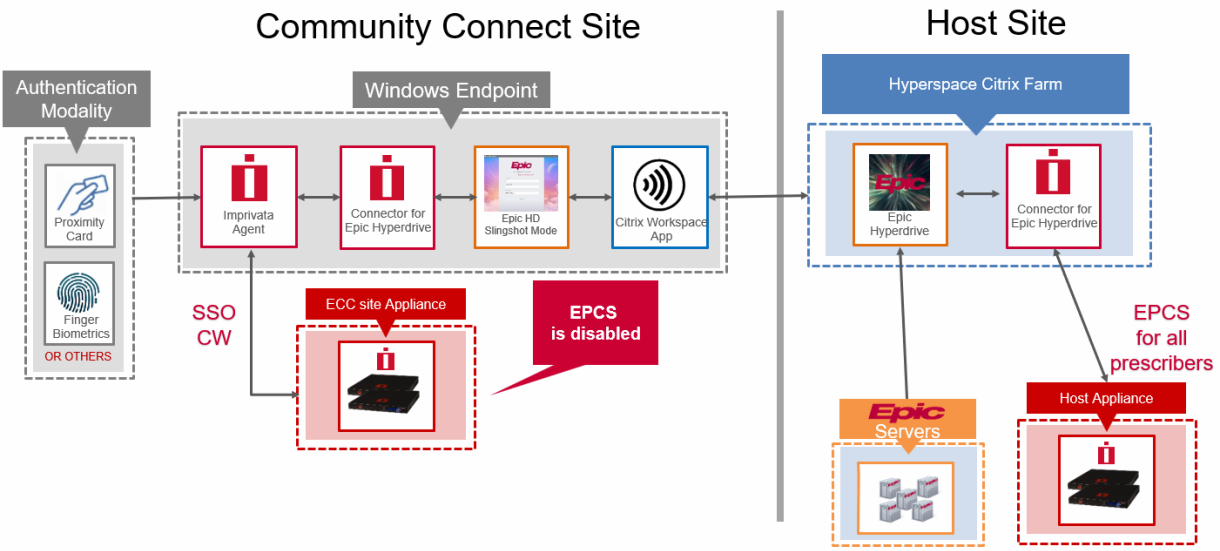
Common existing Community Connect design; host delivers to both host and ECC sites:

Hyperdrive via application virtualization

EPCS authentication via host EAM instance

Host maintains a single application virtualization platform for publishing Hyperdrive to both host and ECC site users.

Host-managed EPCS provides most flexibility for cross-site EPCS users.

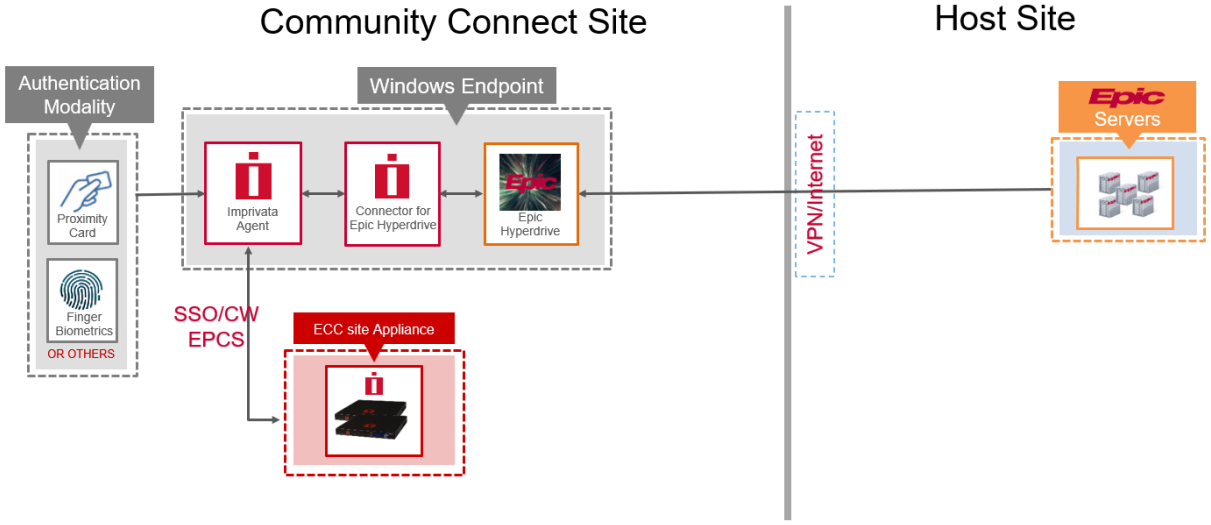


Imprivata currently supports numerous application virtualizations vendors. See the Virtual Desktop Infrastructure section of the Imprivata Enterprise Access Management- SSO Supported Components document.

3.3 – Local Install / Local EPCS

The ECC site provides both single sign-on and EPCS authentication using the local EAM instance. Hyperdrive is installed locally on ECC site endpoints. Host and ECC site(s) each maintain their own separate EPCS enrollments.

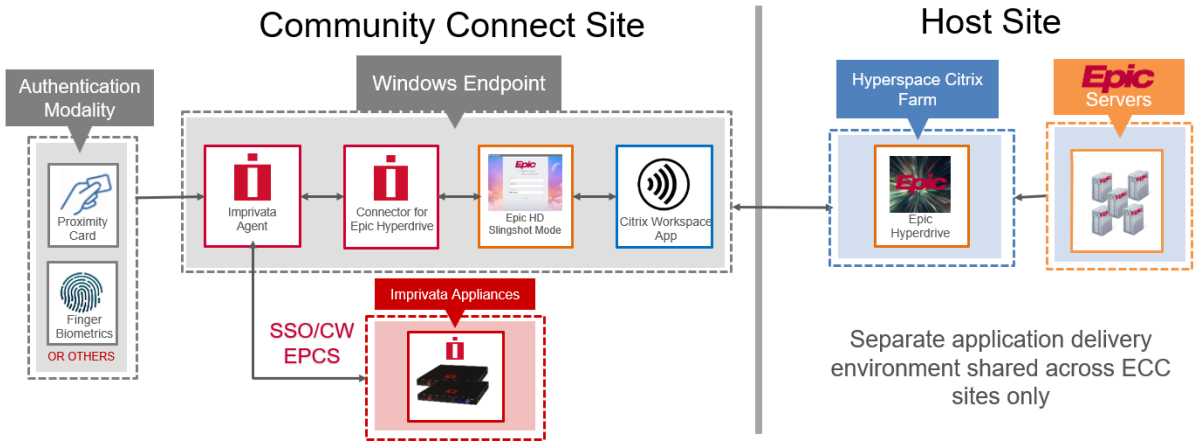
To support cross-site EPCS providers, this configuration requires EPCS providers to enroll into EPCS at each location where they require EPCS authentication.



3.4 – ECC site-shared Hosted App Virtualization / Local EPCS

ECC sites share a common application virtualization cluster that is separate from the host's internal application virtualization cluster. Host and ECC site(s) each maintain their own separate EPCS enrollments.

To support cross-site EPCS providers, this configuration requires EPCS providers to enroll into EPCS at each location where they require EPCS authentication.



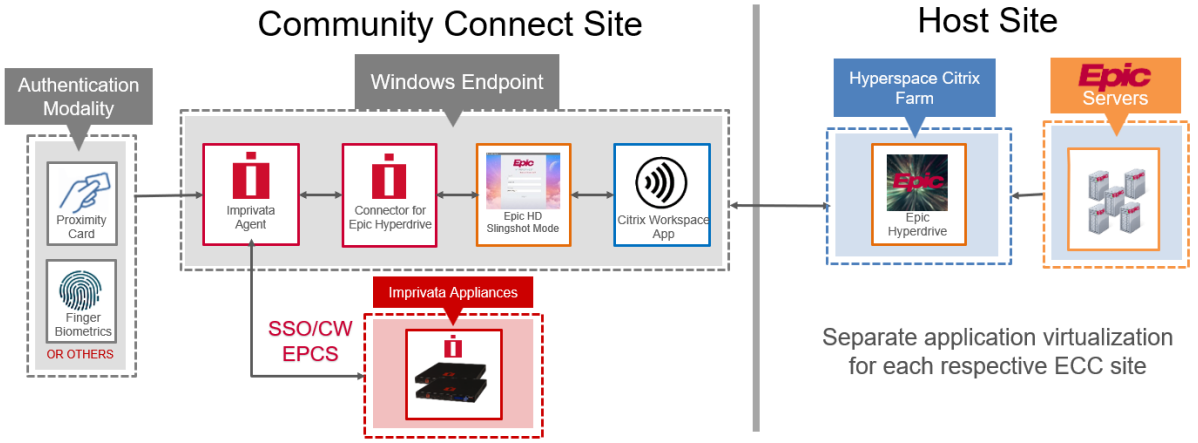
Imprivata currently supports numerous application virtualizations vendors. See the Virtual Desktop Infrastructure section of the Imprivata Enterprise Access Management - SSO Supported Components document.

3.5 – ECC site-dedicated Hosted App Virtualization / Local EPCS

ECC sites each have their own dedicated application virtualization cluster that is separate from the host's internal application virtualization cluster. Host and ECC sites each maintain their own separate EPCS enrollments.

With a dedicated application virtualization server, the host can install and maintain the Imprivata Connector for Epic Hyperdrive directly on the server rather than on each endpoint.

To support cross-site EPCS providers, this configuration requires EPCS providers to enroll into EPCS at each location where they require EPCS authentication.



For each ECC site, the host is supporting a separate bank of application virtualization servers to deliver the Epic Hyperdrive application to each ECC site. This varies from configuration 3.4 in that a separate

cluster of servers (bank) are dedicated to each ECC site on which the Imprivata agent is configured to communicate with each separate ECC's site EAM instance.

Imprivata currently supports numerous application virtualizations vendors. See the Virtual Desktop Infrastructure section of the Imprivata Enterprise Access Management - SSO Supported Components document.

4. Directories

Directories are the source of user identities in an Epic Community Connect (ECC) architecture from which Imprivata Enterprise Access Management synchronizes user accounts and authenticate users that drive decisions across the configurations described in Section 4.

This section focuses on the directory layer itself: which directories exist, how they are used, and what configurations are most common in ECC deployments.

4.1 Directory Roles in ECC Workflows

At a high level, directories participate in four different authentication purposes:

- Endpoint authentication
- Authentication into the application virtualization platform
- Authentication into Epic Hyperdrive
- Authentication for EPCS

Endpoint logon

Most ECC endpoints (shared or private workstations) are joined to a directory (Active Directory or Entra ID) for SSO authentication. Directory membership determines:

- Which user accounts can sign in at a given workstation
- Which EAM security policies apply

Typically, the ECC site has its own directory to access its own endpoints.

Authentication into the application virtualization platform

When Hyperdrive is delivered via an application virtualization platform, user authentication into that platform can be done in different ways.

Authentication into the application virtualization platform is performed using a named user or a generic user.

Slingshot, the successor to "Warp Drive", enables and optimizes the launching of virtualized Hyperdrive instances on endpoint devices.

Typical Slingshot configurations:

- **Calculated password:** Slingshot is configured with a generic account in the host directory used to authenticate to the application virtualization platform. Epic's Kuiper tool is used to run scripts to automatically update randomized passwords on the endpoints.
- **Pass-through authentication:** this requires the endpoint to use the same identity of the application virtualization platform (usually a server dedicated to the ECC or some kind of trust relationship among different directories).
- **Interactive authentication:** the user is prompted to authenticate manually to the application virtualization platform, usually using the host's directory credentials used also to access Epic. In this configuration, Slingshot Launcher is needed to use SSO.

How does the host grant access into the application virtualization environment?

Scenario 1 (most common): Slingshot is installed on ECC site endpoints and is configured to connect to published Hyperdrive. For shared workstations, Epic's Kuiper tool creates and maintains generic credentials for Slingshot. A trust relationship is not required.

Scenario 2: Host has separate domain for ECC site and has trust relationship between host and ECC site. This would allow pass-through authentication for ECC site user.

Scenario 3: Slingshot Launcher launches Slingshot, passing user credentials for Epic, to authenticate into the application virtualization environment. The credentials used to authenticate into the application virtualization environment must match the same credentials used to authenticate into Epic Hyperdrive.

Authentication into Epic Hyperdrive

Epic validates user credentials at Hyperdrive login using the configured authentication source. Section 2.2.1 describes how the choice of LDAP vs non-LDAP drives the exact configuration in both Epic and EAM.

From a directory perspective, the key design decision is:

- Are Epic logins backed by **host-managed directory accounts**, or
- Are Epic logins backed by **ECC-managed directory accounts**

Authentication for EPCS

The reference directory for EPCS is maintained by either the host or the ECC site. Whoever maintains the directory is also responsible for maintaining EPCS enrollments.

If the host maintains the EPCS enrollments, cross-site users can reuse the same EPCS enrollment across all sites. If an ECC site maintains their own EPCS enrollments, EPCS providers must enroll separately in each EAM instance to perform EPCS authentication at that location.

4.2 Directory Types and Technology Choices

Most ECC deployments rely on one or more of the following directory technologies:

- On-premises Microsoft Active Directory (AD)
- Microsoft Entra ID (formerly Azure AD)
- Hybrid AD + Entra ID

Microsoft Active Directory

Microsoft Active Directory remains the predominant directory for healthcare organizations, for both host sites and ECC sites. Domain controllers may run in on-premises data centers, private cloud, or hosted Infrastructure as a Service (IaaS) environments.

Typical characteristics:

- Windows logon uses NT LAN Manager (NTLM) and/or Kerberos to authenticate users against domain controllers.
- LDAP is used by applications and services to:
  - Query directory objects (read/browse)
  - Perform bind operations to validate username/password combinations to authenticate a user

When an Epic environment is configured for LDAP authentication, Epic uses the user's AD credentials for LDAP-bind operations.

When EAM is configured to authenticate into Epic using LDAP configuration, the Epic Connector retrieves credentials via EAM for the user, which are then submitted to Epic. Epic then performs the LDAP-bind query to verify credentials.

Entra ID (Azure AD)

Entra ID is increasingly used as a cloud directory and identity provider for:

- Office 365 and Software as a Service (SaaS) apps
- Modern authentication to on-premises applications via federation or application proxies
- Conditional access policies and MFA

In ECC designs:

- Entra ID may be used as the primary Identity Provider (IdP) for some web-based workflows.
- It can coexist with AD, where AD remains the authority for on-premises workstation logon and Epic LDAP authentication.
- Resource Owner Password Credentials (ROPC) and other flows involving Entra ID must be carefully aligned with how the Epic environment is configured, given that the Imprivata Connector integrates with Epic's generic authentication APIs, not directly with Entra ID.

  For more specific information about ROPC, reach out to your Imprivata account team.

Hybrid AD + Entra ID

Some organizations operate in hybrid mode:

- AD for on-premises endpoints and legacy systems
- Entra ID for cloud-based apps and policy enforcement

If you utilize a Hybrid AD + Entra ID directory environment, consult your Imprivata account team.

4.3 Host and ECC Directories

When selecting a configuration, teams must consider:

- Where users are managed (HR and identity lifecycle)
- Whether the ECC site(s) are owned or independent organizations
- How often users roam between host site and ECC site and in which direction
- Whether or not a trust relationship among domains already exists for other services provided by the host

In ECC architectures, there are usually at least two directory "domains of concern":

- **Host directory**
- **ECC directory**

Depending on the environment, additional configurations are possible, such as host-managed ECC-centric directories, but the core configurations are:

- **Host directory as Epic authentication source**
  - Both host site and ECC site users must have accounts provisioned in host's directory to log into Epic Hyperdrive.
  - All Epic logins are backed by accounts in the host's directory.
  - ECC sites maintain their own local directory for local applications and workstation logon, but Epic does not authenticate against those domains.
- **Separate Host directory shared by all ECC site(s) as Epic authentication source**
  - This is a separate directory established by the host used to provision and manage accounts for all ECC users.
  - ECC site users must have accounts provisioned in the host's ECC-dedicated directory to log into Epic Hyperdrive.
  - ECC site Epic logins are backed by accounts in the host's ECC-dedicated directory.
  - ECC sites maintain their own local directory for local applications and workstation logon, but Epic does not authenticate against those domains.
- **ECC site directories as Epic authentication source (per ECC site)**
  - Epic is configured to also authenticate against each ECC site's directory.
  - Host providers who roam to ECC sites are required to have accounts in those ECC sites' directories to access ECC site endpoints.
    - Alternatively, roaming user accounts could be imported from the host directory into the ECC site's Imprivata Enterprise Access Management.
    - An AD trust relationship is required for the users' host directory account to be accepted for login to Type 1 endpoints.
    - EAM must be able to authenticate users from other ECC sites' domains (Type 1 or 2 endpoints).
  - This configuration is more complex to implement. This configuration presents provisioning challenges in addition to network security requirements (e.g. Epic backend communication for ECC directories and directory-to-directory trust relationships)

If you are considering a configuration that does not match one of the preceding configurations, consult your Imprivata account team.

4.4 Hybrid Imprivata EAM Scenario (ECC SSO Only + Host EPCS)

In the hybrid scenario, ECC site owns EAM for SSO and the host site owns EPCS for both host and all ECC sites.

This is the typical configuration for the ECC site:

- ECC site's EAM synchronizes with the ECC site's directory
- Imprivata Connector for Epic Hyperdrive is configured to:

    - DisableLocalEPCS = Yes (In the configuration file)
    - non-LDAP for SSO (In the EAM Computer Policy)
- ECC site EPCS providers would get EPCS when roaming to host site.
- ECC site users would only get SSO at their own ECC site where an account has been locally provisioned.
- ECC site EPCS providers will need to complete supervised enrollment within the host's EAM for EPCS.

This is the only configuration that allows ECC site providers to utilize EPCS at both the host and ECC site as well as other ECC sites.

NOTE:
Future versions of this document will discuss potential options for trusts with Entra ID as they become available.

5. Hyperdrive Delivery Models

Hyperdrive delivery models specify where Hyperdrive runs and how it is delivered to ECC users.
Common Hyperdrive Delivery Models:

- Local Install (Epic-recommended)
- Application Virtualization
  - Host-shared (Host and ECC sites)
  - Host-managed Shared ECC sites
  - Host-managed Dedicated ECC site

The choice of delivery model will directly impact:

- Whether Slingshot is required and which Slingshot mode is appropriate
- Where the Imprivata agent and Imprivata Connector for Epic Hyperdrive must be installed (endpoint, application virtualization host, or both)
- Which organization's EAM instance is responsible for EPCS authentication (host vs ECC).
- The EPCS configuration based upon which EAM instance (host or ECC site) will perform EPCS authentication

5.0 Imprivata Licensing

These are the Imprivata licenses required to enable SSO authentication and EPCS whether provided by the host or the ECC site:

- EAM SSO and Authentication Management
- Highly Recommended: Confirm ID for EPCS (licensing is applied at host or ECC depending on EPCS authentication source)
- Optional: Virtual Desktop Access, if using thin clients

5.1 Local Install (Epic-recommended)

Hyperdrive is installed on ECC site endpoints and connects over a secure network path to the host's Epic Hyperspace Web server. The Imprivata agent and the Imprivata Connector for Epic Hyperdrive run on the same endpoint to provide Hyperdrive SSO and support EPCS step-up authentication workflows.

Because Hyperdrive runs locally (not as a published application), Slingshot is not required. Slingshot is typically not used in this model. If enabled, it is used only for optional auto-launch and session persistence, not for delivering Hyperdrive.

5.1.1 Directory and Identity Alignment

- User authentication at an endpoint is performed against the ECC site's directory (AD or Entra ID) as discussed in Section 4 - Directory.
- Host directory authenticates Epic login for ECC site users. In practice, this means ECC users require

host-provisioned identities (or a host-managed directory for all ECC users) to access Epic.

- See Section 4 and Section 4.3 – Host and ECC directories.

5.1.2 Required Components

- Hyperdrive client installed on ECC endpoints
- Imprivata agent on ECC endpoints (Type 1 private or Type 2 shared based on workflow)
- Imprivata Connector for Epic Hyperdrive installed on ECC endpoints
- Reliable network connection from ECC endpoints to host's Epic Hyperspace Web server
- Highly recommended authentication peripherals (e.g. badge readers, fingerprint reader, camera for facial biometric. See the Imprivata Supported Components document for current list of supported peripherals and workflows.)

5.1.3 Technical Configuration Highlights

- Hyperdrive is configured to use host Epic Hyperspace Web server.
- Connector for Epic Hyperdrive is installed and configured at the endpoint and with corresponding Imprivata Enterprise Access Management computer policy.
- This model typically simplifies troubleshooting because application virtualization is not used to access Hyperdrive.

5.1.4 Operational Notes

- Lowest delivery complexity (application virtualization not needed for Hyperdrive)
- Highest performance with local instance of Hyperdrive due to reduced latency
- Requires ECC endpoint teams to manage deployments

5.2 Host-shared Application Virtualization

In this model, the host delivers Hyperdrive through a shared application virtualization platform. This same platform is used by the host and all ECC sites. ECC endpoints access the application virtualization platform using Slingshot to launch Hyperdrive and provide SSO into Epic.

5.2.1 How the Host Grants Access into the Application Virtualization Environment (ties to Section 4.1)

In host-delivered models, there are two common access configurations:

Scenario 1 (most common): Host provisions generic accounts to access application virtualization environment

- ECC endpoints establish access to the virtualization platform using a generic identity.
- For Active Directory, this avoids cross-domain trust requirements but increases operational responsibility around password rotation.
- This works for hosts that provision ECC site accounts into their corporate directory or into their separate ECC site directory.

Scenario 2: Host-established trust with ECC directory

- Host must create a trust relationship with each ECC site's directory and provide access to virtualized applications.
- Allows passthrough on private/individual workstations with named user access
- This scenario minimizes host's administrative burden otherwise required to provision accounts for ECC site identities.

5.2.2 Slingshot Configurations (from Section 4.1)

Slingshot is used to launch Hyperdrive via application virtualization:

- Calculated password
  - Slingshot uses a generic account for virtualization access and relies on scripted password rotation using Epic's Kuiper tool.
- Pass-through authentication
  - Requires alignment between endpoint identity and virtualization identity (as discussed in Section 5.2.1)
- Interactive authentication
  - Users manually authenticate into the virtualization platform and Slingshot Launcher passes user credentials for Epic SSO.

5.2.3 Required Components

- Host-managed application virtualization environment publishing Epic Hyperdrive
- Application virtualization client on host and ECC endpoints
- Slingshot on ECC endpoints
- Imprivata agent placement on host endpoints.
- Imprivata agent and Imprivata Connector placement on each ECC endpoints.

5.2.4 Technical Configuration Highlights

- Hyperdrive is delivered via application virtualization and launched using the configured access (generic vs named user).
- ECC endpoint configuration utilizes Slingshot and Imprivata Connector for Epic Hyperdrive to perform SSO.
- Simplifies application virtualization platform infrastructure needed, maintaining a single server image for both host and ECC site(s).

5.2.5 Operational Notes

- ECC relies on host virtualization uptime, performance, and change control.
- Published application Hyperdrive launch performance is slower than locally-installed Hyperdrive
- Trust relationships will reduce administrative tasks for:

- provisioning and de-provisioning directory accounts for ECC endpoints and users
- maintaining calculated passwords for ECC endpoints

5.3 Host-managed Shared ECC Site Application Virtualization

In this model, the host delivers Hyperdrive through an application virtualization platform shared by all ECC sites. This model allows for security and network isolation between the host site and ECC sites.

5.3.1 Common Use Cases (See Section 3.4)

- Host chooses not to provision ECC user accounts into their corporate directory.
- If host chooses virtualization access model that requires a trust, host does not have to build a trust between their corporate directory and each ECC site directory.
  - Trust relationships for each ECC site will be built through the separate host-managed ECC site directory.

5.3.2 Required Components

- Host-managed ECC-shared virtualization environment
- Hyperdrive installed and published within the ECC-shared environment
- ECC endpoints configured with the virtualization client and Slingshot is required

5.3.3 Technical Configuration Highlights

- Hyperdrive is delivered via application virtualization and launched using the configured access (generic vs named user).
- ECC endpoint configuration utilizes Slingshot and Imprivata Connector for Epic Hyperdrive to perform SSO.
- Simplifies application virtualization platform infrastructure needed, maintaining a single server image for both host and ECC site(s).
- Requires separate application virtualization platform
- Requires host to publish a separate application for Epic Hyperdrive for ECC sites to execute on the ECC-shared application virtualization server.

5.3.4 Operational Notes

- ECC relies on host virtualization uptime, performance, and change control.
- Published application Hyperdrive launch performance is slower than locally-installed Hyperdrive
- Requires management of a separate published application specific to ECC user accounts.
- Trust relationships will reduce administrative tasks for:
  - provisioning and de-provisioning directory accounts for ECC endpoints and users
  - maintaining calculated passwords for ECC endpoints

5.4 Host-managed Individual ECC Site Application Virtualization

In this model, the host delivers Hyperdrive through an application virtualization platform dedicated to each ECC site. This model allows for security and network isolation between the host site and ECC sites.

5.4.1 Common Use Cases (See Section 3.5)

- Host chooses not to provision ECC user accounts into their corporate directory.
- If host chooses virtualization access model that requires a trust, host does not have to build a trust between their corporate directory and each ECC site directory.
  - Trust relationships for each ECC site will be built through the separate host-managed ECC site directory.

5.4.2 Required Components

- Host-managed ECC-dedicated virtualization environment
- Hyperdrive installed and published within the ECC-dedicated environment
- ECC endpoints configured with the virtualization client
- Slingshot is optional for auto-launch and 'double hops'

5.4.3 Technical Configuration Highlights

- Hyperdrive is delivered via application virtualization and launched using the configured access (generic vs named user).
- Imprivata Connector for Epic Hyperdrive is installed on the application virtualization server with the Imprivata agent directed to the ECC site's EAM instance to perform SSO authentication.
- Slingshot is optional for auto-launch
- Slingshot is required for 'double hops'
- Optional: Epic can be configured to authenticate users via LDAP, using the ECC site's directory.

5.4.4 Operational Notes

- Requires host to maintain separate application virtualization images for each ECC site.
- There are additional network configuration requirements such as:
  - Security to allow communications between application virtualization servers to communicate with each respective ECC site's EAM appliances.
  - Network path to allow the Imprivata agent on the application virtualization server to communicate with each respective ECC site's EAM appliances.
  - DNS name resolution

5.5 EPCS Workflow Notes

- Host-provided EPCS
  - Host EAM instance is the source of authentication and workflow policy, which defines allowable authentication methods.
  - ECC prescribers must be identity-proofed and enrolled in host's EAM instance for EPCS.
  - Imprivata Connector for Epic Hyperdrive **installed on the ECC endpoint** should be configured to not perform local EPCS authentication
  - Imprivata Connector for Epic Hyperdrive installed on the **application virtualization servers** will perform EPCS authentication with host's EAM instance.
  - EPCS can be alternatively configured to use OIDC in lieu of EPCS installed on application virtualization servers. See Section 6 for more information. Additional configuration needs to be completed in the host EAM instance and in Epic.
  - Any provider could perform EPCS authentication from any host endpoint or their respective ECC endpoint.
- ECC-provided EPCS
  - ECC EAM instance is the source of authentication and workflow policy, which defines allowable authentication methods.
  - ECC prescribers must be identity-proofed and enrolled in ECC's Imprivata EAM for EPCS.
  - Imprivata Connector for Epic Hyperdrive installed on ECC endpoints should be configured to perform local EPCS authentication.
  - Limits ECC EPCS providers from performing EPCS from anywhere but at their respective ECC site.

NOTE:
Electronic Prescribing for Controlled Substances (EPCS) is the secure, digital transmission of prescription data for controlled substances (Schedules II-V) directly from a provider to a pharmacy, mandated in most U.S. states and for Medicare Part D. EPCS requires strict DEA-compliant, two-factor authentication.

6. EPCS and Mobile EPCS

Mobile EPCS allows providers to securely sign and transmit prescriptions for controlled substances using smartphones or tablets. This functionality satisfies DEA's requirements for strong authentication, using facial recognition, that previously prohibited EPCS order signing from being performed on the same device that performed multi-factor authentication.

6.1 Standard EPCS Ownership Configurations

Host-provided EPCS

- Host owns identity proofing, enrollment, and EPCS workflow policy.
- ECC prescribers must be enrolled into the host EAM instance via an Imprivata agent connected to the host Imprivata appliance.
- All providers enrolling into the host EAM instance enables EPCS authentication at both host and ECC site.

ECC-provided EPCS

- ECC owns identity proofing, enrollment, and EPCS workflow policy.
- ECC prescribers who travel to the host site must complete a separate enrollment for EPCS within the host EAM instance.

6.2 Host-provided EPCS (Locally Installed Hyperdrive and Application Virtualization)

Locally Installed Hyperdrive

- EPCS authentication is executed on the ECC endpoint and completed through OIDC.
  - OIDC authentication currently supports the following modalities: Imprivata ID, One Time Password (OTP) tokens and facial recognition.
- Provider must complete supervised enrollment with host EAM instance.
- Workflow policies, managed by the host, define allowable authentication modalities.

Host-delivered application virtualization for Hyperdrive

- EPCS authentication occurs from within virtualized Hyperdrive application and are evaluated against the host EAM instance.
- Provider must complete supervised enrollment with host EAM instance.
- Workflow policies, managed by the host, define allowable authentication modalities.
- Imprivata Connector for Epic Hyperdrive installed on ECC endpoint should be configured to not perform local EPCS authentication

- EPCS authentication can be completed using the Imprivata Connector for Epic Hyperdrive or by OIDC.

6.3 ECC-provided EPCS (Locally Installed Hyperdrive and ECC-managed Application Virtualization)

Locally Installed Hyperdrive

- EPCS authentication occurs from ECC endpoints and are evaluated against the ECC EAM instance.
- Provider must complete supervised enrollment within ECC's EAM instance.
  - Individual Identity Proofing can be provided by completing identity proofing with a Certificate Authority (does not require an EPCS enrollment supervisor).
- Workflow policies, managed by the ECC site, define allowable authentication modalities.
- EPCS authentication can be completed using the Imprivata Connector for Epic Hyperdrive.

ECC-managed application virtualization for Hyperdrive

- EPCS authentication occurs from within virtualized Hyperdrive application and are evaluated against the ECC EAM instance.
- Provider must complete supervised enrollment with ECC EAM instance.
  - Individual Identity Proofing can be provided by completing identity proofing with a Certificate Authority (does not require an EPCS enrollment supervisor).
- Workflow policies, managed by the ECC site, define allowable authentication modalities.
- EPCS authentication can be completed using the Imprivata Connector for Epic Hyperdrive in conjunction with Slingshot
- ECC prescribers who travel to the host site must complete separate enrollment within the host EAM instance.

6.4 Mobile EPCS workflows (Host vs ECC)

Imprivata's Mobile EPCS solution enables an additional modality to complete EPCS authentication using facial recognition via Imprivata ID.

Mobile EPCS workflow policy is configured within the host or ECC EAM instance that evaluates the EPCS authentication.

The required mobile EPCS license must be applied to the reference EAM instance.

7. Thin-client and VDI Scenarios

Thin/zero clients and VDI add another layer between clinicians and Hyperdrive. Imprivata agents and Connectors must execute inside a Windows session (application virtualization server or VDI desktop) for SSO and EPCS workflows to function.

7.1 Thin/Zero Clients with Application Virtualization-based Hyperdrive

Thin or zero clients usually run an application virtualization platform or a vendor-specific client. The Imprivata integration may use thin-client firmware plus the Imprivata agent and Connector inside the application virtualization session.

7.2 Locally Installed Hyperdrive Workflow with Full VDI Desktops Included

- Hyperdrive, Imprivata agent, and Imprivata Connector are installed in a Windows VDI image.
- Thin clients present the VDI session.

This behaves like Locally Installed Hyperdrive from Hyperdrive/EAM perspective but adds the VDI infrastructure overhead.

7.3 EPCS in Thin-client and VDI Environments

EPCS is executed in the Windows session where the Imprivata agent and Imprivata Connector are installed.

If performing EPCS authentication via OIDC, Imprivata agent and Connector are not required to be present on thin-client and VDI environments.

Authentication modalities, as defined in the Imprivata Supported Components document, must be usable from that remote environment.