imprivata®

Product Documentation

Installing and Configuring the Imprivata macOS Agent

Imprivata macOS Agent 26.1

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 26.1

This document includes the following sections:

What's New

The Imprivata macOS agent releases independently of Enterprise Access Management with SSO. As a result, the agent release number might be different than that of Enterprise Access Management.

> **NOTE:**
> Regardless of the Imprivata macOS agent version number, the agent is compatible with all currently maintained versions of Imprivata Enterprise Access Management with SSO. For a list of the maintained versions, see "Imprivata Enterprise Access Management with SSO Supported Components" in the Imprivata Environment Reference.

26.1

This release introduces the following:

Log out Epic on User Switch

This release adds limited support for Epic Hyperdrive locking behavior on a shared workstation. Specifically, through the Imprivata Connector for Epic Hyperdrive, the macOS agent can now log out the Epic Hyperdrive session on user switch. No additional configuration is required as:

- The Connector for Epic Hyperdrive is installed with the macOS agent.
- The Connector for Epic Hyperdrive automatically logs out the Epic Hyperdrive session on user switch. Configuring a computer policy is not required.

This functionality requires the following:

- The macOS agent is configured as a shared workstation (type 2) agent.
- Epic Hyperdrive is running 100.2602.2 (20260217.1137) or later.
- Imprivata appliances are running 26.1 HF 1 or later.

Report on macOS Agent Deployments

You can now view and filter details about:

- Which workstations the macOS agent is deployed.
- The macOS version of those workstations.
- The version of the macOS agent on each workstation.

These details are available from the following pages and reports in the Imprivata Admin Console:

- The **Computers** page, including the individual details pages for a specific host. (**Computers** > **Computers**).
- The **Computer Details** report. (**Report** > **Computer Details**).
- The **Agent Deployment** report (**Report** > **Agent Deployment Report**).

For more information about reporting, see Using Reporting Tools.

Shared Workstation Support

By default, the macOS agent is installed as single-user agent (type 1 agent) for private workstations.

- You can now enable the macOS agent to support multiple users on a shared workstation (type 2 agent).
- In support of shared workstations, the agent can also be configured to clean up users sessions on user switch.

For more information about enabling type 2 support and user session cleanup, see Configuring the Agent for Shared Workstations and Cleanup User Sessions on User Switch.

Interactive Installer and SSL

To further reduce manual steps in the installation process, the interactive installer now lets you import the root CA that signed the Imprivata appliance's SSL certificate into the system keychain.

For more information, see Using the Interactive Installer.

25.7

This release introduces the following:

Web SSO Support for OpenID Connect and SAML Authentication

This releases adds Web SSO support for authenticating to OpenID Connect (OIDC) and SAML-enabled applications. You manage SSO to these applications by configuring Web SSO profiles.

For more information about Web SSO, see getting started with OIDC or SAML.

Using Web SSO requires that the Imprivata Chrome extension be allowed to run in the web browser. While a separate installation is not required, you must enable the extension after installing the Imprivata macOS agent.

- Web SSO support is limited to Google Chrome and Microsoft Edge Chromium. You can enable the extension either manually or through an MDM.

  For more information about enabling it manually, see enabling the Imprivata Chrome extension
- The Island web browser is not supported.

Interactive Installer

The Imprivata macOS agent installer package has added an interactive installer intended for manual, interactive installation on endpoints in a test environment or for installation on just a few endpoints.

The macOS agent installer package contains the following items:

- The `Eam_Agent_Installer.app` application bundle for manual, interactive installation on endpoints.

  The interactive installer guides you through specifying the Imprivata appliance URL and importing the configuration profile (`ImprDesktopAgent.mobileconfig`).

- The `eam-mac-agent.pkg` installer package for distribution via your MDM.
- The `ImprDesktopAgent.mobileconfig` configuration profile for distribution via your MDM.

25.6

This release introduces the following:

Non-disruptive Upgrades

Upgrading the Imprivata macOS agent no longer requires you to restart the Mac device.

Endpoint-specific Events Now Included in Reports

Audit logs have been enhanced to included endpoint-specific events. Examples of events include but are not limited to "Locked" and "Startup Agent".

For more information on reporting, see Using Reporting Tools.

25.5

This release introduces the following:

Added Support for macOS 26 (Tahoe)

This release adds support for macOS 26. The Imprivata macOS agent can now be installed on devices running macOS Tahoe.

Improved Epic Hyperspace Session Security on Multiple Workstations

When a user is logged into Epic on a Mac workstation and then logs into Epic on another Mac or Windows workstation, you can configure Walk-Away Security to lock the first Mac workstation. Consider the following:

- Locking occurs only when the initial workstation is a Mac.
- Locking does not occur if the initial workstation is Windows.

For more information, see Locking a Mac Workstation on Secondary Epic Hyperspace Login.

25.4

This release introduces the following:

Enhanced SSO Capabilities

The OpenID Connect and Epic Hyperspace workflow has been enhanced to support SSO when the Hyperspace client is configured to automatically launch after the user logs in.

Improved User Experience

This release includes the following enhancements:

- **Improved account creation messaging**—When users authenticate to a device for the first time, the account creation message now remains visible for longer, providing clearer feedback during the setup process.
- **New device lock messaging**—When users lock a device, a confirmation message now appears to indicate that the device is being locked, providing clear feedback before the lock screen appears.

25.3

This release introduces the following:

Support for Walk-Away Security Inactivity

You can now secure a Mac device when keyboard and mouse inactivity is detected. When the keyboard and mouse inactivity threshold is reached, the lock and warning behavior is currently limited to obscuring the desktop without a warning.

You manage this functionality from the computer policy in the Admin Console (**Computer policies** > **Walk-Away Security** tab). For more information about configuring inactivity-based detection, see the Imprivata Enterprise Access Management with SSO help.

Support for Imprivata Offline Authentication

Imprivata offline authentication (offline mode) is now supported. Offline authentication lets users log into Enterprise Access Management when an Imprivata agent cannot connect to the Imprivata server (appliance).

You manage this functionality from the user policy in the Admin Console (**User policies** > **Authentication** tab > **Desktop Access authentication** section). For more information about configuring offline authentication, see the Imprivata Enterprise Access Management with SSO help.

NOTE:
By design, the OpenID Connect and Epic Hyperspace workflow does not support offline mode. An OpenID Connect enabled application must be able to communicate with the Imprivata appliance to authenticate users.

25.2

Customize the Imprivata Login Screen

This release introduces the ability to customize the Imprivata login screen. You can now:

- Incorporate your organization's logo.
- Add a background image.
- Add a custom message to the side banner.

You manage these changes from the computer policy in the Admin Console (**Computer policies** > **Customization** tab). For more information, see the Imprivata Enterprise Access Management with SSO help.

Prerequisites

Be sure that your Mac devices, hardware, and the Imprivata enterprise meet the following prerequisites.

Supported macOS Versions

For more information about supported macOS versions, see the Imprivata Enterprise Access Management Supported Components.

> **NOTE:**
> The macOS agent supports Apple silicon processors only.

Minimum Epic Requirements

Epic SSO

SSO into Epic requires the following:

- Epic must be running May 2024 or later.
- Epic Hyperdrive is installed locally on each of your Mac devices.

Log out Epic on User Switch

Managing Epic Hyperspace locking behavior on user switch requires the following:

- The macOS agent is configured as a shared workstation (type 2) agent.
- Epic Hyperdrive is running 100.2602.2 (20260217.1137) or later.
- Imprivata appliances are running 26.1 HF 1 or later.

Supported Proximity Card Readers

For more information about supported proximity card readers, see Imprivata Enterprise Access Management with SSO Supported Components.

Supported Imprivata Appliance Versions

All currently maintained releases of Imprivata Enterprise Access Management are supported.

> **NOTE:**
> For a list of the maintained releases, see "Imprivata Enterprise Access Management with SSO Supported Components" in the Imprivata Environment Reference.

FileVault Considerations

By default, supported Mac devices use full disk encryption. Specifically:

- The volume encryption key is protected by the hardware UID in the Secure Enclave.
- Storage is soldered to the main board and does not operate if removed.

For additional protection, Apple offers FileVault. FileVault protects the volume encryption key with a combination of the hardware UID and a user's password.

The Imprivata macOS agent can co-exist with FileVault. When FileVault is enabled on a Mac device:

- Users must type their user name and password during the boot process.
- The Mac device pauses the boot process to wait for the credentials of a user who had previously logged into the device.
- After a user enters their credentials, and the volume is unencrypted, the Imprivata login screen appears and any user can tap their badge to login to their desktop.

Using the Imprivata macOS agent with FileVault requires that Apple's default credential pass-through be disabled. To disable the default credential pass-through, run the following command from the terminal:

```
sudo defaults write /Library/Preferences/com.apple.loginwindow \
           DisableFDEAutoLogin -bool YES
```

NOTE:
To avoid the required manual interaction at boot, Imprivata recommends relying on the Mac's default disk encryption and disabling FileVault on shared devices. This simplifies the desktop access workflow across multiple users.

To disable FileVault, configure the following setting: **Settings** > **Privacy & Security** > **File Vault** '**Off**'.

Enabling Recovery Lock

Imprivata recommends enabling macOS Recovery Lock via MDM. This prevents unauthorized file access when using the Mac's Recovery Mode.

NOTE:
For more information about enabling Recovery Lock, see your MDM vendor documentation.

Installing the Imprivata Agent

Complete the following steps to install the Imprivata macOS agent.

> **NOTE:**
> A separate installation of the Imprivata Connector for Epic Hyperdrive is not required. The Connector for Epic Hyperdrive is bundled with the agent.

Imprivata Enterprise Access Management Configuration

In this section you:

- Identify the Imprivata appliance URL.
- Enable access to the Imprivata ProveID Web and ProveID Embedded API.

Step 1: Identifying the Imprivata Appliance URL

As part of the installation process, you specify the Imprivata appliance that the Imprivata macOS agent should connect to.

To locate the URL:

1. From the Imprivata Admin Console, go to the **Status** section.
2. Copy the appliance URL.

   During an interactive installation, you enter the Imprivata appliance URL in the installer dialog.

   When deploying the Imprivata macOS agent to endpoints using an MDM, you specify the Imprivata appliance URL in the configuration profile.

Step 2: Enabling Access to the Imprivata ProveID Web and ProveID Embedded API

The Imprivata macOS agent requires access to the Imprivata ProveID Web and ProveID Embedded API.

To enable access:

1. Go to the **gear** icon menu.
2. Click **API Access**, and then go to the **ProveID - API access and security** section.
3. Select **Allow full API access via ProveID Web and ProveID Embedded**.
4. Depending on your version of Enterprise Access Management, select one of the following:
   - 25.1 or later: **Imprivata Agent for macOS**.
   - 24.3 or earlier: **Future 4**.
5. Click **Save**.

Mac Configuration

In this section you:

- Configure several system settings related to display, security, and privacy.
- Install the Imprivata macOS agent, either using the interactive installer or deploying via your MDM.
- Enable device and accessibility permissions for the Imprivata macOS agent.

Option 1: Using the Interactive Installer

The interactive installer is intended for manual, interactive installation on endpoints in a test environment, or for installation on just a few endpoints.

> **NOTE:**
> To deploy the Imprivata macOS agent by distributing it with your MDM, see Option 2: Deployment via an MDM.

Step 1: Configuring System Settings

Configure the following system settings related to display, security, and privacy:

Setting	Required value
Settings > **Displays** > **Automatically adjust brightness**	**Off**
Settings > **Privacy & Security** > **Allow accessories to connect**	**Always**
Settings > **Privacy & Security** > **Lockdown Mode**	**Off**

Step 2: Locating the Root CA

As part of the installation, you import the root CA that signed the appliance's SSL certificate into the system keychain.

Make sure that the root CA is available from a location that is accessible to the installer.

- **Imprivata self-signed certificate** – By default, the Imprivata appliance creates a self-signed SSL certificate as part of its installation process. If the enterprise is continuing to use the self-signed certificate, download the root CA from the Imprivata Appliance Console (**Security** > **SSL** tab).
- **CA-signed certificate** – If the default SSL certificate has been replaced, get the root CA from your certificate authority.

> **NOTE:**
> While the installer imports the root CA into the system keychain, it is not automatically trusted. You are prompted to trust the certificate manually.

Step 3: Running the Interactive Installer

To run the interactive installer:

1. Copy the application bundle file (`Eam_Agent_Installer.app`) to the Mac device.
2. Double-click the application bundle to launch the **Installer** app.
3. On the **Appliance URL setup** page, type the **Imprivata appliance URL** that you saved.
4. To load the configuration profile, click **Load Profile**:
   a. In System Settings, locate the Imprivata EAM Agent Configuration profile (`.mobileconfig`) in the right sidebar. Double-click the profile to review its contents.
   b. Click **Install** and follow the prompts to approve the profile.
5. In the interactive installer, click **Continue**.
6. On the **SSL Certificates** page, click **Select Certificate**, upload the root CA, and follow the prompts to manually verify that the certificate is trusted.
7. In the interactive installer, click **Continue**, then **Install**. Type a username and password to allow the script to make changes, and then click **Finish**.

The Imprivata macOS agent interactive installer automatically configures the following system settings:

Setting	Required value
Settings > **Battery**	• **Low Power Mode** > **Never** • **Options** > **Slightly dim the display on battery**: **OFF** • **Options** > **Prevent automatic sleeping on power adapter when the display is off**: **ON** • **Options** > **'Wake for network access'** > **Always**

NOTE:
When prompted, allow the Connector for Epic Hyperdrive to access the local network.

Step 4: Enabling Device Permissions

The Imprivata macOS agent must be allowed to:

- Control the device.

  As part of the installation, you enabled the Input Monitoring permission for the Imprivata desktop agent. In this step, you are giving the Imprivata device manager the Input Monitoring permission. Both the desktop agent and the device manager must be granted permission.

- Receive USB events.

Configure the following settings:

Mac device setting	Step
Settings > **Privacy & Security** > **Accessibility**	Click **+** and select **/Applications/ Imprivata Desktop Agent.app**.
Settings > **Privacy & Security** > **Accessibility**	Click + and select **/Library/Application Support/imprivata/Imprivata Root Service.app**
Settings > **Privacy & Security** > **Input Monitoring**	Click **+** and select **/Library/Application Support/imprivata/Imprivata Device Manager.app**.

Mac device setting	Step
Settings > **Privacy & Security** > **Input Monitoring**	Applies to macOS 26 (Tahoe) only. In the list of available applications, enable **Imprivata Desktop Agent** to allow input monitoring.

Step 5: Restarting the Device

Completing the installation requires that you restart the Mac device:

1. Restart the Mac device.
2. Authenticate using the Imprivata macOS agent.

Option 2: Deployment via an MDM

Apply the following steps to your MDM profile.

> **NOTE:**
> For more information on deploying configuration profiles, see the documentation for your MDM.

Step 1: Configuring System Settings

Configure the following system settings related to display, security, and privacy:

Setting	Required value
Settings > **Displays** > **Automatically adjust brightness**	**Off**
Settings > **Privacy & Security** > **Allow accessories to connect**	**Always**
Settings > **Privacy & Security** > **Lockdown Mode**	**Off**

Step 2: Running the Installer

To run the installer:

1. Copy the package file (`eam-mac-agent.pkg`) to the Mac device.
2. Double-click the package to launch the **Installer** and complete the installation.

   The Imprivata macOS installer automatically configures the following system settings:

Setting	Required value
Settings > **Battery**	• **Low Power Mode** > **Never** • **Options** > **Slightly dim the display on battery**: **OFF** • **Options** > **Prevent automatic sleeping on power adapter when the display is off**: **ON** • **Options** > **'Wake for network access'** > **Always**

> **NOTE:**
> As part of the installation, you are prompted to enable Input Monitoring permission for the Imprivata desktop agent. Enable the permission.

Step 3: Specifying the Imprivata Appliance URL

You specify the Imprivata appliance URL so the Imprivata macOS agent can connect to it and obtain the enterprise topology.

To specify the URL:

1. Copy the configuration profile (`ImprDesktopAgent.mobileconfig`) to the desktop by running the following command from the terminal:

   ```
   cp "/Library/Application Support/imprivata/ImprDesktopAgent.mobileconfig"
   ~/Desktop
   ```

2. Right-click the `ImprDesktopAgent.mobileconfig` profile, and open it with TextEdit. Edit it to include the Imprivata appliance URL:
   a. Under the line `<key>applianceURL</key>` there is a placeholder `<string></string>`. Add the Imprivata appliance URL within the empty key tags.

      For example:
      `<string>https://example-appliance.com</string>`
   b. Save the file.
3. Install the configuration profile:
   a. Double-click the file to make it accessible from System Preferences.
   b. Go to **System Preferences** > **Device Management**, and double-click it to install it.

Step 4: Enabling Device Permissions

The Imprivata macOS agent must be allowed to:

- Control the device.

  As part of the installation, you enabled the Input Monitoring permission for the Imprivata desktop agent. In this step, you are giving the Imprivata device manager the Input Monitoring permission. Both the desktop agent and the device manager must be granted permission.
- Receive USB events.

Configure the following settings:

Mac device setting	Step
Settings > **Privacy & Security** > **Accessibility**	Click **+** and select **/Applications/ Imprivata Desktop Agent.app**.
Settings > **Privacy & Security** > **Accessibility**	Click + and select **/Library/Application Support/imprivata/Imprivata Root Service.app**
Settings > **Privacy & Security** > **Input Monitoring**	Click **+** and select **/Library/Application Support/imprivata/Imprivata Device Manager.app**.
Settings > **Privacy & Security** > **Input Monitoring**	Applies to macOS 26 (Tahoe) only. In the list of available applications, enable **Imprivata Desktop Agent** to allow input monitoring.

Step 5: Restarting the Device

Completing the installation requires that you restart the Mac device:

1. Restart the Mac device.
2. Authenticate using the Imprivata macOS agent.

> **NOTE:**
> When prompted, allow the Connector for Epic Hyperdrive to access the local network.

Step 6: Configuring Trust between the Imprivata Agent and the Appliance

You must add a signed SSL certificate from the Imprivata appliance to the Mac device. The certificate must either be:

- Signed by an Intermediate Certificate Authority (CA) or root CA equivalent.
- Self-signed by the Imprivata appliance CA that was created when the Imprivata enterprise was deployed.

Using a Self-Signed Certificate

To use a self-signed certificate:

1. From the Imprivata Appliance Console, go to the **Security** page > **SSL** tab.
2. Download the certificate. The default certificate name is `ssoCA.cer`.
3. From the Mac device, use the **Keychain Access** utility to install the certificate under **System** and enable trust (**Always Trust**).

Using a CA-signed Certificate

To use a certificate that is signed by a third-party CA:

1. Save a copy of the third-party root CA that was used to sign certificates on the Imprivata appliance.
2. From the Mac device, open **Keychain Access**, and install the certificate under **System Roots**.

Configuring the Agent for Shared Workstations

By default, the macOS agent is installed as single-user agent (type 1 agent) for private workstations. You can manually enable the agent to support multiple users on a shared workstation (type 2 agent). When configured as a type 2 agent:

- A local generic user is used to establish the login session. The workstation remains logged in under this account.
- When an Imprivata user authenticates to the workstation, the macOS agent manages a named user session for single sign-on (SSO) within the existing generic session.

Disable Password Autofill

To prevent the exposure and reuse of stored credentials across user sessions, disable password autofill on all shared workstations.

Use an MDM to disable the `AllowPasswordAutoFill` flag.

Enable the Agent for Shared Workstations

You use the Imprivata configuration profile (`ImprDesktopAgent.mobileconfig`) to:

- Specify the local generic user credentials.
- Configure the macOS agent as a type 2 agent.

To enable the agent for shared workstations:

1. Copy the configuration profile (`ImprDesktopAgent.mobileconfig`) to the desktop by running the following command from the terminal:

   ```
   cp "/Library/Application Support/imprivata/ImprDesktopAgent.mobileconfig"
   ~/Desktop
   ```

2. Right-click the `ImprDesktopAgent.mobileconfig` profile, and open it with TextEdit.
3. Locate the `agentType` key/value pair and change the value to **2**.
4. Locate the `genUsername` key/value pair and the `genSecret` key/value pair to specify the credentials for the local generic user.
5. Save and install the configuration profile.

Key	Type	Description
`genUsername`	string	Specifies the username of the generic user.
`genSecret`	string	Specifies the password of the generic user. The value must be prefixed to indicate the password format. Supported formats are: • `0:` plain text password • `1:` base64-encoded password • `2:` encrypted password Example values: • `0:example_password` (plain text) • `1:bXlQYXNzd29yZA==` (base64-encoded) • `2:ENCRYPTED_VALUE` (encrypted)

Encrypting a Password Using the Public Certificate

The macOS agent installer includes a public certificate that you can use to encrypt a password before adding it to the Imprivata configuration profile. After the agent is installed, the public certificate (`impr_cert.pem`) is available at `/Library/Application Support/imprivata/`.

For example, navigate to the directory that contains the public certificate and run the following command to create an encrypted password.

```
echo "examplepassword" | openssl pkeyutl -encrypt -pubin -inkey impr_public.pem -
pkeyopt rsa_padding_mode:oaep -pkeyopt rsa_oaep_md:sha256 -pkeyopt rsa_mgf1_
md:sha256 | openssl base64 -A
```

Use the resulting base64-encoded string to specify the password for the local generic user.

Example - Imprivata configuration profile configured as a type 2 agent

```
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
"http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
    <key>PayloadContent</key>
    <array>
        <dict>
        ...
            <key>agentType</key>
            <integer>2</integer>
            <key>genUsername</key>
            <string>example_user</string>
            <key>genSecret</key>
            <string>2:MIIBRgYJKoZIhvcNAQcDoIIBNzCCATMCAQAx...</string>
```

Cleanup User Sessions on User Switch

By default, active sessions are not disconnected on user switch. For example, any application or web browser that a user opens on a shared desktop remains open on user switch:

- The user must manually log out/close all active sessions to prevent the next user from accessing these resources.
- The exception to the default behavior is Epic. When Epic SSO is configured, the Imprivata Connector for Epic Hyperdrive can be used to logout Epic Hyperspace. For more information, see Epic Hyperdrive and Desktop Locking Behavior.

You can configure the Imprivata configuration profile (`ImprDesktopAgent.mobileconfig`) to clean up user sessions by specifying one of the following:

- **Script path** – The absolute path to a script that should execute on user switch.
- **Command** – A command, with optional arguments, that should execute on user switch.

> **NOTE:**
> If both options are configured, the script takes precedence and the command is not executed.

Use a Script to Cleanup User Sessions

You can specify a single script to be executed on user switch. The script can run as:

- The interactive user.
- Root, including a privileged helper process that runs as root.

> **NOTE:**
> The script cannot be world-writable.

To configure the configuration profile:

1. Copy the configuration profile (`ImprDesktopAgent.mobileconfig`) to the desktop by running the following command from the terminal:

```
cp "/Library/Application Support/imprivata/ImprDesktopAgent.mobileconfig"
~/Desktop
```

2. Right-click the `ImprDesktopAgent.mobileconfig` profile, and open it with TextEdit.
3. Add the following keys:

Key	Type	Description
`userSwitchScriptPath`	String	Specifies the absolute path of the script.
`userSwitchRunAs`	String	Specifies the execution context for the script. Supported values include `interactiveUser` or `root`.

Example - Imprivata configuration profile: user switch script (interactive user)

```
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
"http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
    <key>PayloadContent</key>
    <array>
        <dict>
        ...
            <key>userSwitchScriptPath</key>
            <string>/Library/Imprivata/scripts/user_switch.sh</string>
            <key>userSwitchRunAs</key>
            <string>interactiveUser</string>
```

Example - Imprivata configuration profile: user switch script (root / privileged helper)

```
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
"http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
    <key>PayloadContent</key>
    <array>
        <dict>
        ...
            <key>userSwitchScriptPath</key>
            <string>/Library/Imprivata/scripts/user_switch_root.sh</string>
            <key>userSwitchRunAs</key>
            <string>root</string>
```

Sample - Script that closes Google Chrome

```
#!/bin/sh
/usr/bin/touch /tmp/hook_ran_ok
/usr/bin/pkill -f "Google Chrome"
/bin/mkdir -p /tmp/Google_ChromeTestFolder
exit 0
```

Use a Command to Cleanup User Sessions

You can specify a single command, including optional arguments, to be executed on user switch. The command can run as:

- The interactive user.
- Root, including a privileged helper process that runs as root.

To configure the configuration profile:

1. Copy the configuration profile (`ImprDesktopAgent.mobileconfig`) to the desktop by running the following command from the terminal:

   ```
   cp "/Library/Application Support/imprivata/ImprDesktopAgent.mobileconfig"
   ~/Desktop
   ```

2. Right-click the `ImprDesktopAgent.mobileconfig` profile, and open it with TextEdit.
3. Add the following keys:

Key	Type	Description
`userSwitchCommand`	Array	The first element is the command, followed by optional arguments.
`userSwitchRunAs`	String	Specifies the execution context for the command. Supported values include `interactiveUser` or `root`.

Example - Imprivata configuration profile: user switch command with arguments (interactive user)

```
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
"http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
    <key>PayloadContent</key>
    <array>
        <dict>
        ...
            <key>userSwitchCommand</key>
            <array>
            <string>/usr/bin/pkill</string>
            <string>-f</string>
            <string>Google Chrome</string>
```

```
            </array>
            <key>userSwitchRunAs</key>
            <string>interactiveUser</string>
```

Example - Imprivata configuration profile: user switch command (root / privileged helper)

```
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
"http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
    <key>PayloadContent</key>
    <array>
        <dict>
        ...
            <key>userSwitchCommand</key>
            <string>/usr/bin/killall cfprefsd</string>
            <key>userSwitchRunAs</key>
            <string>root</string>
```

Managing Background User Sessions on Mac Devices

By default, the macOS lets multiple users login, but only allows one user session to be interactive at any time. All other user sessions remain in the background.

- This behavior conflicts with how Epic Hyperspace operates.
- Epic Hyperspace requires that all background user sessions be signed out.

To enable the Epic Hyperspace workflow, background user sessions are signed out by the Imprivata macOS agent.

> **NOTE:**
> If the background user session contains a modal dialog, it is not possible to sign out of the session. This is due to a limitation in the macOS API. Apple is investigating.

If you are not configuring the Epic Hyperspace workflow, you can disable the default Imprivata agent behavior.

To stop signing out of background sessions:

1. Go to `/Library/Application\ Support/imprivata/` and edit `ImprDesktopAgent.mobileconfig`.
2. Locate **SignOutBackgroundSession**. The default value is **<true/>**.
3. Set the value to **<false/>** and apply the profile to your Mac devices.

Upgrading and Uninstalling the Imprivata Agent

You upgrade and uninstall the Imprivata macOS agent manually.

Upgrading

To upgrade the Imprivata macOS agent:

1. Copy the upgraded package file (`eam-mac-agent.pkg`) to the Mac device.
2. Double-click the package file to launch the **Installer** app and complete the installation.
3. Allow the Imprivata agent to receive USB events. This step is not required in most cases, if it was performed during the initial installation.
   a. Go to **Settings** > **Privacy & Security** > **Input Monitoring**.
   b. Click **+**, and then select **/Library/Application Support/imprivata/Imprivata Device Manager.app**.

Uninstalling

To uninstall the Imprivata macOS agent:

1. *(Optional)* Disable the Imprivata agent from controlling the device:
   a. Go to **Settings** > **Privacy & Security** > **Accessibility**.
   b. Select **Imprivata Desktop Agent.app**, and click **-**.
   c. If prompted, enter root credentials.
2. *(Optional)* Disable the Imprivata agent from receiving USB events:
   a. Go to **Settings** > **Privacy & Security** > **Input Monitoring**.
   b. Select **Imprivata Device Manager.app**, and click **-**.
   c. If prompted, enter root credentials.
3. Copy `eam-mac-agent-uninstaller.pkg` to the Mac device.
4. Double-click the package file to launch the **Uninstaller** app to remove the Imprivata agent.

OpenID Connect and Epic Hyperspace

Imprivata Web SSO with OpenID Connect (OIDC) extends single sign-on (SSO) functionality to Epic Hyperspace. When implemented:

- The Imprivata Identity Provider (IdP) window appears when the Hyperspace client is launched.
- The Imprivata macOS agent logs the authenticated user in.

Support for OIDC requires that:

- Imprivata appliances be configured to communicate with the Imprivata Cloud service and SSO is configured and enabled.
- Epic Hyperspace is configured to communicate with the Imprivata environment.

> **NOTE:**
> If the Imprivata macOS agent is not present or the user is not enabled in Enterprise Access Management, the Imprivata IdP windows does appear, but can be closed. The user can authenticate to Hyperspace with their username and password, instead of using Imprivata ID plus a password.

Imprivata Enterprise Access Management Configuration

In this section you:

- Configure the Imprivata appliance to connect to the Imprivata cloud.
- Create and deploy an Imprivata single sign-on application profile using a template that is designed for applications that use OpenID Connect.
- Associate the application profile with your Mac device users.
- Configure a trusted certificate for the web server that is installed with the Imprivata macOS agent.

Step 1: Configuring a Connection to the Imprivata Cloud

Imprivata provides you with an Enterprise ID and one-time cloud provisioning code. This information is required to configure a connection to the Imprivata cloud.

1. In the Imprivata Admin Console, click the **gear** icon, and then click **Cloud connection**.
2. Enter your Enterprise ID and cloud provisioning code.
3. Click **Establish Trust**.

You can review the status of your enterprise's connection to the Imprivata cloud at any time:

- You can view status notifications in the Imprivata Admin Console. The cloud connection status of every appliance within every site is available (**gear** icon menu > **Cloud connection** page).
- Every appliance host is listed with its status. If there are problems with a connection, a recommendation for resolving the problem is provided.

Step 2: Creating an OIDC Application Profile

An Imprivata application profile is required for Epic Hyperspace. The profile allows the Imprivata appliance to manage the Epic authentication request.

Creating the profile requires that you coordinate with Epic TS:

- Epic TS provides you a redirect URI. You need this URI to configure the application profile.

  Example of a redirect URI:

  ```
  https://<epic_interconnect_instance_
  name/path>/api/epic/security/oidc/authorizationcodereceiver
  ```

- You provide Epic TS with client credentials and the Imprivata OIDC metadata.

  Epic requires this information to update your Epic OIDC configuration.

To create the application profile:

1. From the Admin Console, click **Applications** > **Single sign-on application profiles**.
2. Click add **App Profile** > **Application using Open ID Connect**.
3. In **Application profile name**, enter **Epic login**.
4. In **Application user-friendly name**, enter **Epic Hyperdrive**.
5. In **Redirect URIs**, enter the URI that Epic provided you.
6. Click **Generate client credentials**, and copy the **Client ID** and **Client secret**.
7. Click **View and Copy Imprivata IdP OpenID Connect Metadata**.

> **NOTE:**
> Provide this information to Epic TS. Epic uses this information to update the Epic OIDC configuration.

Step 3: Deploying the Application Profile

1. From the list of application profiles, select the profile you created, and then click **Deploy**.
2. Go to the **Deployment** section, and select **Deploy this Application?**
3. Optional: By default, an application profile is configured to deploy to all users. If you want to limit the deployment to specific organizational units, groups, or users, deselect **Deploy to All Users and Groups?** and do the following.
   a. Select the domain that contains the target users.
   b. Select **These OUs, groups, and users**.
   c. Do one, two, or all three of the following:

- Click **Select OUs**, select the target organizational units, and then click **Done**.
- Click **Select Groups**, select the target groups, and then click **Close**.
- Enter a semi-colon separated list of specific users.

4. Leave the remaining settings unchanged, and click **Save**.

Step 4: Associating the OIDC Application Profile with Users

You associate the OIDC application profile with your macOS users by applying a user policy to Imprivata Web SSO workflows. This enables the OIDC workflows for your users.

To apply a user policy to Imprivata Web SS) workflows:

1. From the Imprivata Admin Console, click **Users** > **Workflow policy**.
2. Go to the **Web SSO workflows** section.

   This section includes a link on the right side. The text of this link varies depending on whether a user policy has been assigned.

   For example, the link might appear as **Associate user policies (0 users)**.
3. Click the link and select the user policy that is associated with your Mac devices.

Step 5: Configuring a Web Server Certificate

The Imprivata macOS agent must send Enterprise Access Management user session information to Epic using HTTPS. To meet this requirement, a local web server is installed with the Imprivata agent.

You must configure this web server with a trusted certificate. This certificate can be signed by the root certificate of one of the following:

- An external third-party CA.
- An internal enterprise CA, such as Microsoft Active Directory Certificate Services.

Installing the Root Certificate in to the Device Keychain

If the Mac device does not already have the root CA certificate, use the Keychain Access application to install it to the macOS keychain. Installing the root certificate ensures that the device trusts certificates that the root CA signs.

To install the root certificate:

1. From the Mac device, open the **Keychain Access** utility.
2. Install the certificate under **System** and enable trust (**Always Trust**).

Creating the Web Server Certificate

Create the web server certificate and sign it with the root CA certificate.

To create the certificate:

1. Create a private key for the web server by running the following command from the terminal:

```
openssl genrsa -out impr_server.key 2048
```

2. Create an OpenSSL configuration file with a Subject Alternative Name.

   An example of this file is available below.

3. Create a Certificate Signing Request for the private key by running the following command:

```
openssl req -new -key impr_server.key -out impr_server.csr -config
localhost.cnf
```

4. Sign the Certificate Signing Request by running the following command:

```
openssl x509 -req -in impr_server.csr -CA <root_certificate> \
                        -CAkey <root_key> \
                        -CAcreateserial -out impr_server.crt -days 500 \
                    -sha256 -extfile localhost.cnf -extensions v3_ext
```

   Where:

   - <*root_certificate*> is the root CA certificate. For example, `rootCA.pem`.
   - <*root_key*> is the private CA key. For example, *rootCA.key*.

The certificate (`impr_server.crt`) is signed by the CA and ready for use.

Example of the required OpenSSL configuration file

```
[ req ]
               default_bits       = 2048
               prompt             = no
               default_md         = sha256
               req_extensions     = req_ext
               distinguished_name = dn

               [ dn ]
               C = <US>
               ST = <State>
               L = <City>
               O = <Organization>
               CN = localhost

               [ req_ext ]
               subjectAltName = @alt_names

               [ alt_names ]
               DNS.1 = localhost

               [ v3_ext ]
            subjectAltName = @alt_names
```

Where:

- <*us*> represents your country
- <*State*> represents your state.
- <*city*> represents your city.
- <*organization*> represents your organization.

Configuring the Web Server to use the Certificate

The web server can now use the certificate (`impr_server.crt`).

To configure the web server to use the certificate:

1. Copy and replace the following files to**/Library/Application\ Support/imprivata/ImprWebServer**:
   - `impr_server.crt`
   - `impr_server.key`
2. Restart the web server by running the following command from the terminal:

```
sudo launchctl kickstart –k system/com.imprivata.ImprWebServer
```

Epic Hyperspace OpenID Connect Configuration

Completing the integration requires that you coordinate with Epic TS:

- Trust must be established between Epic Hyperspace and the Imprivata appliance.
- Additional Epic-specific parameters must be configured.

Step 1: Establishing Trust with the Imprivata appliance

Using the Imprivata single sign-on application that you created, provide the following to Epic TS:

- The client ID and client secret.
- The Imprivata (IdP) OpenID Connect Metadata.

Step 2: Configuring Epic Parameters

Coordinate with Epic TS to have the following parameters configured:

- Set the IdP window height to 756 pixels. This allows the Imprivata IdP window to display properly.
- Add **ACR** for the login device **OIDC** configuration. The login device configuration with OIDC needs to send an ACR as part of the request.

  The ACR should have the following value:
  `com:imprivata:oidc:epic:sso`
- Enable multiple sessions in the LWS record.
- Set **Close Hyperdrive on Logout** to **Yes** in the LWS record.

Locking a Mac Workstation on Secondary Epic Hyperspace Login

You can configure Walk-Away Security application inactivity to prevent a user from being concurrently logged in to Epic Hyperspace from multiple workstations. Consider the following:

- Detecting application inactivity is supported when Epic Remote Actions are set to either "Quit Last Session" or "Logout Last Session".
- This functionality applies to Mac workstations only.

Expected Workflow

1. A user is logged in to a Mac workstation and the Hyperspace client is launched. After working, they leave the workstation unattended.
2. The same user then logs in to another Mac or Windows workstation and the Hyperspace client is launched.
3. The initial Mac workstation is automatically locked.

> **NOTE:**
> The initial workstation must be a Mac. Locking does not occur if the initial workstation is Windows.

Step 1: Importing and Deploying the Hyperspace Client Application Profile

Import and deploy the required Imprivata application profile for the Hyperspace client (`macOS-profile-for-Epic-Hyperspace.xml`). This profile ships with the Imprivata macOS agent.

To deploy the application profile:

1. From a workstation where the Imprivata macOS agent is installed, go to **/Library/Application\ Support/imprivata/**
2. Locate the Imprivata application profile (`macOS-profile-for-Epic-Hyperspace.xml`) and download it to a location that is accessible to the Imprivata Admin Console.
3. In the Imprivata Admin Console, go to the **Applications** menu, and click> **Single sign-on application profiles**.
4. Select **Add App Profile**, and then click **Import from file** to upload the profile.
5. From the list of application profiles, select **Epic Hyperspace for macOS**, and then click **Deploy**.
6. Go to the **Deployment** section, and select **Deploy this Application?**
7. Optional: By default, an application profile is configured to deploy to all users. If you want to limit the deployment to specific organizational units, groups, or users, deselect **Deploy to All Users and Groups?** and do the following:

a. Select the domain that contains the target users.
b. Select **These OUs, groups, and users**.
c. Do one, two, or all three of the following:
   - Click **Select OUs**, select the target organizational units, and then click **Done**.
   - Click **Select Groups**, select the target groups, and then click **Close**.
   - Enter a semi-colon separated list of specific users.

8. Leave the remaining settings unchanged, and click **Save**.

Step 2: Configuring a Computer Policy for Application Inactivity

Configure your computer policy for application inactivity (Walk-Away Security). Enabling application inactivity requires that Epic Remote Actions be set to one of the following options:

- Logout Last Session
- Quit Last Session

To configure the computer policy:

1. In the Imprivata Admin Console, go to the **Computers** menu, and click **Computer policies**.
2. Open the computer policy assigned to your Mac devices, and click **Walk-Away Security**.
3. If it is not enabled, configure keyboard and mouse inactivity.

> **NOTE:**
> Lock and warning behavior is currently limited to obscuring the desktop without a warning.

4. Open **Advanced settings**, and go to the **Application activity tracking** section.
5. Under **Inactivity target app1**, select **Epic Hyperspace for macOS**.

> **NOTE:**
> Specifying a second target application is not supported.

6. Under **Target app 1 state**, select one of the following:
   - **User is logged off**
   - **Application is not running**
   - **User is logged off OR Application is not running**
7. Specify a period of time after which the workstation is locked, and click **Save**.

> **NOTE:**
> Specify a period of time that is less than the keyboard and mouse inactivity value. Specifying an inactivity warning for application inactivity is not supported.

Step 3: Conditional - Detecting User Logout

If Epic Remote Actions are set to "Logout Last Session", the following steps are required.

Enabling Device Accessibility Permissions

The Imprivata Root Service requires Accessibility permissions for the Imprivata macOS agent to detect when a user logs out.

To grant permission:

1. Go to **Settings** > **Privacy & Security** > **Accessibility.**
2. Click the **+** button, and select **/Library/Application Support/imprivata/Imprivata Root Service.app**.

Configuring the Hyperspace Title Bar Message

The Imprivata macOS agent detects user inactivity using the Hyperspace title bar message. Specifically, the agent must identify when:

- No one is logged into Hyperspace.
- A user is logged into Hyperspace.

To configure the agent to detect user inactivity:

1. Go to **/Library/Application\ Support/imprivata/** and edit `ImprDesktopAgent.mobileconfig`.
2. Locate the following key/value pair and enter the Hyperspace title bar message exactly as it appears when no one is logged into Hyperspace.

```
<key>PayloadContent</key>
                        <array>
                        <dict>
                        ...
                        <key>TitleMessageOnLogout</key>
                        <string></string>
                        ...
                        </dict>
                    </array>
```

3. Ensure that the message is different when a user is logged in to Hyperspace. For example, you can use other Epic data elements to append the user ID to the message.

> **NOTE:**
> The Imprivata macOS agent begins to detect the title bar message after the device has been locked and subsequently unlocked.

Imprivata SSO to the Citrix Storefront Web Portal

You can configure an Imprivata application profile to enable SSO to the Citrix Storefront Web Portal.

Limitations and Requirements

Consider the following:

- You must create the application profile from a Windows endpoint. The Imprivata macOS agent does not support the Imprivata Application Profile Generator (APG).

  As such, it is presumed that the Windows and macOS versions of the Citrix Storefront Web Portal use the same web controls to manage authentication.
- You can profile the Citrix Storefront Web portal login screen only:
  - Profiling any other screen type, such as login failure or success, is not supported.
  - No other options of the application profile are supported.

Profiling the Citrix Storefront Web Portal

When configuring the Imprivata APG application profile, you profile the browser tab in which the Citrix Storefront Web Portal is opened.

Step 1: Enabling the Imprivata Chrome Extension Object

Profiling an application that opens in a Chromium-based browser requires the Imprivata Chrome Extension.

- The Imprivata macOS agent installs, but does not enable, the extension from the Chrome Web store.
- After installing the Imprivata agent, enable the extension using a Mobile Device Management (MDM) solution, such as Jamf.

Step 2: Creating the Application Profile

Profile the browser tab in which the Citrix Storefront Web Portal opens.

To create the application profile:

1. From a Windows endpoint, log into the Imprivata Admin Console, and click **Applications** > **single sign-on application profiles**.
2. From **Add app Profile**, click **Windows application using APG**.
3. Profile the Citrix Storefront Web Portal login screen. At a minimum, the profile must include the following:
   - The username and password fields.
   - The control (button) that is used to submit the credentials.
4. Save the application profile and deploy it to your users.