HP Sure Access Enterprise 8.1 Release 3 Deployment Guide

Contents

Contents **2**
Notices **4**
Overview **5**
What problem does SAE solve? 5
How does SAE work? 5
How do I get started? 6
Deploy the HP Wolf Security Controller **7**
Enable SAE **8**
Manage SAE signing certificates manually 8
Provision endpoint devices **9**
Device requirements 9
Deploy the SCE and SAE endpoint software to users' devices 10
Configure SAE apps **12**
User permissions 12
App setup and settings 12
App appearance 13
App security features 13
App type configuration 14
Microsoft RDP 14
Host RDP 15
Match criteria 15
Other Host RDP settings 15
Citrix Receiver 16
Web Portal 16
SSH 16
Configure authentication with server certificates 17
Configure authentication with client certificates 17
Client certificate enrollment via SCEP 17
Windows certificate store 19
Static client certificates for testing 19
Connect over a VPN 19
Restrict outgoing connections 20
Combine allow-list with VPN connection 20
Logging 21
Deploy SAE apps to users' devices **22**

Create device groups 22
Apply SAE security policies to device groups 22
Deploy SAE apps to device groups 23
Update SAE app configurations 25
Remove SAE apps from devices 25
Monitor and troubleshoot SAE usage 26
Common errors and troubleshooting steps 26
"Warning: This app appears to be being used on this machine for the first time" 26
"Warning: The app cannot be used because the application definition could not be verified" 26
"Warning: The app cannot be used because there is a problem with persistent storage" 27
"Warning: The app cannot be used because the security requirements could not be met" 27
Ensure SAE policy is up to date 27
Reset the SAE Trusted Config on a user's device 27
Enable logging 28
Encrypt guest logs 28
Retrieve guest logs 29
Decrypt guest logs 29
Getting help 30

Notices

29 March 2024

Overview

HP Sure Access Enterprise (SAE) secures privileged access to high-value assets, including remote access to critical systems and infrastructure and connections to enterprise applications. By using hardware-enabled endpoint isolation to protect privileged activities, SAE effectively defends your organization's sensitive systems and data from targeted attacks.

What problem does SAE solve?

Users with access to mission-critical and high-value assets, including IT administrators, CIOs, OT and remote IoT administration staff, are often the subjects of targeted attacks. If a phishing scam or similar attack is successful and a privileged user's device is compromised, an attacker can exploit the user's privileges to gain access to business-critical systems.

With SAE, any privileged activity – such as connecting to an IAM server or accessing customer payment details or medical records – is isolated within a protected virtual machine. This isolation prevents attackers from gaining access to the high-value asset.

For example, consider an IT administrator opening a remote desktop session on their device to connect to an Active Directory server. As a user with elevated privileges, they are a likely target for spear-phishing attacks. If an attacker has compromised the privileged user's device, they can exploit the remote session to run commands directly on the remote server and/or capture the user's credentials for use in a future attack.

SAE addresses these risks by isolating the remote desktop session from both the host OS and any other software running on the privileged user's device. As a result, the malware has no way to access the Active Directory server and the attack is prevented.

How does SAE work?

To protect activity with SAE, you need to configure a dedicated app for each high-value asset and deploy these apps to your privileged users' devices. When a privileged user needs to connect to a high-value asset, they open the relevant SAE app from their endpoint device. SAE opens the connection to the high-value asset in a protected virtual machine, isolating the activity from any malware that may be present on the privileged user's device.

You configure these SAE apps and deploy them to privileged users' devices from the Wolf Security Controller. Each SAE app definition is signed using a certificate managed from the Wolf Security Controller. Each time the SAE app is launched, the signature is verified by the SAE endpoint software on the privileged user's device to ensure the app came from a trusted source and has not been tampered with.

If required, you can configure SAE apps so that privileged users can *only* connect to high value assets by using the SAE app on the specified device. This prevents privileged users from connecting to high-value assets directly, bypassing the security provided by SAE. It also precludes an attacker from cloning either the SAE app definition or the entire device disk to a compromised device and connecting to the high-value asset from there.

Using SAE apps gives privileged users the confidence that their access to high-value assets is secure without interrupting their workflow or requiring use of a dedicated workstation. SAE also supports IT administrators by allowing you to monitor usage of SAE apps and demonstrate compliance for audit purposes.

How do I get started?

To deploy SAE within your organization, you will need to:

1. Either deploy the HP Wolf Security Controller to your own infrastructure or sign up for a cloud-hosted HP Wolf Security Controller.

   Note: Sure Access Enterprise requires core elements of SCE, including the Wolf Security Controller and SCE endpoint software. If you are already using SCE to protect devices from malware, you do not need to perform this step.

2. Enable SAE from the controller and optionally configure signing certificates.
3. Provision your privileged users' endpoint devices with the Sure Click Enterprise (SCE) and SAE endpoint software.
4. Configure one or more SAE app definitions to protect connections to remote servers and other high-value assets.
5. Use the Wolf Security Controller to deploy the SAE app(s) and security settings to your privileged users' devices.

Deploy the HP Wolf Security Controller

The HP Wolf Security Controller is used to configure SAE app definitions, deploy these apps to privileged users' endpoint devices, and monitor SAE usage.

For information about deploying the Wolf Security Controller, including hardware and operating system requirements, refer to the latest version of the HP Sure Click Enterprise Installation and Deployment Guide. For more information about the cloud-hosted Wolf Security Controller, contact your HP Solution Architect.

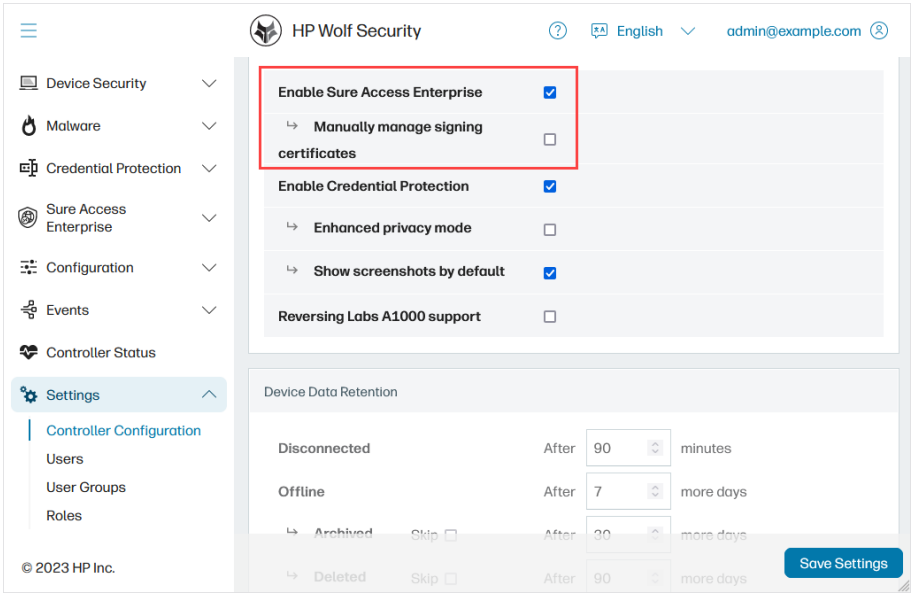
If you are already using SCE, you can use your existing controller to configure and deploy SAE apps. You will need to apply the SAE security policy and install the SAE endpoint software on privileged users' endpoint devices, as described below.

Enable SAE

Once you have deployed the Wolf Security Controller, enable SAE:

1. Open **Settings > Controller Configuration**.
2. Select **Enable Sure Access Enterprise**.
3. Click **Save Settings**.

The **Sure Access Enterprise** menu item is added to the controller navigation. For example:



Manage SAE signing certificates manually

SAE app definitions are signed before being deployed to devices. When an app is launched on a privileged user's device, the signature is verified by the SAE endpoint software using the root certificate provided during device provisioning.

By default, signing certificates are generated and managed by the controller. You can also manage signing certificates manually to ensure compliance with your organization's security requirements.

If you want to manage signing certificates manually, this should be configured before provisioning endpoint devices. To manage signing certificates manually:

1. Add a signing certificate to the Windows certificate store of the server hosting the Wolf Security Controller. If you're running the controller on a cluster, ensure the certificate is added to the Windows certificate store of each node.
2. From the controller, navigate to **Settings** > **Controller Configuration**.
3. Enable **Manually manage signing certificates** and then click **Save Settings**.
4. Navigate to **Sure Access Enterprise** > **Configuration** and select the appropriate certificate from the **Signing certificate** list.
5. Click **Save**. The selected signing certificate will be used by default for all new SAE apps.

Provision endpoint devices

Before an SAE app can be deployed to a privileged user's device, both the SCE and SAE endpoint software must be installed and the device connected to the Wolf Security Controller.

Together, the SCE and SAE endpoint software provide the hardware-enabled isolation that protects remote desktop sessions and connections to web-hosted systems from any malware present on the user's device. The endpoint software also communicates with the controller to receive SAE apps and security settings.

To run SAE apps in production, devices should have compatible SCE and SAE endpoint software versions that are suitable for your version of the controller, as listed in the SAE Release Notes "Required Software" section. Note that some features of SAE are only available with later versions of the endpoint software.

Tip: If you are already using SCE, you can view the SCE software version currently installed on each device, together with other details, from the controller. Select **Device Security > Devices** and then click **Columns** and add the relevant items to the view.

Device requirements

To run the SCE and SAE endpoint software, devices require:

- CPU:
  - Intel Core i5 and higher, 6th generation minimum.
    - VT-x must be enabled.
    - While both vPro and non-vPro versions are supported, vPro is recommended.
  - AMD Ryzen 1 (Zen "1") minimum.
    - AMD-v must be enabled.
  - Up to 64 CPU cores are supported.
- Memory:
  - 8 GB minimum
  - 256 GB maximum
- Disk space:
  - 8 GB minimum
- TPM:
  - TPM 2.0 is required

- Keyboard protection support:
  - PS/2
  - USB 1.1+ devices connected via xHCI USB controller are supported
- Docking station support:
  - USB 3+ and Thunderbolt 3+ docking stations are supported (subject to a specific vendor/model/firmware version)
- UEFI firmware required:
  - Secure Boot must be enabled with the Microsoft 3rd Party UEFI CA permitted.
  - TCG EFI Protocol and Platform Specification Version 1.2 or later is required.
- Operating System:
  - Microsoft Windows 10 x64
    - Supported versions: LTSC-only, 1809 (LTSC 2019) and later
  - Microsoft Windows 11 x64
    - Supported versions: 22H2 (SV2) and later
  - Microsoft Hyper-V is required
  - UEFI boot is required
- Recommended security features:
  - IOMMU (Intel VT-d)

Deploy the SCE and SAE endpoint software to users' devices

The SCE and SAE endpoint software MSIs will be provided directly by your HP Solution Architect. You can use a centralized deployment solution such as SCCM to install the SCE and SAE endpoint software on multiple devices. Alternatively you can run the MSIs manually on individual devices.

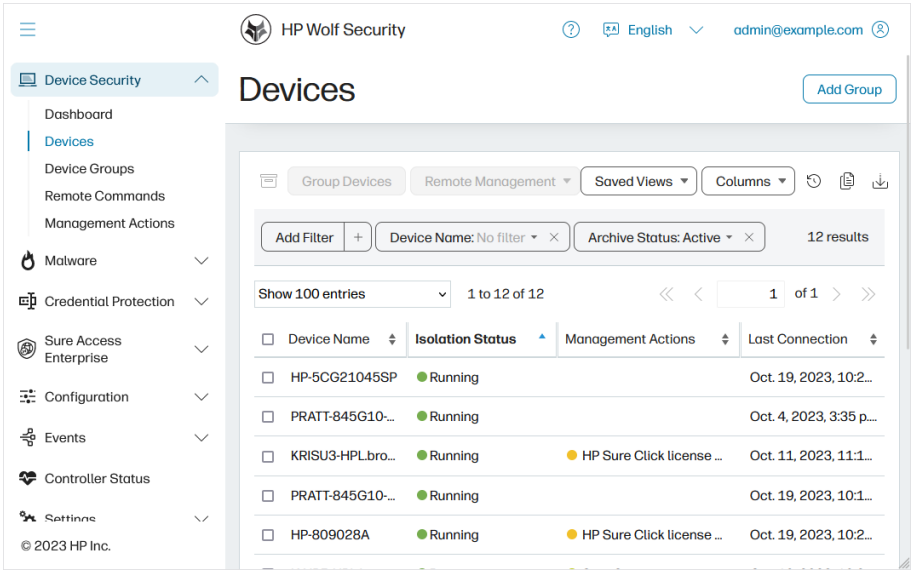
Tip: Installing the SAE endpoint software first can reduce the number of times the device has to be restarted.

During the installation process, you will be prompted to enter the URL of the Wolf Security Controller. If you are using SCCM, specify the `SERVERURL` as a command argument. For more information, refer to the HP Sure Click Enterprise Installation and Deployment Guide.

Note: If you are already using SCE, ensure users' devices are upgraded to the required SCE version before installing the SAE endpoint software. You can use SCCM or the "Install package" remote command to upgrade the SCE endpoint software on users' devices. For more information, refer to the HP Sure Click Enterprise Installation and Deployment Guide.

Devices must be rebooted to complete the installation. To reduce the number of times that each device must be rebooted, you can deploy the SAE security policy to devices after the SCE and SAE endpoint software has been installed but before you reboot. To do this, create a device group for the devices and apply either the "Sure Access Enterprise" policy (if you are also using SCE) or "Sure Access Enterprise (standalone)" policy (if you are only using SAE). For more information, see Deploy SAE apps to users' devices.

Once the device has rebooted, the SCE endpoint software will attempt to connect to the Wolf Security Controller and report the status of the device. Devices that have successfully connected to the controller are listed on the **Devices** page.



You can also check whether the device has established a connection to the controller by opening HP Wolf Security Desktop Console from the device's system tray.

Configure SAE apps

SAE is configured using apps. For each type of remote session or connection to a web-hosted resource that you want to protect with SAE, you will need to define an SAE app and deploy it to a device group.

You can create new SAE app definitions and view or edit existing app definitions from the Wolf Security Controller: navigate to **Sure Access Enterprise** > **App definitions**.

User permissions

Your user group determines the level of access you have to manage SAE apps for different device groups:

- To create SAE apps, you must have the "View" and "Create" permissions for at least one device group.
- To edit SAE apps created by other users, you must have the "Edit" permission for the device group specified in the app definition.
- To get full access to SAE apps, you must have SAE permissions for "All devices".

Controller administrators can configure users, roles and groups from the controller **Settings** pages. For more information about user groups, refer to the Sure Click Enterprise online help.

App setup and settings

To configure a new SAE app, navigate to **Sure Access Enterprise** > **App definitions** and click **Add App**. Alternatively, select an existing app definition to edit it.

To start configuring the app:

1. Specify the Virtual Hardware Version (VHV) to be used by the app. By default, the latest VHV is selected. Some app features are unavailable with older VHVs. Newer versions of the SAE endpoint software may add additional VHVs.

   When you select a device group in order to deploy the app, the available VHV on each device is checked. If the selected VHV is not supported by any of the devices in the group, a warning will be displayed.

2. Select the type of activity you want to protect from the **App Type** list:
   - **Microsoft RDP** - For remote desktop sessions launched using the Microsoft remote desktop protocol (mstsc.exe). This app type uses the SAE RDP UI.
   - **Host RDP** - For remote desktop sessions launched from existing RDP client apps on the user's device. This option is useful if you want to intercept users attempting to connect to a remote server directly rather than by launching an SAE app. Note that only RDP clients based on Remote Desktop ActiveX control interfaces are supported.
   - **Citrix Receiver** - To use Citrix Receiver or the Citrix Workspace App to connect to enterprise apps, desktops and data on Citrix Workspace or StoreFront.
   - **Web Portal** - To connect to a web app, such as a SaaS product, online banking system, or a Remote Desktop web client.

- **SSH** - To open a terminal on a remote server.

Configure the basic app details from the **Settings** tab:

- If you have selected VHV 4.8 or earlier, enter a name for the SAE app in the **Identifier** box. This is the name displayed in the controller; the app name displayed on users' devices is specified from the Appearance tab. If you have selected VHV 4.9 or later, a UUID is displayed instead.
- SAE apps are deployed to devices using device groups. If you have the "Create" SAE permission for all devices, you can save the app definition without selecting a device group from the **Groups** list. Otherwise, we recommend selecting a suitable staging device group while you configure the app, and updating the **Groups** setting when you are ready to deploy the app. For more information, see Deploy SAE apps to users' devices.
- Each SAE app is securely signed using a certificate provided by the controller. If you have opted to manage signing certificates manually, select the relevant certificate from the list.

Tip: You can complete the app configuration in stages. Ensure the mandatory fields on the Settings, Appearance and **Configuration** tabs are populated and then click **Save**.

App appearance

Use the **Appearance** tab to define how the SAE app will appear on users' devices:

- You can upload a custom icon for the SAE app and choose whether it is displayed on the desktop or included in the Start menu. If no icon is provided, the default HP SAE icon is used. Note that icons cannot be provided for Host RDP apps (because Host RDP apps are launched via the other RDP client(s) installed on the host).
- Adding a border around the window provides a visual indication to users that the remote session or connection to the web-hosted resource is protected by SAE.
- Adding a watermark can help to discourage users from taking pictures of sensitive data.

App security features

Use the **Security** tab to define the types of protection you want to apply to the remote session or connection to a web-hosted resource.

If a security feature is required but is not supported by one or more devices in the selected device group, select the "if supported" or "if possible" variant. This will enable the security feature if it is available on the endpoint device, while still allowing use of the SAE app if the feature is not available.

- To isolate the memory allocated to the protected session from the operating system and all other activity on the device, enable **Memory Protection**. To prevent any peripherals connected to the device from gaining access to the memory allocated to the protected session, ensure memory protection is required and then select **Require DMA protection**.

Note: DMA protection is only available if the user's device supports IOMMU (Vt-d). For more information, see Device requirements.

- To prevent key loggers and synthetic keystroke injectors from accessing the protected session, enable **Key Capture and Injection Prevention**.

Note: If Memory Protection is also enabled, Bluetooth keyboards are not compatible with Key Capture and Injection Prevention and cannot be used with the SAE app.

- To prevent other processes from recording the display or taking screenshots, enable **Screen Capture Prevention**. Note that this feature is not supported by Host RDP apps when using a client other than Microsoft RDP (mstsc.exe).
- To turn on the integrated privacy screen on HP laptops when the SAE app is launched, enable **Sure View**.
- To allow the user to copy and paste text from another app running on the device into the SAE app, enable **Allow pasting text into app**.

App type configuration

Configuration options vary according to the **App Type** selected.

Note: We recommend only allowing SSL errors. That is, silencing any SSL errors that are raised while running the SAE app during testing. When deploying an SAE app for production use, this option should be cleared.

Microsoft RDP

Enter the host name, port and logon settings for the remote server or remote desktop connection broker as required.

Use the display options to control the quality of the remote desktop display. If network bandwidth is constrained, consider disabling some or all of these settings to improve performance.

Configure further Microsoft RDP settings as per your system requirements. Note that:

- Proxy server settings are only available with SAE Virtual Hardware Version 4.6 and later.
- Using Active Directory for user authentication is only available with SAE Virtual Hardware Version 4.7 and later.

You can enable the RD Gateway to secure the connection to the remote desktop session with SSL encryption. If **Use Gateway Credentials for Remote Session** is enabled, the SAE app will use the same user-provided credentials to authenticate to both the gateway server and the host.

To authenticate the remote server to the SAE app, upload the static public server certificate to the **Certificates** tab. For more information, see Configure authentication with server certificates.

To authenticate the SAE app to the remote server, configure client certificates with enrollment via SCEP and configure an IPsec VPN connection. For more information, see Configure authentication with client certificates.

Host RDP

You can use the Host RDP app type to ensure that SAE protection is applied when users open an RDP connection in their own choice of RDP client, rather than using a dedicated SAE app.

Note: Only RDP clients based on Remote Desktop ActiveX control interfaces are supported. Some advanced configuration options available on the RDP client may not be supported when running the client in a protected virtual machine.

Match criteria

Enter the host addresses or host address ranges for the servers that you want to protect in the **Addresses** box as a newline separated list. Use "*" to specify a wildcard. To exclude a host address or range, preface the entry with "-". In the event that an address is both included an excluded, the exclusion takes priority.

Once the SAE app has been deployed, if the user opens a supported RDP client and attempts to connect to a host that matches one of the specified addresses or address ranges, the session is isolated in a protected virtual machine. Connections to hosts that are not included in the SAE app definition (either explicitly or implicitly) are not protected.

If you create multiple SAE apps for Host RDP and deploy them to the same devices, you can specify the order in which the SAE endpoint software checks each app for a matching host address. This is useful if you have one SAE app that applies to a broad range of hosts and another SAE app with a narrow range of hosts and more stringent security settings. Setting the **Precedence** to a higher value for the SAE app with a narrower range of hosts will ensure that the more stringent security settings are applied when connecting to the specified hosts.

You can also give users the option to apply SAE protection when connecting to specified remote hosts from a supported RDP client, rather than intercepting every connection to those hosts. To achieve this, set a negative precedence value. When a negative precedence is set for a host address or range of host addresses, SAE protection is only applied if the user selects **Open with** > **HP Sure Access Enterprise** to launch an .rdp file.

If you have multiple Host RDP SAE apps with negative values, the specified host is checked against the SAE app definition with the highest precedence value first. That is, -1 is checked before -10.

Other Host RDP settings

Configure further Host RDP settings as per your system requirements. Note that:

- Proxy server settings are only available with SAE Virtual Hardware Version 4.6 and later.
- Using Active Directory for authentication is only available with SAE Virtual Hardware Version 4.7 and later.
- Smart cards and authentication via client certificates are not supported for Host RDP.
- Screen capture prevention (enabled from the Security tab) is only supported when using the Microsoft RDP client (mstsc.exe). Selecting **Block screen capture if possible** will enable screen capture prevention if

the user opts to use the Microsoft RDP client, but will still allow the user to connect to the host with another RDP client. Selecting **Block screen capture** will prevent the user from connecting to the host with SAE unless they are using the Microsoft RDP client.

To authenticate the remote server to the SAE app, upload the static public server certificate to the **Certificates** tab. For more information, see Configure authentication with server certificates.

Client certificate authentication is not supported for Host RDP SAE apps.

Citrix Receiver

Enter the URL of the relevant Citrix Store. This can be a cloud-hosted Citrix Workspace or on-premises StoreFront.

To authenticate the Citrix Store to the SAE app, specify one or more trusted certificate authorities (CAs) from the **Certificates** tab. For more information, see Configure authentication with server certificates.

To authenticate the SAE app to the Citrix Store, configure client certificates with enrollment via SCEP. You can also use client certificates in a Windows certificate store on the user's device to authenticate the *device* to the Citrix services. For more information, see Configure authentication with client certificates.

Web Portal

Enter the URI of the web app, SaaS product or remote desktop web client.

To route the request via a proxy server, SAE Virtual Hardware Version 4.6 or later is required.

To authenticate the web app to the SAE app, specify one or more trusted certificate authorities (CAs) from the **Certificates** tab. For more information, see Configure authentication with server certificates.

To authenticate the SAE app to the web app, configure client certificates with enrollment via SCEP. You can also use private certificates in a Windows certificate store on the user's device to authenticate the *device* to the web app. For more information, see Configure authentication with client certificates.

SSH

In the **SSH Host Address** and **SSH Host Port** fields, enter the IP address or host name and TCP port of the SSH server. If no port number is specified, port 22 is used.

In the **SSH Host Public Key** field, enter the public key for the SSH host in OpenSSH key format. Host keys are typically stored in the server's `etc/ssh` directory.

If a public key is not provided, **Allow SSL errors** must be enabled for the SAE app to connect to the SSH server.

Note: Allow SSL errors should *not* be enabled in production settings.

Optionally provide the username to connect with. If the username is not provided as part of the SAE app definition, the user will be prompted to enter their username when the SSH connection is launched.

You can enable user authentication via a smart card device, such as a YubiKey. Before selecting **Enable Smart Cards**, ensure the SSH server is configured to accept a smart card key pair for authentication.

To authenticate the SAE app to the SSH server, configure client certificates with enrollment via SCEP and an IPsec VPN connection. For more information, see Configure authentication with client certificates.

Server authentication via certificates is not supported for SSH SAE apps.

Configure authentication with server certificates

You can use server certificates to authenticate the high-value asset to the SAE app. This ensures that the SAE app is connecting to the correct resource. If the certificate cannot be authenticated, the SAE app will not connect to the remote server or web-hosted service.

Specify the location of the public server certificates that you want the SAE app to use from the **Certificates** tab.

The most secure option is to include a static public certificate in the SAE app definition. Enable **Static Certificates** and upload the certificate files. A TLS server should provide intermediate certificates in the handshake, so it is normally sufficient to upload only the root certificate. This is the only server authentication option available for Microsoft RDP and Host RDP SAE apps.

For Citrix Receiver and Web Portal SAE apps, you can also trust other certificate authorities:

- NSS CA certificates. By default, well-known public CAs are trusted. This allows the SAE app to connect to an internet-facing site without further configuration. To restrict the SAE app to trusting only the certificate authorities that you have explicitly configured (either static certificates or Host P11 options), select **Disable built-in objects**.
- Public server certificates stored in a Windows certificate store on the user's device. To enable this option, select **Host P11** and then enable or disable certificate stores as required.

> **Note:** Although this is a convenient way to distribute enterprise CA roots, if the device is compromised, CA certificates may be replaced or new roots of trust added to enable a “man in the middle” attack.

If you want the SAE app to connect to the high-value asset over an IPsec VPN, you will also need to upload static certificates to establish the root of trust for the VPN Gateway certificate.

Configure authentication with client certificates

You can use client certificates to authenticate the SAE app to the high-value asset. This allows the remote server or web-hosted resource to distinguish between access via the SAE app and access via a browser or another application running on the host OS. To use client certificate authentication for Microsoft RDP and SSH SAE apps, the app must connect to the host server via an IPsec VPN connection.

By configuring the remote server or web resource to trust only certificates generated by SAE apps, you can prevent users from accessing high-value assets directly and force them to connect via SAE.

Client certificate enrollment via SCEP

The most secure option is to store private key certificates in the virtual TPM of the protected virtual machine that runs the SAE app. To add certificates to the virtual TPM, enrollment must be used.

For Citrix Receiver and Web Portal SAE apps, certificate enrollment alone may be used to authenticate the app to the web-hosted service. For Microsoft RDP and SSH SAE apps, certificate enrollment must be used in conjunction with a VPN connection.

Currently, only enrollment via SCEP is supported. This requires an SCEP server, such as a Microsoft NDES server, to act as the certificate authority.

To enable this option:

1. From the **Enrollment** tab, select **SCEP**. The SCEP configuration options are displayed.
2. In the **FQDN** field, enter either the fully qualified domain name or the user principal name (in the format `UserName@DNSDomainName.com`), and then specify which you have provided from the **FQDN Type**.
3. In the **Address** field, enter the full URL to your SCEP server. For NDES, specify the host on which the IIS component is installed. The path is typically: `/certsrv/mscep/mscep.dll/pkclient.exe`
4. If your SCEP server requires a client certificate to authenticate the connection:
    a. Open the **Certificates** tab, enable **Host P11**, and enable the certificate store(s) on the users' devices that contain the client certificate for the SCEP server.
    b. Return to the **Enrollment** tab and enable **HTTPS Authentication**.
    c. By default, each available client certificate will be tried until one works. To limit the number of certificates that need to be checked and speed up this process, you can:
        - Enter the name of the certificate issuer in the **Issuer** field.
        - Enter the name of the Windows certificate store that contains the certificate in the **Token** field. This will usually be Personal Certificates. Ensure this certificate store is also enabled from the **Certificates** tab.
5. SCEP uses its own CA certificates that are specific to the enrollment protocol and distinct from any HTTPS certificates. Download these certificates from your SCEP server and upload them to the **CA Certificates** field:
    a. In a web browser, go to the SCEP server URL and append the following query string: `?operation=GetCACert&message=CAIdentifier`
    b. Your browser should download a file called `pkclient.exe` or similar. This is a DER-encoded degenerate PKCS#7 file that contains the certificates.
    c. Extract the certificates into another file using this command:

    bash
    openssl pkcs7 -print_certs -in pkclient.exe -inform der -out cacerts.pem
6. Upload the `cacerts.pem` file to the **CA Certificates** field.

When SCEP enrollment is configured, the SAE app automatically obtains a certificate on first launch (and on subsequent uses if the certificate has expired).

The authentication for issuing a certificate in SCEP is a PIN code provided out of band to the user, which the user types into the SAE app. The user is responsible for using the code only when expected, and the administrator is responsible for noticing unexpected requests.

Note: If an enabled certificate store also contains a public key certificate for the Citrix Store or Web Portal, this certificate can be used to authenticate the resource to the SAE app. This method of server authentication comes with an inherent risk. For more information, see Configure authentication with server certificates.

Windows certificate store

For Citrix Receiver and Web Portal SAE apps, you can also use private key certificates located in a Windows certificate store on the user's device to authenticate the device to the high-value asset.

To enable this option, open the **Certificates** tab, select **Host P11** and then enable or disable certificate stores as required. Note that if an enabled certificate store also contains a public key certificate for the Citrix Store or Web Portal, this certificate can be used to authenticate the resource to the SAE app. This method of server authentication comes with an inherent risk. For more information, see Configure authentication with server certificates.

Static client certificates for testing

For testing purposes, a static private key certificate can be included in the SAE app definition. This method is not secure but is useful for testing the app configuration separately from certificate enrollment.

Connect over a VPN

By default, SAE apps connect to the remote server or web-hosted resource directly.

If you want to authenticate a Microsoft RDP or SSH SAE app to the remote server using client certificates issued via SCEP enrollment, an IPsec VPN connection is required. You can also use an IPsec VPN to connect to a web app hosted on a private network or to Citrix Workspace (if you are not already using NetScaler).

This option is also useful if you want to prevent users from being able to connect to remote servers or web apps directly. You can configure an IPsec VPN connection for the SAE app and use a client certificate to authenticate the connection to the remote server or web app. Provided that no other client certificates are available, users will only be able to authenticate to the remote server or web app when using the SAE app.

To connect the SAE app to the high-value asset over a VPN, first configure client certificate authentication with enrollment via SCEP.

To allow the SAE app to validate the private certificate presented by the VPN gateway, open the **Certificates** tab, enable **Static certificates** and upload the root and intermediate CA certificates required to validate the VPN gateway's certificate.

Then configure the VPN settings from the **Connection** tab:

1. Set the Connection Type to IPsec VPN.
2. In the **Gateway Address** field, enter the hostname or IP address of the VPN gateway.
3. If you're using SAE Virtual Hardware Version 4.8 or later, you can choose whether to use IPsec **Tunnel** mode or **Transport** mode. For earlier Virtual Hardware Versions, tunnel mode is always used.

4. Choose whether to disable revocation checks for certificates received from the VPN gateway. If you are using an outgoing firewall configuration that does not permit access to the OCSP/CRL URLs in your VPN gateway's certificate, we recommend disabling revocation checks to avoid delays or timeouts while establishing the VPN connection.
5. Specify the **Re-keying Time**, **Re-authentication Time** and **Extra Proposals** as per your VPN gateway provider's recommendations.
6. If you entered a DNS name in the **FQDN** field on the **Enrollment** tab, select **Enrolled Certificate DNS Fully Qualified Domain Name**. If you entered a user principal name in the **FQDN** field on the **Enrollment** tab, select either **Enrolled Certificate Subject Distinguished Name** or **Enrolled Certificate Microsoft User Principal Name** as appropriate.
7. In the **Gateway Identity** field, enter the identity that the VPN gateway should report. If the reported identity does not match, the VPN connection will fail.
    - Select **Any** to accept any remote address. This option is not secure and should only be used for testing purposes.
    - Select **Use Address** to check that the reported identity matches the values provided in the **Gateway Address** field.
    - Select **Custom** to specify another address.
8. For SAE Virtual Hardware Version 4.7 and earlier, IKE v2 is always used. From Virtual Hardware Version 4.8 onwards you can choose whether to use IKE v1 or v2. We recommend using IKE v2 where possible; support for IKEv1 is provided to allow interoperability with some proprietary IPsec VPN solutions, including Windows Firewall.
9. If IKE v1 is selected, you can specify one or more remote traffic selectors to use for the connection: click **Add** and specify the allowed address(es) and protocol(s).
10. If your VPN gateway requires ESP tunnel settings, enter the relevant details. Refer to your VPN provider's documentation for more information.

Restrict outgoing connections

By default, there are no limits on the hosts or networks that an SAE app can connect to. You can define an allow-list of the outgoing network connections that an SAE app can make from the **Firewall** tab. This is useful if you want to ensure the SAE app can only communicate with the specified resources.

To restrict the SAE app to specific hosts or networks, enter the permitted destinations in the **Outgoing Connections** box. Each destination must be an address in IPv4 or CIDR notation, entered on separate lines. Destinations cannot be specified as DNS names.

To remove all restrictions on outgoing connections, delete all destinations in the **Outgoing Connections** text box.

Combine allow-list with VPN connection

The outgoing connections firewall configuration only applies to packets sent outside of an IPsec VPN connection.

If you have configured an IPsec VPN connection:

- Use traffic selectors and/or a separate firewall on your VPN gateway to restrict connections over your private network.
- Add the SCEP server and VPN gateway IP address(es) to the **Outgoing Connections** list.
- If your VPN gateway's certificate contains OCSP and/or CRL URLs that may be used for revocation checks, either add the OCSP/CRL server IP address(es) to the **Outgoing Connections** list, or disable revocation checks for IPsec VPN connections.

Logging

By default, guest logging is disabled. If you encounter an issue with an SAE app, HP Support may ask you to enable logging before replicating the issue on the endpoint device. For more information about encrypting and retrieving logs, see Enable logging.

Deploy SAE apps to users' devices

Once you have configured one or more SAE apps, you can deploy them to users' devices.

Before you begin, open **Device Security** > **Devices** and check that your users' devices have connected to the controller. If a device is not listed, open HP Wolf Security Desktop Console from the device system tray and check that the SCE endpoint software has been installed and the device can connect to the network hosting the controller.

Create device groups

SAE apps are deployed to users' devices via device groups. If you are already using Sure Click Enterprise, you may already have a number of device groups. We recommend creating a dedicated device group to identify users' devices.

If you have configured multiple SAE apps for different types of users, you will need to create a separate device group for each subset of users.

To create a new device group, navigate to **Device Security** > **Devices** and click **Add Group**. You can add devices to the group manually or define rules to add and remove devices from the group automatically.

Tip: Assigning devices to groups automatically based on rules is useful if you want to deploy SAE apps to all devices that have the appropriate endpoint software.

For more information about adding and managing device groups, refer to the Sure Click Enterprise online help .

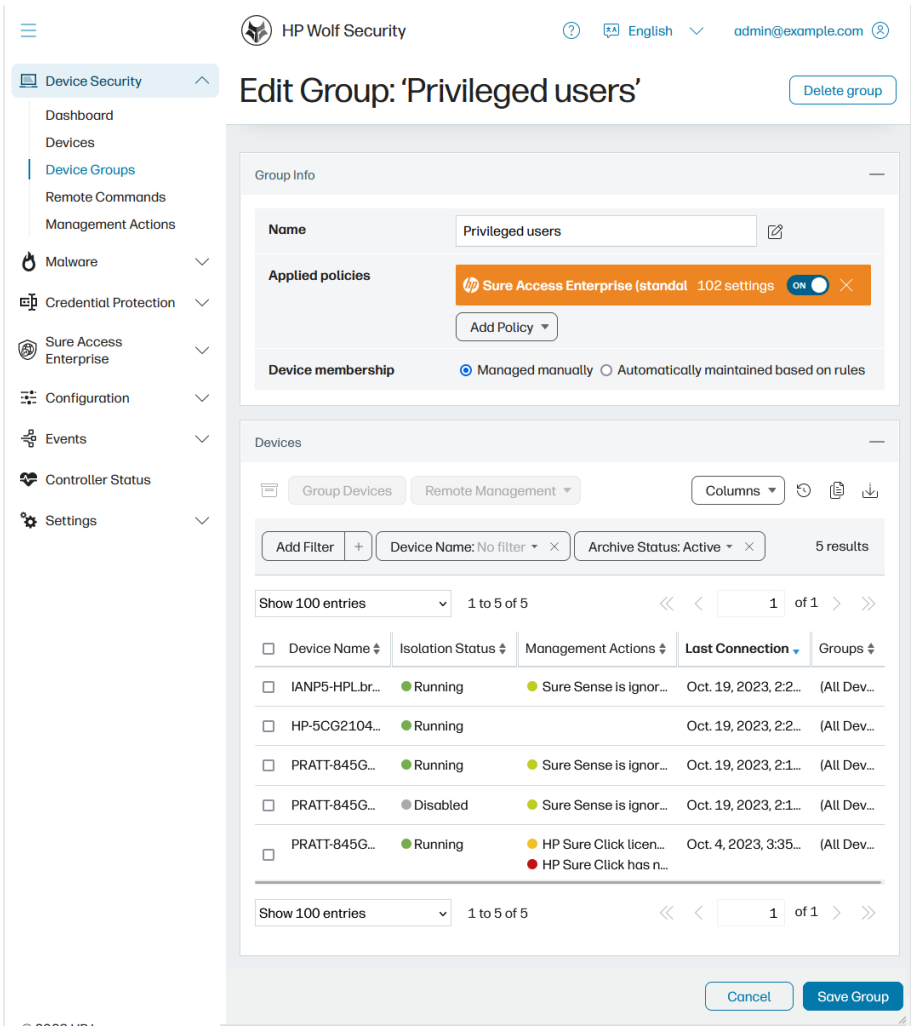
Apply SAE security policies to device groups

To use the SAE features, devices must have the appropriate SAE security policy:

- If you are also using SCE, apply the "Sure Access Enterprise" policy to the relevant device groups.
- If you are only using SAE, apply the "Sure Access Enterprise (Standalone)" policy to the relevant device groups.

To apply security policies to users' devices, edit the device group, select the appropriate policy from the **Applied policies** list and then save the changes. If you are enabling the SAE policy on a device for the first time, you will need to reboot the device for the policy to take effect.

For more information about applying security policies to devices, refer to the Sure Click Enterprise online help .

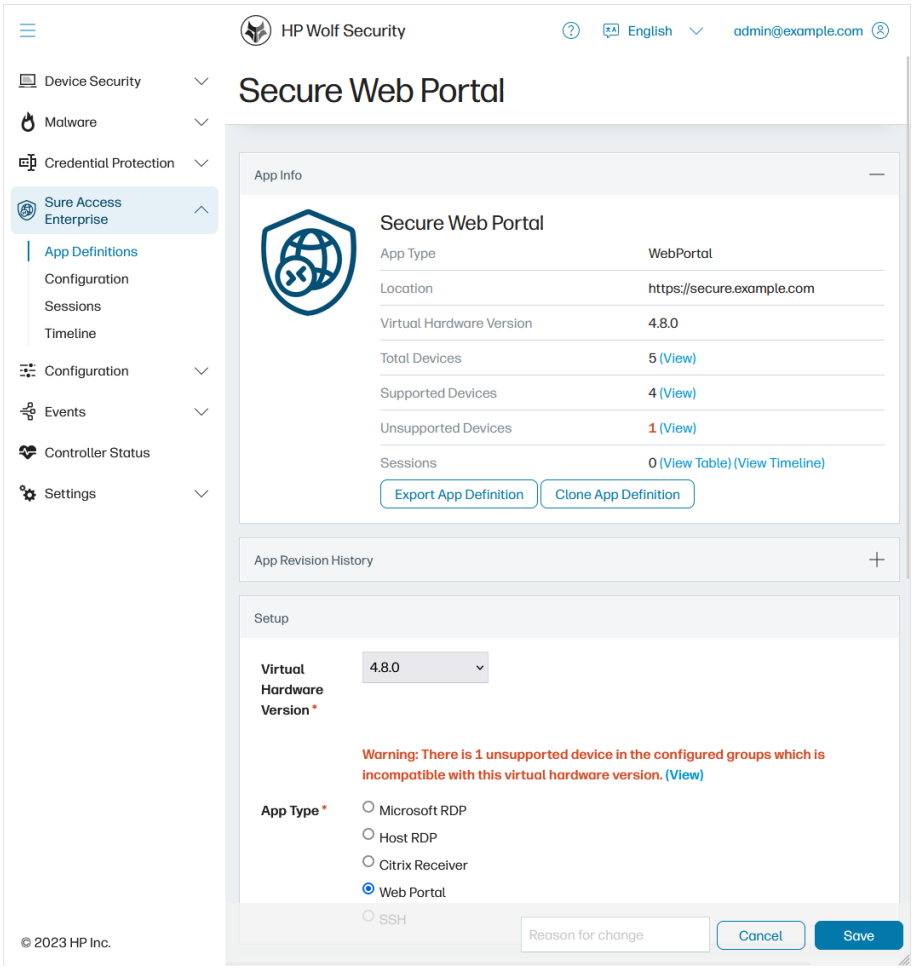


Once a security policy has been applied to a device, the device receives policy updates from the controller automatically. You can also force a device to fetch the latest policy updates. From the device system tray, open the HP Wolf Security Desktop Console and select **Settings** > **Security Management** > **Update policy**.

Deploy SAE apps to device groups

Tip: Before deploying SAE apps for production use, ensure **Allow SSL** errors is cleared in the app definition.

To deploy SAE apps to all devices in a group, edit the app definition and from the **Settings** tab select the relevant device group(s). Then, click **Save**.



Note: If the app definition includes settings that are not supported by the SAE Virtual Hardware Version on any of the devices in the group, a warning is displayed.

Provided that the devices in the group can connect to the network on which the controller is hosted, the SAE app is installed automatically. Devices typically connect to the controller several times per hour.

Depending on the SAE app settings, the app is added to either the device's desktop or Start menu. The first time that a user launches an SAE app on a device, a warning is displayed: "Warning: This app appears to be being used on this machine for the first time." In this scenario, the warning can safely be ignored. For more information about errors and warnings, see Monitor and troubleshoot SAE usage.

Update SAE app configurations

When you make changes to an existing SAE app, the changes are applied to the devices in the selected groups automatically. To force a device to fetch the updated app definition (together with any security policy updates), open the HP Wolf Security Desktop Console and select **Settings** > **Security Management** > **Update Policy**.

To make changes to an SAE app without applying the changes to devices immediately, clone the existing app definition and clear the device group selection (or select a dedicated staging group). When you are ready, archive the previous version of the app and apply the new version to the relevant device group(s) from the **Settings** tab.

Note: To edit an SAE app, you must have the SAE Edit permission for the device group to which the app has been deployed.

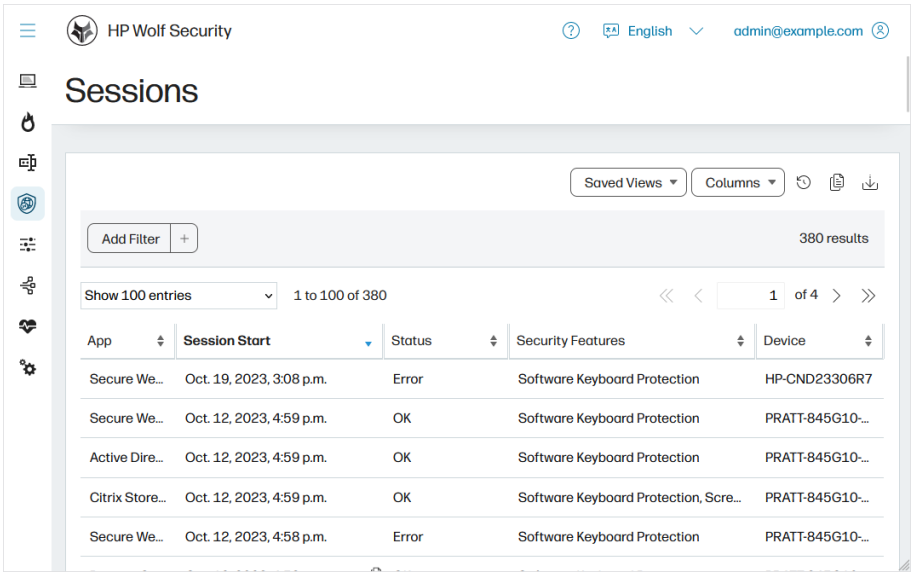
Remove SAE apps from devices

Archiving an SAE app removes it from users' devices. This is useful for any apps that are no longer required or that you have replaced with a new SAE app.

To archive an app, open the **App Definitions** list, use the checkboxes to select the app and then click the **Archive** icon.

Monitor and troubleshoot SAE usage

You can use the controller **Sessions** and **Timeline** views to monitor usage of SAE apps. Click a session to view the app's security features, details of the endpoint device, and the app event log. Any errors or warnings that have been reported by the app to the controller are listed in the event log.



Common errors and troubleshooting steps

Common errors that may be displayed on a user's device and steps to resolve them are listed below.

"Warning: This app appears to be being used on this machine for the first time"

This message is displayed the first time an SAE app is launched from a user's device. Acknowledge the warning to proceed and prevent the warning from being displayed the next time the app is launched.

This warning is also displayed if:

- An issue has arisen on the device's TPM, potentially causing the BitLocker "recovery screen" to appear. If you are not aware of such an issue, consider it possible that the user's device has been compromised.

"Warning: The app cannot be used because the application definition could not be verified"

From the controller, open **Sure Access Enterprise** > **Sessions** or **Timeline** to view details of the failed session. Any errors are listed in the **Event log**:

- "Verification config not available" or "Trusted verification config not available".

  Ensure that a valid Signing Certificate is set on the SAE app's Settings tab and Ensure SAE policy is up to date.

- "Failed to find trusted verification config chain in latest config".

The Signing Certificate for this SAE app does not match the SAE Trusted Configuration on the endpoint device. This can occur if a device is reconfigured to connect to a different controller or if the SAE Trusted Configuration is removed from the device. For more information, see Reset the SAE Trusted Config on a user's device.

"Warning: The app cannot be used because there is a problem with persistent storage"

This warning can occur if the BitLocker recovery key has been used on the user's device or a change has been made to the device's TPM PCR measurement.

Delete the SAE Trusted Configuration on the user's device and reinstall it. For more information, see Reset the SAE Trusted Config on a user's device.

"Warning: The app cannot be used because the security requirements could not be met"

This error is displayed if:

- The SAE app includes security features that are not supported by the user's device, such as Sure View or memory protection. To address this, either update the SAE app definition to only apply the security features if they are supported or remove the app from the device.
- The "Sure Access Enterprise" or "Sure Access Enterprise (standalone)" policy has not been deployed to the user's device and/or the device has not been rebooted to complete the installation process. For more information, see Apply SAE security policies to device groups.
- Secure Boot is not enabled on the user's device. Enable Secure Boot from the device's BIOS settings.

Ensure SAE policy is up to date

Devices connected to the controller normally receive updates to the SAE policy and any app definitions every few minutes. To check the status and force the device to fetch the latest policy and app definitions, open the HP Wolf Security Desktop Console, select the **Settings** tab and click **Update Policy**.

Reset the SAE Trusted Config on a user's device

In some situations, it may be necessary to delete the SAE Trusted Configuration and reinstall it. Resetting the Trusted Configuration will cause all SAE apps to revert to their initial state and enroll new client certificates (if configured).

To delete and reinstall the SAE Trusted Configuration:

1. Ensure the device can connect to the controller.
2. From a command prompt, run `C:\Program Files\HP\Sure Click\ApplicationSupport\pvm\7.0.406\BrProtectedAppCmd.exe" reset-tvconfig` (updating the version number as required).
3. Reboot the device.

Note: each SAE app will display "Warning: This app appears to be being used on this machine for the first time" when launched.

Enable logging

If you have encountered an issue with an SAE app, HP Support may ask you to enable logging for the app and retrieve the logs from the endpoint device.

Encrypt guest logs

To enable logging for a particular SAE app, edit the app definition from the controller, open the **Logging** tab and select **Enable guest logging**.

Plain text logging should only be used for testing purposes. For production deployments, guest logs should be encrypted using either a certificate (generated using a private key) or a public key file.

The private key should be stored on a trusted administrative device running Windows 10 64-bit and kept separate from other devices running SAE apps. The certificate should be associated with an RSA key-pair with a key size of 1024 bits or greater. A key size of 2048 bits is recommended.

If the trusted device uses a hardware mechanism to protect the private key (such as a smart card, Trusted Platform Module (TPM) or Hardware Security Module (HSM)), then the following requirements should be met:

- The hardware mechanism must be supported by a Windows Cryptographic Service Provider (CSP) or Key Storage Provider (KSP).
- The hardware mechanism must support decryption of RSA blocks with EME-OAEP PKCS#1 v2.0 padding (SHA-1 hash function, Mask Generation Function (MGF) 1, empty encoding parameter).
- Decryption is performed with the Win32 CNG API `NCryptDecrypt()`, with `dwFlags=NCRYPT_PAD_OAEP_FLAG` and a `BCRYPT_OAEP_PADDING_INFO` instance specifying the `BCRYPT_SHA1_ALGORITHM` hashing algorithm with no padding data buffer.

For reference, CSPs and KSPs provided by Microsoft for software-based private key storage comply with the above requirements.

For more information about generating certificates from a private key, refer to Microsoft's documentation.

To export the certificate from Windows 10:

1. Open the Certificate Manage MMC snap-in (`certmgr.msc`).
2. Locate your certificate in the appropriate store.
3. Right-click the certificate and select **All Tasks** > **Export**.
4. When prompted, choose not to export the private key.
5. Set the export file format to **Base-64 encoded X.509 (.CER)**.
6. Click **Finish**. The certificate is exported.

Return to the SAE app definition, open the **Logging** tab and upload the certificate to the **Guest Log Encryption Key**. Click **Save** to update the app definition.

Note: If you subsequently remove the certificate or public key from the app definition, ensure logging is disabled to prevent logs from being generated and stored in plain text on the endpoint device.

Retrieve guest logs

When you enable logging for an SAE app that has already been deployed to users' devices, the updated app definition is applied to all devices in the specified device group. However, logs are only generated if logging is also enabled on the endpoint device. By default, the SAE security policy enables logging on users' endpoint devices. If you are also using SCE, ensure this setting has not been overridden by a custom security policy.

To retrieve SAE app logs from a device, use the controller to run the "Collect isolation logs from device" remote management command. Guest logs can be found in the log archive under `Logs\LocalLow_logs_<user>\BrGuestLogs\pVM<vmid>` where `<user>` is the name of the user running an SAE app and `<vmid>` identifies the app.

The device user can view the IDs for any SAE apps that are currently running from the HP Wolf Security Desktop Console.

Decrypt guest logs

You can decrypt guest logs using the `BrProtectedAppLog.exe` command line tool on the trusted device that contains your private key.

To deploy `BrProtectedAppLog.exe`, install the SAE app-pack (without HP Sure Click) on the trusted device.

By default, the tool is located in `%Program Files%\HP\Sure Click\ApplicationSupport\pvm\<version>\tools\BrProtectedAppLog.exe` where `<version>` is the app-pack version.

To decrypt a guest log, run `BrProtectedAppLog.exe` with the decrypt operation, specifying:

- The path of the encrypted guest log file.
- The destination path for the decrypted guest log file.
- The Windows certificate store name.
- The path of the certificate file.

For example, the following command decrypts `pVM0001.dat` to `pVM0001_decrypted.dat`, using the certificate in the current user's Windows store that was previously exported to `pvm-guest-logging.cer`:

```
bash
BrProtectedAppLog.exe decrypt pVM0001.dat pVM0001_decrypted.dat My --certfile pvm-guest-logging.cer
```

The decrypted file is created as a plain text file and contains the guest logs.

Getting help

If you need further assistance, please contact HP Support:

- Visit https://enterprisesecurity.hp.com.
  If you need an account, please contact your Account Executive or Customer Support Agent.
- Email questions to enterprise.support@hpwolf.com.
- Call HP Enterprise Security Customer Support at 1-800-518-0845.
- Call your technical account representative directly.