Imprivata OneSign Version 7.9 Common Criteria Administration Guide

Imprivata OneSign® 7.9
September 12, 2023

Security Functionality

Enterprise Security Management

Imprivata maintains user accounts and authentication data in its database. Users of the managed endpoints and of the Imprivata Admin Console are validated against this database of users.

Imprivata supports both Computer Policies and User Policies:

- Computer Policies apply to every user attempting to use the endpoint. These policies define the set of features accessible to any user on that endpoint. Imprivata OneSign supports the creation (including modification and deletion) of multiple Computer Policies and the application of different Computer Policies to different endpoints. This allows for different Computer Policies to be assigned to different endpoints at any given time. Computer Policies can control many endpoint features such as the types of allowed authentication methods (e.g., passwords, proximity cards, fingerprints), inactivity lockouts, and virtual desktops (e.g., Citrix, VMware).
- User Policies apply to a specific user attempting to use any endpoint. These policies define the set of endpoint features the user is allowed to use on any endpoint, assuming the endpoint's Computer Policy allows it and the endpoint supports the feature. Imprivata OneSign supports the creation (including modification and deletion) of multiple User Policies and the application of different User Policies to different users. This allows for different User Policies to be assigned to different users at any given time. User Policies can control user access to many endpoint features such as the types of allowed authentication methods (e.g., passwords, proximity cards, fingerprints), inactivity lockouts, and virtual desktops (e.g., Citrix, VMware).

Imprivata supports multiple Computer Policies and User Policies. One Computer Policy is assigned to each managed endpoint and one User Policy is assigned to each user.

Imprivata OneSign supports multiple authentication mechanisms at the endpoints and for the Imprivata Admin Console, but in the evaluated configuration, only the password authentication mechanism is allowed as an authentication mechanism. Imprivata enforces password complexity rules on these passwords. The authentication mechanism for a user is defined in each User Policy.

The Imprivata Appliance Console uses a separate account database/file from the rest of the appliance. This database supports only two password-based accounts: Super Administrator and Administrator. This interface is only used for low-level configuration of the appliance.

Auditing

Imprivata generates audit records for the PP-required events. An administrator can select events to be audited by Imprivata based on the event type. The records are protected from unauthorized modification and deletion within Imprivata.

Imprivata supports two separate mechanisms for storing its audit records externally. Some audit records can be transmitted as individual audit records to an external audit server (a syslog server) over a protected communications channel. The remaining audit records can be transmitted in log files to external audit log storage over a protected communications channel. In addition, Imprivata allows an administrator to select the events audited by the agent based on event type.

Cryptographic Support

Imprivata employs the HTTPS protocol, SSH (a.k.a. SSHv2) protocol, and TLS protocol to protect communication channels.

The HTTPS protocol is implemented by the Apache HTTP Server. The Apache HTTP Server uses Apache's Network Security Services (NSS) for its TLS implementation. Apache NSS is a cryptographic module that implements both the TLS protocol and cryptographic algorithms.

The SSH protocol is implemented using Apache SSHD. Apache SSHD requires Apache MINA which requires the Java Virtual Machine (VM). The Java VM uses a Bouncy Castle software cryptographic module as the cryptographic provider for the Java Secure Socket Extension (JSSE). Apache SSHD uses the JSSE API to perform its cryptographic operations in the SSH protocol.

The syslog-ng client uses OpenSSL for its TLS implementation. OpenSSL is a software module that implements both the TLS protocol and cryptographic algorithms.

Cryptographic provider	Protocol	Usage
Apache NSS v3.77	HTTPS (TLS 1.2)	Apache HTTP Server
Bouncy Castle v1.68	SSHv2	Java VM (Apache SSHD)
OpenSSL v1.0.2p	TLS 1.2	syslog-ng

Imprivata OneSign, specifically its syslog-ng client, acts as a TLS client when communicating with the external audit server (syslog server). The syslog-ng client supports TLS 1.2 (RFC5246) for communicating with the external audit server (syslog). It rejects all other TLS versions of the protocol and all SSL versions. It uses the OpenSSL v1.0.2p software library (module) for its TLS implementation and cryptographic provider.

The syslog-ng client supports the following PP-specified TLS ciphersuites:

- TLS_RSA_WITH_AES_128_CBC_SHA as defined in RFC 5246
- TLS_RSA_WITH_AES_256_CBC_SHA as defined in RFC 5246
- TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246
- TLS_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246
- TLS_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288
- TLS_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288

Imprivata OneSign, specifically its Apache HTTP Server, acts as an HTTPS server handling inbound HTTPS requests. The Apache HTTP Server supports TLS 1.2 (RFC5246) for HTTPS connections. It rejects all other TLS versions of the protocol and all SSL versions. It uses the Apache NSS v3.77 software library (module) for its TLS implementation and cryptographic provider.

The Apache HTTP Server supports the following PP-specified TLS ciphersuites with HTTPS:

- TLS_RSA_WITH_AES_128_CBC_SHA as defined in RFC 5246
- TLS_RSA_WITH_AES_256_CBC_SHA as defined in RFC 5246
- TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246
- TLS_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246
- TLS_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288

- TLS_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289

Identification and Authentication

Imprivata enforces authentication failure handling for the agent, the Imprivata Admin Console, and the Imprivata Appliance Console. The guidance calls it the User Lockout Policy. The User Lockout Policy is a component of a User Policy.

Security Management

Imprivata supports multiple security management functions required by the ESM PP. Most of which are for managing the appliance features, but some are for managing agent features. These include user account management and policy management.

Protection of Imprivata Security Functions

Imprivata obscures authentication data (passwords) before storing them in non-volatile memory. No interface is provided by Imprivata to view the passwords in plaintext. Similarly, Imprivata provides no interface to view pre-shared keys, symmetric keys, and private keys. Imprivata also provides its own reliable time stamp capabilities.

Access

Imprivata terminates the remote sessions of the Imprivata Admin Console and Imprivata Appliance Console after an administrator-configurable time interval of inactivity. It also allows administrators to terminate their own sessions on the Imprivata Admin Console or Imprivata Appliance Console at any time by clicking **Log Out**.

The Imprivata Admin Console and Imprivata Appliance Console display configurable advisory messages prior to authentication.

Administrators can deny session establishment for all Imprivata Admin Console users, except Super Administrators, based on day, time, and duration. The attributes are day, time, duration, and user role, where the user role is hardcoded to be all roles except for the Super Administrator role. The Imprivata Appliance Console denies session establishment based on usernames. Enterprise users cannot log in to this interface.

Trusted Path/Channels

Imprivata acts as an HTTPS server supporting TLS 1.2 when communicating with the Imprivata agents. Administrators externally manage Imprivata via the Imprivata Admin Console and Imprivata Appliance Console on a web browser, over HTTPS with TLS 1.2.

Imprivata uses SFTP (SSHv2) to protect the communication channel when transferring audit data from Imprivata to external audit log storage.

Imprivata uses TLS 1.2 to protect the communication channel when transferring audit data from Imprivata to the external audit server (syslog).

Protocol	Initiator
HTTPS (TLS 1.2)	Imprivata Admin Console to Imprivata
	Imprivata Appliance Console to Imprivata
	Imprivata agent to Imprivata
SSHv2 client	Imprivata to external audit log storage
TLS 1.2	Imprivata to external audit server (syslog)

Assumptions and Organizational Security Policies

Enrollment

Imprivata provides a defined enrollment process that confirms user identity before the assignment of credentials.

ESM

Imprivata establishes connectivity to other ESM products in order to share security data.

Federate

Third-party entities that exchange attribute data with the Imprivata enterprise are assumed to be trusted.

Manage

There will be one or more competent individuals assigned to install, configure, and operate the Imprivata enterprise.

Robust

The Operational Environment will provide mechanisms to Imprivata that reduce the ability for an attacker to impersonate a legitimate user during authentication.

User ID

The Imprivata enterprise will receive validated identity data from the Operational Environment.

Banner

Imprivata provides an initial banner to describe restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the system.

Objectives for the Operational Environment

OE.ADMIN

There will be one or more administrators of the Operational Environment that will be responsible for providing subject identity to attribute mappings within the Common Criteria evaluated configuration.

O.ADMIN

There will be one or more administrators of the Operational Environment that will be responsible for managing the Common Criteria evaluated configuration.

OE.INSTALL

Those responsible for the Common Criteria evaluated configuration shall ensure that the Common Criteria evaluated configuration is delivered, installed, managed, and operated in a secure manner.

OE.PERSON

Personnel working as Imprivata OneSign administrators shall be carefully selected and trained for proper operation of the Common Criteria evaluated configuration.

OE.PROTECT

One or more ESM Access Control products will be deployed in the Operational Environment to protect organizational assets.

OE.ROBUST

The Operational Environment provides mechanisms to reduce the ability for an attacker to impersonate a legitimate user during authentication.

OE.USERID

The Operational Environment is able to identify a user requesting access to the Common Criteria evaluated configuration.

Establish The Enterprise

This document is the customer guidance supplement for configuration and use of the NIAP Protection Profile for Enterprise Security Management Policy Management, version 2.1-evaluated configurations for Imprivata OneSign Version 7.9 Hot Fix 9 (HF9).

This document assumes that you are familiar with the basic concepts and terminologies used in internetworking, protocols, and so on, along with Imprivata OneSign.

This document provides guidance on the secure installation and secure use of Imprivata OneSign for the evaluated configuration. This document provides clarifications and changes to the standard documentation and should be used as the guiding document for the configuration and administration of Imprivata OneSign in the Common Criteria evaluated configuration. Official Imprivata OneSign product documentation should be referred to and followed only as directed within this guiding document.

The information in this guide supersedes related information in other Imprivata OneSign documentation. If any discrepancy appears between information in this guide and information in other Imprivata OneSign documentation, the information in this guide takes precedence.

This document is available for download here:

https://imprivatadownloads.hostedftp.com/~Imprivata/Download/NIAP_OneSign_CCGuide/CommonCriteria_AdminGuide.pdf

Deploy VMware ESXi 6.7 Update 3

The following sections detail how to install a virtual appliance to VMware and add it to the network.

Before You Begin

Review the following requirements and considerations before you begin. The following constraints are applicable to the Common Criteria evaluated configuration:

- Offline Authentication is not allowed. This mode must be disabled in User Policy and Computer Policies;
- Temporary Codes for Windows Access must be disabled. Temporary codes are disabled for your enterprise by default. In the Imprivata Admin Console, go to the gear icon > **Settings** > **Temporary Codes** to confirm.
- Username / password authentication is the only authentication method allowed. This is set by default. Other authentication methods are disabled by default; All other authentication methods cited in Imprivata documentation are forbidden;
- Authentication using domain users is not allowed. Only users in an Imprivata domain are allowed;
- Imprivata Confirm ID is not allowed;
- Apache HTTP Server TLS 1.3 support is disabled.
- File servers for backup functionality is disallowed.
- Network Time Protocol (NTP) is disabled.

More On The Imprivata Agent

When the Imprivata agent contacts the Imprivata appliance for the first time (enrollment), the appliance sends the agent a unique 128-bit identifier over an HTTPS connection that the agent securely stores. This key allows the Imprivata appliance to uniquely identify the agent when the agent contacts it. When the agent contacts the appliance when no user is logged into the endpoint (for example, during a refresh interval), the agent uses its unique key to identify itself to the Imprivata appliance after the HTTPS connection is established.

Installing the Imprivata Agent

Download the Imprivata agent installer from the Imprivata Admin Console:

1. In the Imprivata Admin Console, go to **Computers** > **Deploy agents**.
2. In the section **Deployment procedure**, click **Imprivata agent installer 64-bit**.

   The filename is **ImprivataAgent_x64.msi**

Uninstalling the Imprivata Agent

Users whose accounts were deleted or disabled may want to uninstall the Imprivata agent from the former user's computer. To uninstall the agent, the user should use the Windows Control Panel **Add/Remove Programs** utility and then restart the computer.

> ⓘ **NOTE:** When you uninstall the Imprivata agent, the service is disabled, but the computer remains in the computers list on the Computers page until you delete it. User information remains on the Imprivata server until the user account is removed.

Network Services Configuration

The Imprivata appliance supports the initial assignment of the following:

- IP address, subnet mask, and default gateway.
- DNS servers.

IP Address and Default Gateway Configuration

As part of the initialization process, an IP address, subnet, and default gateway are initially assigned.

This is achieved using either DHCP, if enabled in your environment, or later using the Imprivata Appliance Console when adding the appliance to a network. If required, you can change the settings using one of the following:

- The Imprivata Appliance Console before running the Imprivata appliance configuration (setup) wizard.
- The Imprivata Appliance Console (https://<appliance IP address>:81/) after completing the appliance configuration (setup) wizard.

> ⓘ **NOTE**: If DHCP is used to assign these values, be sure to take the necessary steps to prevent duplicate IP address conflicts on the DHCP network. The Imprivata appliance requires a static IP address.

DNS Server Configuration

As part of the initialization process, up to three DNS servers are initially assigned.

- This is achieved using either DHCP, if enabled in your environment, or using the Imprivata Appliance Console.
- If required, the appliance configuration (setup) wizard lets you change these settings as part of the initial setup of the network services. Additionally, after the appliance has been added to the enterprise, you can use the Imprivata Appliance Console (**Network** > **Name Resolution**) to update them.

Deploy The Imprivata OVF Template

The following sections detail how to deploy the Imprivata appliance add it to the network.

Contact your Imprivata sales representative or sales engineer to have Imprivata Operations send you a fulfillment letter that includes the download links and license required for installation.

To deploy the appliance:

1. From your fulfillment letter, download and extract the Imprivata Virtual Appliance RAR file.

   > ⓘ **NOTE**: If deploying to VMware ESXi 6.7, deploy one appliance at a time. Deploying multiple appliance in parallel can result in the process timing out.

2. In the vSphere Client, highlight **ESXi Host system**, right-click and select **Deploy OVF template**.
3. Follow the **OVF Deploy Template** wizard to complete the deployment. Consider the following:
   - ESXi 6.7 only — Select both the OVF and VMDK files.
   - When prompted to customize **Networking Properties**, leave all values blank. You network the appliance using the Appliance Configuration wizard.

Disabling the vApp Options

To disable the vApp options:

1. Highlight the appliance and select the **Configure** tab
2. Under **Settings**, select **vApp Options**.
3. Select **Edit**.
4. Uncheck **Enable vApp options**.

Adding the Appliance to the Network

1. Power on the appliance, and open the console to start the appliance initialization scripts.
   - The G4 initialization scripts run in the background and do not display progress. The time to complete is approximately 15 minutes.
   - The Imprivata virtual appliance console displays the IP address, subnet mask, and gateway that is initially assigned to the appliance.
2. (*Optional*) If required, you can change the network configuration manually:
   a. At the **login** prompt type **menu**, and then press **Enter**.
   b. Type **1**, and then press **Enter** to reassign the values.

> **NOTE**: If you receive a database error messaging when trying to log in, the appliance has not finished initializing.

3. Exit the Imprivata virtual appliance console.
4. In a web browser, enter https://<*appliance_IP_address*>:81 to complete the setup using the appliance configuration wizard.

To access the Imprivata virtual appliance menu:

1. Open the virtual machine console.
2. At the login prompt, enter **menu** and press **Enter**. If prompted, enter the menu password and press **Enter**. The Imprivata virtual appliance functions menu opens.

The menu options are:

1. **Configure Network** — Lets you change the default gateway for the appliance. It is for installation only. Change this setting from the **Network** tab under the **Network** page of the Imprivata Appliance Console.
2. **Reset SSL** — Clears all SSL information, including the optional SSL 2.0 setting.
3. **Reset admin password for Appliance UI**— Resets the Administrator password to *admin*. You cannot reset the Super Administrator password.
4. **Modify Password**— Lets you set or clear the password for this menu.
5. **Restage** — Resets the appliance to factory settings. Contact Imprivata Customer Support for assistance with restaging an appliance.
6. **Reboot** — Restarts the appliance. It is best to restart the appliance by clicking the **Restart** button in the **Operations** tab under the **System** page of the Imprivata Appliance Console, unless the Imprivata Appliance Console is unreachable.
7. **Shutdown** — Shuts down the appliance. The Virtual Machine is still deployed in the VMware host.
8. **Quit**

Troubleshooting

Verify the RAR File Download 7.9_PROD_G4_OVF.rar

Verify that the files were not corrupted during download.

1. In the Imprivata Virtual Appliance RAR file, there should be three files:
   - .mf - a manifest files, containing checksums for the OVF and VMDK files.
   - .ovf - the virtual machine template file, containing a description of the virtual machine.
   - .vmdk - the virtual machine hard disk file.
2. Open the .mf file in a text editor. It is formatted similar to the following example:

   ```
   SHA1(imprivata6.2.ovf)= a956be53480a2d6f4ca43a9c6ef46fba2e326150
   SHA1(system-disk1.vmdk)= a2bedcb3bfb14e7bbbf5ad481d58104aa1ec79ba
   ```

3. Run a hash of each of these two files to verify the resulting checksums against the contents of the manifest file.

Use the following PowerShell command to get the file hash and convert it to lower case for easy comparison:

```
$(Get-FileHash .\imprivata6.2.ovf -Algorithm SHA1 | Select -ExpandProperty
Hash).ToLower()
```

4. Compare the output of the PowerShell command with the checksum in the manifest file.
   - If the checksums match, it confirms that the download is good and that the extracted files are good.
   - If the checksums do not match, it indicates that the files may be corrupted and may indicate a problem with either the extraction or download process.

Recommended Steps

1. Do not delete the existing RAR archive; it may still be usable.
2. Download the archive again, using an alternate browser from the original download method. While the download is in process, you can recheck the original file:
   a. Use a different extraction utility to extract the original RAR archive. The choice of extraction utility may affect the outcome when extracting large archives.
   b. Run the checksum process on the newly extracted files to determine whether the files are good.
      - If the checksums match, cancel the new download.
      - If the checksums do not match, continue the new download and repeat the verification process.

Issues Deploying OVF File to VMware

If you experience problems deploying the OVF file, consider the following:

- When deploying, select only the OVF and VMDK files, not the MN (manifest) file.

  The hypervisor may attempt to run a checksum on the manifest file, which does not contain a checksum for itself.

- If you still experience problems, deploy the files using the vSphere command line tool instead of the Web Client.

  Example

  ```
  ovftool.exe -ds=VMFS005_3PAR109 --net:"Network 1”=”Network A VLAN 432"
  -n=WSLXIMP1901 "D:\Temp\S3x64\Imprivata5.5hf1demo_OVF10.ovf"
  vi://adminrb@100.64.0.25/
  ```

  Syntax

  ```
  ovftool --net: "source_network_name"="destination_network_name"
  -ds="destination_datastore" -n="destination_virtual_machine_name"
  "vi://domain\username@source_vcenter_fqdn/source_datacenter_name/
  virtual_machine_name/virtual_machine_folder/virtual_machine"
  "vi://domain\username@destination_vcenter_fqdn/host/cluster_name"
  ```

Configure the Enterprise Settings

1. Open a supported browser window to **https://*<Appliance IP address>*:81/.**

   The Appliance Configuration Wizard start page opens.

2. Select **Create a new Imprivata enterprise** and then enter the name for the first Imprivata site.
3. Click **Next**. The Imprivata License Key Configuration page opens.
4. Browse to and upload your Imprivata license, then click **Next**. The System Settings page opens.

   System settings include Host and domain name, Email forward address, and Time zone.
5. Enter passwords for the appliance Super Administrator and Administrator. A Super Administrator can perform all appliance administration functions across the enterprise, while an Administrator cannot perform some actions that affect the entire enterprise.
   - The Common Criteria evaluated configuration only requires the Super Administrator account to configure the Imprivata Appliance Console.

   > **NOTE:** These passwords are for the Imprivata Appliance Console only; you can have different passwords for the Imprivata Admin Console.
6. Click **Next**. The Network Services page opens.

   Network services include DNS servers, an SMTP server, and NTP Servers.

   NTP servers are not allowed in a Common Criteria certified configuration. Uncheck the NTP option and manually enter the current date and time instead.
7. Click **Next**. The appliance restarts.

Increase File Upload Size

To allow the successful upload of the Appliance IPM file in the following section, install the following special IPM that enables uploads larger than 2 GB to the Imprivata appliance:

increasePHPmaxPOST-2021-1-22.ipm

Download location:

https://imprivatadownloads.hostedftp.com/~Imprivata/Download/appliance-platform-update/NIAP+IPMS/Archive/increasePHPmaxPOST-2021-1-22.ipm

This download is available from the Imprivata software downloads page:

1. Log into the the Imprivata Support and Learning Center at support.imprivata.com.
2. Go to **Products** > **Imprivata OneSign**
3. At the Product Downloads drop-down, select **Imprivata OneSign 7.9**
4. Download **Increase PHPMaxPOST**
5. Log into the Imprivata Appliance Console. Go to the **Packages** tab.
6. Click **Upload Imprivata Package**, specify the IPM you just downloaded, and then click **Upload**.
7. From the Imprivata Appliance Console, select the IPM and click **Install**.
8. Click **Install**. Upon successful installation, the Imprivata appliance will reboot without further notification.

Install Imprivata Appliance IPM

Update your Imprivata appliance software stack to the evaluated configuration, including the cipher suite limitations. The file name is

virtual-applianceG4-IMPRIVATA-2023-2-1.ipm

This download is available here:

https://imprivatadownloads.hostedftp.com/~Imprivata/Download/appliance-platform-update/NIAP+IPMS/virtual-applianceG4-IMPRIVATA-2023-2-1.ipm

1. Log into the Imprivata Appliance Console. Go to the **Packages** tab.
2. Click **Upload Imprivata Package**, specify the IPM you just downloaded, and then click **Upload**.
3. From the Imprivata Appliance Console, select the IPM and click **Install**.
4. Click to acknowledge you have read and understand the upgrade installation instructions.
5. Click **Install**. Upon successful installation, the Imprivata appliance will reboot without further notification.

Install Imprivata OneSign 7.9.9 Hotfix

Imprivata OneSign 7.9.9 includes additional features not included in the base Imprivata OneSign 7.9 release.

You can verify your Imprivata OneSign version at any time: on the Imprivata Admin Console, hover over the question mark icon to view the version number and build.

Imprivata OneSign Version 7.9 Hot Fix 9 (HF9) is required for the Common Criteria evaluated configuration. The filename is

virtual-imprivataG4-7-9-9.ipm

This download is available here:

https://imprivatadownloads.hostedftp.com/~Imprivata/Download/appliance-platform-update/NIAP+IPMS/virtual-imprivataG4-7-9-9.ipm

1. Log into the Imprivata Appliance Console. Go to the **Packages** tab.
2. Click **Upload Imprivata Package**, specify the IPM you just downloaded, and then click **Upload**.
3. From the Imprivata Appliance Console, select the IPM and click **Install**.
4. Click to acknowledge you have read and understand the upgrade installation instructions.
5. Click **Install**. Upon successful installation, the Imprivata appliance will reboot without further notification.

Appliance Downtime and the Upgrade

Upgrading to Imprivata OneSign 7.9.9 supports a zero–downtime upgrade.

- The Imprivata server remains up throughout the entire upgrade.
- The appliance does not have to be rebooted after an upgrade.
- Scheduled jobs are skipped until their next scheduled time. Skipped jobs include audit record maintenance, automated domain password changes, automated domain synchronization, and scheduled reports.

Bandwidth Requirement

The upgrade requires at least 10 MBps of available bandwith. If your network has fewer than 10MBps available, then agent authentication failures or upgrade failure may occur.

BEST PRACTICE: Perform the upgrade during off-peak network utilization hours to provide as much bandwidth as possible for the upgrade.

Data Loss and the Upgrade

Consider the following:

- Audit records are retained during the upgrade.
- As part of the appliance upgrade, the Imprivata database is synchronized. The enterprise remains online during the synchronization, which can result in infrequent data loss.

Although unlikely, data that is collected while the database is being synchronized may be lost. As a result, some users may be required to re–enter credentials that were captured during the upgrade. Examples of lost data include:

- User credentials captured during user authentication
- Passwords that are reset
- Changes made through Imprivata's provisioning interface

This type of data loss may occur only when the Imprivata database is being synchronized as part of the upgrade. It does not occur when synchronizing the Imprivata database outside of the upgrade process.

Upgrade the Imprivata Appliance

1. Log into the Imprivata Appliance Console. Go to the **Packages** tab.
2. Click **Upload Imprivata Package**, specify the file, and then click **Upload**.
3. From the Imprivata Appliance Console, click **Install**.

CAUTION: Even if the Imprivata Admin Console is available after you start the upgrade, do not use it. Changes may be lost during the upgrade.

If the upgrade fails for any reason, error messages are displayed on the Imprivata Appliance Console. Collect the appliance logs and contact Imprivata Technical Support to resolve the issue and complete your upgrade.

1. In the Imprivata Appliance Console, go to the **System** page > **Logs** tab.
2. Select a log from either the Imprivata server **Logs** drop-down list box or the **Appliance Logs** drop-down list box.
3. Click **Display Log** to view the log in a new browser window.
4. To export logs, go to **Log data export** > **Log data to include**
5. Select **all available data** or **data since** and select a date and time range.
6. To automate the delivery of logs to Imprivata, select **Send a copy to Imprivata Technical Support**; when selected, enter the case number provided by Imprivata Customer Support.
7. Click **Start Export**. The appliance will copy logs from various system directories and create an archive file. When you click **Start Export**, the previous log report will be overwritten. A progress indicator is displayed while the logs are collected and exported; you can click **Stop Export** to cancel.
8. After the export is complete, click **View Files** to open the archive.

Install Common Criteria Feature Flag

This IPM enables Imprivata OneSign functionality exclusive to the Common Criteria evaluated configuration. The filename is

enableAccessControlNIAP-2022-9-12.ipm

- Restricts SSH traffic algorithms allowed in the Common Criteria-certified configuration
- Limits Apache NSS and OpenSSL to TLS v1.2
- Assures identity on every connection from the Imprivata Agent to the Server
- Performs a compliant destruction of secrets on HEAP cleanup

The file is available here:

https://imprivatadownloads.hostedftp.com/~Imprivata/Download/appliance-platform-update/NIAP+IPMS/enableAccessControlNIAP-2022-9-12.ipm

1. Log into the Imprivata Appliance Console. Go to the **Packages** tab.
2. Click **Upload Imprivata Package**, specify the IPM you just downloaded, and then click **Upload**.
3. From the Imprivata Appliance Console, select the IPM and click **Install**.
4. Click to acknowledge you have read and understand the upgrade installation instructions.
5. Click **Install**. Upon successful installation, the Imprivata appliance will reboot without further notification.

Create the Super Administrator Account

This procedure creates the Imprivata Super Administrator account, the first domain, and enrolls the Imprivata Super Administrator's credentials.

1. From the browser, go to `https://<Imprivata Admin Console IP Address>/sso/login.html`. The **Create your first admin account** page opens. Enter the information for your existing directory server or choose **New Imprivata directory** to create a new directory.
2. Fill in the fields:
   - Directory type
   - Domain
   - Host name / IP address (fully-qualified host name or IP address)
   - Username
   - Password
3. Click **Create admin**. The Home page opens.

   After you create the initial Super Administrator account, all Administrators log into the Imprivata Admin Console at: `https://<Imprivata Admin Console IP Address>/sso/administrator.html`.

- If a browser security prompt appears, click **Accept**.
- If the Imprivata Admin Console fails to open, add it to your browser's trusted site list.

NOTE:
Creating the Super Administrator is a one-time procedure, necessary only the first time you establish an Imprivata OneSign enterprise.

Server Configurations

Use the **Security** page in the Imprivata Appliance Console to manage certification, and to configure automatic notification of abnormal requests made to the web server.

Certificate Authorities

The following are the available certificate authorities from which a server certificate for the syslog server can be obtained.

- AC CamerFirma S.A.
- ACCV
- Actalis S.p.A./03358520967
- AffirmTrust
- Amazon
- Atos
- Baltimore
- Buypass AS-983163327
- Certificate Hall
- certSign
- Chunghwa Telecom Co., Ltd.
- Comodo CA Limited
- CyberTrust, Inc.
- Dhimyotis
- Digicert Inc
- Disig a.s.
- D-Trust GmbH
- EC-ACC Agencia Catalana de Certificacio
- emSign
- Entrust, Inc.
- E-Tuğra EBG Bilişim Teknolojileri ve Hizmetleri A.Ş.
- Firmaprofesional
- GeoTrust Inc
- GlobalSign
- GoDaddy.com, Inc.
- Google Trust Services
- Guangdong Certificate Authority (GDCA)
- Hellenic Academic and Research Institutions Cert. Authority
- Hongkong Post e-Cert
- IdenTrust
- Internet Security Research Group
- Izenpe S.A.
- Japan Certification Services, Inc.
- Microsec Ltd.
- Microsoft
- NetLock Kft.
- Network Solutions L.L.C.
- QuoVadis Limited
- SECOM Trust Systems CO.,LTD.
- SecureTrust Corporation
- Sonera
- SSL.com
- Staat der Nederlanden
- Starfield Technologies, Inc
- SwissSign AG
- Szafir
- TAIWAN-CA
- TeliaSonera
- Thawte Consulting cc
- The USERTRUST Network
- TrustCor
- Trustis Limited
- Trustwave
- T-Systems Enterprise Services GmbH
- Türkiye Bilimsel ve Teknolojik Araştırma Kurumu - TÜBİTAK
- Unizeto Technologies S.A.
- VeriSign, Inc.
- WISekey
- XRamp Security Services Inc

The SSL Tab

Use the **SSL** tab to view, edit, download, import, and recreate the self-signed SSL certificate for the Imprivata appliance. The appliance creates a self-signed SSL certificate during installation. When you initially view the **SSL** tab, the information from the self-signed certificate opens.

Editing the Current Certificate Information

To edit the information for the current certificate:

1. Click **Edit**. A window opens where you can enter the new information.
2. Enter the new information.
3. Click **Recreate Self Signed Certs**. A notice appears informing you to restart the appliance.

4. Click **OK**. You return to the SSL tab, with a notice that the information has changed. Changes are not reflected in the certificate until the appliance is restarted.

Secure Copy Protocol for Audit File Data

In the Common Criteria evaluated configuration, transferring audit records with FTP is forbidden.

A secure connection is required for an external audit server.

Your audit record and backup file servers must support SSHv2.

Add SCP Server

Before you add the SCP server, configure the appliance's SSH public key authentication by copying and pasting the public key into the trusted hosts configuration of the SCP server. Refer to your SSH documentation for further details.

1. On the File Servers tab of the Imprivata Appliance Console, click **Add Server** >
2. **Secure (SCP) Server** checkbox.
3. Enter the IP address or hostname of the SCP server.
4. Enter the username.
5. Configure the appliance's SSH public key authentication by copying and pasting the public key into the trusted hosts configuration of the SCP server.
6. Click **Add**.

Configure SCP for Audit Records

1. In the Imprivata Admin Console, go to the **gear icon** > **Settings**.
2. In the section **Audit Records** > **File server configuration**, Select **Protocol** > **SCP (Secure copy)**
3. Complete the **Server**, **Username**, and **Password** fields.
4. Configure the appliance's SSH public key authentication by copying and pasting the public key into the trusted hosts configuration of the SCP server.
5. Click **Save**.
6. On the **System** page > **Operations** tab > **Backup** section, click **Configure** to configure the appliance to automatically store backups on the designated file server.

> **NOTE:**
> The password authentication method cannot be changed. The SSH Public Key authentication method cannot be changed. The algorithms for the SSH protocol cannot be changed; Refer to the SSH documentation for further details.
>
> The SSH Public Key:
>
> - is set by default;
> - does not require manual configuration; and
> - rejects all other encryption algorithms.

Auditing Mechanisms

Imprivata OneSign uses two separate local auditing mechanisms to fulfill the audit requirements. Different events are recorded by each mechanism. One mechanism stores audit records in Imprivata OneSign's local database. The other mechanism uses syslog and a local syslog file. In both cases, the audit records are protected from unauthorized deletion and modification. Imprivata OneSign only allows administrators with the appropriate administrator role attributes access to the audit records.

The audit records in Imprivata OneSign's local database can be saved to external audit log storage using SSH to protect the channel. The syslog audit records can be saved to an external audit server (syslog server) using TLS to protect the channel.

External Audit Log Storage

The external audit log storage mechanism can be configured to transfer audit records two different ways: periodically and on-demand. When configured for periodic transfers, Imprivata OneSign automatically transfers audit records in log files to the external audit log storage at administrator-defined intervals. See Audit Record Maintenance.

If the connection fails during the transfer or the external audit log storage is unavailable, Imprivata OneSign retains the log files and attempts to transfer them at the next interval. When configured for on-demand transfers, Imprivata OneSign transfers audit records in log files to the external audit log storage at the request of the administrator.

External audit server (syslog)

The external audit server mechanism connects and continuously sends audit records to the external audit server. If the connection fails or the external audit server is unavailable, all audit events generated while the connection is broken are lost.

When the connection is reestablished, only audit records generated after the reestablishement are sent to the external audit server. No alert or notification is provided to the administrator regarding these lost audit records.

Imprivata OneSign recovers from such an outage as quickly as possible, and the Administrator can make no specific configuration changes that will improve upon the recovery time.

Manage Audit Records

1. In the Imprivata Admin Console, go to the **gear icon** > **Settings**.

   In the section **Audit records**, you can exclude event types from future logging to facilitate troubleshooting:
2. Click **Manage audit records**. Select a time period to review audit record types that have been logged.

   To aid in your decision whether to exclude future audit record logging, each audit record type is listed with the quantity of records logged.
3. Clear the checkbox for each audit record type you need to exclude going forward.
4. Click **OK**.
5. At the bottom of the Imprivata Admin Console page, click **Save**.

Audit Record Maintenance

This section describes how to archive (transfer) audit records periodically, and on demand:

1. In the Imprivata Admin Console, go to the **gear icon** > **Settings**.
2. In the section **Audit records** go to **Manage audit records**.
3. Configure archiving and/or deletion of old records;
4. In the **Frequency** section, select the frequency and time of day when reports automatically run and export: never, daily, weekly, or monthly;
5. **Optional** - select **Perform now**; When you are prompted to confirm the number of records to be archived and/or deleted, click **OK**.
6. Click **Save**.

Information in the Audit Logs

Component	PP	Additional Information	Location	Example Value(s)
FAU_GEN.1.1		Start-up of the audit functions		OSC Logs 07/11/2023 08:19:58 Info-- SetValue [10.4.146.49]: imprivata/pa_uilocked to 1 07/11/2023 08:19:58 Info-- SetValue [10.4.146.49]: imprivata/pa_uilockmesg to Appliance Rebooting 07/11/2023 08:19:58 Info-- Script system/reboot.pl system.pa_reboot 5, status: Success … 07/11/2023 08:21:23 Info-- OSC RESTART 07/11/2023 08:21:31 enterpriseAgent-- Enterprise Agent Daemon Started 07/11/2023 08:21:32 Info-- Script enterprise/rewritefw.pl enterprise.rewritefw refresh, status: Success 07/11/2023 08:22:31 Info-- SetValue [10.4.146.49]: system/health/servers/onesign/pa_state to normal 07/11/2023 08:19:58 Info-- SetValue [10.4.146.49]: imprivata/pa_uilocked to 1 07/11/2023 08:19:58 Info-- SetValue [10.4.146.49]: imprivata/pa_uilockmesg to Appliance Rebooting 07/11/2023 08:19:58 Info-- Script system/reboot.pl system.pa_reboot 5, status: Success … 07/11/2023 08:21:23 Info-- OSC RESTART 07/11/2023 08:21:31 enterpriseAgent-- Enterprise Agent Daemon Started 07/11/2023 08:21:32 Info-- Script enterprise/rewritefw.pl enterprise.rewritefw refresh, status: Success 07/11/2023 08:22:31 Info-- SetValue [10.4.146.49]: system/health/servers/onesign/pa_state to normal

Component	PP	Additional Information	Location	Example Value(s)
FAU_GEN.1.1 continued		Start-up of the audit functions		Imprivata Server Logs 2023-07-11 08:22:18,232| sso-win INFO [main]: ***************************************. 2023-07-11 08:22:18,232| SSO INFO [main]: ******************** OneSign Server is in FIPS-compliant mode *******************. 2023-07-11 08:22:18,232| sso-win INFO [main]: ******************** OneSign Server is in FIPS-compliant mode *******************. 2023-07-11 08:22:18,233| SSO INFO [main]: ***************************************. 2023-07-11 08:22:18,233| sso-win INFO [main]: ***************************************. 2023-07-11 08:22:18,233| SSO INFO [main]: ************ Database symmetric encryption:. 2023-07-11 08:22:18,233| sso-win INFO [main]: ************ Database symmetric encryption:. 2023-07-11 08:22:18,233| SSO INFO [main]: ************ Provider : WOLFCRYPT. 2023-07-11 08:22:18,233| sso-win INFO [main]: ************ Provider : WOLFCRYPT. 2023-07-11 08:22:18,233| SSO INFO [main]: ************ Algorithm: AES-256. 2023-07-11 08:22:18,233| sso-win INFO [main]: ************ Algorithm: AES-256. 2023-07-11 08:22:18,233| SSO INFO [main]: ***************************************. 2023-07-11 08:22:18,233| sso-win INFO [main]: ***************************************. 2023-07-11 08:22:18,233| SSO INFO [main]: ************ Digipass data symmetric encryption:. 2023-07-11 08:22:18,233| sso-win INFO [main]: ************ Digipass data symmetric encryption:. 2023-07-11 08:22:18,233| SSO INFO [main]: ************ Provider : WOLFCRYPT. 2023-07-11 08:22:18,233| sso-win INFO [main]: ************ Provider : WOLFCRYPT. 2023-07-11 08:22:18,233| SSO INFO [main]: ************ Algorithm: AES-256. 2023-07-11 08:22:18,233| sso-win INFO [main]: ************ Algorithm: AES-256. 2023-07-11 08:22:18,233| SSO INFO [main]: ***************************************.

Component	PP	Additional Information	Location	Example Value(s)

FAU_GEN.1.1 continued		Start-up of the audit functions		Imprivata Server Logs (continued)
				`2023-07-11 08:22:18,233| sso-win INFO [main]: ***************************************.`
				`2023-07-11 08:22:18,233| SSO INFO [main]: ************ Agent-facing symmetric encryption:.`
				`2023-07-11 08:22:18,233| sso-win INFO [main]: ************ Agent-facing symmetric encryption:.`
				`2023-07-11 08:22:18,233| SSO INFO [main]: ************ Provider : WOLFCRYPT.`
				`2023-07-11 08:22:18,233| sso-win INFO [main]: ************ Provider : WOLFCRYPT.`
				`2023-07-11 08:22:18,234| SSO INFO [main]: ************ Algorithm: AES-256.`
				`2023-07-11 08:22:18,234| sso-win INFO [main]: ************ Algorithm: AES-256.`
				`2023-07-11 08:22:18,234| SSO INFO [main]: ************ Legacy support enabled: false.`
				`2023-07-11 08:22:18,234| sso-win INFO [main]: ************ Legacy support enabled: false.`
				`2023-07-11 08:22:18,234| SSO INFO [main]: ***************************************.`
				`2023-07-11 08:22:18,234| sso-win INFO [main]: ***************************************.`
				`2023-07-11 08:22:18,234| SSO INFO [main]: ************ Session negotiation:.`
				`2023-07-11 08:22:18,235| sso-win INFO [main]: ************ Session negotiation:.`
				`2023-07-11 08:22:18,235| SSO INFO [main]: ************ Provider : SUN.`
				`2023-07-11 08:22:18,235| sso-win INFO [main]: ************ Provider : SUN.`
				`2023-07-11 08:22:18,235| SSO INFO [main]: ************ Algorithm: EC/ECDH-SECP256R1.`
				`2023-07-11 08:22:18,235| sso-win INFO [main]: ************ Algorithm: EC/ECDH-SECP256R1.`
				`2023-07-11 08:22:18,235| SSO INFO [main]: ************ Legacy support enabled: false.`
				`2023-07-11 08:22:18,235| sso-win INFO [main]: ************ Legacy support enabled: false.`
				`2023-07-11 08:22:18,235| SSO INFO [main]: ***************************************.`

FAU_GEN.1.1		Shutdown of the audit functions		`07/11/2023 08:32:50 Info-- SetValue [10.4.146.49]: imprivata/pa_uilockmesg to Appliance Shutting Down`
				`07/11/2023 08:32:50 Info-- Script system/shutdown.pl system.pa_shutdown 1, status: Success`
				`07/11/2023 08:32:50 Info-- SetValue [10.4.146.49]: system/pa_shutdown to 1`

Component	PP	Additional Information	Location	Example Value(s)
ESM_ACD.1	PM	Unique policy identifier	Imprivata server log	Added User Policy: "{col id=""0""}May-11-22 1:00:34 PM{/col} {col id=""1""}Administrator@imp.eng{/col} {col id=""2""}Added User Policy NIAP Test{/col}" Created User Policy: 2020-06-17 11:30:33,264| SSO INFO [00bbb77a-65e0-4b5f-bbb7-7a65e04b5f1b]: 2020-06-17T11:30:33.264699 Action : Added User Policy 'New Policy', Subscriber : Administrator@test.directory , Status : SUCCESS . Modified User Policy: 2022-05-11 13:04:39,638| SSO INFO [5caea5e8-dd41-4fb7-aea5-e8dd41ffb76f]: 2022-05-11T13:04:39.638614976 Action : Modified User Policy 'NIAP Test', Subscriber : Administrator@imp.eng , Status : SUCCESS . Deleted User Policy: 2022-05-11 13:04:55,259| SSO INFO [http-nio-8080-exec-2]: 2022-05-11T13:04:55.259250199 Action : Deleted User Policy 'NIAP Test', Subscriber : Administrator@imp.eng , Status : SUCCESS .
ESM_ACT.1	PM	Destination of policy		2023-07-11 09:12:08,137| SSO DEBUG [http-nio-8080-exec-2]: Action : Computer policy Default Computer Policy (e4d4c53f-6943-4984-94c5-3f69439984c0) has been updated, Status : SUCCESS.
ESM_ATD.1	PM	Identification of the attribute defined	Imprivata server log	2020-06-16 07:38:41,267| SSO INFO [http-apr-8080-exec-4]: 2020-06-16T07:38:41.266854 Action : Assigned Policy 'Default User Policy' to user 'test test' , Subscriber : Administrator@inferno.imp.eng , Status : SUCCESS .

ESM_ATD.1	PM	Identification of the object and the attribute		2023-06-19 13:07:28,156| SSO DEBUG [http-nio-8080-exec-2]: Received the request:
				{AdminComputerUpdate xmlns="urn:ImprivataSOAPService"}
				{session}UtBcKHQVkXiEKcgUEFraXPQVQOKGlAmL{/session}
				{computer selected="false"
				uid="cfa131d8-92a0-45cc-a131-d892a055cce5" xmlns=""}
				{hostname}Win10-atsec-06{/hostname}
				{MAC}00-50-56-81-E0-0C{/MAC}
				{IPAddress}10.4.146.31{/IPAddress}
				…
				2023-06-19 13:18:55,536| SSO DEBUG [http-nio-8080-exec-1]: Action : Computer policy ESM_ATD.2 Computer (5389c106-c9c9-400f-89c1-06c9c9800fff) has been updated, Status : SUCCESS.

Component	PP	Additional Information	Location	Example Value(s)

ESM_ATD.2	PM	Identification of the attribute defined	same as ESM_ATD.1	Definition of subject attributes
				`2023-07-11 10:32:14,414| SSO DEBUG [http-nio-8080-exec-3]: Received the request:`
				`{AdminUserPolicyCreate xmlns="urn:ImprivataSOAPService"}`
				`{session}urPilWNknmasbGxSNAXpaeDURuXVcQUv{/session}`
				`{policy default="false" editAllowed="true" selected="false" uid="" xmlns=""}`
				`{common}`
				`{policyName}ESM_ATD.2 User{/policyName}`
				`{createdBy}`
				`{adminRole name="Super Administrator" uid="445f7479-e208-4be2-9f74-79e208dbe293"/}`
				`{/createdBy}`
				`{authentication}`
				`{fingerAttempts}2{/fingerAttempts}`
				`{failureCount}3{/failureCount}`
				`{failureCountInterval}5{/failureCountInterval}`
				`{lockoutInterval}3{/lockoutInterval}`
				`{isAllowedToShutdownAndRestart}false {/isAllowedToShutdownAndRestart}`
				`{/niapAccessControl}`
				`{/policy}`
				`{/AdminUserPolicyCreate}`
				`.`
				`…`
				`2023-07-11 10:32:14,444| SSO INFO [36f45724-af9c-4f1a-b457-24af9c8f1a7a]: 2023-07-11T10:32:14.442623054 Action : Set shutdown and restart configuration for User Policy 'ESM_ATD.2 User', Subscriber : superadmin@osa.local , Status : SUCCESS .`
				`2023-07-11 10:32:14,449| SSO INFO [36f45724-af9c-4f1a-b457-24af9c8f1a7a]: 2023-07-11T10:32:14.449802475 Action : Added User Policy 'ESM_ATD.2 User', Subscriber : superadmin@osa.local , Status : SUCCESS .`

ESM_ATD.2	PM	Association of attributes with subjects	same as ESM_ATD.1	`2023-06-19 12:45:53,584| SSO INFO [http-nio-8080-exec-2]: 2023-06-19T12:45:53.584377232 Action : Assigned Policy 'ESM_ATD.2 User' to user 'testuser' , Subscriber : superadmin , Status : SUCCESS .`
				`…`
				`2023-06-19 13:18:56,130| SSO DEBUG [http-nio-8080-exec-2]: No launching Enrollment`

Component	PP	Additional Information	Location	Example Value(s)

ESM_EAU.2	PM	All use of the authentication mechanism	User Activity Report	Type of events: Keyboard-mouse inactivity, AMShutdownAgentSuccessful, LoginSuccessfulPassword
				`81ea1e49-2d12-490b-a464-b28d353776e4, "17 June 2020 at 09:46:43 GMT", "ahavr", "OneSign", "Shared Workstation Login", "Password", "Successful", "N/A", "ahavrwin10-01", "10.153.154.23", "00-50-56-81-C0-D1", "LV1304", "10.15.225.230", "LV1304", "N/A", "N/A", "N/A", "N/A", "N/A"`
				Desktop agent login:
				`Jun-17-20 5:51:13 AM Shared Workstation Login Successful Password N/A ahavrwin10-01 10.153.154.23 00-50-56-81-C0-D1 N/A N/A LV1304 10.15.225.230 LV1304 N/A N/A`
				Desktop agent lock:
				`Jun-17-20 4:51:53 AM Locked Successful N/A N/A ahavrwin10-01 10.153.154.23 00-50-56-81-C0-D1 N/A N/A N/A N/A N/A N/A N/A`
				Desktop agent exit:
				`Jun-17-20 5:12:40 AM Shutdown Agent Successful N/A N/A ahavrwin10-01 10.153.154.23 00-50-56-81-C0-D1 N/A N/A N/A N/A N/A N/A N/A`
				Desktop agent inactivity lock:
				`Jun-17-20 5:28:19 AM Keyboard-mouse inactivity lock Successful N/A N/A ahavrwin10-01 10.153.154.23 00-50-56-81-C0-D1 N/A N/A N/A N/A N/A N/A N/A`
				Desktop agent lock:
				`Password N/A ahavrwin10-01 10.153.154.23 00-50-56-81-C0-D1 N/A N/A LV1304 10.15.225.229 LV1304 N/A N/A`

FAU_SEL_EXT.1	PM	None	Imprivata server log	`020-06-17 08:13:51,850| SSO INFO [http-apr-8080-exec-4]: Action: Updated File Server by administrator Administrator, Type: FTP, Status : SUCCESS .`

FAU_STG_EXT.1	PM	Identification of audit server (including external audit log storage)	Imprivata server log	Syslog Success
				`06/20/2023 10:47:28 Info-- Script validate/check_syslog_tls.pl system.syslog_tls 10.4.146.251, status: Success`
				`06/20/2023 10:47:29 Info-- Script validate/check_syslog_entry.pl system.syslog 10.4.146.251, status: Success`
				`06/20/2023 10:47:29 Info-- Script system/fix_syslog_conf.pl system.syslog 10.4.146.251, status: Success`
				`06/20/2023 10:47:29 Info-- SetValue [10.4.146.49]: system/syslog to 10.4.146.251`
				Syslog Failure
				`06/28/2023 08:55:25 ERROR-- Script validate/check_syslog_tls.pl system.syslog_tls 10.4.146.251, status: 256, message: Not a TLS-enabled syslog host: 10.4.146.251:6514: No certificate from the SSL server-EOL-`

Component	PP	Additional Information	Location	Example Value(s)

FCS_HTTPS_ EXT.1	PM	Non-TOE endpoint of connection (IP address), reason for failure (if applicable)	Imprivata server log	Agent Success
				`2023-06-27 13:59:56,206| SSO INFO [http-nio-8080-exec-4]: CS: ClientAuthenticate30 5 ms rAoeqqUYWsqeGIVmoddKlbhgyXMvEZFs on Jun-27-23 1:59 PM at Win10-atsec-06/10.4.146.31 for superadmin@osa.local with Password.`
				Agent Failure
				`2023-06-22 12:22:56,003| SSO INFO [http-nio-8080-exec-4]: testuser authenticated UNSUCCESSFULLY with modality Password.`

FCS_SSH_ EXT.1	PM	Non-TOE endpoint of connection (IP address), reason for failure (if applicable)		SCP Success
				`2023-06-20 10:59:21,487| SSO DEBUG [http-nio-8080-exec-2]: ReportClientSCPUploader.testConnection().`
				`2023-06-20 10:59:21,490| SSO DEBUG [http-nio-8080-exec-2]: ReportClientSCPUploader.getSession().`
				`2023-06-20 10:59:21,614| SSO DEBUG [http-nio-8080-exec-2]: ReportClientSCPUploader.testConnection() connection is valid.`
				`2023-06-20 10:59:21,621| SSO INFO [http-nio-8080-exec-2]: Action: Updated File Server by administrator superadmin, Type: SCP, Status : SUCCESS .`
				SCP Failure
				`2023-06-28 09:12:28,797| sso-win ERROR [http-nio-8080-exec-3]: [id: 20221025.1230]ReportClientSCPUploader.testConnection() can't connect to remote host.`
				`2023-06-28 09:12:28,799| SSO DEBUG [http-nio-8080-exec-3]: Sending the response:`
				`{AdminAuditlogMaintainResponse}`
				`{Status}Failed{/Status}`
				`{Code}ArchiveFailed{/Code}`
				`{Reason}Unable to connect to the server. Please check the connection parameters.{/Reason}`
				`{/AdminAuditlogMaintainResponse}`

FCS_TLS_ EXT.1(C), FCS_TLS_ EXT.1(S)	PM	Non-TOE endpoint of connection (IP address), reason for failure (if applicable)		`2020-06-17 09:00:01,359| SSO INFO [http-apr-8080-exec-2]: Action: Add/Update File Server by administrator Administrator, Type: WFS, Status : FAILED .`
FIA_AFL.1	PM	Action taken when threshold is reached		`"un 17 04:31:01 localhost 2020-06-17 04:31:01,359| esso WARN [http-apr-8080-exec-2]: *********** Primary User Lock-out Notification - Start ************ User: ahavr Domain: OneSign Lockout expiry date: 17 Jun 2020 08:34:01 GMT Status: Success *********** Primary User Lock Notification - End ************"`

Component	PP	Additional Information	Location	Example Value(s)

FMT_SMR.1	PM	Modifications to the members of the management roles		Change Role to Admin
				2023-06-26 08:52:20,591| SSO DEBUG [http-nio-8080-exec-2]: Received the request:
				{AdminUserEdit xmlns="urn:ImprivataSOAPService"}
				{session}MvWSGzcplWpbnArrAeQHGslENKKToSrl{/session}
				{Subscriber editAllowed="true" selected="false"
				uid="91725908-9403-48a8-b259-08940348a8c8" xmlns=""}
				{thirdPartyDirectory}false{/thirdPartyDirectory}
				{adminRole isSuperAdmin="false" uid="445f7479-e208-4be2-9f74-79e208dbe293"}
				{superAdmin}false{/superAdmin}
				{/adminRole}
				{subscriberName/}
				{firstName}USB{/firstName}
				{lastName}User{/lastName}
				{emailAddress domain="osa.local" edit="false" emailID="usbuser"}usbuser@osa.local{/emailAddress}
				…
				2023-06-26 08:52:20,619| SSO DEBUG [http-nio-8080-exec-2]: Sending the response:
				{AdminUserEditResponse}
				{Status}OK{/Status}
				{licenseLimitEnforced}false{/licenseLimitEnforced}
				{attemptedToDisableSelf}false{/attemptedToDisableSelf}
				{attemptedToExpireSelf}false{/attemptedToExpireSelf}
				{attemptedToDemoteSelf}false{/attemptedToDemoteSelf}
				{attemptedToSetDisallowedAdminRole}false {/attemptedToSetDisallowedAdminRole}
				{/AdminUserEditResponse}
				.

<table>
<tr><th>Component</th><th>PP</th><th>Additional Information</th><th>Location</th><th>Example Value(s)</th></tr>
<tr><td>FMT_SMR.1 continued</td><td>PM</td><td>Modifications to the members of the management roles</td><td></td><td>Change Role to Non-Admin
2023-06-26 09:54:35,565| SSO DEBUG [http-nio-8080-exec-2]: Received the request:
{AdminUserEdit xmlns="urn:ImprivataSOAPService"}
{session}fRuNFWYmyyfVDIqfxZgvuazwfTRfDPga{/session}
{Subscriber editAllowed="true" selected="false"
uid="91725908-9403-48a8-b259-08940348a8c8" xmlns=""}
{thirdPartyDirectory}false{/thirdPartyDirectory}
{adminRole isSuperAdmin="true" uid=""}
{superAdmin}true{/superAdmin}
{/adminRole}
{subscriberName/}
{firstName}USB{/firstName}
{lastName}User{/lastName}
{emailAddress domain="osa.local" edit="false" emailID="usbuser"}usbuser@osa.local{/emailAddress}
…
2023-06-26 09:54:35,590| SSO DEBUG [http-nio-8080-exec-2]: Sending the response:
{AdminUserEditResponse}
{Status}OK{/Status}
{licenseLimitEnforced}false{/licenseLimitEnforced}
{attemptedToDisableSelf}false{/attemptedToDisableSelf}
{attemptedToExpireSelf}false{/attemptedToExpireSelf}
{attemptedToDemoteSelf}false{/attemptedToDemoteSelf}
{attemptedToSetDisallowedAdminRole}false {/attemptedToSetDisallowedAdminRole}
{/AdminUserEditResponse}</td></tr>
<tr><td>FTA_SSL.3</td><td>PM</td><td>All session termination events</td><td>User activity report
audit log</td><td>"Jun-17-20 11:09:07 AM Administrator Logout Successful N/A N/A N/A N/A N/A N/A N/A N/A N/A N/A N/A N/A ed8b0335-9dd1-41c5-8fb0-9423640cf125, "15 June 2020 at 09:22:13 GMT", "Administrator", "inferno.imp.eng", "Administrator Logout", "N/A", "Successful", "N/A", "N/A", "N/A", "N/A", "N/A", "N/A", "N/A", "N/A", "N/A", "N/A", "N/A", "N/A"</td></tr>
<tr><td>FTA_SSL.4</td><td>PM</td><td>All session termination events</td><td>User activity report</td><td>2020-06-16 05:16:35,333| SSO ERROR [http-apr-8080-exec-4]: [id: 20200611.0515]2020-06-16T05:16:35.333489, system, Session Timeout for user: administrator, Status : SUCCESS.</td></tr>
</table>

<table>
<tr><th>Component</th><th>PP</th><th>Additional Information</th><th>Location</th><th>Example Value(s)</th></tr>
<tr><td>FTA_TSE.1</td><td>PM</td><td>Denial of session establishment</td><td></td><td>System Lockout Settings
2023-06-27 12:55:53,174| SSO DEBUG [http-nio-8080-exec-4]: Scheduling Enterprise lockout job for lock operation.
2023-06-27 12:55:53,174| SSO DEBUG [http-nio-8080-exec-4]: Enterprise lockout scheduled for @ Tue Jun 27 13:00:00 CDT 2023.
Attempted Login
{/ClientAuthenticate30}
.
2023-06-27 13:16:32,123| SSO DEBUG [http-nio-8080-exec-3]: Unable to get SAML request form SOAP request
.
2023-06-27 13:16:32,133| SSO WARN [http-nio-8080-exec-3]: The server is locked.
2023-06-27 13:16:32,133| sso-win WARN [http-nio-8080-exec-3]: The server is locked.
Manual Unlock Function
2023-06-27 13:37:51,623| SSO DEBUG [http-nio-8080-exec-4]: Received the request:
{AdminRealmSetLock xmlns="urn:ImprivataSOAPService"}
{session}YAxzXjoxTEBufvfPZSgnGnEmManZAOhw{/session}
{setLockStatus}unlocked{/setLockStatus}
{/AdminRealmSetLock}</td></tr>
</table>

Component	PP	Additional Information	Location	Example Value(s)

FTP_ITC.1	PM	Identity of the initiator and target of the trusted channel		Syslog
				06/28/2023 08:54:31 Info-- SetValue [10.4.146.49]: system/syslog to
				06/28/2023 08:54:31 Info-- Script validate/check_syslog_tls.pl system.syslog_tls 10.4.146.251, status: Success
				06/28/2023 08:54:31 Info-- SetValue [10.4.146.49]: system/syslog_tls to 10.4.146.251
				06/28/2023 08:54:31 Info-- Script validate/check_syslog_entry.pl system.syslog 10.4.146.251, status: Success
				SSH
				2023-06-28 09:12:47,219| SSO DEBUG [http-nio-8080-exec-1]: Received the request:
				{AdminAuditlogMaintain xmlns="urn:ImprivataSOAPService"}
				{session}hGNoAkVhAnzilsVZOlSGFleCuUiGHHDE{/session}
				{actNow}false{/actNow}
				{actType}2{/actType}
				{customRetentionYears/}
				{site uid="dd25ed5a-318f-464c-8250-c69cb3485961" xmlns=""/}
				{site uid="dd25ed5a-318f-464c-8250-c69cb3485961" xmlns=""/}
				{site uid="dd25ed5a-318f-464c-8250-c69cb3485961" xmlns=""/}
				{site uid="dd25ed5a-318f-464c-8250-c69cb3485961" xmlns=""/}
				{criterionCode xmlns=""}1{/criterionCode}
				{criterionValue xmlns=""}1{/criterionValue}
				{action xmlns=""}1{/action}
				{FTP path="/home/atsec/testing/logs/SCP" xmlns=""/}
				{AdminFTPServerViewResponse xmlns=""}
				{Status}OK{/Status}
				{server uid="d2f364e9-6017-4d1f-b364-e96017dd1fbe"}10.4.146.251{/server}
				{username}atsec{/username}
				{password}**********{/password}
				{domain/}
				{protocolType}1{/protocolType}
				{port}22{/port}
				{sshPublicKey}ssh-rsa
				{/sshPublicKey}
				{/AdminFTPServerViewResponse}
				{schedule AM="PM" auto="true" date="1" day="Sun" interval="Daily"
				time="3:00" xmlns=""/}
				{site uid="dd25ed5a-318f-464c-8250-c69cb3485961" xmlns=""/}
				{/AdminAuditlogMaintain}

Component	PP	Additional Information	Location	Example Value(s)

FTP_ITC.1 continued	PM	Identity of the initiator and target of the trusted channel		SSH Successful Connection After Reconnect
				`2023-06-28 09:12:48,962| SSO DEBUG [http-nio-8080-exec-4]: ReportClientSCPUploader.testConnection().`
				`2023-06-28 09:12:48,967| SSO DEBUG [http-nio-8080-exec-4]: ReportClientSCPUploader.getSession().`
				`2023-06-28 09:12:49,050| SSO DEBUG [http-nio-8080-exec-4]: ReportClientSCPUploader.testConnection() connection is valid.\`
				`2023-06-28 09:12:49,056| SSO DEBUG [http-nio-8080-exec-4]: ReportClientSCPUploader.getSession().`
				`2023-06-28 09:12:49,135| SSO DEBUG [http-nio-8080-exec-4]: ReportClientFileShareUploader.transferFile(). Start tranfer file.`
				`2023-06-28 09:12:49,251| SSO DEBUG [http-nio-8080-exec-4]: SCPTransferEventListener: filecopy started for /usr/share/tomcat/enrollment_archive_20230628_091248.csv (size 738 bytes).`
				`2023-06-28 09:12:49,251| SSO DEBUG [http-nio-8080-exec-4]: SCPTransferEventListener: filecopy completed for /usr/share/tomcat/enrollment_archive_20230628_091248.csv (size 738 bytes).`
				`2023-06-28 09:12:49,253| SSO DEBUG [http-nio-8080-exec-4]: ReportClientFileShareUploader.transferFile(). Finish tranfering file.`
				`2023-06-28 09:12:49,253| SSO DEBUG [http-nio-8080-exec-4]: Temporary file: enrollment_archive_20230628_091248.csv has been deleted.`
				`2023-06-28 09:12:49,255| SSO INFO [http-nio-8080-exec-4]: Temporary file: tmp_iczkhlsX.csv has been deleted.`
				`2023-06-28 09:12:49,255| SSO INFO [http-nio-8080-exec-4]: Finished archiving enrollment records. 0 records have been archived. It took 299 milli seconds.`
				`2023-06-28 09:12:49,256| SSO DEBUG [http-nio-8080-exec-4]: Instructing the health agent that it may again shut down Tomcat at its discretion.`
				`2023-06-28 09:12:49,258| SSO INFO [http-nio-8080-exec-4]: CS: AdminAuditlogMaintain 717 ms hGNoAkVhAnzilsVZOlSGFleCuUiGHHDE on Jun-28-23 9:11 AM at {location omitted} for superadmin@osa.local.`
				`2023-06-28 09:12:49,258| SSO DEBUG [http-nio-8080-exec-4]: Sending the response:`
				`{AdminAuditlogMaintainResponse}`
				`{Status}OK{/Status}`
				`{count}0{/count}`
				`{/AdminAuditlogMaintainResponse}`

Component	PP	Additional Information	Location	Example Value(s)

FTP_ITC.1 continued	PM	Identity of the initiator and target of the trusted channel		Agent
				2023-06-27 14:01:24,218| SSO INFO [http-nio-8080-exec-1]: CS: ClientAuthenticate30 9 ms idMQpblalfnoyUnjbcUMZndevuMpOVVd on Jun-27-23 2:01 PM at Win10-atsec-06/10.4.146.31 for superadmin@osa.local with Password.
				2023-06-27 14:01:24,219| SSO DEBUG [http-nio-8080-exec-1]: Sending the response:
				{ClientAuthenticate30Response}
				{Status}OK{/Status}
				{compression compressed="false" size="0"/}
				{SecureData}(opaque data omitted from logfile){/SecureData}
				{serverVersion build="0" major="7" minor="9" release="" subminor="0"/}
				{IPTXClientVersion}7,9,006,41{/IPTXClientVersion}
				{/ClientAuthenticate30Response}

<table>
<tr><th>Component</th><th>PP</th><th>Additional Information</th><th>Location</th><th>Example Value(s)</th></tr>
<tr><td>FTP_TRP.1</td><td>PM</td><td>Identification of user associated with all trusted path functions, if available</td><td>User activity report</td><td>Server logs
2023-06-28 10:16:51,362| SSO INFO [http-nio-8080-exec-1]: CS: ClientPing40 19 ms owFuhCUTNALATUiNMZtTZPhqmuXdULTN on Jun-28-23 8:34 AM at Win10-atsec-06/10.4.146.31 for superadmin@osa.local with Password.
2023-06-28 10:16:51,362| SSO DEBUG [http-nio-8080-exec-1]: Sending the response:
{ClientPing40Response}
{Status}OK{/Status}
{data}(opaque data omitted from logfile){/data}
{serverVersion build="0" major="7" minor="9" release="" subminor="0"/}
{/ClientPing40Response}
.
…
2023-06-28 10:25:51,627| SSO INFO [http-nio-8080-exec-1]: CS: ClientPing40 13 ms owFuhCUTNALATUiNMZtTZPhqmuXdULTN on Jun-28-23 8:34 AM at Win10-atsec-06/10.4.146.31 for superadmin@osa.local with Password.
2023-06-28 10:25:51,627| SSO DEBUG [http-nio-8080-exec-1]: Sending the response:
{ClientPing40Response}
{Status}OK{/Status}
{data}(opaque data omitted from logfile){/data}
{serverVersion build="0" major="7" minor="9" release="" subminor="0"/}
{/ClientPing40Response}
APPCS
06/28/2023 09:54:11 Info-- Script imprivata/loginAttempt.pl imprivata.LoginOk admin===10.4.146.31_1687964051, status: Success
06/28/2023 09:54:11 Info-- SetValue [10.4.146.49]: imprivata/LoginOk to admin===10.4.146.31_1687964051
…
06/28/2023 09:55:34 Info-- SetValue [10.4.146.49]: imprivata/UIlastuse to 1687964134
06/28/2023 09:55:35 Info-- SetValue [10.4.146.49]: imprivata/UIlastuse to 1687964135
06/28/2023 09:56:01 dbConnMgr [Info]-- Starting /home/install/valueroot/scripts/enterprise/dbConnMgr.pl
06/28/2023 09:56:03 dbConnMgr [Info]-- Original connIP: 10.4.146.49, new connIP: 10.4.146.49.</td></tr>
</table>

The audit logs contain up to 16 columns, in this order:

1. Internal ID of the Imprivata appliance where the record was created
2. Timestamp
3. Username*
4. Domain name*
5. Type of activity
6. Authentication method*
7. Authentication result*
8. Application name*
9. Client hostname*
10. Client IP address*
11. Client MAC address*
12. Alternate hostname * ‡
13. Alternate IP address* ‡
14. Alternate MAC address* ‡
15. Notes specific to the authentication method, such as the ID token serial number.
16. Notes specific to the type of activity, for example (excluding the password) the credentials that were proxied to the application.

> **NOTE:** Columns marked * are listed only if relevant. Columns marked ‡ are for VMware View.

SSH Connections From The Imprivata Appliance

SSH connections from the Imprivata appliance come from **Bouncy Castle v1.68** — Imprivata OneSign uses MINA in its default MAC configuration; 'none' is excluded. The administrator cannot edit or alter this list of MACs. This list:

- is set by default;
- does not require manual configuration; and
- rejects all other encryption algorithms.

Imprivata OneSign will automatically rekey the SSH connection after the conditions stated in the Security Target.

Remote Syslog Server

> **NOTE:**
> TLS, Bouncy Castle, and NSS are the only cryptography engines used by Imprivata OneSign. Imprivata OneSign administrators cannot configure this. Any other cryptography engines are prohibited in the Common Criteria evaluated configuration.

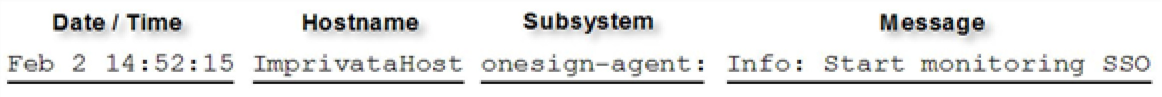
A remote syslog server must be TLS enabled and RFC 5425 compliant:

1. In the Imprivata Appliance Console go to **System** > **Logs**.
2. Click **Syslog Server** > **Edit**.

3. Enter the IP address or hostname of the syslog server.
4. Click **TLS enabled**.
5. Click **OK**.

Syslog Entry Format

The format of a syslog entry is: **Mon DD HH:MM:SS Hostname Subsystem: Message**



```
Feb 2 14:52:15 ImprivataHost onesign-agent: Info: Start monitoring SSO
```

- **Hostname** is the IP address of the Imprivata appliance that logged an entry in the syslog.
- **Subsystem** — the identity of the Imprivata subsystem entry to the syslog.

Administrator Roles (Delegated Administration)

Imprivata uses administrator roles and sub-Administrator roles with nested scope so you can delegate administrative authority throughout the enterprise. Administrator roles help delegate Imprivata OneSign administration operations throughout an enterprise.

1. In the Imprivata Admin Console, go to the gear icon and select **Administrator roles**.
2. Select an existing role or click **Add Role**.
3. When selecting Add Role, Choose the role the new Administrator role will be based on, and click **Next**.
4. Specify a **Role Name**.
5. Select the **operations** this role can perform.
6. Select the **users and sites** this role can manage.
7. **Add users** to this new role.
8. Click **Save**.

Note that scoping administrator roles by site relates to the end-user computers those Administrators can manage, not to the end-users they can manage. End-user scoping is related to domains and organizational units (OUs) and is unrelated to Imprivata sites.

Delegated administration employs three important concepts: administrative operations, scope of delegation, and inheritance of these two properties, described in the following sections.

Administrator Levels

Imprivata provides two levels of administrator roles. There can be any number of users assigned to an administrator role. You do not have to use all three levels; you can create all administrator roles from the Super Administrator role.

The Super Administrator

There is only one Super Administrator role, named Super Administrator, and it cannot be edited or deleted. The Super Administrator can perform all operations in the enterprise. All other administrator roles are subordinate to the Super Administrator role, including any other roles you create with enterprise-wide scope and full operational authority.

Administrators

You can create as many subordinate roles as you need, and have any number of users in each role. Administrators in subordinate roles can run reports allowed by their role, but they do not see results from actions that occur outside their scope.

Each administrator is a member of an administrator role. Multiple Administrators can share a role, but an administrator can have only one administrator role.

Administrator Operations

Operations are the administrative activities that an administrator can perform. Imprivata allows fine granularity of delegated administration to create a variety of specialist administrator roles based on users, administrative operations, or geography.

An administrator role can include individual or classes of activities. Examples of administrator roles limited by operations might include Help Desk Administrator or Compliance Auditor.

Imprivata operations can be further restricted by administrative scope, described in Understanding Administrator Scope.

The following tables list the attributes that are available and can be assigned to administrator roles in a Common Criteria evaluated configuration.

Properties

Operation(s)	Description
Update System Properties	Ability to define system operations and maintenance such as: • Lockdown • Posting system status • Setting logging level • Refresh Interval • Administrator session timeout • Excluding unregulated audit events from future logging • Configuring an advisory message at Administrator login
System Lockdown	Administrators with System Lockdown privileges can still access Imprivata applications when they are locked down.
Maintain Audit Log	Gives the user the ability to maintain Imprivata audit logs. Users with this role are allowed to: • archive and delete • archive only • delete only
Download Agent MSI Files	Allows the user to download the agent MSI files. 32-bit and a 64-bit MSI files are available for download.
Create/Edit Security Questions **Delete Security Questions**	Allows users to maintain security questions that are used by Imprivata OneSign Self-Services.

Operation(s)	Description
Create/Edit Procedure Code **Delete Procedure Code** **Update Extension Object**	Extends the capabilities of Imprivata OneSign with extension objects or procedure codes. There are two extension objects available: Carefx and MediTech. Other procedure codes can be created as command sequences to be executed as a batch file or vbs scripts. **NOTE:** Not supported in the Common Criteria evaluated configuration.
Enable/disable temporary codes	Allows administrators to turn on and off the temporary codes feature for your whole enterprise. **NOTE:** Not supported in the Common Criteria evaluated configuration.
Update proxy to RADIUS **Delete proxy to RADIUS** **Enable/disable proxy to RADIUS** **Update RADIUS host clients** **Delete RADIUS host clients**	The Imprivata appliance has a built-in RADIUS server that can be configured to be a trusted client to other external servers. **NOTE:** Not supported in the Common Criteria evaluated configuration.
Configure ProveID	ProveID is a built-in API that allows external applications to access the Imprivata agent's authentication services and devices. The external application's name is mapped to the name used in the application profile within SSO. **NOTE:** Not supported in the Common Criteria evaluated configuration.

Policies

Operation(s)	Description
Create/Edit User Policy **Delete User Policy** **Assign User Policy**	User policy are assigned to users across the enterprise. User policies apply to the user wherever the user authenticates, even at a satellite office at another Imprivata site. User policies allow you to set different authentication parameters for different user groups. User policies are configured on the **User policies** page (**Users** menu > **User policies**).
Create Computer Policy **Update Computer Policy** **Delete Computer Policy**	Computer policies govern security-related behaviors that are controlled at specific computers. A computer policy created by an Administrator at one site is available to Administrators across the enterprise at any Imprivata site. The **Computer Policies** page under the **Computers** menu lists the computer policies, and the number of computers that use them.

Users

Operation(s)	Description
Add/Edit Users	Allows the administrator to add or edit users after the connection between the Imprivata Directory and an external source (Microsoft AD, NT Domain, Oracle Internet Dire allowed the Admin to reset an Imprivata domain user's PINctory, etc.) is established. See Managing User Accounts in the Imprivata Online Help.
Enable/Disable User	Allows the administrator to enable and disable users. Users must be enabled to use SSO and other Imprivata application privileges. See Managing User Accounts in the Imprivata Online Help.
Delete User	Allows the administrator to delete users from the Imprivata directory. See Managing User Accounts in the Imprivata Online Help.
Reset Imprivata Directory User Password	Allows the administrator to reset an Imprivata domain user's password and PIN.

Operation(s)	Description
Trust/Upload TLS Certificate **Delete TLS Certificate**	Allows the administrator to upload new TLS certificates or delete an existing trusted TLS certificate. Both roles must be selected for the administrator to perform these operations. TLS certificates are required for operations that allow users to change their Imprivata password, such as the Self-Service Password Reset feature.
Upload Kerberos Key **Delete Kerberos Key**	Allows the administrator to upload a Kerberos keytab file to the Imprivata appliance. **NOTE:** Not supported in the Common Criteria evaluated configuration.
Update Imprivata Directory pending users **Delete Imprivata Directory pending users** **Approve Imprivata Directory pending users**	Allows the administrator to update the status of pending users. All three operations must be assigned to the administrator to perform the final update status function. **Pending users** are users who are imported from a CSV file as potential Imprivata users. After imported, they are assigned a Pending status. Not supported in the Common Criteria evaluated configuration.
Update Computers **Delete Computers** **Assign Computer Policy**	Allows the administrator to update computer records, such as by assigning computer policies. Computers are automatically added to the **Computers** page (Imprivata Admin Console > **Computers** menu > **Computers**) when an Imprivata agent is installed and the agent communicates with the Imprivata appliance. If a computer is deleted, it will be re-added the next time the Imprivata agent pings the Imprivata server. See Managing Computer Accounts and Creating and Managing Computer Policies in the Imprivata Online Help
Create/Edit Administrator Roles **Delete Administrator Roles**	Allows the administrator to create and delete additional administrator roles. There can only be one Super Administrator role. See Assigning an Administrator Role in the Imprivata Online Help.

Reports

Functions	Description
View Report **Update Report**	Allows the administrator to view and update Imprivata reports. Both roles must be selected.
Delete Report	Allows the administrator to delete existing Imprivata reports.
Export Report	Allows the administrator to export Imprivata data to a .CSV file.

> Note: To create and run an Administrator Activity report, in the Imprivata Admin Console, go to **Reports** > **Add new report**.

Understanding Administrator Scope

The scope of an administrator role determines the users and computers that can be seen and acted upon by Administrators in the role. However, the scope cannot control who the end users are; end-user scoping is related to domains and organizational units (OUs) and is unrelated to Imprivata sites. End-user scoping is out of the scope of the Common Criteria-evaluated configuration.

A Super Administrator can act upon all users and computers within an enterprise. Other administrator roles can be restricted in scope.

Setting the Imprivata Appliance Console Session Timeout

1. In the Imprivata Appliance Console, go to the **System** page > **Settings** tab
2. Go to **Auto Logout Idle Time (Minutes)** and select a value between zero (timeout disabled) and 600 (ten hours). The default is five minutes.

Auto logout is the period of time that the Imprivata Appliance Console sits idle before automatically logging out the last administrative user and requiring a fresh login. Auto Logout can be set up to 600 minutes.

> **NOTE:**
> You can terminate a session at the Imprivata Appliance Console at any time by clicking the **LOG OUT** button at the top of the console window.

Setting the Imprivata Admin Console Session Timeout

> **NOTE:**
> You can terminate a session at the Imprivata Admin Console at any time by clicking the **Log out** button at the top of the console window.

For security reasons, the Imprivata Admin Console imposes a timeout period for inactive Administrator sessions.

1. In the Imprivata Admin Console, go to the **gear icon** > **Settings**.
2. On the Settings page, go to **Imprivata Admin Console session timeout** and select a value from **5-90 minutes**.
3. Click **Save**.

Computers and Computer Policy

You must use an Imprivata computer policy to select computers and enforce policies for Imprivata OneSign.

All attributes for endpoint computers are defined in Imprivata OneSign user and computer policies, and enforced by the Imprivata agent, installed on the endpoint computer.

To view the definition and configure a computer policy:

1. In the Imprivata Admin Console, go to **Computers** > **Computer policies** and select your computer policy.
2. Review definitions and settings, make changes as needed, and click **Save**.

   Changes to computer policy are sent to Imprivata agents at affected computers at the next refresh interval.

Imprivata Shared Kiosk Workstation Agent

The Imprivata agent is installed on an endpoint computer; it monitors authentication behavior from user workstations and periodically uploads the information to the Imprivata appliance. The Imprivata agent manages:

- Username and password authentication;
- User and computer policies;
- Audit data;
- Application authentication.

The Imprivata agent downloads user and policy information from the Imprivata appliance when a user logs in, and checks for updates again periodically at an interval the Imprivata administrator sets in the Imprivata Admin Console.

When the users authenticate to Imprivata OneSign, the authentication of the username and password entered and the endpoint computer is done at the Imprivata appliance only.

The Imprivata appliance returns to the Imprivata agent an authentication success or failure message only.

The Imprivata agent controls the logging of:

- Users enrolling their passwords for Windows access.
- Offline data.

The Imprivata Shared Kiosk Workstation Agent is out of the scope of the Common Crtieria-evaluated configuration.

Allowing Users to Restart the Workstation from a Lock Screen

Configure the computer policy for shutdown/restart workstation from the lock screen:

1. In the Imprivata Admin Console, go to **Computers** > **Computer Policies** and select a computer policy.
2. On the **General** tab, select **Allow users to shut down and restart workstation from lock screen**.

This will display Shut down button and Restart commands to the user on the Imprivata GINA.

3. Click **Save**.

Browser Support

Item	Support Information
Microsoft Edge Chromium	Imprivata OneSign 7.1 and later: Supports the Imprivata Admin Console and Imprivata Appliance Console
Google Chrome (minimum version: 39)	Imprivata OneSign 7.1 and later: Supports the Imprivata Admin Console
Google Chrome (minimum version: 39)	All maintained Imprivata OneSign versions Supports the Imprivata Appliance Console

Users and User Policy

You must use an Imprivata user policy to select users and enforce policies for Imprivata OneSign.

All attributes for endpoint computers are defined in Imprivata OneSign user and computer policies, and enforced by the Imprivata agent, installed on the endpoint computer.

To view and configure the user policy for authentication:

1. In the Imprivata Admin Console, go to **Users** > **User policies** and select your user policy.
2. Go to **Desktop Access authentication** and confirm **Allow offline authentication** is not checked.
3. Go to Primary factors and only select **Password**.
4. Go to Second factors and select **No second factor**.
5. Review definitions and settings, make changes as needed, and click **Save**.

   Changes to user policy are sent to Imprivata agents at the next refresh interval.

Imprivata Directory Users

An Imprivata Directory Domain is a virtual domain that you create to provide accounts for users who are not members of any of your network domains.

Only users in the Imprivata domain are allowed in the Common Criteria evaluated configuration.

Adding Users

To add a new individual user:

1. In the Imprivata Admin Console, go to **Users** > **Users**.
2. On the **Users** page, click **Add**. The **Add user** page opens.
3. Deselect **Have an account in any external user directory?**
4. Fill in the Name, Email, and Username fields.
5. Optional — Next to the **Imprivata Domain** field, click **New** to create a new Imprivata Directory Domain.
6. Select whether this new user will be a Super Administrator.
7. Select a User Policy.
8. Enter a user password manually or allow Imprivata OneSign to generate a random password.
9. Click **Save**. You are returned to the User List.

NOTE:
The password created here is not communicated to the user with Imprivata OneSign. The administrator is responsible for securely communicating the user's password to the user - in person, by telephone call, or however the administrator sees fit.

User Status

You can view the status of a user at any time.

1. In the Imprivata Admin Console, go to **Users** > **Users** and select a user.
2. At the top of the page, their Username, Status, Role, and User Policy are displayed.

   You can change their Status, Role, or the User Policy they're associated with here.

   You can also delete the enrollment of their authentication methods from this page.
3. Click **Save**.

Delete a User

You can delete a user at any time.

1. In the Imprivata Admin Console, go to **Users** > **Users** and select a user.
2. Click the **trash can icon** to delete the user.
3. Click **Save**.

User Lockout Policy

After a number of consecutive authentication failures, the user account is locked. Even if the user authenticates correctly during the lockout period, the account remains locked.

To configure the lockout rules:

1. In the Imprivata Admin Console, go to **Users** > **User Policies** and select a user policy.
2. Go to the **Lockout** section at the bottom of the page.
3. Change the default settings if needed:

   Lock user account after 5 consecutive failures within 5 minutes
   Lock account for 5 minutes
4. Click **Save**.

Password Complexity

To set password complexity rules, in the Imprivata Admin Console go to **Users** > **Directories** > **Imprivata Directory** and select the directory:

1. Select **Implement Password Change Policy**?
2. Set the minimum password length to 15 characters or greater.
3. Select a character set:
   - Letters (a..z, A..Z) only;
   - CAPITAL letters (A..Z) only;
   - Small letters (a..z) only;
   - Numerals (0..9) only;
   - Letters and numerals (a..z, A..Z, 0..9) only;
   - Special characters required; Letters and numerals (a..z, A..Z, 0..9) allowed
4. You can require 1, 2, or 3 special characters. Special characters include: ~ ! @ # $ * - _ = | \ ; : ? , . /
5. On a password change:

- At least one character must be changed; you can require up to 10 characters changed.
- The user cannot reuse the two most recent passwords; you can increase this requirement up to the 10 most recent.

6. Password expiration: you can set the expiration up to 365 days maximum, or choose a specific expiration date.
7. Click **Save**.

Offline Authentication Prohibited

Offline Authentication is forbidden in the Common Criteria evaluated configuration.

1. In the Imprivata Admin Console, go to **Users** > **User policies** and select a user policy.
2. Go to the **Authentication** tab > **Desktop Access authentication** section.
3. Confirm **Allow offline authentication** is not selected.
4. Click **Save**.

Confirm that there is no Computer Policy Override that allows Offline Authentication:

1. In the Imprivata Admin Console, go to **Computers** > **Computer policies** and select a computer policy.
2. Go to the **Override and Restrict** tab > **Desktop Access Authentication Restrictions** section.
3. If **Restrict User Policy** is selected, you must confirm **Allow offline authentication** is not selected.
4. Click **Save**.

Setting the System Logging Level

Imprivata provides two levels of logging:

1. In the Imprivata Admin Console, go to the **gear icon** > **Settings**.
2. Go to **System logging level in this site** and select **Info** or **Debug:**
   - **Info** — Logs the basic record information of the running system.
   - **Debug** — Generates more information for use in troubleshooting. Use **Debug** logging only with the guidance of an Imprivata Customer Support representative.
3. Click **Save**.

Setting the Imprivata Agent Refresh Interval

Each time the Imprivata agent contacts the Imprivata server, the agent uploads audit log information and downloads user policy information and any new or updated application profiles.

1. In the Imprivata Admin Console, go to the **gear icon** > **Settings** page.
2. Go to **Refresh interval when agents check server for updates in this site** and select a value (minimum 3 minutes; maximum 24 hours)
3. Click **Save**.

NOTE:
If the Imprivata agent cannot reach the Imprivata server, the agent switches to Disabled status.

Because Offline Authentication is not allowed in the Common Criteria certified configuration, users cannot authenticate when the agent is disabled.

The connection status of the Imprivata agent can be viewed at any time in the Windows system tray of the endpoint computer.

When the Imprivata server responds, the agent re-authenticates and resumes Online Mode. Users transitioning to Online Mode will be prompted to re-authenticate.

Managing System Settings

The **System Settings** section of the **Settings** page contains system operation and maintenance tools, which are described in the following sections.

Lockdown Status

System Lockdown indicates whether the Imprivata server is locked down and service is suspended for all users, including Imprivata Administrators.

1. In the Imprivata Admin Console, go to the **gear icon** > **Settings**.
2. In the section **System lockdown**, select a lockdown schedule and duration from the drop-down menu.
3. Click **Save**.

- **Administrators and Super Administrators**: Users with Administrator privileges cannot access the Imprivata Admin Console while the system is locked. Super Administrators are not locked out.
- **Users**: Users who are not authorized for Offline Authentication can continue to work only until the next refresh interval. The next time the user’s agent contacts the Imprivata server, the user’s session is terminated. Users who are not logged in cannot log into Imprivata OneSign or Imprivata Confirm ID while the system is locked; they can still log into their computers. Users who are authorized for Offline Authentication are still subject to the offline data expiration feature.
- **Lock / Unlock Behavior**: If the Imprivata server is off when a scheduled lock or unlock would have taken place, the action does not happen. When the the Imprivata server is started again, it will still be in the same state it was in when it was shut down.

  Changing the existing lockdown schedule does not cause the server to lock or unlock. Select the **Lock** or **Unlock** button to manually change the lockdown status.

Banner

Display an advisory warning message above the username and password fields on the Imprivata Admin Console and Imprivata Appliance Console login screens.

1. In the Imprivata Admin Console, go to the **gear icon** > **Settings**.
2. In the section **Administrator login message**, enter an advisory warning message. 500 characters maximum.
3. Select a duration:
   - 7 days
   - 14 days
   - 30 days
   - 90 days
   - Always show message
4. Click **Save**.

Security Functional Requirements — Common Criteria Guidance

A list of Security Functional Requirements and the sections of the Common Criteria guidance where they are documented.

ESM_ACD.1 — For details of the endpoint computer policy, see Computers and Computer Policy. For details of the user policy, see Users and User Policy.

ESM_ACT.1 — Secure communication between the appliance and the endpoint is defined in Computers and Computer Policy. For details of the user policy, see Users and User Policy.

ESM_ATD.1 — for details of the endpoint computer policy, see Computers and Computer Policy. For details of the user policy, see Users and User Policy.

ESM_ATD.2 — for details of the endpoint computer policy, see Computers and Computer Policy. For details of the user policy, see Users and User Policy.

ESM_EAU.2 — Secure communication between the appliance and the endpoint is defined in Computers and Computer Policy. For details of the user policy, see Users and User Policy.

ESM_EID.2 — Secure communication between the appliance and the endpoint is defined in Computers and Computer Policy. For details of the user policy, see Users and User Policy.

ESM_ICD.1 — see Password Complexity. For details of the user policy, see Users and User Policy.

ESM_ICT.1 — for details on creating users, user policies, user passwords, user lockout policy, see Imprivata Directory Users. For details of the user policy, see Users and User Policy.

FAU_GEN.1 — see Managing System Settings

FAU_SEL.1 — see Secure Copy Protocol for Audit File Data

FCS_TLS_EXT.1 — Secure communication between the appliance and the endpoint is defined in Computers and Computer Policy.

FIA_AFL.1 — for details on the user lockout policy, see User Lockout Policy.

FIA_USB.1 — for details on Imprivata OneSign administrator roles and privileges, see Administrator Roles (Delegated Administration).

FMT_MOF.1 — for details on Imprivata OneSign administrator roles and privileges, see Administrator Roles (Delegated Administration).

FMT_MOF_EXT.1 — for details on Imprivata OneSign administrator roles and privileges, see Administrator Roles (Delegated Administration).

FMT_SMR.1 — for details on the user policy definition, see see Imprivata Directory Users.

FTA_SSL.3 — for details on idle time threshold, see Establish The Enterprise and Setting the Imprivata Appliance Console Session Timeout

FTA_SSL.4 — for details on idle time threshold, see Establish The Enterprise and Setting the Imprivata Appliance Console Session Timeout

FTA_TAB.1 — for details, see Banner

FTA_TSE.1 — for details, see Establish The Enterprise

AGD_OPE.1 — for details on cryptography, see Server Configurations