

Ivanti Policy Secure 22.2 Common Criteria Configuration Guide

Document Version: 1.1



2400 Research Blvd
Suite 395
Rockville, MD 20850

Revision History

VERSION	DATE	CHANGES
1.0	10-06-2023	Initial Release
1.1	20-11-2023	ECR comments addressed

Table of Contents

- Common Criteria Configuration Instructions6
- 1. Introduction6
 - 1.1 Audience.....6
 - 1.2 Purpose6
 - 1.3 Supported TOE Platforms6
 - 1.4 Operational Environment.....6
- 2. Commissioning the Appliances8
 - 2.1 Secure Acceptance of the TOE8
 - 2.2 Physical Installation8
 - 2.3 Initial Setup Through Serial Console9
 - 2.4 Connect Administrator Web Console.....9
 - 2.5 Configuring External, Management Interfaces/Ports.....10
 - 2.5.1 Configure external port10
 - 2.5.2 Configure management port.....10
 - 2.6 Configuring DNS Server11
 - 2.7 Set System time11
 - 2.8 Software updates.....12
 - 2.9 Software Version Verification14
 - 2.9.1 Version verification via GUI14
 - 2.9.2 Version verification via local console.....15
- 3. TOE configuration.....16
 - 3.1 Prerequisites for TOE Configuration16
 - 3.2 System Reboot.....16
 - 3.3 Password Minimum Length Configuration16
 - 3.4 Reset Password.....18
 - 3.5 User Creation19
 - 3.5.1 User Creation via GUI.....19
 - 3.5.2 User Creation via Console20
 - 3.6 Role Mapping21
 - 3.7 Serial Console Access Control Configuration22
 - 3.8 Logging into the Console.....23
 - 3.9 Terminating a Local Console Session24

3.10	Administrative Banner Configuration	24
3.11	Enable NDcPP mode	26
3.12	Disable NDcPP mode via the Console	28
3.13	Configure Inactivity Timeout Period	29
3.14	Terminating a GUI Session	29
3.15	Configuring authentication lockout.....	30
3.16	Import Trusted Client CA	31
3.17	Import Trusted Server CA	34
3.18	Device Certificates	35
3.18.1	Generate RSA or ECC Certificate.....	37
3.19	Configure Secure Channel to Syslog Server	41
3.20	Import Client Auth Certificate	42
3.21	Configuring Syslog Server	43
3.21.1	Configure Syslog Server for Event Log.....	43
3.21.2	Configure Syslog Server for Admin Access Log.....	43
3.21.3	Configure Syslog Server for User Access Log.....	44
3.22	Configure Syslog Server Parameters	44
3.23	CRL checking configuration.....	46
3.23.1	Understanding CRL	46
3.23.2	Enable CRL checking.....	47
3.24	Removing Cached CRL Entry of CA Chain	48
3.25	Delete CA Chain from Trusted Client CA	48
3.26	Delete CA Chain from Trusted Server CA	49
3.27	Zeroization process	49
4.	Self-Test	50
5.	Hash Functions	51
6.	Keyed Hash Cryptographic Operation (Keyed Hash Algorithm)	51
7.	Sample audit logs	51
7.1	Audit log records.....	51
7.2	Audit Data Generation	52
7.2.1	Start-up and shutdown of the audit functions	52
7.2.2	Administrative login and logout.....	53
7.2.3	Console access.....	53
7.2.4	Changes to TSF data related to configuration changes	53

7.2.5	Generating/import of, changing, or deleting of cryptographic keys	54
7.2.6	Resetting passwords.....	54
7.3	NDcPP and FIPS mode.....	54
7.4	HTTPS session.....	55
7.5	Access banner configuration logs	55
7.6	Session inactivity time configuration log	55
7.7	Successful TLS session	55
7.8	Failure to establish a TLSC Session.....	55
7.8.1	Failure due to Invalid extension	55
7.8.2	Failure due to unsupported certificate type and protocols.....	56
7.8.3	Failure due to CN and SAN.....	56
7.8.4	Failure due to failed certificate path.....	56
7.8.5	Failure due to expired certificate	57
7.9	Failure to establish a TLSS connection	57
7.10	Authentication failure parameters configuration log	57
7.11	Unsuccessful login attempts limit is met or exceeded.....	57
7.12	Successful and unsuccessful login attempts.....	57
7.12.1	Remote connection	57
7.12.2	Local connection.....	57
7.13	Configure/ modify audit behaviour logs	58
7.14	Unsuccessful attempt to validate a certificate	58
7.14.1	Certificate revoked	58
7.14.2	Invalid key	58
7.14.3	Certificate verification failed	59
7.14.4	Basic Constraints failure.....	59
7.15	CRL check logs	59
7.15.1	Certificate CRL addition.....	59
7.15.2	CA CRL download log.....	59
7.15.3	CA CRL validation log.....	59
7.16	Initiation of update	60
7.16.1	Update initiated	60
7.16.2	Update completed successfully	60
7.16.3	Update failed.....	60
7.17	Power-on Self-Test	60

Common Criteria Configuration Instructions

Follow the instructions in this document to install Ivanti Policy Secure, and to make the configuration changes required after installation to bring the system into the “Common Criteria mode”.

This document is a guide to the Ivanti Policy Secure implementation of the Common Criteria Network Device Protection Profile v2.2e (NDcPP v2.2e).

1. Introduction

1.1 Audience

This document is written for administrators to configure the TOE, specifically the Ivanti Policy Secure. It requires broad understanding of networks in general, the internet in particular, as well as networking principles and network configuration.

1.2 Purpose

This document details the operational and preparative procedures for the Common Criteria evaluation. It highlights the specific TOE configuration and administration functions and interfaces necessary to configure and maintain the TOE in the evaluated configuration as defined in the Security Target [Ivanti Policy Secure 22.2 Security Target]. This document does not mandate configuration settings for features of the TOE outside the evaluation scope.

1.3 Supported TOE Platforms

The following tables describe the appliance hardware included in the evaluated configuration.

Table 1 – TOE Platforms

PLATFORM	VERSION/MODEL NUMBER
Virtual appliance hardware Platform (ISA-V)	VMware ESXi 6.7 with Dell PowerEdge R640
ISA appliances	ISA-6000, ISA-8000C, ISA-8000F

The Ivanti Policy Secure software runs on any one of the TOE hardware platforms. The platforms provide different amounts of processing power and network connectivity options as described below.

Table 2 – Hardware Details

Hardware Details	
Model	Processor
ISA-6000	Intel Core i3 10100E 10th gen (Comet Lake)
ISA-8000C	Intel Xeon Gold 5317 (Ice Lake)
ISA-8000F	Intel Xeon Gold 5317 (Ice Lake)

1.4 Operational Environment

The TOE supports the following hardware and software components in its operational environment. Each component is identified as being required or not based on the claims made in the ST [Ivanti Policy Secure 22.2 Security Target].

- Management laptop with web browser for TLS Client (Web Admin Interface)
 - Workstation providing local console access to the TOE

- Provides remoted management of TOE
- Microsoft Edge 101, Google Chrome 102, or Firefox 100
- Supporting TLSv1.1 and/or TLSv1.2
- Supporting Client Certificate authentication
- Supporting at least one of the following ciphersuites:
 - TLS_RSA_WITH_AES_128_CBC_SHA
 - TLS_RSA_WITH_AES_256_CBC_SHA
 - TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
 - TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
 - TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
 - TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
 - TLS_RSA_WITH_AES_128_CBC_SHA256
 - TLS_RSA_WITH_AES_256_CBC_SHA256
 - TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
 - TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
 - TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
 - TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
 - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
 - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

2. Syslog server

- Workstation providing local console access to the TOE
- The syslog audit server is used for remote storage of audit records that have been generated by and transmitted from the TOE.
- Conformant with RFC 5424 (Syslog Protocol)
- Supporting Syslog over TLS (RFC 5425)
- Acting as a TLSv1.1 and/or TLSv1.2 server
- Supporting Client Certificate authentication
- Supporting at least one of the following cipher suites:
 - TLS_RSA_WITH_AES_128_CBC_SHA
 - TLS_RSA_WITH_AES_256_CBC_SHA
 - TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
 - TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
 - TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
 - TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
 - TLS_RSA_WITH_AES_128_CBC_SHA256
 - TLS_RSA_WITH_AES_256_CBC_SHA256
 - TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
 - TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
 - TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
 - TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
 - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
 - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

3. The TOE supports communications with an external CRL to verify client certificates. CRL Server is required to be conformant with RFC 5280.
4. DNS Server
The DNS Server is used for resolving hostnames.
 - Conformant with RFC 1035

2. Commissioning the Appliances

2.1 Secure Acceptance of the TOE

In order to ensure the correct TOE is received, the TOE should be examined to ensure that it is not tampered with during delivery.

Verify that the TOE software and hardware were not tampered with during delivery by performing the following actions:

- Before unpacking the TOE, inspect the physical packaging the equipment was delivered in. Verify that the external cardboard packing is printed with the Ivanti logo and motifs. If it is not, contact the supplier of the equipment (Ivanti or an authorized Ivanti distributor / partner).
- Verify that the packaging had not obviously been opened and resealed by examining the tape that seals the package. If the package appears to have been resealed, contact the supplier of the equipment (Ivanti or an authorized Ivanti distributor / partner).
- Verify that the box has a white tamper-resistant, tamper-evident Ivanti car coded label applied to the external cardboard box. If it does not, contact the supplier of the equipment (Ivanti or an authorized Ivanti distributor / partner). This label will include the Ivanti product number, serial number, and other information regarding the contents of the box.
- Note the serial number of the TOE on the shipping documentation. The serial number displayed on the white label affixed to the outer box will be that of the device. Verify the serial number on the shipping documentation matches the serial number on the separately mailed invoice for the equipment. If it does not, contact the supplier of the equipment (Ivanti or an authorized Ivanti distributor / partner).
- Verify that the box was indeed shipped from the expected supplier of the equipment (Ivanti or an authorized Ivanti distributor / partner). This can be done by verifying with the supplier that they shipped the box with the courier company that delivered the box and that the consignment note number for the shipment matches that used on the delivery. Also verify that the serial number of the item shipped match the serial numbers of the items delivered. This verification should be performed by some mechanism that was not involved in the actual equipment delivery, for example, phone/FAX or other online tracking service.
- Once the TOE is unpacked, inspect the unit. Verify that the serial number displayed on the unit itself matches the serial number on the shipping documentation and the invoice. If it does not, contact the supplier of the equipment (Ivanti or an authorized Ivanti distributor / partner).

2.2 Physical Installation

Hardware setup can be found in each platform's Hardware Guide. These hardware guides contain preparative procedures specific to each platforms, such as environmental requirements and system measurements, to securely install the TOE in the operational environment. These hardware guides are written specifically for each platform and versioned by year and month. The hardware guides are reviewed quarterly and updated as needed.

2.3 Initial Setup Through Serial Console

1. Plug a null modem crossover cable from a console terminal or laptop into the device serial port. This cable is provided in the product box. Do not use a straight serial cable.
2. Configure a terminal emulation utility, such as HyperTerminal, with the following serial connection parameters:
 - a) 9600 bits-per-second.
 - b) 8-bit No Parity (8N1).
 - c) 1 Stop Bit.
 - d) No flow control.
3. Press Enter until the serial console is displayed.
4. On the serial console, the following text is shown:

Please choose from among the following factory-reset personality images:
[1] Ivanti Policy Secure <release version>
5. Enter **1** to install the Ivanti Policy Secure package. The system will start Installation and reboot. The process may take a few minutes.
6. Enter **y** to accept the license terms (or enter **r** to read the license first).
7. Follow the directions in the console, and enter the machine information for which you are prompted:
 - a) Configure internal port
 - i) IP address
 - ii) Network mask
 - iii) Default gateway address
 - b) Configure DNS
 - i) Primary DNS server address
 - ii) Secondary DNS server address (optional)
 - iii) Default DNS domain name (for example, acmegizmo.com)
 - c) WINS server name or address (optional)
 - i) Enter to go to next step
 - d) Configured network setting is displayed for you to review. Enter **y** to accept or **n** to modify.
 - e) Configure the administrator
 - i) Administrator username – Enter an administrator username. This will create an administrator user account with all of the necessary privileges. This username and password will be used thereafter through the web console interface for administrator management functions.
 - ii) Administrator password – Must adhere to the password complexity requirements. See <Administrator Passwords> section for password requirements and recommendations.
 - f) Enter information to create a self-signed certificate
 - i) Common machine name (for example, connect.acmegizmo.com)
 - ii) Organization name (for example, Acme Gizmo, Inc .)
 - iii) Enter random text (used for auth certificate)

2.4 Connect Administrator Web Console

The Administrator Web Console is available after the initial setup through the serial console:

1. Launch a web browser from a network connected laptop.

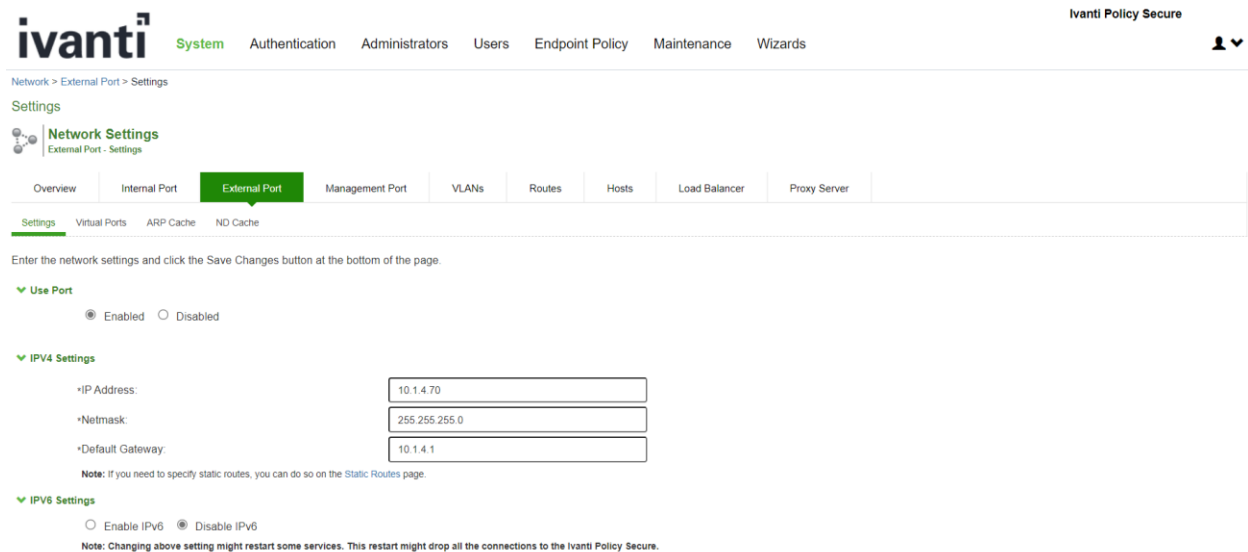
2. Point the browser at the same IP address that was assigned to the internal port followed by /admin (for example, <https://a.b.c.d/admin>).
3. When prompted with the security alert to proceed without a signed certificate, click **Yes**. When the administrator sign-in page appears, you have successfully connected your device to the network.
4. On the sign-in page, enter the administrator username and password you created earlier. Then click **Sign In**.
5. The Administrator Web Console opens to the **System > Status > Overview** page.

2.5 Configuring External, Management Interfaces/Ports

2.5.1 Configure external port

On admin web console:

- Navigate to **System > Network > External Port > Settings**
- Click on **Enabled**
- Enter IP address, Netmask, and Default Gateway

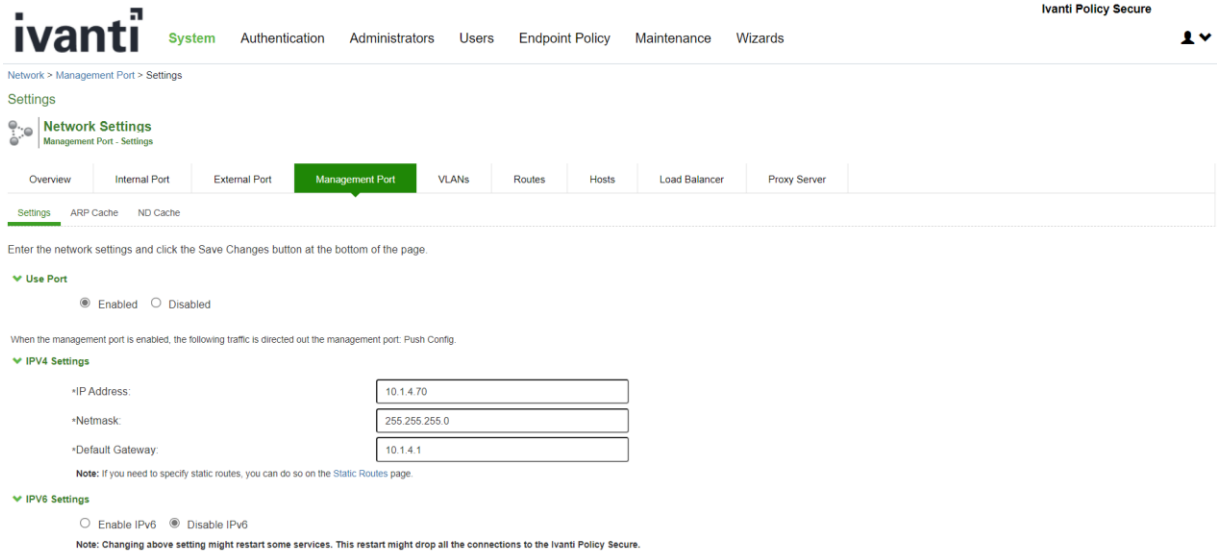


2.5.2 Configure management port

On the supported platforms that management port is available, you may also configure a management port to use it for communication with syslog server.

To configure management port, on Administrator Web Console,

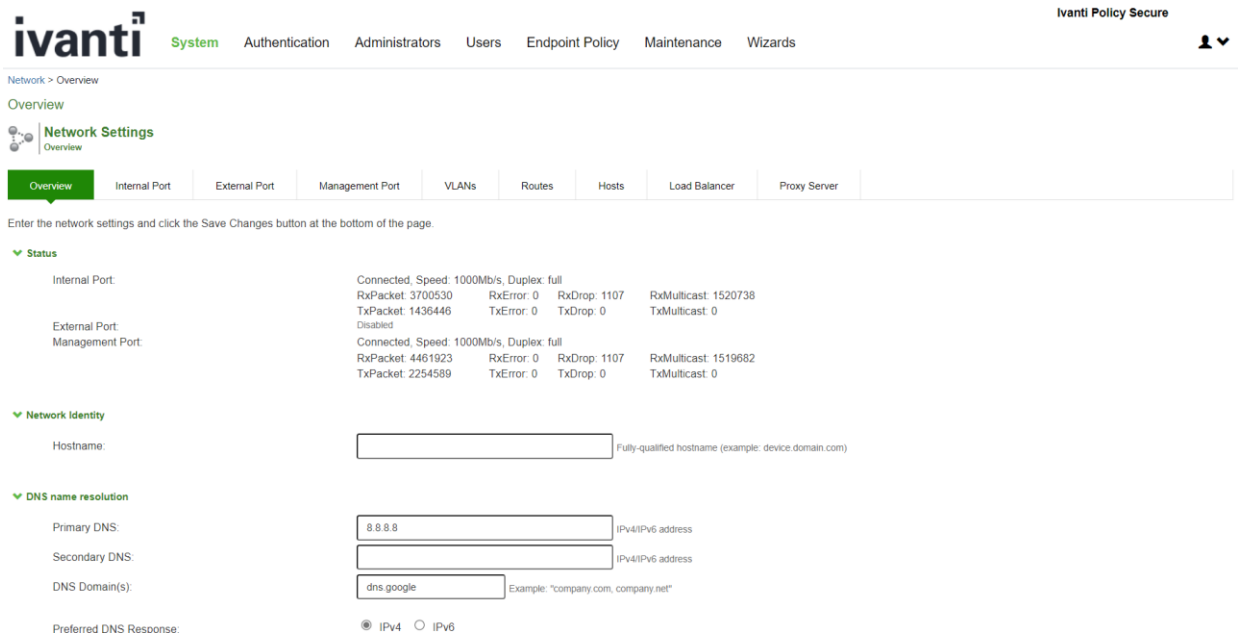
1. Navigate to **System > Network > Management Port > Settings**
2. Click on **Enabled**
3. Enter IP address, Netmask, and Default Gateway



2.6 Configuring DNS Server

On Administrator Web Console,

1. Navigate to **System > Network > Overview**
2. Enter IP address for **Primary DNS**, and DNS Domain
3. **Secondary DNS** is an optional field



2.7 Set System time

1. Go to **System > Status > Overview** page.
2. Click on the **Edit** link next to **System Date & Time**.

3. On the **Date and Time** page:
 - a. In the **Set Time Manually** section, click on **Get from Browser** button.
 - b. Click on **Save Changes** button

ivanti System Authentication Administrators Users Endpoint Policy Maintenance Wizards Ivanti Policy Secure

Status > Overview > Date and Time

Date and Time

System Date: 3/6/2023
System Time: 10:17:43 AM

Time Zone: (GMT) Coordinated Universal Time

Time Source

Use Pool of NTP Servers
Configure pool of NTP servers (IP Address/Hostname)
Please make sure NTP server is reachable via port configured at Advanced Networking page.
For troubleshooting use ntpq command under Troubleshooting page

* NTP Server 1: Key 1: (optional)
NTP Server 2: Key 2: (optional)
NTP Server 3: Key 3: (optional)
NTP Server 4: Key 4: (optional)

Set Time Manually

Date: (mm/dd/yyyy)
Time: AM (hh:mm:ss)

Get from Browser

Note: Save Changes will result in restarting of services which will disconnect all the connected users.

Save Changes

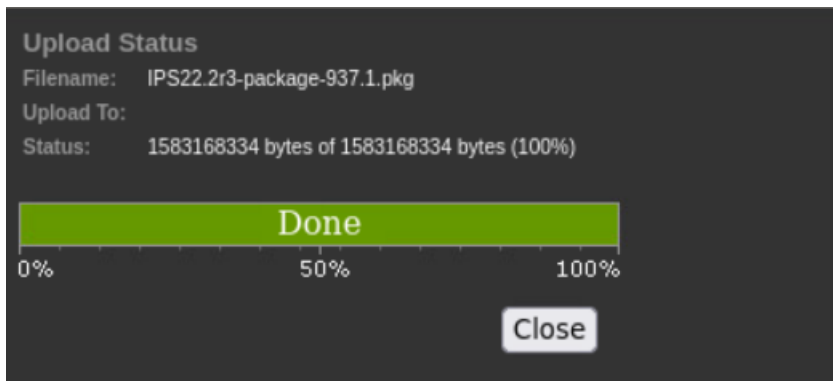
2.8 Software updates

If a new NDcPP-compliant software package is available, follow the instructions in this section to update the software package on the TOE. The verification of the authenticity of the software package is performed by digital signature verification.

1. Download the TOE software package received from Ivanti to a trusted computer system
2. On Administrator Web Console,
Navigate to **Maintenance > System > Upgrade/Downgrade**
3. In the expanded **Install Server Package** section, click on **From File** option, then click on **Browse** to select the server package downloaded earlier
4. Click **Install** to start the installation process

The screenshot shows the Ivanti Policy Secure web interface. At the top, the navigation menu includes System, Authentication, Administrators, Users, Endpoint Policy, Maintenance (highlighted), and Wizards. The breadcrumb trail is System Maintenance > Install Service Package. The main heading is 'Install Service Package' with sub-tabs for Platform, Upgrade/Downgrade (active), Change Personality, Options, and Installers. A warning message states: 'Installing a service package can take several minutes and requires the system to reboot. Because existing system data is backed up during this process, you can decrease installation time by clearing your system log before trying to install a service package.' A red note says: 'Note: Browsing away from this page while uploading the package will abort the installation.' Under the 'Install Service Package' section, the 'From File' option is selected. A 'Browse' button is present with a warning: 'No file chosen (WARNING: Please ensure that the steps recommended in KB44877 have been performed without fail before initiating upgrade.)'. The 'From Staged Package' option is also visible with a checkbox for 'DELETES all system and user configuration data before installing the service package; restoring the member to an unconfigured state. Use this option if you want to downgrade to an older service package than the currently installed package. Do NOT check this box if you want to retain existing settings and data during a system upgrade to a newer service package.' A note below states: 'Note: This option does not change the factory image.' An 'Install' button is at the bottom of this section. The 'Manage Staged Service Package' section has an 'Upload new package into staging area' option with a 'Browse' button and the same warning, and a 'Delete Staged Package' option. A 'Submit' button is at the bottom of this section.

- Once the package is uploaded, and the system validates the image, the installation is complete.





Service Package Installation Status

The installation process takes a few minutes. When complete, the system needs to reboot. Please wait...

- Step 1: Verifying package integrity complete (65 seconds)
- Step 2: Extracting install script complete (19 seconds)
- Step 3: Boot partition factory Version Value:22.1R ... complete (0 seconds)
- Step 4: Checking For Legacy Active Directory mode Configuration complete (0 seconds)
- Step 5: Running system compatibility checks ... complete (0 seconds)
- Step 6: Saving copy of system config complete (26 seconds)
- Step 7: Preparing disk partitions complete (5 seconds)
- Step 8: Generating Grub2 Configuration... .. complete (0 seconds)
- Step 9: Done. ... complete (1 seconds)
- Step 10: Extracting contents of new package complete (20 seconds)
- Step 11: Saving package complete (18 seconds)
- Step 12: Finalizing installation complete (2 seconds)

✔ Installation completed successfully and the system will now reboot.: Note that the Administrator Console will be unavailable while the system reboots. ✕
 (Watch the serial console for messages).
 When the system reboots click [here](#) to continue using the Administrator Console.

Note: The administrator Console (Web UI) will be unavailable while the system reboots. The Serial console will be available to check the logs/messages. When the system reboot is completed administrator console (Web UI) will be available for use.

When the Security Administrator uploads a firmware update, the TSF performs an RSA 2048 SHA-256 digital signature verification of the update using the Ivanti Secure firmware update public key. The public key is distributed as part of the firmware package. Ivanti Secure retains control over the private key used to sign firmware updates.

If the signature check is successful, the TSF installs the update. If the signature check detects tampering with the update and/or signature, the TSF presents the user with an error message and discards the update.

2.9 Software Version Verification

2.9.1 Version verification via GUI

The current software version can be found on the web console.

Navigate to **Maintenance > Platform**

System Maintenance > Platform

Platform

- Platform
- Upgrade/Downgrade
- Change Personality
- Options
- Installers



Hostname: localhost2
Model: ISA-6000
Machine ID: 0461MPQ8A0QX71VGE
Serial Number: 0461102021109917
Uptime: 33 days, 22 hours, 39 minutes, 7 seconds
Current version: 22.2R3 (build 937)
Rollback version: 22.2R3 (build 893)

Node operations: Restart Services Reboot... Shut Down... Rollback...

Connectivity:
 This will ping various configured servers to test the device's connectivity.

Test Connectivity

Hardware Status

Fan Status:

Fan (Slots)	Status
1	●
2	●
3	●
4	●

Temperature: 25 °C

2.9.2 Version verification via local console

The current software version can be found on the local console.

The version details will be displayed once the user login to the local console.

```

This is notice and consent warning message. Authorized users only.

Please input an administrator username and password.
Admin username: admin
Password:

Current version: 22.2R3 (build 1033)
Rollback version: 22.2R3 (build 1013)
Reset version: 22.1R1 (build 421) Ivanti Connect Secure
                22.1R1 (build 211) Ivanti Policy Secure

Licensing Hardware ID: 0461MPQ8A0QX71VGE
Serial Number: 0461102021109917

Please choose from among the following options:
 1. Network Settings and Tools
 2. Create admin username and password
 3. Display log/status
 4. System Operations
 5. Toggle password protection for the console (0n)
 6. Create a Super Admin session
 7. System Maintenance
 8. Turn off NDcPP Mode and reset allowed encryption strength for SSL
11. Exit Serial Console Session
Choice: █
    
```


3. TOE configuration

3.1 Prerequisites for TOE Configuration

- You have configured the TOE as per the instructions in section [Commissioning the Appliance](#) of this document.
- External DNS Server should be able to resolve the hostnames used in the testing.
- External Syslog server is up and running.
- External CRL is up and running.

3.2 System Reboot

The Ivanti Policy Secure appliance can be restarted from the Web Management interface or console. To restart the appliance:

1. From the Web Management interface
Navigate to **Maintenance > System > Platform** and click on **Reboot**
2. From the Administrator console
Select **option 1** to reboot the device

```

Please choose the operation to perform:
  1. Reboot this Ivanti Policy Secure
  2. Shutdown this Ivanti Policy Secure
  3. Restart services at this Ivanti Policy Secure
  4. Rollback this Ivanti Policy Secure
  5. Factory reset this Ivanti Policy Secure
  6. Clear all configuration data at this Ivanti Policy Secure
  7. Install self-signed certificate
 20. Manage RAID
 21. Clear all session data at this Ivanti Policy Secure
 22. Clear all Named Users at this Ivanti Policy Secure
 31. Clean up disk space on this Ivanti Policy Secure
 93. Toggle resource throttling (Enabled)
 94. Clear custom HTTP headers
<return to go back to main menu>
Choice: 1

Are you sure you want to reboot this Ivanti Policy Secure? (y/n) y

Doing reboot.
Reboot action message: user initiated, via serial console

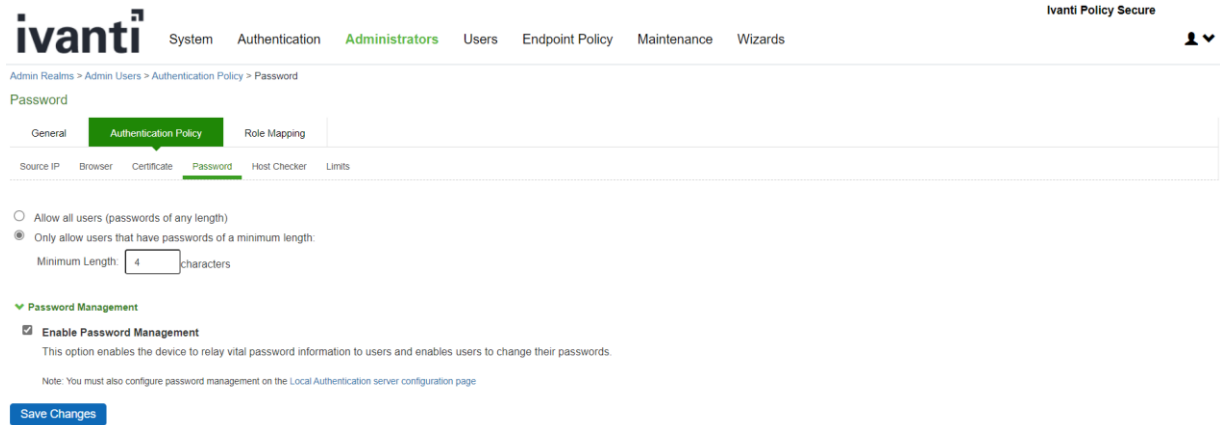
```

3.3 Password Minimum Length Configuration

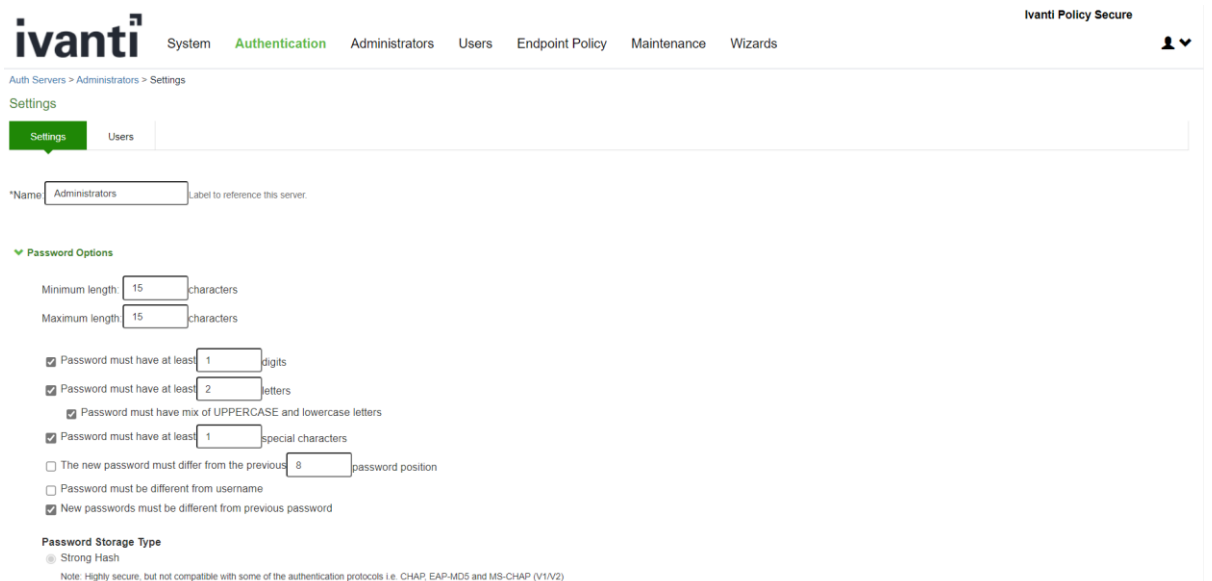
On the Administrator Web Console, do the following to set the administrator minimum password length to 15:

1. Set in Admin Realm:
 - a. Navigate to **Administrators > Admin Realms**

- b. Click on **Admin Users**
- c. Click on **Authentication Policy** tab
- d. Click on **Password** tab
- e. Click on **Only allow users that have passwords of a minimum length**
- f. Enter **15** as **Minimum Length**



2. Set in local auth server configuration:
 - a. Navigate to **Authentication -> Auth. Servers**
 - b. Click on **Administrators**
 - c. On **Settings** tab, click on **Password Options** section
 - d. Configure 15 characters as Minimum Length
 - e. Configure **Maximum Length 15** characters.
3. Review all previously configured administrator passwords, update to ensure all are at least 15 characters.
4. Passwords, by default, can include the following characters: “!”, “@”, “#”, “\$”, “%”, “^”, “&”, “*”, “(”, “)”, [and standard printable ASCII characters (values 0x20 – 0x7E)



3.4 Reset Password

On Administrator Web Console, follow the below instruction to reset the password.

Navigate to **Auth Servers > Administrators > Users > Update Administrator admin**

	Username	Name	Console Access	Last Sign-in Statistic			Status
				Date&Time	IPAddress	Agent	
<input type="checkbox"/>	acumensec	Platform Administrator	No	2022/12/08 11:25:38	192.168.254.249	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36 Edg/108.0.1462.42	
<input type="checkbox"/>	admin	Platform Administrator	Yes	2023/03/06 11:06:03	192.168.254.250	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/110.0.0.0 Safari/537.36 Edg/110.0.1587.63	
<input type="checkbox"/>	admin1	admin1	Yes	2022/09/16 06:35:07	10.1.4.67	REST Client	
<input type="checkbox"/>	good	good	No	2022/11/03 09:28:35			
<input type="checkbox"/>	good1	good1	No	2022/11/03 09:29:53			

Select the username and click on **reset password** and click on save changes.

3.5 User Creation

3.5.1 User Creation via GUI

1. Go to **Auth Servers > Administrators > Users** and click on **New**

The screenshot shows the Ivanti Policy Secure web interface. The breadcrumb trail is "Auth Servers > Administrators > Users". The "Users" tab is selected. Below the breadcrumb, there are buttons for "Settings" and "Users". A section for "Import Users from CSV file" includes a "Browse" button, "No file chosen", and an "Import" button. Below that, there is a "Show users named" input field, a "Show 200 users" dropdown, and an "Update" button. At the bottom of this section are "New...", "Delete...", and "Unlock..." buttons, along with a pagination control showing "Page 1 of 1".

i	I	Username	Name	Console Access	Last Sign-in Statistic		
					Date&Time	IPAddress	Agent

2. Create **Username** and **Password**, click on **Save Changes**

The screenshot shows the "New Administrator" form in the Ivanti Policy Secure web interface. The breadcrumb trail is "Auth Servers > Administrators > Users > New Administrator". The form fields include:

- Username: admin
- Full Name: (empty)
- Authenticate using: Administrators
- Password: (masked with dots)
- Confirm Password: (empty)
- Start Time: (empty)
- End Time: (empty)
- Time Zone: (GMT) Coordinated Universal Time

 Below the form are several checkboxes:

- One-time use (disable account after the next successful sign-in)
- Allow console access
- Allow access to REST APIs
- Enabled
- Require user to change password at next sign in

 A note states: "Note: You must also configure password management on the Authentication server Settings with 'Allow users to change their passwords' option enabled. Use options on the Administrators/Users > Authentication > [Realm] > Authentication Policy > Password page to specify which realms should inherit the server's password management capabilities." At the bottom, there is a "Custom Attributes" section and a "Delete" button.

3.5.2 User Creation via Console

1. Log in to the console
2. Select the option **“Create admin username and password”**.

```

This is notice and consent warning message.Authorized users only.

Please input an administrator username and password.
Admin username: admin
Password:

Current version: 22.2R3 (build 1011)
Rollback version: 22.2R3 (build 937)
Reset version: 22.1R1 (build 421) Ivanti Connect Secure
                22.1R1 (build 211) Ivanti Policy Secure

Licensing Hardware ID: 0461MPQ8A0QX71VGE
Serial Number: 0461102021109917

Please choose from among the following options:
 1. Network Settings and Tools
 2. Create admin username and password
 3. Display log/status
 4. System Operations
 5. Toggle password protection for the console (0n)
 6. Create a Super Admin session
 7. System Maintenance
 8. Turn off NDcPP Mode and reset allowed encryption strength for SSL
11. Exit Serial Console Session
Choice: 2
    
```

3. Input the Admin username to be created.
4. Input the Password and Confirm password.
5. Confirm if REST API access is to be given to this administrator with yes (y) or no (n).

```

Please create an administrator username and password.
Admin username: newuser

Password:
Confirm password:
Do you want to enable REST API access for this administrator (y/n): n

The administrator newuser was successfully created.
    
```

3.6 Role Mapping

Assign privilege level to users using role mapping.

1. Go to **Admin Realms > Admin Users > Role Mapping** and click on **New Rule**

ivanti System Authentication **Administrators** Users Endpoint Policy Maintenance Wizards Ivanti Policy Secure

Admin Realms > Admin Users > Role Mapping

Role Mapping

General Authentication Policy **Role Mapping**

Specify how to assign delegated admin roles to users when they sign in. Users that are not assigned a role will not be able to sign in.

[New Rule...](#) [Duplicate](#) [Delete](#) [↕](#) [↕](#) [Save Changes](#)

	When users meet these conditions	assign these roles	Rule Name	Stop
<input type="checkbox"/>	1. username is "test"	→ .Read-Only Administrators	test1	✓
<input type="checkbox"/>	2. username is ""	→ .Administrators	rule 0	
<input type="checkbox"/>	3. username is "admin1"	→ .Administrators	admin1	✓

When more than one role is assigned to a user:

- Merge settings for all assigned roles
- User must select from among assigned roles
- User must select the sets of merged roles assigned by each rule

Note: Users that do not meet any of the above rules will not be able to sign into this realm.

- The TSF protects audit data from unauthorized modification and deletion through the restrictive administrative interfaces.
- Read-Only administrators have lower privilege level and cannot modify or delete security related parameters or trust store. Administrators have high privilege level and have rights to modify configuration on device.

2. Create a rule based on Username and assign role to Username

ivanti System Authentication **Administrators** Users Endpoint Policy Maintenance Wizards Ivanti Policy Secure

Admin Realms > Admin Users > Role Mapping > Role Mapping Rule

Role Mapping Rule

Rule based on Username [Update](#)

* Name: test

Rule: If username...

is test

then assign these roles

Available Roles: Administrators, Read-Only Administrators

Selected Roles: (none)

Stop processing rules when this rule matches

To manage roles, see the Roles configuration page.

[Save Changes](#) [Save + New](#)

3.7 Serial Console Access Control Configuration

Configure administrator access control for the local serial console is a two-step process.

Step 1, Enable allow console access for the administrator. In Administrator Web Console:

1. Go to **Authentication > Auth. Servers**
2. Select **Administrators**
3. Click on **Users** tab.
4. Click on administrator name configured in section [Initial Setup Through Serial Console](#) of this document.
5. Click on **Allow console access** checkbox.
6. Click on **Save Changes**

The screenshot shows the Ivanti Policy Secure web interface. The breadcrumb trail is: Auth Servers > Administrators > Users > Update Administrator admin. The page title is 'Update Administrator admin'. The 'Full Name' field is 'Platform Administrator'. The 'Authenticate using' dropdown is set to 'Administrators'. There are two radio buttons for 'Reset Password' and 'Change Password'. The 'Start Time' and 'End Time' fields are empty, each with a '5' icon. The 'Time Zone' is '(GMT) Coordinated Universal Time'. The 'One-time use (disable account after the next successful sign-in)' checkbox is unchecked. The 'Allow console access' checkbox is checked and highlighted in yellow. The 'Allow access to REST APIs' checkbox is checked. The 'Status' dropdown is set to 'Enabled'. The 'Require user to change password at next sign in' checkbox is unchecked. A note at the bottom states: 'Note: You must also configure password management on the Authentication server Settings with 'Allow users to change their passwords' option enabled. Use options on the Administrators/Users > Authentication > [Realm] > Authentication Policy > Password page to specify which realms should inherit the server's password management capabilities.' At the bottom left, there is a 'Custom Attributes' section and a 'Delete' button.

Step 2, Enable password protection for the console.

1. Connect to the local serial console, the serial console menu is shown as below.
2. Choose option **5** on the local serial console. You should see a confirmation: “Password protection enabled, make sure you have at least one local administrator”.

```

Press <Enter> to view or update your appliance settings.

This is notice and consent warning message.Authorized users only.

Please input an administrator username and password.
Admin username: admin
Password:

Current version: 22.2R3 (build 937)
Rollback version: 22.2R3 (build 893)
Reset version: 22.1R1 (build 421) Ivanti Connect Secure
                22.1R1 (build 211) Ivanti Policy Secure

Licensing Hardware ID: 0461MPQ8A00X71VGE
Serial Number: 0461102021109917

Please choose from among the following options:
 1. Network Settings and Tools
 2. Create admin username and password
 3. Display log/status
 4. System Operations
 5. Toggle password protection for the console (0n)
 6. Create a Super Admin session
 7. System Maintenance
 8. Turn off NDcPP Mode and reset allowed encryption strength for SSL
11. Exit Serial Console Session
Choice:

```

This interface is only available to administrators of the TOE. The authentication prevents non-administrative users from gaining access to the TSF-data-manipulating functions.

3.8 Logging into the Console

After authentication is configured, the user is presented with an authentication prompt when accessing the local console.

```

This is notice and consent warning message.Authorized users only.

Please input an administrator username and password.
Admin username: admin
Password:

```

The following options are available from the console.

```

Please choose from among the following options:
 1. Network Settings and Tools
 2. Create admin username and password
 3. Display log/status
 4. System Operations
 5. Toggle password protection for the console (0n)
 6. Create a Super Admin session
 7. System Maintenance
 8. Turn off NDcPP Mode and reset allowed encryption strength for SSL
11. Exit Serial Console Session
Choice: 11

```


No preparatory steps are required to ensure that authentication data is not revealed while entering the credentials, the TOE does not provide any feedback while entering the password at both the directly connected and remote login prompt.

3.9 Terminating a Local Console Session

To exit a console session, choose option 11 on the local serial console.

```

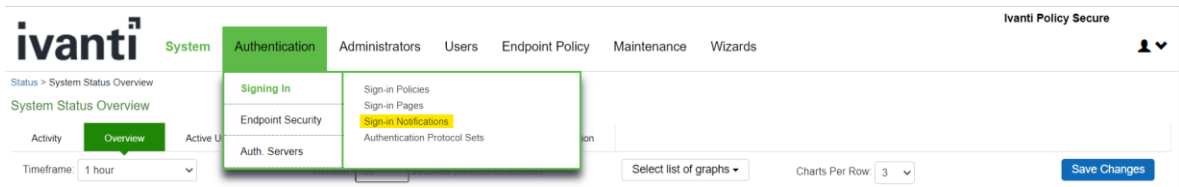
Please choose from among the following options:
 1. Network Settings and Tools
 2. Create admin username and password
 3. Display log/status
 4. System Operations
 5. Toggle password protection for the console (On)
 6. Create a Super Admin session
 7. System Maintenance
 8. Turn off NDCPP Mode and reset allowed encryption strength for SSL
11. Exit Serial Console Session
Choice: 11
    
```

3.10 Administrative Banner Configuration

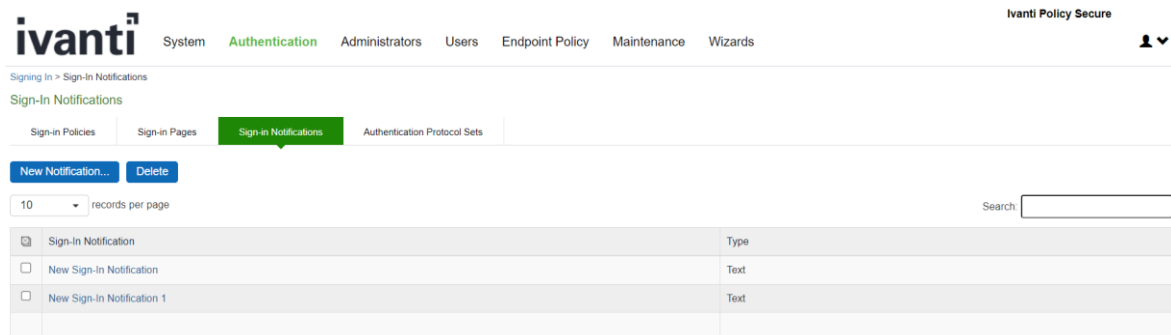
Configure administrator banner for the Administrator Web Console and the local serial console is a two- step process.

Step 1, create a Sign-in notification. On Administrator Web Console:

1. Navigate to **Authentication -> Signing In -> Sign-in Notifications**



2. This screen is shown



3. Click on **New Notification**

ivanti System **Authentication** Administrators Users Endpoint Policy Maintenance Wizards Ivanti Policy Secure

Signing In > Sign-In Notifications > New Sign-In Notification

New Sign-In Notification

Name: Label to reference the sign-in notification.

Type: Text Package

Text:

This is notice and consent warning message Authorized users only.

65 character(s)

Text for the sign-in notification.
NOTE: For Pulse desktop L3 VPN connections, the combined length of all the sign-in notification messages cannot exceed 3000 characters. If it does then the notifications will not be displayed to the user.

4. Enter a name for the new notification in the **Name:**
5. In **Type:**, select **Text**
6. Enter banner message in the **Text:**
7. Click on **Save Changes**

Step 2, associate the notification with an admin URL. On Administrator Web Console,

1. Navigate to **Authentication -> Signing In -> Sign-In Policies**
2. Click on admin URL ***/admin/**
3. In the **Configure SignIn Notifications** section, select the check box **Pre-Auth Sign-in Notification**.

ivanti System **Authentication** Administrators Users Endpoint Policy Maintenance Wizards Ivanti Policy Secure

Signing In > Sign-In Policies > */admin/

***/admin/**

User type: Users Administrators

Sign-in URL: Format: *-host-(+path)-/. Use * as wildcard in the beginning of the host name.

Description:

Default Admin Sign In

Sign-in page: To create or manage pages, see Sign-In pages.

Authentication realm

Specify how to select an authentication realm when signing in.

User types the realm name
The user must type the name of one of the available authentication realms.

User picks from a list of authentication realms
The user must choose one of the following selected authentication realms when they sign in. If only one realm is selected, it is automatically used (the sign-in page will not display the list). To create or manage realms, see the Administrator Authentication page.

Available realms: Selected realms:

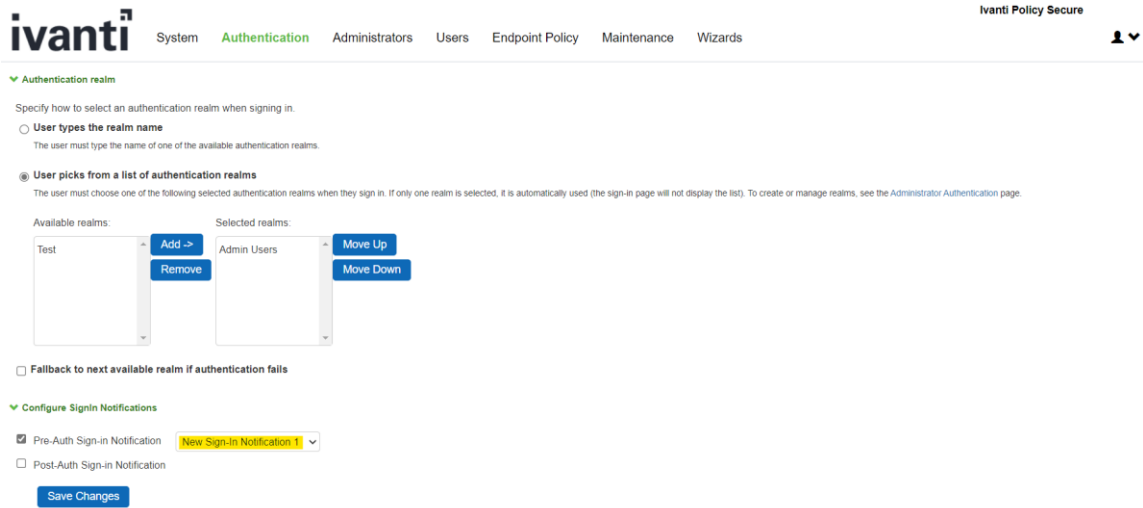
Fallback to next available realm if authentication fails

Configure Signin Notifications

Pre-Auth Sign-in Notification

4. A drop-down box appears next to **Pre-Auth Sign-in Notification** once it is selected, in the drop-

down box, select the notification you created in **Step 1** above.



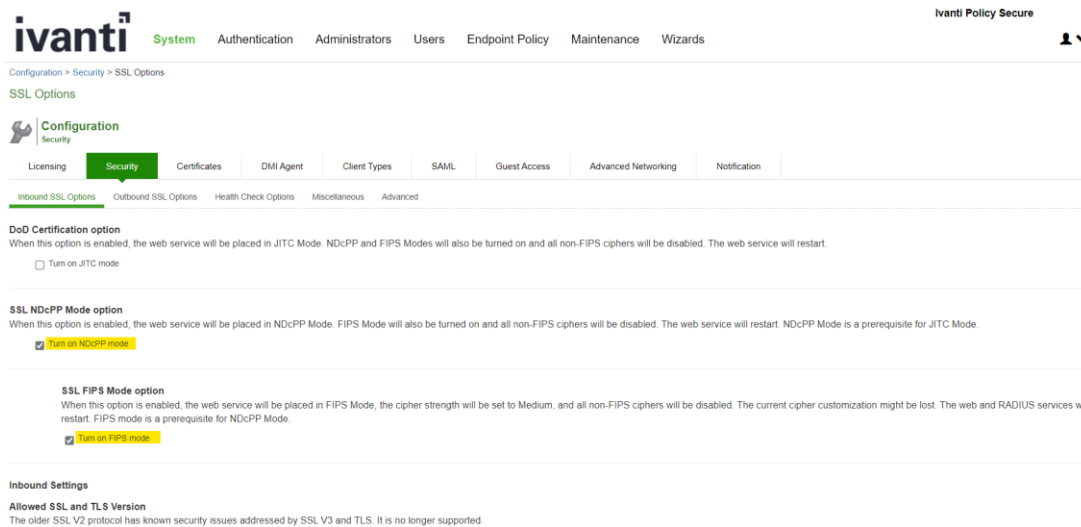
5. Click on **Save Changes**

The banner configured within the GUI will be applied to both local and remote connections.

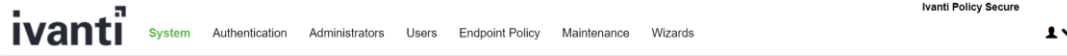
3.11 Enable NDcPP mode

On Administrator Web Console,

1. Navigate to **System -> Configuration > Security > Inbound SSL Options**
2. Click on **Turn on NDcPP mode** checkbox to make the TOE common criteria compliant.
3. Once **Turn on NDcPP mode** is enabled, **Turn on FIPS mode** is also automatically enabled.

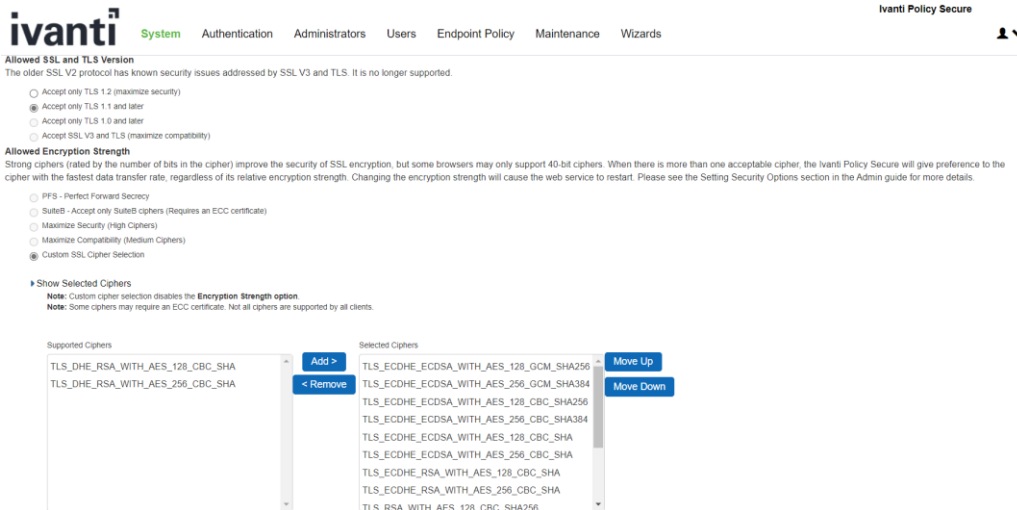


4. Once NDcPP mode is selected, **Accept only TLS 1.1 and later** is selected by default.



If the TSF receives a ClientHello message that requesting TLSv1.0 or earlier, the TSF sends a fatal handshake_failure message and terminates the connection.

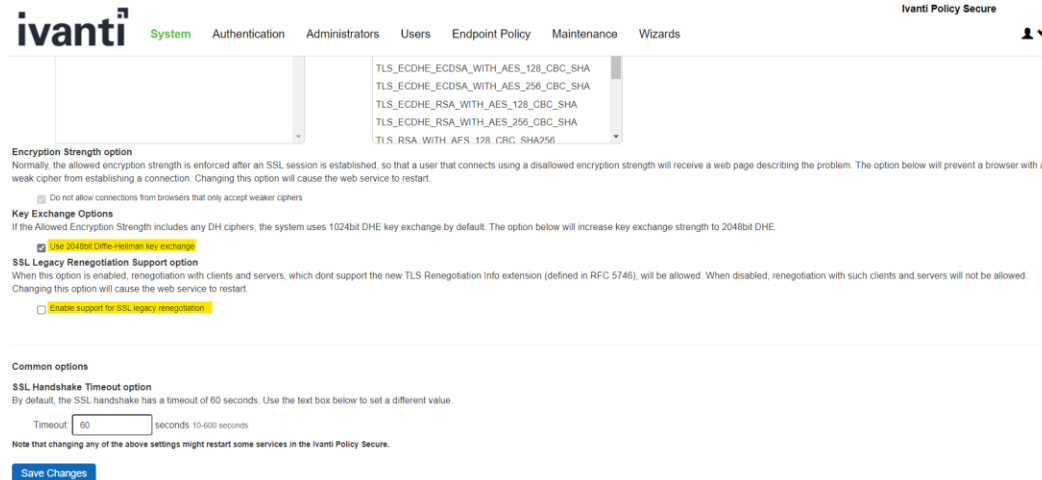
5. Custom SSL Cipher Selection Allowed Encryption Strength are automatically selected. Click on displays below 16 Ciphers in the right panel labelled **Selected Cipher**. **Show Selected Ciphers**



Select TLS_DHE_RSA_WITH_AES_128_CBC_SHA and TLS_DHE_RSA_WITH_AES_256_CBC_SHA on the right panel and click **Remove** button to remove it from the **Selected Ciphers**.

When the TSF selects an ECDHE ciphersuite, it sends the client secp256r1 or secp384r1 key agreement parameters.

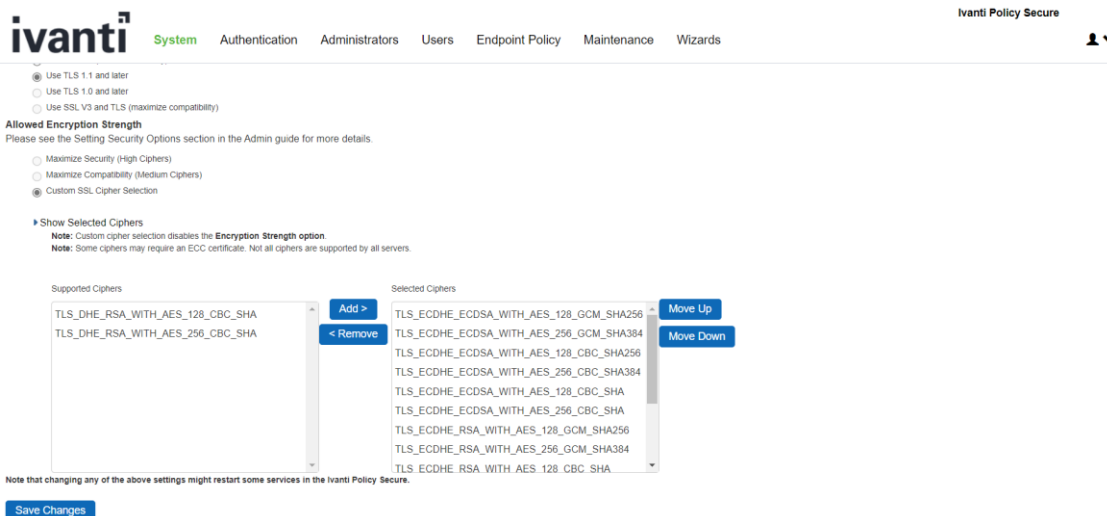
6. Enable **Use 2048bit Diffie-Hellman key exchange checkbox**
7. Uncheck **SSL Legacy Renegotiation Support option**



8. Click on **Save Changes**

9. Navigate to **System > Configuration > Security > outbound SSL Options**

- a. Custom SSL Cipher Selection Allowed Encryption Strength are automatically selected. Click on **Show Selected Ciphers** displays below 16 Ciphers in the right panel labelled **Selected Cipher**.
- b. Select TLS_DHE_RSA_WITH_AES_128_CBC_SHA and TLS_DHE_RSA_WITH_AES_256_CBC_SHA on the right panel and click **Remove** button to remove it from the **Selected Ciphers**.



10. Optionally, you may check log to confirm NdcPP mode is enabled.

11. Navigate to **System > Log/Monitoring > Admin Access > Logs** and Check for the logs mentioned in Audit logs section **NdcPP mode enabled**.

In NdcPP mode, the RNG is not configurable and there are no instances when key destruction could be delayed.

3.12 Disable NdcPP mode via the Console

NdcPP mode may also be configured via the console. On the initial console screen, press 8

```

This is notice and consent warning message. Authorized users only.

Please input an administrator username and password.
Admin username: admin
Password:

Current version: 22.2R3 (build 937)
Rollback version: 22.2R3 (build 893)
Reset version: 22.1R1 (build 421) Ivanti Connect Secure
                22.1R1 (build 211) Ivanti Policy Secure

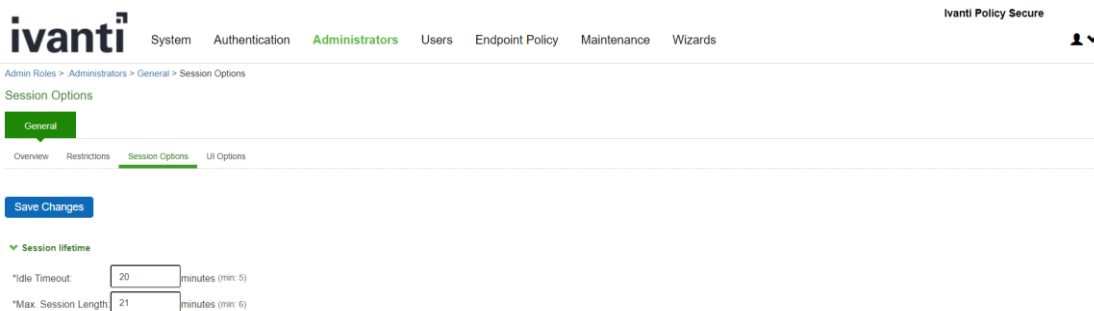
Licensing Hardware ID: 0461MPQ8A0QX71VGE
Serial Number: 0461102021109917

Please choose from among the following options:
1. Network Settings and Tools
2. Create admin username and password
3. Display log/status
4. System Operations
5. Toggle password protection for the console (On)
6. Create a Super Admin session
7. System Maintenance
8. Turn off NDcPP Mode and reset allowed encryption strength for SSL
11. Exit Serial Console Session
Choice: 8
    
```

Pressing 8 will disable the NDcPP mode of operation.

3.13 Configure Inactivity Timeout Period

1. Navigate to **Administrators > Admin Roles > <Role Name> > Session Options**



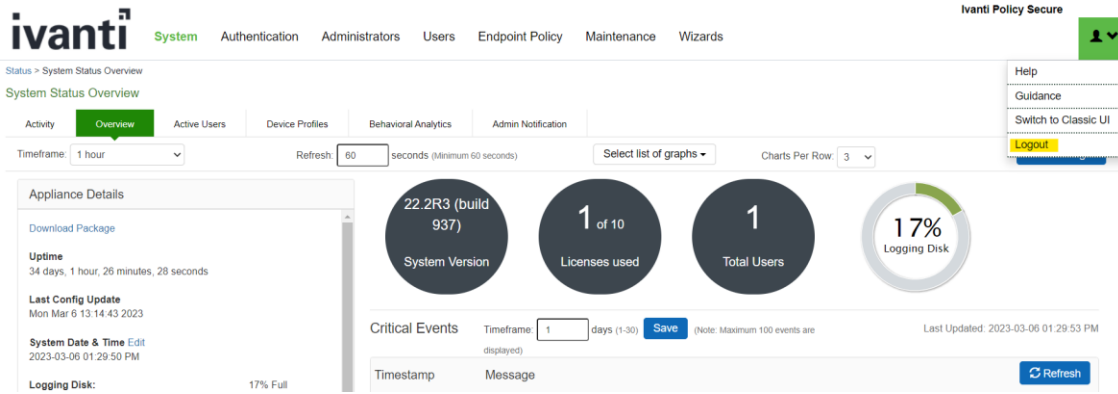
2. Under the **'Session lifetime'** section, enter the Idle timeout in minutes.

To log out of the web administrative session, on any screen click on the **“Logout”** link at the top right of the screen. After the inactivity is triggered, the administrative session will be terminated.

This configured timeout period applies to both remote GUI sessions and the local console sessions.

3.14 Terminating a GUI Session

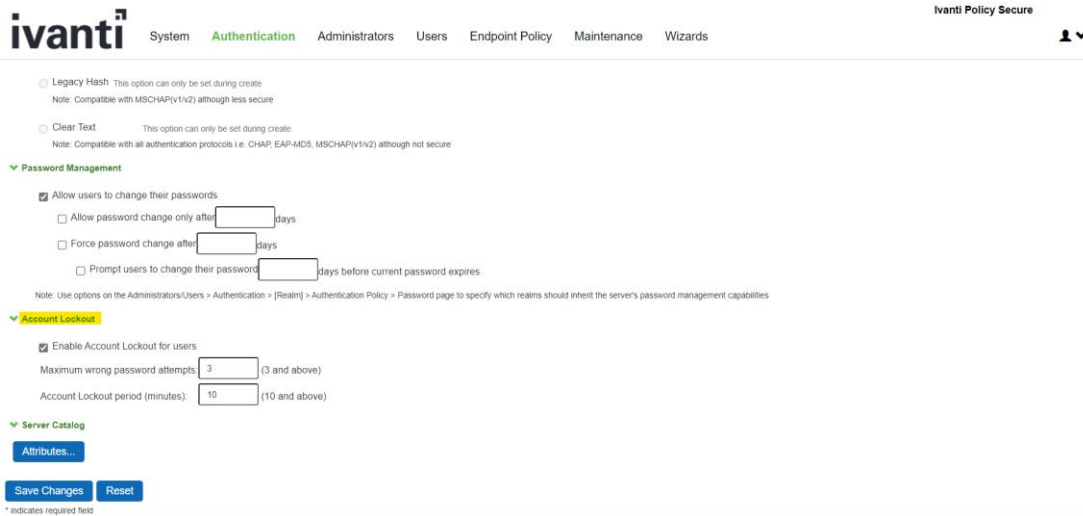
To log out of the web administrative session, on any screen click on the **“Logout”** link at the top right of the screen.



3.15 Configuring authentication lockout

Authentication failure lockout is configured on the Administrator Web Console. Perform the following,

1. Navigate to **Authentication > Auth Servers > Administrators > Settings**

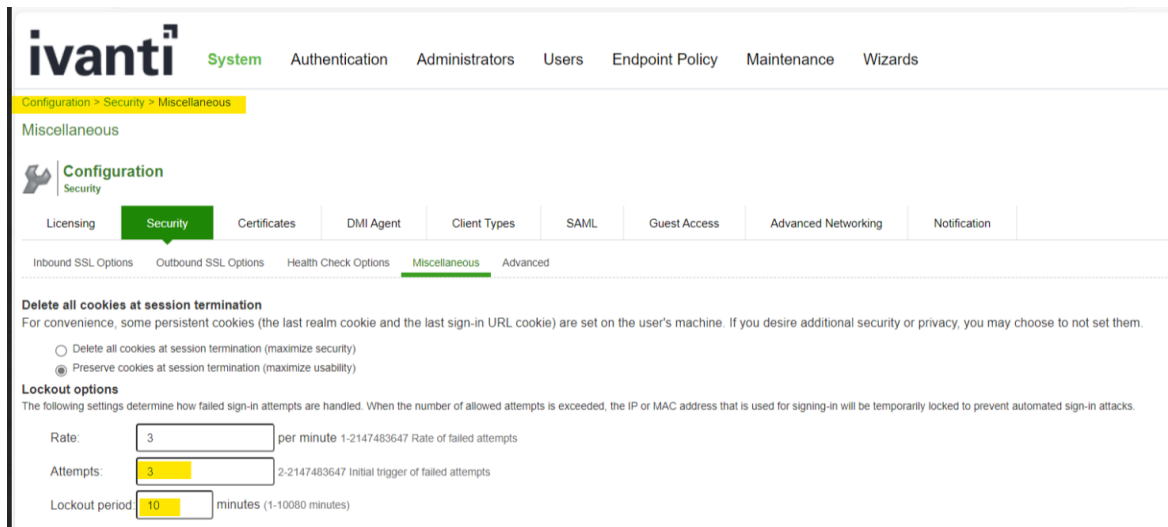


On this screen the number of attempts, and the lockout period is specified.

- Maximum wrong password attempts should be configured to be 3 and above (Max 10).
- If the user enters an incorrect password the configured number of times, the user is locked out they cannot login through any remote interface on the TOE.
- The lock out time is configurable between 10 minutes to 999 minutes. When the lockout time has expired, the administrator is allowed to authenticate to the TOE again.
- Lockouts are not enforced on the TOE’s console interface. This ensures that authentication failures cannot lead to a situation where no administrator access is available.

Additionally, the following settings determine how failed sign-in attempts are handled. When the number of allowed attempts is exceeded, the IP address that is used for signing-in will be temporarily locked to prevent automated sign-in attacks.

2. Navigate to **Configuration > Security > Miscellaneous**



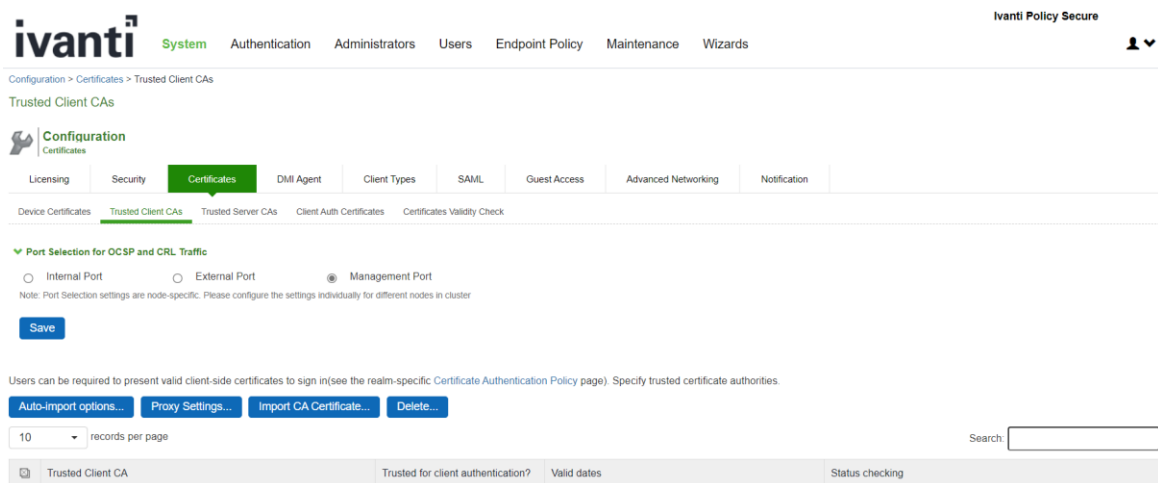
Note: Login attempts, and Lockout period should be same for both the settings

3.16 Import Trusted Client CA

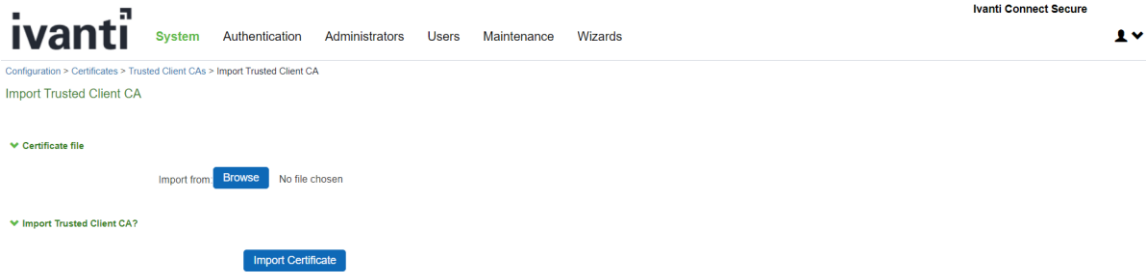
Trusted Client CA is required to validate the client certificate that is used by the TOE to authenticate to syslog server.

On Administrator Web Console,

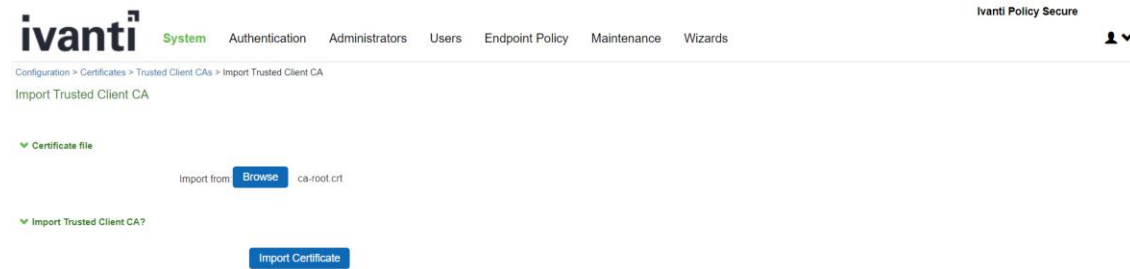
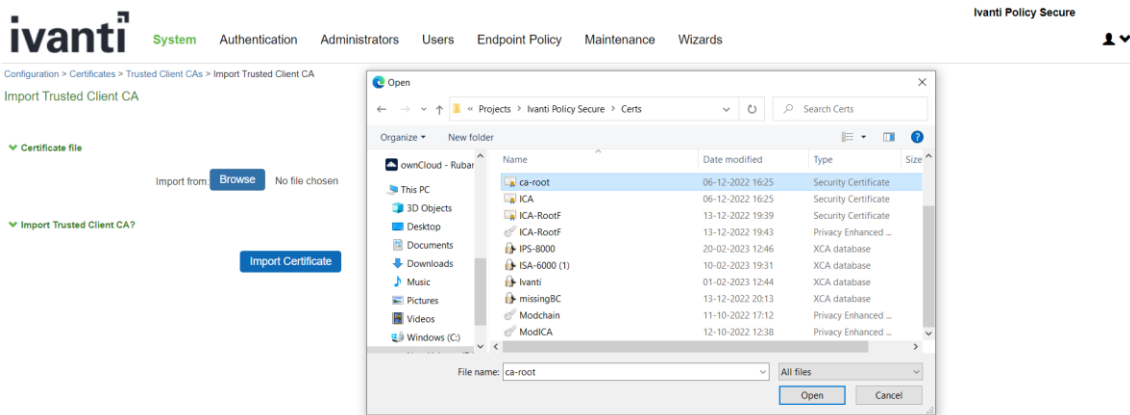
1. Navigate to **System > Configuration > Certificates > Trusted Client Cas**




2. Click **Import CA Certificates...** to import CA or Chain of CAs one by one as explained below in different Screenshots.




3. Click on **Browse** and select the certificate, then click on **Import Certificate**



4. The imported trusted client CA is shown in the **Trusted Client CAs** table



[System](#)
[Authentication](#)
[Administrators](#)
[Users](#)
[Endpoint Policy](#)
[Maintenance](#)
[Wizards](#)

Ivanti Policy Secure


Configuration > Certificates > Trusted Client CAs

Trusted Client CAs

Configuration
Certificates

Licensing
Security
Certificates
DMI Agent
Client Types
SAML
Guest Access
Advanced Networking
Notification

Device Certificates
Trusted Client CAs
Trusted Server CAs
Client Auth Certificates
Certificates Validity Check

Port Selection for OCSP and CRL Traffic

Internal Port
 External Port
 Management Port


Note: Port Selection settings are node-specific. Please configure the settings individually for different nodes in cluster

[Save](#)

Users can be required to present valid client-side certificates to sign in(see the realm-specific Certificate Authentication Policy page). Specify trusted certificate authorities.

[Auto-import options...](#)
[Proxy Settings...](#)
[Import CA Certificate...](#)
[Delete...](#)

10 records per page
Search

Trusted Client CA	Trusted for client authentication?	Valid dates	Status checking
 ca-root	Yes	2022/07/25 - 2023/07/25	None

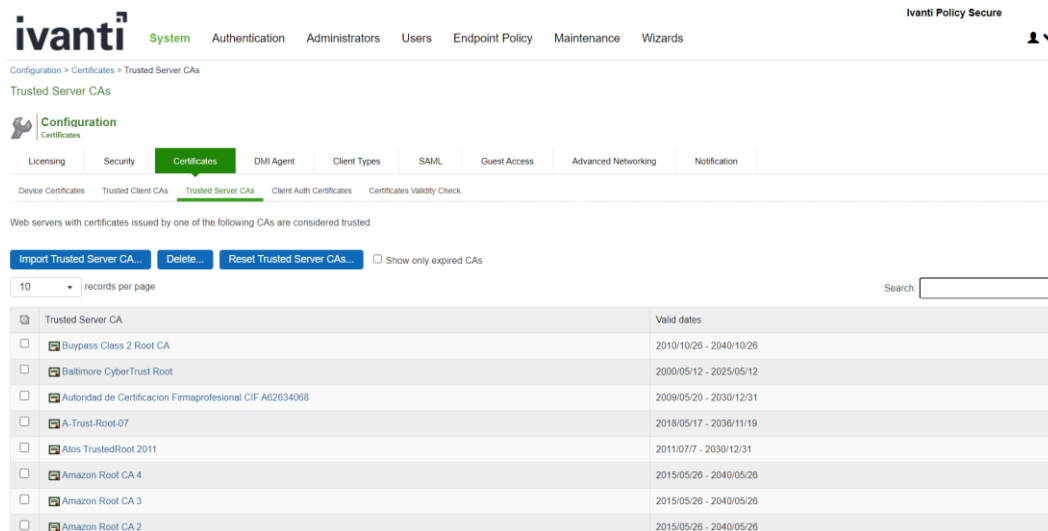
3.17 Import Trusted Server CA

Trusted Server CA is used in two situations:

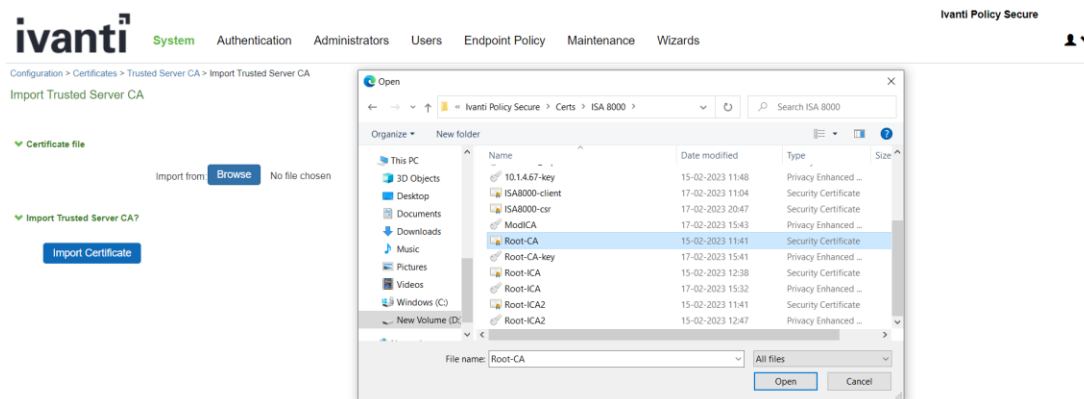
- To validate the device certificate that is generated for TLS handshake when a TLS client is connecting to the TOE.
- To validate the server certificate received in TLS handshake when the TOE connects to syslog server.

On Administrator Web Console,

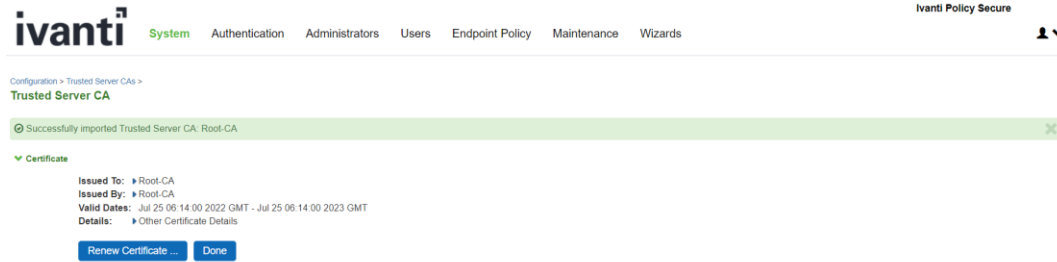
1. Navigate to **System -> Configuration -> Certificates -> Trusted Server CAs.**



2. Click on **Import Trusted Server CA**
3. On the **Import Trusted Server CA** screen, click on **Browse**, import the Root CA certificate file

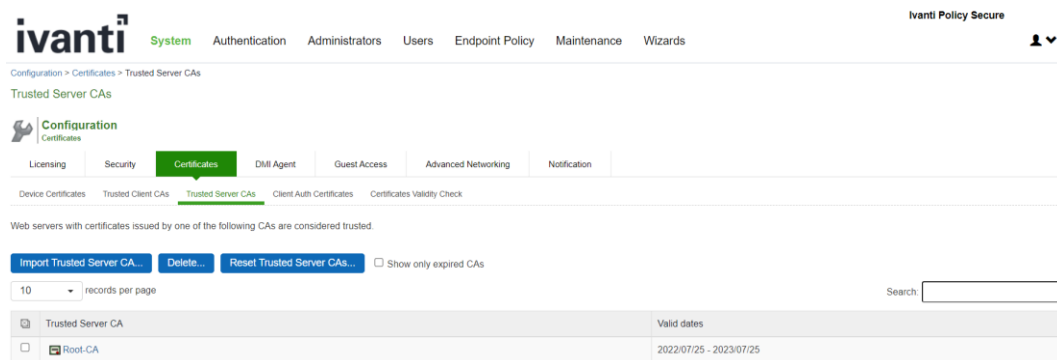


4. Once CA or CA Chain is Imported, click **Done**



Note: To import CA Chain, all Sub CAs must be imported one by one.

- The CA Common Name of the imported trusted server CA should be seen in the **Trusted Server CA** table on screen **System > Configuration > Certificates > Trusted Server CAs**.



Set User Account Password

3.18 Device Certificates

Device certificate needs to be configured for the TOE to use in TLS handshake when a TLS client connects to the TOE.

The TOE supports RSA device certificate and ECC device certificate. If the generated device certificate is RSA, then the following ciphersuite are supported:

- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

Key establishment is not configurable when RSA device certificate is installed. The TOE is capable of negotiating an ECDHE or RSA key establishment.

When the installed device certificate is an ECC certificate, the following ciphersuites are supported:

- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

Only ECDHE key establishment is used when an ECC device certificate is installed.

3.18.1 Generate RSA or ECC Certificate

On Administrator Web Console,

1. Navigate to **System > Configuration > Certificates > Device Certificate**
2. Click on **New CSR...**

The screenshot shows the 'Device Certificate' configuration page in the Ivanti Policy Secure web console. The page has a navigation bar with 'System', 'Authentication', 'Administrators', 'Users', 'Endpoint Policy', 'Maintenance', and 'Wizards'. Below the navigation bar, there are tabs for 'Licensing', 'Security', 'Certificates', 'DM Agent', 'Client Types', 'SAML', 'Guest Access', 'Advanced Networking', and 'Notification'. The 'Certificates' tab is active, and there are sub-tabs for 'Device Certificates', 'Trusted Client CA', 'Trusted Server CA', 'Client Auth Certificates', and 'Certificates Validity Check'. The 'Device Certificates' sub-tab is selected. The page contains a table of certificates with the following columns: Certificate issued to, Issued by, Valid Dates, and Used by. The table lists several certificates, including those issued by ICA and ca-root. Below the table, there are buttons for 'New CSR' and 'Delete'.

Certificate issued to	Issued by	Valid Dates	Used by
ISA6000R	ICA	Sep 12 10:16:00 2022 GMT to Jul 25 06:14:00 2023 GMT	
10.1.4.70	ICA	Feb 9 10:09:00 2023 GMT to Jul 25 06:14:00 2023 GMT	
ISA6000CSR.acumen.com	ICA	Oct 6 13:53:00 2022 GMT to Jul 25 06:14:00 2023 GMT	
ivanti.acumen.com	ivanti.acumen.com	Jul 22 07:02:11 2022 GMT to Jan 12 07:02:11 2028 GMT	
ca-root	ca-root	Jul 25 06:14:00 2022 GMT to Jul 25 06:14:00 2023 GMT	
10.1.4.70	ICA	Jul 26 12:50:00 2022 GMT to Jul 25 06:14:00 2023 GMT	<Management Port>
secure.ivanti.com	ICA	Oct 21 13:20:00 2022 GMT to Jul 25 06:14:00 2023 GMT	
ICA	ca-root	Jul 25 06:14:00 2022 GMT to Jul 25 06:14:00 2023 GMT	
CA-CRL3c	CA-CRL3c	Oct 7 13:23:00 2022 GMT to Oct 7 13:23:00 2034 GMT	

3. Fill in CSR fields:

The screenshot shows the 'New Certificate Signing Request' form in the Ivanti Policy Secure web console. The form contains the following fields:

- Common Name: secure1.ivanti.com
- Organization Name: acumensecurity.pvt.ltd
- Org. Unit Name: CC
- Locality: Rockville
- State (fully spelled out): Maryland
- Country (2 letter code): US
- Email Address: lest@ivanti.com
- Key Type: RSA (selected), ECC
- Key Length: 1024 bits
- Random Data: (used for key generation)

At the bottom of the form, there is a 'Create CSR' button.

Common Name: The fully qualified domain name (FQDN) for your web server. This must be an exact match. Eg: secure.ivanti.com

Organization Name: The exact legal name of your organization. Do not abbreviate your organization name. Eg: acumensecurity.pvt.ltd

Org. Unit Name: Section of the organization, can be left empty if this does not apply to your case. Eg: CC

Locality: The city where your organization is legally located. Eg: Rockville

State: The state where your organization is legally located. Must not be abbreviated. Eg: Maryland

Country: The two-letter ISO abbreviation for your country. Eg: US

Email Address: The email address used to contact your organization. Eg: test@ivanti.com

Key Type: Public/Private Key Pair Type.

To generate RSA device certificate, click on **RSA** radio button, then select 2048 bits or 3072 bits as **Key Length**. Optionally, **Random Data** can be entered for generating Key Pair.

To generate ECC device certificate, click on **ECC** radio button, select **P-256** or **P-384** as **ECC Curve**. Optionally, **Random Data** can be entered for generating Key Pair.

See below for ECC device certificate request screenshot:

ivanti System Authentication Administrators Users Endpoint Policy Maintenance Wizards Ivanti Policy Secure

Configuration > Certificates > New Certificate Signing Request

New Certificate Signing Request

Use this page to create a new Certificate Signing Request (CSR) to send to your Certificate Authority of choice.

Common Name:
 (e.g., secure.company.com)

Organization Name:
 (e.g., Company Inc.)

Org. Unit Name:
 (e.g., IT Group)

Locality:
 (e.g., SomeCity)

State (fully spelled out):
 (e.g., California)

Country (2 letter code):
 (i.e., US)

Email Address:

Key Type: RSA ECC

ECC Curve:

Create CSR

4. Click on **Create CSR**

ivanti System Authentication Administrators Users Endpoint Policy Maintenance Wizards Ivanti Policy Secure

CSR created successfully: Your CSR was created successfully. See below for instructions on sending the CSR to a Certificate Authority. The certificate approval process may take several days. When you receive the signed certificate from the Certificate Authority, you will need to import the certificate to complete this process.

Configuration > Pending Certificate Signing Request

Pending Certificate Signing Request

CSR Details

Common Name: secure1.ivanti.com
 Created: 3/8/2023 12:52:24

Org. Name: acumensecurity.pvt.ltd Locality: Rockville
 Org. Unit Name: CC State: Maryland
 Email Address: test@ivanti.com Country: US
 Key Size: 2048 bits

[Back to Device Certificates](#)

Step 1. Send CSR to Certificate Authority for signing

To send the CSR to a Certificate Authority (CA), you need to copy the encoded text below, including the BEGIN and END lines, and submit it to the CA in one of the following ways:

- Save the text as a .cert file and attach it to an email message to the CA
- Paste the text into an email message to the CA
- Paste the text into a Web form provided by the CA

Note: Manage the CSR process carefully. If you submit more than one CSR to a CA, you may be billed for each CSR.

```
-----BEGIN CERTIFICATE REQUEST-----
MIIDTCAgICAQAgZBcCZAJBgNVBAYTMRkwDwYDVQQIDANNYX
J5bGFUZEES
MBAQCAIUEBwwJUm9jY3ZpGmMR8wHQYDVQKDBZHY3VZWSZWN1C
rR8eSsdndQu
```

Step 2. Import signed certificate

When you receive the signed certificate file from the CA, select it below and click import. This will add the signed certificate and remove this pending CSR.

Signed certificate: No file chosen

5. Copy CSR content shown in the text field. **Send CSR to Certificate Authority for signing** to generate a certificate.

[Back to Device Certificates](#)

Step 1. Send CSR to Certificate Authority for signing

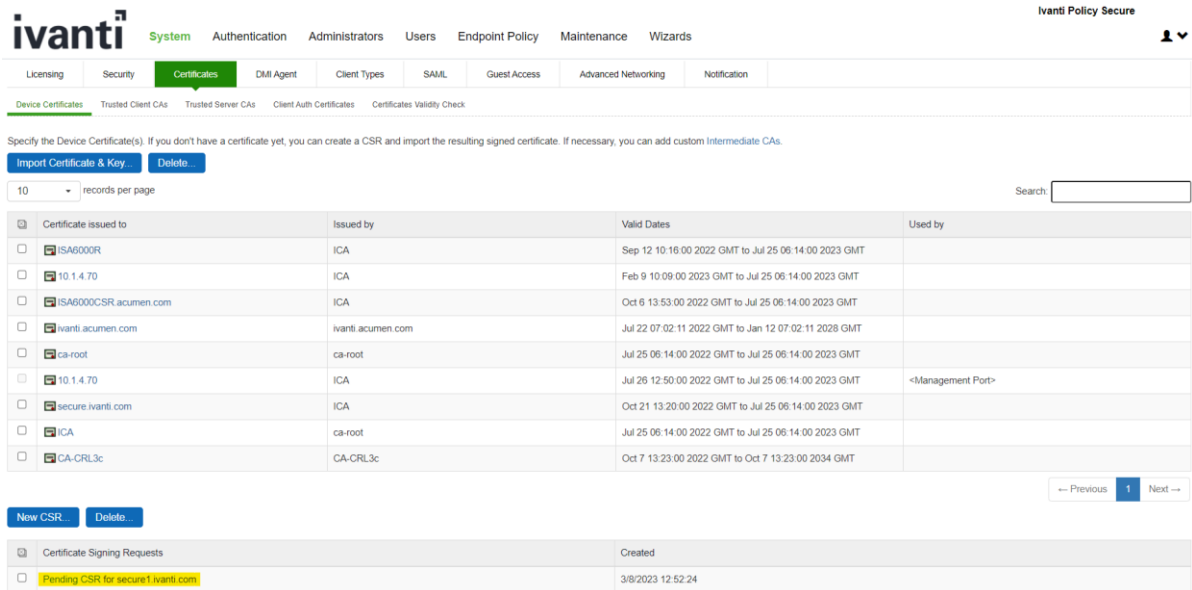
To send the CSR to a Certificate Authority (CA), you need to copy the encoded text below, including the BEGIN and END lines, and submit it to the CA in one of the following ways:

- Save the text as a .cert file and attach it to an email message to the CA
- Paste the text into an email message to the CA
- Paste the text into a Web form provided by the CA

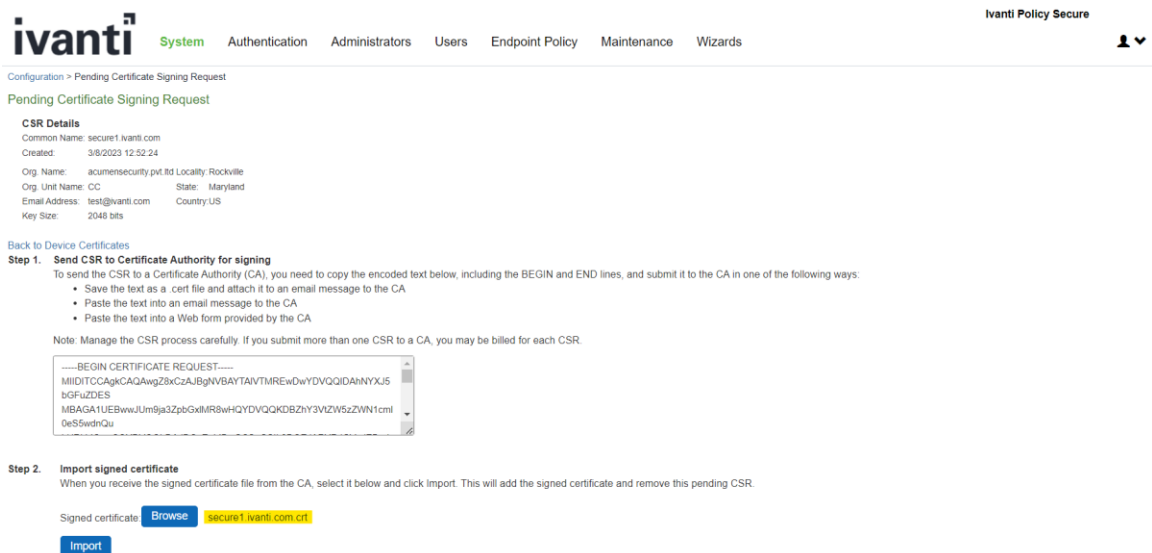
Note: Manage the CSR process carefully. If you submit more than one CSR to a CA, you may be billed for each CSR.

```
-----BEGIN CERTIFICATE REQUEST-----
MIIDITCCAqkCAQAwZ8xZCzAJBgNVBAYTAiVhbnRlcmwYDzYVQVQIDAhNYX
J5bGFuZDES
MBAGA1UEBwwJUm9ja3ZpbGxMR8wHQYDVQQKDBZlbnRlcmwYDzYVQVQIDAh
ml0eS5wdnQu
-----END CERTIFICATE REQUEST-----
```

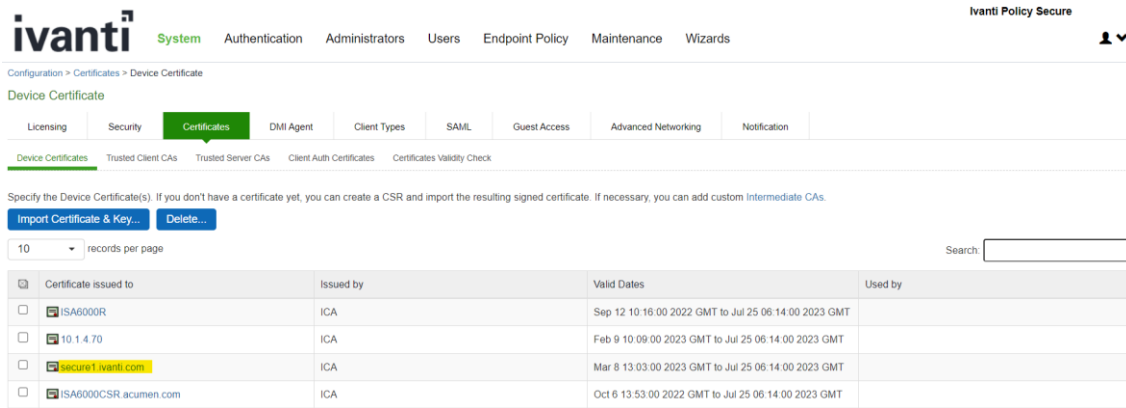
6. Navigate to **System > Configuration > Certificates > Device Certificates** and click on **Pending CSR** link in the table at the bottom of the screen.



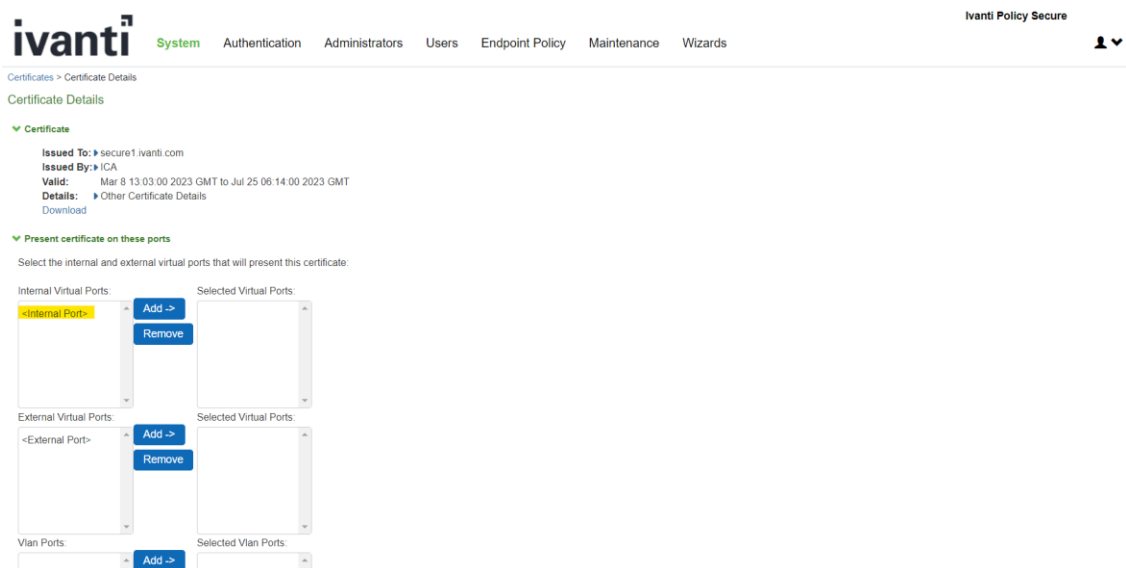
7. On the **Pending Certificate Signing Request Page**, in the expanded **Import signed certificate** section, click on **Browse** to select the certificate file.



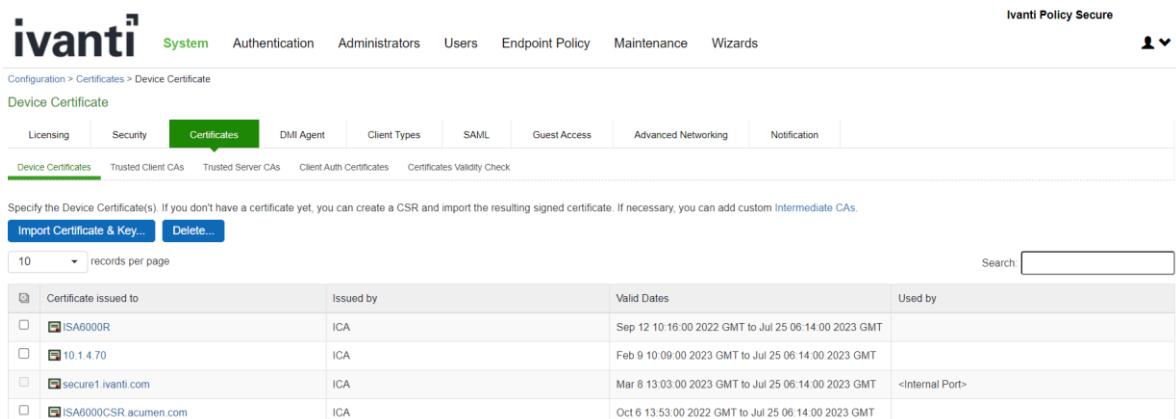
8. Click on **Import**
 9. The new certificate is shown in **System > Configuration > Certificates > Device Certificates**



- Click on the certificate name that was created.
- The **Certificate Details** screen is shown, in the expanded **Present certificate on these ports** section, select **<Internal Port>** in the left panel that is labelled **Internal Virtual Ports**, click on **Add >** to map it to the new device certificate.
- If the **<Internal Port>** is not available in the left panel that is labelled **Internal Virtual Ports**, then the internal port is already mapped to a different device certificate, please see NOTE on instructions to remove the internal port from the currently mapped device certificate.



- Click on **Save Changes**, the selected port in step 11 is shown in the **Used by** field for the new certificate.



If the internal port is already mapped to a different device certificate, do the following:

- a) Click the device certificate that is mapped to the internal port and select **<Internal Port>** from **Selected Virtual Ports** box.

The screenshot shows the 'Certificate Details' page in the Ivanti Policy Secure interface. The 'Certificate' section displays details such as 'Issued To: secure1.ivanti.com', 'Issued By: ICA', and 'Valid: Mar 8 13:03:00 2023 GMT to Jul 25 06:14:00 2023 GMT'. The 'Present certificate on these ports' section is expanded, showing a list of 'Internal Virtual Ports' and 'Selected Virtual Ports'. The 'Internal Port' is currently selected in the 'Selected Virtual Ports' list. The 'Remove' button is highlighted in blue.

- b) Click on **Remove** to unmap the device certificate from the Internal port and **Save Changes**

The screenshot shows the 'Certificate Details' page in the Ivanti Policy Secure interface. The 'Certificate' section displays details such as 'Issued To: secure1.ivanti.com', 'Issued By: ICA', and 'Valid: Mar 8 13:03:00 2023 GMT to Jul 25 06:14:00 2023 GMT'. The 'Present certificate on these ports' section is expanded, showing a list of 'Internal Virtual Ports' and 'Selected Virtual Ports'. The 'Internal Port' is currently selected in the 'Selected Virtual Ports' list. The 'Remove' button is highlighted in blue.

3.19 Configure Secure Channel to Syslog Server

The evaluated configuration uses TLS to protect the communications between the TOE and the external audit storage (Syslog) server. To configure the secure channel from the TOE to Syslog Server, the following configuration is required:

- A trusted server CA needs to be imported into the TOE which is used to authenticate the Syslog server. Refer the section [Import Trusted Server CA](#) on importing the trusted server CA for communication with Syslog server.

- A RSA 2048/3072 client auth certificate needs to be imported in order to authenticate to the Syslog server. Refer the section [Import Client Auth Certificate](#).
- A trusted client CA must be imported to validate the client auth certificate. Refer the section [Import Trusted Client CA](#) for instructions to import a trusted client CA.

If the TLS connection unintentionally broke, TOE automatically reconnects following an exponentially increasing timer. The reconnect timer starts at 15 seconds and doubles after each failed to reconnect attempt until reaches 15 minutes, and TOE continuously reconnects at 15-minute intervals.

3.20 Import Client Auth Certificate

Client auth certificates are used for mutual authentication.

Follow instructions below to import a RSA 2048/3072 Client Auth Certificate into the TOE.

On Administrator Web Console,

1. Navigate to **System > Configuration > Certificates > Client Auth Certificates**

Certificate issued to	Issued by	Valid Dates
<input type="checkbox"/> ISA6000R.MA	ca-root	Sep 23 11:27:00 2022 GMT to Jul 25 06:14:00 2023 GMT
<input type="checkbox"/> ec_ivanti.acumen	ICA	Sep 28 07:27:00 2022 GMT to Jul 25 06:14:00 2023 GMT
<input type="checkbox"/> clientctrl.com	ICA-root-ec	Oct 11 08:10:00 2022 GMT to Oct 11 07:48:00 2023 GMT
<input type="checkbox"/> ivanti.acumen.com	ICA	Aug 5 05:57:00 2022 GMT to Jul 25 06:14:00 2023 GMT

2. Click on **Import Certificate & Key...**
3. Follow instructions on **Import Certificate & Key** screen to import the client auth certificate.

4. The imported certificate should be shown in the table in **System > Configuration > Certificates > Client Auth Certificates** screen.

Configuration > Certificates > Client Auth Certificates

Client Auth Certificates

Specify the Client Auth Certificate(s). If you don't have a certificate yet, you can create a CSR and import the resulting signed certificate. If necessary, you can add custom [Intermediate CAs](#).

Certificate issued to	Issued by	Valid Dates
ISA6000R.MA	ca-root	Sep 23 11:27:00 2022 GMT to Jul 25 06:14:00 2023 GMT
ec_ivanti.acumen	ICA	Sep 28 07:27:00 2022 GMT to Jul 25 06:14:00 2023 GMT
clientcrl.com	ICA-root-ec	Oct 11 08:10:00 2022 GMT to Oct 11 07:48:00 2023 GMT
ivanti.acumen.com	ICA	Aug 5 05:57:00 2022 GMT to Jul 25 06:14:00 2023 GMT
ISA60003C	ICA-CRL3c	Oct 14 06:45:00 2022 GMT to Oct 14 06:45:00 2023 GMT
ISA6000RMA	ca-root	Sep 23 11:04:00 2022 GMT to Jul 25 06:14:00 2023 GMT
ISA6000crl2	ICA-CRL2	Oct 10 09:37:00 2022 GMT to Oct 10 09:37:00 2023 GMT
ISA6000EC.acumen.com	ICA-ec	Oct 7 06:32:00 2022 GMT to Jul 25 06:14:00 2023 GMT
ISA6000EC	ICA-root-ec1	Oct 11 09:49:00 2022 GMT to Oct 11 07:48:00 2023 GMT
ISA6000crl	ICA-CRL1	Oct 10 07:06:00 2022 GMT to Oct 10 07:06:00 2023 GMT

3.21 Configuring Syslog Server

The Syslog server can be configured for event log, admin access log and User access log.

3.21.1 Configure Syslog Server for Event Log

To configure Syslog server settings for event logs, navigate to **System > Log/Monitoring > Events > Settings**. Configure parameters based on below evaluated settings:

Table 3 – Event Log Parameters

PARAMETER	SELECTION
Maximum Log Size	
Max Log Size	1 MB (up to 500 MB)
Select Events to Log	
Connection Requests	Enable
System Status	Enable
System Errors	Enable
Rewrite	Enable
Statistics	Enable
Performance	Enable
License Protocol Events	Disable
Reverse Proxy	Enable
Syslog Servers	See Section Configure Syslog Server Parameters

3.21.2 Configure Syslog Server for Admin Access Log

To configure the Syslog server for admin log, navigate to **System > Log/Monitoring > Admin Access > Settings**.

Select the following settings for the Admin Access logging options in the evaluated configuration:

Table 4 – Admin Access Log Parameters

PARAMETER	SELECTION
Maximum Log Size	
Max Log Size	200 MB (up to 500 MB)
Select Events to Log	
Administrator changes	Enable
Administrator logins	Enable
License changes	Enable
Syslog Servers	See Section Configure Syslog Server Parameters

3.21.3 Configure Syslog Server for User Access Log

To configure Syslog server for admin log, navigate to **System > Log/Monitoring > User Access > Settings**

Select the following settings for the Admin Access logging options in the evaluated configuration:

Table 5 – User Access Log Parameters

PARAMETER	SELECTION
Maximum Log Size	
Max Log Size	200 MB (up to 500 MB)
Select Events to Log	
Login/logout	Enable
SAM/Java	Disable
User Settings	Enable
Meeting Events	Disable
Client Certificate	Enable
Active Sync Proxy	Disable
IF-MAP Client User Messages	Disable
Pulse Client Messages	Disable
HTML5 Access	Disable
Web Requests	Enable
File Requests	Enable
Meeting	Disable
Secure Terminal	Enable
VPN Tunneling	Enable
SAML	Disable
Syslog Servers	See Section Configure Syslog Server Parameters

3.22 Configure Syslog Server Parameters

In the **Syslog Servers** expanded section, enter information as stated in table below:

Table 6 – Syslog Server Parameters

PARAMETER	SELECTION
Server name/IP	Fully qualified domain name or IP address for the syslog server. This should match with the common name of the TLS Syslog server certificate.

Facility	Syslog server facility level (LOCAL0 - LOCAL7). Chose the option that is appropriate based on your Syslog configuration.
Type	TLS
Client Certificate	Select the client auth certificate imported in Import Client Auth Certificate to authenticate to the syslog server.
Filter	Standard (Default)

The screenshot shows the 'Syslog Servers' configuration page in the Ivanti Policy Secure interface. At the top, there are navigation tabs: System, Authentication, Administrators, Users, Endpoint Policy, Maintenance, and Wizards. Below the navigation, there are several checkboxes for event logging: MDM API Trace (unchecked), Ivanti Neurons for Secure Access Events (checked), Profiler Events (checked), Admission Control Events (checked), and Attribute Server Events (unchecked). The 'Syslog Servers' section is expanded, showing a table with the following columns: Server name/IP, Facility, Type, Client Certificate, Filter, and Source Interface. A 'Delete' button is located above the table. The table contains one row with the following values: Server name/IP (empty), Facility (LOCAL0), Type (UDP), Client Certificate (Select Client Cert), Filter (Standard: Standard (default)), and Source Interface (Global). An 'Add' button is located to the right of the table. Below the table, there are 'Save Changes' and 'Reset' buttons.

Click on **Add** and then **Save Changes**.

By default, the TSF allocates 200 MB to local audit storage; however, the administrator can configure the amount of space allocated to local audit storage, up to 500 MB. The TSF divides the local audit storage between two audit files. When the current audit file reaches capacity; the TSF deletes the inactive log file, creates a new log file, switches logging to the new log file, and generates an audit log indicating that a log file reached capacity.

When reached 90% of configured “Max Log Size (MB)”, a log message is audited.

The TSF protects audit data from unauthorized modification and deletion through the restrictive administrative interfaces. The filesystem of the TSF is not exposed to the administrative user over the HTTPs GUI or the local CLI. The administrative user must be positively identified and authenticated prior to being allowed to clear the local audit log or change audit settings. Logs are sent to the syslog server in real-time, that is when an audit event is generated, it is simultaneously sent to the external server and stored locally.

The TSF establishes reference identifiers for the remote server as follows:

- When the server is specified using a domain name, the TSF verifies that the domain name matches a Subject Alternative Name DNS Name field in the certificate using exact or wildcard matching specified in Section 3.1 of RFC 2818. If the certificate does not contain any Subject Alternative Name fields, the TSF matches the domain name against the Common Name in the certificate.
- When the server is specified using an IP address, the TSF verifies that the IP address exactly matches a Subject Alternative Name IP Address field in the certificate using the rules specified in Section 3.1 of RFC 2818. If the certificate does not contain any Subject Alternative Name fields, the

TSF matches the IP address against the Common Name in the certificate.

- When the reference identifier is an IP address, the TOE converts the IP address to a binary representation in network byte order. IPv4 addresses are converted directly from decimal to binary as specified in RFC 3986. The TOE compares the binary IP address against all the IP Address entries in the Subject Alternative Name.
- The TSF does support wildcards but does not support certificate pinning and determines if the certificate is valid for the specified server based on the DNS name or IP address of the server. Wildcards are supported only at the left-most label of the identifier.

3.23 CRL checking configuration

3.23.1 Understanding CRL

A certificate revocation list (CRL) is a mechanism for canceling a client-side certificate. As the name implies, a CRL is a list of revoked certificates published by a CA or a delegated CRL issuer. The system supports base CRLs, which includes the company's revoked certificates in a single, unified list.

Certificate Security Administration The system determines the correct CRL to use by checking the client's certificate. (When it issues a certificate, the CA includes CRL information for the certificate in the certificate itself.) To ensure that it receives the most up-to-date CRL information, the system periodically contacts a CRL distribution point to get an updated list of CRLs. A CRL distribution point (CDP) is a location on an LDAP directory server or Web server where a CA publishes CRLs. The system downloads CRL information from the CDP at the interval specified in the CRL, at the interval that you specify during CRL configuration, and when you manually download the CRL. The system also supports CRL partitioning. CRL partitioning enables you to verify portions of very large CRLs without spending the time and bandwidth necessary to access and validate a very large CRL or collection of large CRLs. CRL partitioning is only enabled when you employ the Specify the CDP(s) in the client certificates method (described below). In this case, the system validates the user by verifying only the CRL specified in the client certificate.

Although CAs include CRL information in client-side certificates, they do not always include CDP information as well. A CA can use any of the following methods to notify the system of a certificate's CDP location:

- Specify the CDP(s) in the CA certificate—When the CA issues a CA certificate, it might include an attribute specifying the location of the CDPs that the system should contact. If more than one CDP is specified, the system chooses the first one listed in the certificate and then fails over to subsequent CDPs, if necessary.
- Specify the CDP(s) in the client certificates—When the CA issues a client-side certificate, it might include an attribute specifying the location of the CDPs that the system must contact. If more than one CDP is specified, it chooses the first one listed in the certificate and then fails over to subsequent CDPs, if necessary. When the system employs CRL partitioning and the client certificate specifies only one CRL, it performs verification using only that CRL
- Require the administrator to manually enter the CDP location—If the CA does not include the CDP location in the client or CA certificates, you must manually specify how to download the entire CRL object. You can specify a primary and backup CDP. (Manually entering the CDP location provides the greatest flexibility because you do not need to reissue certificates if you change the CDP location.)
- The system compares the user's certificate against the appropriate CRL during authentication. If it determines that the user's certificate is valid, the system caches the certificate attributes and applies them, if necessary, during role and resource policy checks. If it determines that the user's certificate is invalid, if it cannot contact the appropriate CRL, or if the CRL is expired, it denies the user access.

- The system supports only CRLs that are in a PEM or DER format and that are signed by the CA for which the revocations apply.
- The system only saves the first CRL in a PEM file.
- The TOE uses a CRLs to verify whether intermediate CA certificate has been revoked when intermediate certificate is uploaded in TOE's trust store.
- The TOE uses a CRLs to verify whether the leaf certificate has been revoked when a leaf certificate is presented to the TOE as part of the certificate chain during authentication.

3.23.2 Enable CRL checking

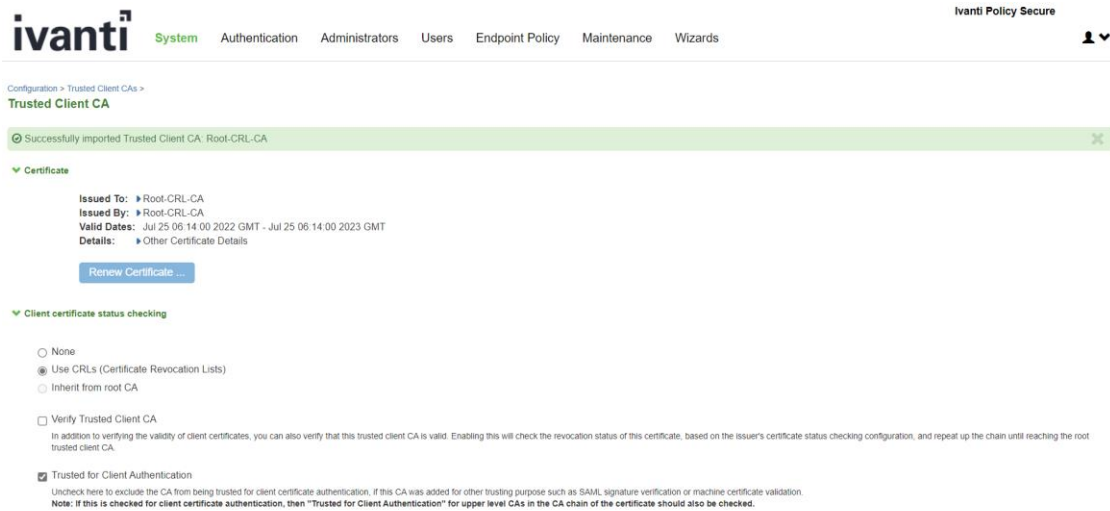
1. Navigate to **Configuration > Trusted Client CAs** and select the port for CRL traffic
2. Click on **Import CA certificate**

The screenshot shows the Ivanti Policy Secure web interface. The breadcrumb trail is Configuration > Certificates > Trusted Client CAs. The 'Certificates' tab is active. Under 'Port Selection for OCSP and CRL Traffic', the 'Management Port' radio button is selected. Below this, there are buttons for 'Proxy Settings...', 'Import CA Certificate...', and 'Delete...'. A table with columns 'Trusted Client CA', 'Trusted for client authentication?', 'Valid dates', and 'Status checking' is partially visible.

3. Click on **Browse** and select the certificate, click on **Import certificate**

The screenshot shows the Ivanti Policy Secure web interface. The breadcrumb trail is Configuration > Certificates > Trusted Client CAs > Import Trusted Client CA. The 'Certificate file' section is expanded, showing 'Import from' with a 'Browse' button and the filename 'Root-CRL-CA.crt'. The 'Import Trusted Client CA?' section is expanded, showing an 'Import Certificate' button.

4. Once certificate is imported select **Use CRLs(Certificate Revocation Lists)**



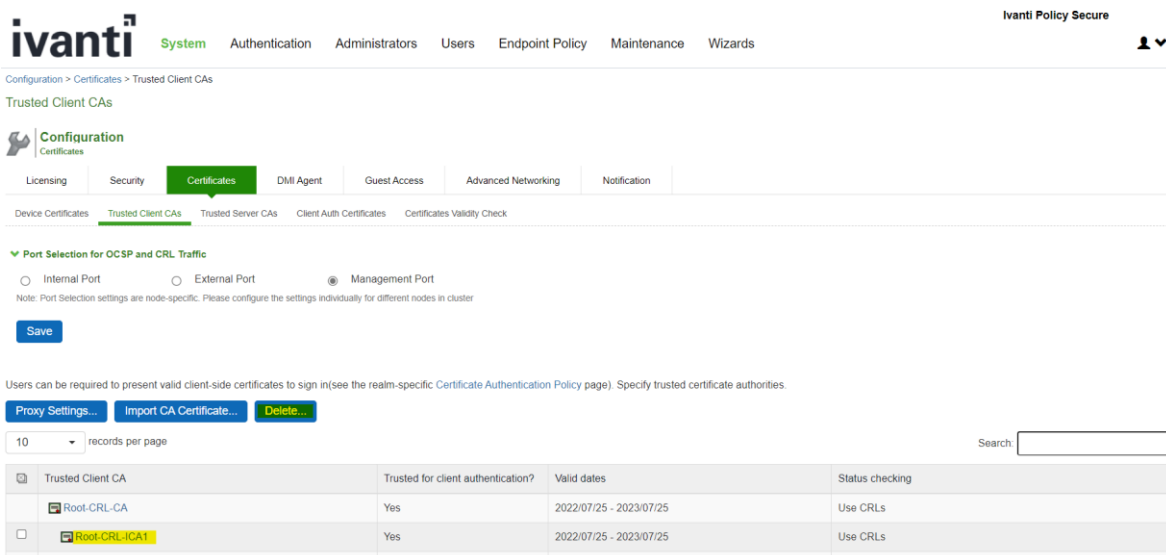
5. Click on **Save changes**
6. The certificate is not listed on the CRL. If the TSF has a cached response that has not expired, the TSF uses the cached response in lieu of querying the CRL server.
7. If the TSF cannot contact the CRL server or the server does not respond, the TSF logs the failure and considers the certificate valid.

3.24 Removing Cached CRL Entry of CA Chain

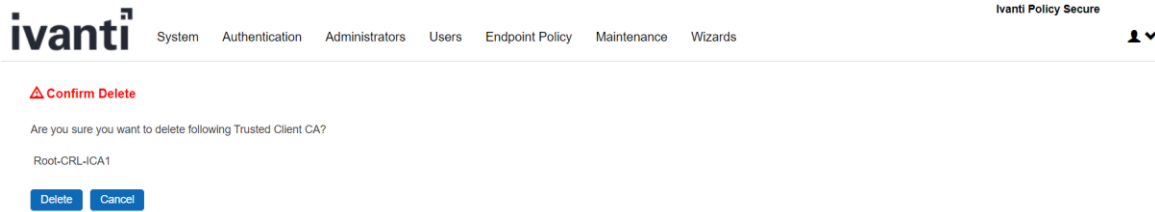
Note: To remove cached CRL entry of CA Chain in Ivanti Policy Secure, follow the sections [Delete CA Chain from trusted client CA](#) and [Delete CA Chain from trusted server CA](#).

3.25 Delete CA Chain from Trusted Client CA

1. Go to **System > Configuration > Certificates > Trusted Client CAs**
2. Select CA Chain one by one and Click **Delete**



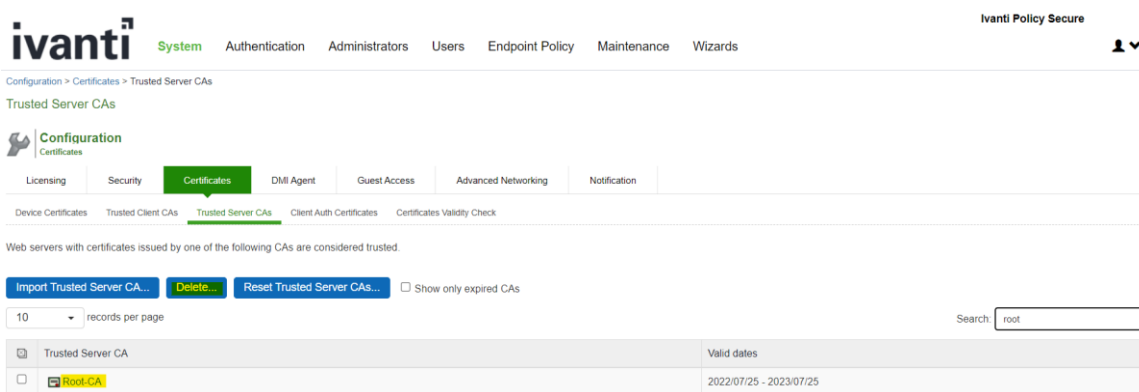
3. Confirm the delete by clicking **Delete**



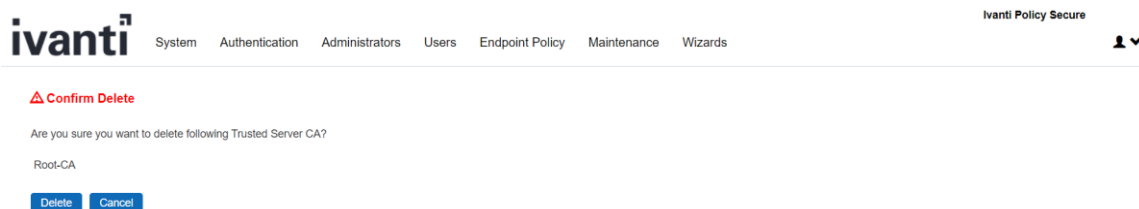
4. Repeat the **Step 2** till all the CA Chain is Deleted

3.26 Delete CA Chain from Trusted Server CA

1. Go to **System > Configuration > Certificates > Trusted Server CAs**
2. Select CA Chain one by one and Click **Delete**



3. Confirm the delete by clicking **Delete**



4. Repeat **Step 2** and **Step 3** till all the CA Chain is Deleted

3.27 Zeroization process

- The HTTPS/TLS Private Host Key and the Syslog/TLS Private Client key are zeroized from the disk when the Security Administrator deletes the key, replaces the key, or zeroizes the entire TOE.
- The TSF zeroizes the HTTPS/TLS Private Host Key and the Syslog/TLS Private Client key on the hard disk drives by overwriting the file location with data from /dev/random three times. Each overwrite calls /dev/random ensuring that a different pseudo random pattern is used each time.
- HTTPS/TLS keys are zeroized from RAM when the HTTP or Syslog process terminates. The TLS Session keys are zeroized from RAM when the associated TLS session is terminated.
- The DRBG state and all ephemeral keys are zeroized when the TSF is shutdown, suffers loss of power, or restarted. The TSF zeroizes keys in RAM by writing zeros to the memory location one time and performing a read verify to ensure that the memory location was set to all zeros. If the read verify fails, the TSF repeats the zeroization process.
- The above key destruction methods apply to all configurations and circumstances, except one. The

only situation where the key destruction may be prevented would be if the system suffers a crash or loss of power. This situation only impacts the keys that are stored on the disk. Since the TOE is inaccessible in this situation, administrative zeroization cannot be performed. However, all keys on the disk are protected because the TOE enables full disk encryption by default.

4. Self-Test

Hardware and software system integrity self-tests execute automatically at system boot-up time. No user intervention is required.

The TSF performs the following hardware self-tests at power-on:

- BIOS checks at power-on
 - Verify boot block checksum.
 - Verify main BIOS checksum.
 - Check CMOS diagnostic byte to determine if battery power is OK and CMOS checksum is OK.
 - Verify CMOS checksum manually by reading the storage area. If the CMOS checksum is bad, update CMOS with power-on default values and clear passwords.

The BIOS checks and the successful use of the hardware to perform cryptographic operations provide basic assurance that the hardware is working properly.

If any of the tests fail, the TOE does not power up. When this happens, the administrator should shut down the TOE and contact Ivanti Policy Secure customer support.

- File integrity check at power-on
 - RSA 2048 SHA-512 digital signature verification of the manifest file. The manifest file contains a list of all executables that are part of the TSF
 - SHA-256 integrity check of each executable file in the TSF using the pre-calculated hashes from the manifest file.

Successful completion of the file integrity check provides assurance that the firmware has not tampered.

If the executable software integrity check fails, the TOE generates a log entry “[Failed integrity check](#)” and continues to boot. The administrator should shut down the TOE and contact Ivanti Policy Secure customer support.

- Cryptographic library tests
 - HMAC-SHA-256 integrity check of the library
 - HMAC-SHA-1 KAT
 - HMAC-SHA-256 KAT
 - HMAC-SHA-384 KAT
 - AES 128 ECB Encrypt and Decrypt KAT
 - AES 256 GCM Encrypt and Decrypt KAT
 - RSA 2048 SHA-256 Sign and Verify KAT
 - ECDSA P-224 SHA-512 Sign and Verify PCT
 - DRBG AES-CTR-256 KAT (invoking the instantiate, reseed, and generate functions)
 - The TSF only tests a single set of parameters for each cryptographic algorithm.

The Cryptographic library test verifies that each cryptographic algorithm specified in FCS_COP.1 requirement is passing a KAT. The KAT demonstrates that algorithm is functioning properly by

invoking the algorithm with hard coded keys and messages and comparing the result to a pre-computed, known to be the correct value. The ECDSA PCT shows that the ECDSA algorithm is functioning properly by signing a known value with a known key and verifying that verifying the computed signature indicates that the signature is valid.

If cryptographic library tests fail, the TSF will not start up, and an error log entry “[Unable to set FIPS mode for web server](#)” is generated. When this happens, the administrator should shut down the TOE and contact Ivanti Policy Secure customer support.

5. Hash Functions

Hash Functions The TOE supports SHA-1, SHA-256, SHA-384 and SHA-512 hashing functions in TLS, Digital Signature hashing, File integrity check and administrator password obfuscation. Here is a table shows the hash algorithms used in the TOE and their usages.

Table 7 – Hash Functions

Hash	Usage
SHA-1	HMAC used in TLS, Hashing for Digital Signatures
SHA-256	HMAC used in TLS, Hashing for Digital Signatures, File integrity checking, Password Obfuscation
SHA-384	HMAC used in TLS, Hashing for Digital Signatures
SHA-512	Hashing for Digital Signatures

- TLS uses the appropriate hash algorithm is selected based on TLS protocol definition. Administrator configuration is not required.
- Hashing for Digital Signatures uses the appropriate hash function based on the attribute configured in digital signatures. Administrator configuration is not required.
- File integrity check uses SHA-256 to hash each executable file and compare with a pre-calculated hash. Administrator configuration is not required.
- Administrator password is obfuscated using SHA-256, administrator configuration is not required.
- The TOE comes preconfigured for these sizes and no additional configuration is required.

6. Keyed Hash Cryptographic Operation (Keyed Hash Algorithm)

- The TOE supports keyed-hash message authentication in accordance with a specified cryptographic algorithm HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384 and cryptographic key sizes 160-bits, 256-bits, 384- bits, and message digest sizes 160, 256, 384 bits that meet the following: ISO/IEC 9797-2:2011, Section 7 “MAC Algorithm 2”.
- The TOE comes preconfigured for these sizes and no additional configuration is required.

7. Sample audit logs

7.1 Audit log records

The Audit log records contain the following information:

- Severity
- Log ID – Log ID starts with a three-letter prefix, such as “SYS”, “ADM”, “AUT”, “ERR” and “STS”.

Depends on the prefix, the log message is stored in one of three log files:

- “SYS”, “ERR”, “STS” – log message is stored in event log file
- “ADM” – log message is stored in admin access log
- “AUT” – log message is stored in user access log
- Message which includes:
 - Date/time of the event
 - Node name
 - Source IP address
 - User ID
 - Realm and Role information
 - Description of event outcome
 These fields are laid out as follows:
 Severity – Log ID - year-month-day HH:MM:SS - Node name - [Source IP address] - User ID – User Realm – User Role – Message

e.g.

Severity	ID	Message
Info	ADM22668	2023-03-09 06:37:22 - ic - [192.168.254.250] admin/Admin Users[Administrators] - Login succeeded for admin/Admin Users from 192.168.254.250 via management port.

In this example,

Severity is Info – an informational message

ID is ADM22668 – The ID. This also indicated the type of event in the first 3 letters.

Date and time is 2023-03-09 06:37:22

Node name is ic

Source IP is 192.168.254.250

User is admin

The **Realm** is Admin Users

Role is Administrators

The log **message** is Login succeeded for admin/Admin Users from 192.168.254.250 via management port.”

<current timestamp> <node name> <IP Address> <user id> <Realm> <Role> <Log Message>

7.2 Audit Data Generation

7.2.1 Start-up and shutdown of the audit functions

Start-up of the audit functions

Info SYS31437 <current timestamp> <node name> [127.0.0.1] System()[]
– Successful syslog connection to peer: '<IP/FQDN>'

Info	SYS31437	2022-11-25 09:55:01 - ic - [127.0.0.1] System()[] - Successful syslog connection to peer: '10.1.4.67'
------	----------	-------------------------------------------------------------------------------------------------------

Info SYS31408 <current timestamp> <node name> [127.0.0.1] System()[]
– Started to process pending logs for TLS syslog server '<IP/FQDN>'

Info	SYS31408	2022-11-25 09:55:01 - ic - [127.0.0.1] System()[] - Started to process pending logs for TLS syslog server '10.1.4.67'.
------	----------	------------------------------------------------------------------------------------------------------------------------

Shutdown of the audit function

Major SYS31048 <current timestamp> <node name> [127.0.0.1] System()[]
– Lost syslog connection to server: '<IP/FQDN>'

Major	SYS31048	2022-11-25 09:55:31 - ic - [127.0.0.1] System()[] - Lost syslog connection to server: 10.1.4.67
-------	----------	-------------------------------------------------------------------------------------------------

7.2.2 Administrative login and logout

Info ADM22668 <current timestamp> <node name> <IP Address> <user id> <Realm> <Role>
– Login succeeded for <user id> from < IP> via management port.

Info	ADM22668	2023-02-23 06:54:12 - ic - [192.168.254.250] admin(Admin Users)[Administrators] - Login succeeded for admin/Admin Users from 192.168.254.250 via management port.
------	----------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------

Info ADM22671 <current timestamp> <node name> <IP Address> <user id> <Realm> <Role>
– Logout from IP.

Info	ADM22671	2023-02-23 06:54:17 - ic - [192.168.254.250] admin(Admin Users)[Administrators][44b0526721] - Logout from 192.168.254.250
------	----------	---------------------------------------------------------------------------------------------------------------------------

7.2.3 Console access

Administrator login through local serial console successfully

Info ADM31274 <current timestamp> <node name> [127.0.0.1] System()[] []- User
<username> logged in successfully through the local console.

Info	ADM31274	2023-02-22 12:04:19 - ic - [127.0.0.1] System()[] [] - User 'admin' logged in successfully through the local console
------	----------	----------------------------------------------------------------------------------------------------------------------

Administrator through local serial console login Failed

Info ADM31275 < current timestamp> <node name> [127.0.0.1] System()[] []- Login
attempt from the local console failed for user <username>

Info	ADM31275	2022-11-29 13:10:03 - ic - [127.0.0.1] System()[] [] - Login attempt from the local console failed for user 'admin'
------	----------	---------------------------------------------------------------------------------------------------------------------

7.2.4 Changes to TSF data related to configuration changes

Time and date change

Info ADM20647 <current timestamp> <node name> <IP Address> <user id> <Realm> <Role>
– System date modified to Month Day HH:MM:SS Year.

Info	ADM20647	2020-07-16 10:42:04 - ic - [192.168.228.44] admin(Admin Users)[Administrators][3a36fb85ff] - System date modified to Jul 16 10:42:03 2020.
------	----------	--------------------------------------------------------------------------------------------------------------------------------------------

Addition of the certificate to the TOE's Trust store:

Info ADM23053 <current timestamp> <node name> <IP Address> <user id> <Realm> <Role>
– Added CA Certificate <Cert subject>

Info	ADM23053	2023-03-09 05:47:34 - ic - [192.168.254.250] admin(Admin Users)[Administrators][b86e3862bc] - Added CA Certificate 'CN=Root-CRL-ICA1, OU=CC, O=acumen, C=US'
------	----------	--------------------------------------------------------------------------------------------------------------------------------------------------------------

Deleting of the certificate from the TOE’s Trust store:

Info ADM23054 <current timestamp> <node name> <IP Address> <user id> <Realm> <Role>
 – Removed CA Certificate <Cert subject>

Info	ADM23054	2023-03-08 13:46:04 - ic - [192.168.228.40] admin(Admin Users)[Administrators][7fe405a86f] - Removed CA Certificate 'ca-root'
------	----------	-------------------------------------------------------------------------------------------------------------------------------

7.2.5 Generating/import of, changing, or deleting of cryptographic keys

Info ADM23081 <current timestamp> <node name> <IP Address> <user id> <Realm> <Role>
 – Created Certificate Signing Request: Key Size <Size> <Cert subject>

Info	ADM23081	2022-11-08 08:27:23 - ic - [192.168.228.44] admin(Admin Users)[Administrators][1771c6ccc4] - Created Certificate Signing Request: key size 2048, 'CN=ISA8000_updatecert,OU=CC,O=acumen,L=??,ST=??,C=US,Email=??'
------	----------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Info ADM23082 <current timestamp> <node name> <IP Address> <user id> <Realm> <Role>
 - Removed CSR <Cert CN>

Info	ADM23082	2022-09-05 15:12:19 - ic - [192.168.254.203] admin(Admin Users)[Administrators][1cba011003] - Removed CSR 'ISA8000.acumen'
------	----------	----------------------------------------------------------------------------------------------------------------------------

7.2.6 Resetting passwords

Info ADM20720 <current timestamp> <node name> <IP Address> <user id> <Realm> <Role>
 - User Accounts modified. Change password for username <username>

Info	ADM20720	2023-03-09 10:19:01 - ic - [192.168.254.250] admin(Admin Users)[Administrators][ad8d850ba3] - User Accounts modified. Changed password for username good.
------	----------	-----------------------------------------------------------------------------------------------------------------------------------------------------------

7.3 NDcPP and FIPS mode

NDcPP mode enable

Info ADM31273 <current timestamp> <node name> <IP Address> <user id> <Realm> <Role>
 - NDcPP Mode is now turned on. The web server will restart.

Info	ADM31273	2022-11-07 08:40:33 - ic - [192.168.254.169] admin(Admin Users)[Administrators][03664eb8fc] - NDcPP Mode is now turned on. The web server will restart.
------	----------	---------------------------------------------------------------------------------------------------------------------------------------------------------

Info ADM30965 <current timestamp> <node name> [127.0.0.1] System()[][] - FIPS Mode is now turned on. The web and RADIUS servers will restart

Info	ADM31028	2023-03-10 05:58:15 - ic - [127.0.0.1] System()[][] - FIPS Mode is now turned on. The web and RADIUS servers will restart.
------	----------	----------------------------------------------------------------------------------------------------------------------------

Info ADM31346 <current timestamp> <node name> <IP Address> <user id> <Realm> <Role>
 Changed outbound custom cipher for Allowed Encryption Strength from '<ciphersuites>' to '<ciphersuites>'

Info	ADM31346	2022-11-17 06:37:38 - ic - [192.168.254.203] admin(Admin Users)[Administrators][e9ec94d128] - Changed outbound custom cipher for Allowed Encryption Strength from 'ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-SHA:ECDHE-ECDSA-AES256-SHA:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-SHA:ECDHE-RSA-AES256-SHA:TLS13-CHACHA20-POLY1305:ECDHE-RSA-AES128-SHA:ECDHE-RSA-AES256-SHA:TLS13-CHACHA20-POLY1305' to 'ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-SHA:ECDHE-RSA-AES256-SHA:TLS13-CHACHA20-POLY1305'
------	----------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

NDcPP mode disable

Info ADM31273 <current timestamp> <node name> <IP Address> <user id> <Realm> <Role>
 - NDcPP Mode is now turned off. The web server will restart.

Info	ADM31273	2022-11-01 07:25:24 - ic - [192.168.228.61] admin(Admin Users)[.Administrators][fd20ab72db] - NDcPP Mode is now turned off. The web server will restart.
------	----------	----------------------------------------------------------------------------------------------------------------------------------------------------------

Info ADM30965 <current timestamp> <node name> <IP Address> <user id> <Realm> <Role>
- FIPS Mode is now turned off. The web server will restart.

Info	ADM30965	2022-11-01 09:42:22 - ic - [127.0.0.1] System()[] - FIPS Mode is now turned off. The web server will restart.
------	----------	---------------------------------------------------------------------------------------------------------------

7.4 HTTPS session

Failure to establish a HTTPS Session through GUI

Minor AUT24604 <current timestamp> <node name> [127.0.0.1] System()[]
– SSL negotiation failed while client at source IP <IP> was trying to connect to <IP>.Reason: 'no shared cipher'

Minor	AUT24604	2023-02-09 10:14:21 - ic - [10.1.4.67] System()[] - SSL negotiation failed while client at source IP '10.1.4.67' was trying to connect to '10.1.4.70'. Reason: 'no shared cipher'
-------	----------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

7.5 Access banner configuration logs

Info ADM30467 <current timestamp> <node name> <IP Address> <user id> <Realm> <Role>
- Created new sign-in notification <Notification name>

Info	ADM30467	2023-03-09 11:42:41 - ic - [192.168.254.250] admin(Admin Users)[.Administrators][351547063c] - Created new sign-in notification 'New Sign-In Notification (test)'
------	----------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------

Info ADM23440 <current timestamp> <node name> <IP Address> <user id> <Realm> <Role>
- Updated the sign-in policy <policy name>

Info	ADM23440	2023-03-09 11:44:23 - ic - [192.168.254.250] admin(Admin Users)[.Administrators][351547063c] - Updated the sign-in policy '*/admin'
------	----------	-------------------------------------------------------------------------------------------------------------------------------------

7.6 Session inactivity time configuration log

Info ADM10245 <current timestamp> <node name> <IP Address> <user id> <Realm> <Role> -
SESSION_IDLE_TIMEOUT in Role 'Administrators' is modified from [Previous time] [Modified time]

Info	ADM10245	2023-01-10 07:53:24 - ic - [192.168.228.42] admin(Admin Users)[.Administrators][3d8192bc3d] - SESSION_IDLE_TIMEOUT in Role 'Administrators' is modified from [10] to [20]
------	----------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------

7.7 Successful TLS session

Info SYS31437 <current timestamp> <node name> [127.0.0.1] System()[] - Successful
syslog connection to peer: <Server name/IP>

Info	SYS31437	2023-02-09 10:52:34 - ic - [127.0.0.1] System()[] - Successful syslog connection to peer: '10.1.4.67'
------	----------	-------------------------------------------------------------------------------------------------------

7.8 Failure to establish a TLSC Session

7.8.1 Failure due to Invalid extension

Major SYS31377 <current timestamp> <node name> [127.0.0.1] System()[]
 – ‘Inbound Server’ Certificate <Cert Subject> has invalid extension

Major	SYS31377	2023-02-21 11:39:41 - ic - [127.0.0.1] System()[] - 'Inbound Server' Certificate 'CN=10.1.4.67, OU=CC, O=acumen, C=US' issued by 'CN=Root-ICA, OU=CC, O=acumen, C=US' has invalid extension
-------	----------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

7.8.2 Failure due to unsupported certificate type and protocols

Critical SYS31439 <current timestamp> <node name> [127.0.0.1] System()[]
 – SSL handshake with peer: <IP> failed with Error message:<error code>
 <Error message in detail>

Critical	SYS31439	2022-11-18 06:25:04 - ic - [127.0.0.1] System()[] - SSL handshake with peer: 10.1.4.67 failed with Error message: 336134527: error:1409017F:SSL routines:ssl3_get_server_certificate:wrong certificate type
Critical	SYS31439	2022-11-18 06:40:06 - ic - [127.0.0.1] System()[] - SSL handshake with peer: 10.1.4.67 failed with Error message: 336142584: error:140920F8:SSL routines:ssl3_get_server_hello:unknown cipher returned
Critical	SYS31439	2022-11-18 06:55:07 - ic - [127.0.0.1] System()[] - SSL handshake with peer: 10.1.4.67 failed with Error message: 336142597: error:14092105:SSL routines:ssl3_get_server_hello:wrong cipher returned
Critical	SYS31439	2022-11-18 07:10:11 - ic - [127.0.0.1] System()[] - SSL handshake with peer: 10.1.4.67 failed with Error message: 336122234: error:1408D17A:SSL routines:ssl3_get_key_exchange:wrong curve
Critical	SYS31439	2022-11-18 08:25:18 - ic - [127.0.0.1] System()[] - SSL handshake with peer: 10.1.4.67 failed with Error message: 336032002: error:14077102:SSL routines:SSL23_GET_SERVER_HELLO:unsupported protocol
Critical	SYS31439	2022-11-18 08:40:20 - ic - [127.0.0.1] System()[] - SSL handshake with peer: 10.1.4.67 failed with Error message: 336121979: error:1408D07B:SSL routines:ssl3_get_key_exchange:bad signature
Critical	SYS31439	2022-11-18 08:55:29 - ic - [127.0.0.1] System()[] - SSL handshake with peer: 10.1.4.67 failed with Error message: 336117909: error:1408C095:SSL routines:ssl3_get_finished:digest check failed
Critical	SYS31439	2022-11-18 09:10:35 - ic - [127.0.0.1] System()[] - SSL handshake with peer: 10.1.4.67 failed with Error message: 336150673: error:14094091:SSL routines:ssl3_read_bytes:data between ccs and finished

7.8.3 Failure due to CN and SAN

Critical SYS31051 <current timestamp> <node name> [127.0.0.1] System()[] Syslog TLS
 validation of server <server name/IP> with Client-
 Cert: <cert identifier> failed (err: <error reason>).

Critical	SYS31051	2022-11-18 13:14:55 - ic - [127.0.0.1] System()[] - Syslog TLS validation of server '10.1.4.67' with Client-Cert: 'ivanti.acumen2.com'; Server-Cert: 'CN=10.1.4.67, OU=CC, O=acumen, C=US' failed (err: There is no SAN and the CN did not match the Configured Reference Identifier)
Critical	SYS31051	2022-11-18 13:37:55 - ic - [127.0.0.1] System()[] - Syslog TLS validation of server '10.1.4.67' with Client-Cert: 'ivanti.acumen2.com'; Server-Cert: 'CN=10.1.4.67, OU=CC, O=acumen, C=US' failed (err: None of the certificate's Subject Alternative Names(SAN) match the Configured Reference Identifier)
Critical	SYS31051	2022-11-23 13:33:28 - ic - [127.0.0.1] System()[] - Syslog TLS validation of server 'foo.syslog.acumensec.local' with Client-Cert: 'ivanti.acumen2.com'; Server-Cert: 'CN=*acumensec.local, OU=CC, O=acumen, C=US' failed (err: There is no SAN and the CN did not match the Configured Reference Identifier)
Critical	SYS31051	2022-11-21 09:11:36 - ic - [127.0.0.1] System()[] - Syslog TLS validation of server 'my.syslogserv.com' with Client-Cert: 'ivanti.acumen2.com'; Server-Cert: 'CN=my.syslogserv.com, OU=CC, O=acumen, C=US' failed (err: None of the certificate's Subject Alternative Names(SAN) match the Configured Reference Identifier)

7.8.4 Failure due to failed certificate path

Critical SYS31051 <current timestamp> <node name> [127.0.0.1] System()[] Syslog TLS
 validation of server <server name/IP> with Client-
 Cert: <cert identifier> failed (err: This is an untrusted server certificate).

Critical	SYS31051	2022-11-25 07:58:07 - ic - [127.0.0.1] System()[] - Syslog TLS validation of server '10.1.4.67' with Client-Cert: 'ivanti.acumen2.com'; Server-Cert: 'CN=10.1.4.67, OU=CC, O=acumen, C=US' failed (err: This is an untrusted server certificate.)
----------	----------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

7.8.5 Failure due to expired certificate

Critical **SYS31051** <current timestamp> <node name> [127.0.0.1] System()[] Syslog TLS validation of server <server name/IP> with Client-Cert: <cert identifier> failed (err: This certificate is expired).

Critical	SYS31051	2022-11-25 08:12:08 - ic - [127.0.0.1] System()[] - Syslog TLS validation of server '10.1.4.67' with Client-Cert: 'ivanti.acumen2.com', Server-Cert: 'CN=10.1.4.67, OU=CC, O=acumen, C=US' failed (err: This certificate is expired).
----------	----------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

7.9 Failure to establish a TLSS connection

Minor **AUT24604** <current timestamp> <node name> [IP] System ()[] - SSL negotiation failed while client at source IP <IP> was trying to connect <IP>. Reason:<Reason for failure>

Minor	AUT24604	2023-02-08 11:53:53 - ic - [10.1.4.67] System()[] - SSL negotiation failed while client at source IP '10.1.4.67' was trying to connect to '10.1.4.71'. Reason: 'no shared cipher'
-------	----------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Minor	AUT24604	2023-02-08 13:38:06 - ic - [10.1.4.67] System()[] - SSL negotiation failed while client at source IP '10.1.4.67' was trying to connect to '10.1.4.71'. Reason: 'digest check failed'
-------	----------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Minor	AUT24604	2023-02-09 12:38:21 - ic - [10.1.4.67] System()[] - SSL negotiation failed while client at source IP '10.1.4.67' was trying to connect to '10.1.4.71'. Reason: 'unknown protocol'
-------	----------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

7.10 Authentication failure parameters configuration log

Info **ADM31782** <current timestamp> <node name> [IP] System ()[] - Update the account lockout period from <previous time> minutes to <updated time> minutes.

Info	ADM31782	2023-03-09 13:03:38 - ic - [192.168.254.250] admin(Admin Users)[Administrators][c70f50ed14] - Local Authentication server 'Administrators': Update the account lockout period from '11' minutes to '10' minutes.
------	----------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Info	ADM31781	2023-03-09 13:03:38 - ic - [192.168.254.250] admin(Admin Users)[Administrators][c70f50ed14] - Local Authentication server 'Administrators': Update the number of tries for account lockout from '4' to '3'.
------	----------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

7.11 Unsuccessful login attempts limit is met or exceeded

Minor **AUT22675** <current timestamp> <node name> <IP Address> <user id> - Login failed from <IP> after <no. of attempts> failed attempts. Subsequent attempts will be blocked for <time> minutes.

Minor	AUT22675	2023-02-23 06:54:47 - ic - [192.168.254.250] admin(Admin Users)[Administrators] - Login failed from 192.168.254.250 after 4 failed attempts. Subsequent attempts will be blocked for 10 minutes.
-------	----------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

7.12 Successful and unsuccessful login attempts

7.12.1 Remote connection

Info **ADM22668** <current timestamp> <node name> <IP Address> <user id> - Login succeeded for <username> Users from <IP> via management port.

Info	ADM22668	2023-03-09 13:13:09 - ic - [192.168.254.250] admin(Admin Users)[Administrators] - Login succeeded for admin/Admin Users from 192.168.254.250 via management port.
------	----------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------

Info **AUT23458** <current timestamp> <node name> <IP Address> <user id> - Login failed using auth server Administrators (Local Authentication). Reason: <Reason for failure>

Info	AUT23458	2023-02-23 06:54:34 - ic - [192.168.254.250] admin(Admin Users)[Administrators] - Login failed using auth server Administrators (Local Authentication). Reason: Invalid Credentials
------	----------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

7.12.2 Local connection

Info ADM31274 <current timestamp> <node name> [127.0.0.1] System()[] - User <username> logged in successfully through the local console

Info	ADM31274	2023-02-22 12:04:19 - ic - [127.0.0.1] System()[] - User 'admin' logged in successfully through the local console
------	----------	-------------------------------------------------------------------------------------------------------------------

Info ADM31275 <current timestamp> <node name> [127.0.0.1] System()[] - Login attempt from the local console failed for user <username>

Info	ADM31275	2022-11-29 13:10:03 - ic - [127.0.0.1] System()[] - Login attempt from the local console failed for user 'admin'
------	----------	------------------------------------------------------------------------------------------------------------------

7.13 Configure/ modify audit behaviour logs

Info ADM20601 <current timestamp> <node name> <IP Address> <user id> - Syslog server <IP/name> (facility LOCAL0, filter standard, type UDP, interface Management) removed from Admin Access logs

Info	ADM20601	2022-11-24 07:34:51 - ic - [192.168.254.203] admin(Admin Users)[Administrators][35130a2166] - Syslog server 10.1.4.67 (facility LOCAL0, filter , type TLS, interface Global) removed from Admin Access logs
------	----------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Info ADM20600 <current timestamp> <node name> <IP Address> <user id> - Syslog server <IP/name> (facility LOCAL0, filter standard, type UDP, interface Management) added for Event logs

Info	ADM20600	2022-11-23 13:58:19 - ic - [192.168.228.51] admin(Admin Users)[Administrators][a696aeac0b] - Syslog server 10.1.4.67 (facility LOCAL0, filter Standard, type TLS, interface Global) added for Admin Access logs
------	----------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

7.14 Unsuccessful attempt to validate a certificate

7.14.1 Certificate revoked

Major SYS31375 <current timestamp> <node name> <IP Address> <user id> <Realm> <Role> - <Certificate type> <Certificate subject> issued by <Cert issuer> is revoked.

Major	SYS31375	2023-02-16 11:29:05 - ic - [192.168.254.250] admin(Admin Users)[Administrators][fa680ef7c4] - 'Server CA' CN=Root-CRL-ICA1, OU=CC, O=acumen, C=US issued by 'CN=Root-CRL-CA, OU=CC, O=acumen, C=US' is revoked
-------	----------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

7.14.2 Invalid key

Major SYS31513 <current timestamp> <node name> <IP Address> <user id> <Realm> <Role> - <Certificate type> <Certificate subject> issued by <Cert issuer> has invalid key usage: cRLSign bit is not set

Major	SYS31513	2022-10-18 10:22:14 - ic - [127.0.0.1] System()[] - 'Server CA' Certificate 'CN=ICA-root-CRL5, OU=CC, O=acumen, C=US' issued by 'CN=CA-CRL5, OU=CC, O=acumen, C=US' has invalid key Usage: cRLSign bit is not set.
-------	----------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Major SYS31463 <current timestamp> <node name> [127.0.0.1] System ()[] - 'Inbound Server' Certificate <certificate subject> issued by <Cert issuer> has invalid public key

Major	SYS31463	2022-12-01 10:39:27 - ic - [127.0.0.1] System()[] - 'Inbound Server' Certificate 'CN=10.1.4.67, OU=CC, O=acumen, C=US' issued by 'CN=ICA2, OU=CC, O=acumen, C=US' has invalid public key.
-------	----------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Info ADM32221 <current timestamp> <node name> <IP Address> <user id> <Realm> <Role> - <Certificate type> <Certificate subject> issued by <Cert issuer> has invalid key

Info	ADM32221	2023-02-17 08:41:49 - ic - [127.0.0.1] System()[] - 'Inbound Server' Certificate 'CN=10.1.4.67, OU=CC, O=acumen, C=US' issued by 'CN=Root-ICA, OU=CC, O=acumen, C=US' has invalid public key.
------	----------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

7.14.3 Certificate verification failed

Critical SYS31439 <current timestamp> <node name> [127.0.0.1] System ()[][] – SSL handshake with peer <IP> failed with Error message:<error code> <error message in detail>

Critical	SYS31439	2022-12-01 10:28:30 - ic - [127.0.0.1] System()[][] - SSL handshake with peer: 10.1.4.67 failed with Error message: 336134278: error:14090086:SSL routines:ssl3_get_server_certificate:certificate verify failed
----------	----------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Critical	SYS31439	2022-11-29 13:57:38 - ic - [127.0.0.1] System()[][] - SSL handshake with peer: 10.1.4.67 failed with Error message: 218529960: error:0D0680A8:asn1 encoding routines:ASN1_CHECK_TLEN:wrong tag
----------	----------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

7.14.4 Basic Constraints failure

Info ADM32228 <current timestamp> <node name> <IP Address> <user id> <Realm> <Role> - Basic Constraints failure <Certificate type>

Info	ADM32228	2023-02-17 09:36:11 - ic - [192.168.254.250] admin(Admin Users)[Administrators][087acbc827] - Basic Constraints failure 'Server CA'
------	----------	-------------------------------------------------------------------------------------------------------------------------------------

7.15 CRL check logs

7.15.1 Certificate CRL addition

The log means Certificate CRL was added successfully.

Info ADM31374 <current timestamp> <node name> <IP Address> <user id> <Realm> <Role> – Added CDP <URL> for trusted server CA <certificate>.

Info	ADM31374	2023-03-09 05:47:34 - ic - [192.168.254.250] admin(Admin Users)[Administrators][b86e3862bc] - Added CDP 'URI:http://10.1.4.67/Root-CA-CRL.der' for Trusted Client CA 'Root-CRL-CA'
------	----------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

7.15.2 CA CRL download log

This log describes the successful CRL Download from CRL Server for the CA on the TOE.

Info SYS23068 <current timestamp> <node name> [127.0.0.1] System ()[][] – Downloaded new CRL (size in bytes) from <CA CRL URL>

Info	SYS23068	2023-02-16 10:00:04 - ic - [127.0.0.1] System()[][] - Downloaded new CRL (414 bytes) from 'http://10.1.4.67/Root-CA-CRL.der'
------	----------	------------------------------------------------------------------------------------------------------------------------------

7.15.3 CA CRL validation log

This log describes the certificate passed CRL check.

Info SYS30970 <current timestamp> <node name> <IP Address> – The X.509 certificate for <Certificate DN> successfully passed CRL checking

Info	SYS30970	2023-02-16 10:00:04 - ic - [192.168.254.250] admin(Admin Users)[Administrators][e5afe7b990] - The X.509 certificate for 'CN=Root-CRL-ICA1, OU=CC, O=acumen, C=US' issued by CN=Root-CRL-CA, OU=CC, O=acumen, C=US successfully passed CRL checking
------	----------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Info AUT30972 <current timestamp> <node name> [127.0.0.1] System ()[][] – CRL checking started for certificate <Certificate Subject DN> issued by <Issuer Subject DN>

Info	AUT30972	2023-03-09 05:47:34 - ic - [192.168.254.250] admin(Admin Users)[Administrators][b86e3862bc] - CRL checking started for certificate 'CN=Root-CRL-ICA1, OU=CC, O=acumen, C=US' issued by CN=Root-CRL-CA, OU=CC, O=acumen, C=US
------	----------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

7.16 Initiation of update

7.16.1 Update initiated

Info ADM31438 <current timestamp> <node name> <IP Address> <user id> <Realm> <Role>
- Initializing the system software upgrade process.

Major	ADM31438	2023-02-22 11:44:51 - ic - [10.1.4.67] admin(Admin Users)[.Administrators][e56f417717] - Initializing the system software upgrade process.
--------------	----------	--------------------------------------------------------------------------------------------------------------------------------------------

7.16.2 Update completed successfully

Info SYS20413 <current timestamp> <node name> [127.0.0.1] System()[][] - Started
system software version 22.2R3 (build 1369) successfully

Info	SYS20412	2023-02-22 12:00:25 - ic - [127.0.0.1] System()[][] - Starting system software version 22.2R3 (build 937)
-------------	----------	-----------------------------------------------------------------------------------------------------------

7.16.3 Update failed

Major ADM31317 <current timestamp> <node name> <IP Address> <user id> <Realm> <Role>
System software upgrade failed. The service package uploaded is not valid.

Major	ADM31317	2023-02-23 06:17:57 - ic - [10.1.4.67] admin(Admin Users)[.Administrators][1d68fe6b78] - System software upgrade failed. The service package uploaded is not valid.
--------------	----------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------

7.17 Power-on Self-Test

Info SYS10314 <current timestamp> <node name> [127.0.0.1] System()[][] - Server restart

Minor	SYS10314	2022-11-29 13:10:53 - ic - [127.0.0.1] System()[][] - Server restart
--------------	----------	----------------------------------------------------------------------

Info SYS10306 <current timestamp> <node name> [127.0.0.1] System()[][] - Starting services:
web server

Minor	SYS10306	2022-11-28 03:33:31 - ic - [127.0.0.1] System()[][] - Starting services: web server
--------------	----------	-------------------------------------------------------------------------------------

Info SYS30966 <current timestamp> <node name> [127.0.0.1] System()[][] -Web server
running in FIPS mode

Info	SYS30966	2022-11-28 03:40:14 - ic - [127.0.0.1] System()[][] - Web server running in FIPS mode
-------------	----------	---------------------------------------------------------------------------------------

End of Document