

Ivanti Connect Secure v22.2 Common Criteria Configuration Guide

Document Version: 1.2



2400 Research Blvd
Suite 395
Rockville, MD 20850

Revision History

| VERSION | DATE | CHANGES |
|---------|------------|------------------------|
| 1.0 | 10-06-2023 | Initial Release |
| 1.1 | 12-15-2023 | ECR comments addressed |
| 1.2 | 02-01-2024 | Minor update |

Contents

| | |
|---|-----------|
| Common Criteria Configuration Instructions | 7 |
| 1. Introduction..... | 7 |
| 1.1. Audience..... | 7 |
| 1.2. Purpose..... | 7 |
| 1.3. Supported TOE Platforms..... | 7 |
| 1.4. Operational Environment | 8 |
| 2. Commissioning the Appliances | 9 |
| 2.1. Secure Acceptance of the TOE..... | 9 |
| 2.2. Physical Installation | 10 |
| 2.3. Initial Setup Through Serial Console..... | 10 |
| 2.4. Connect Administrator Web Console | 11 |
| 2.5. Configuring External, Management Interfaces/Ports | 12 |
| 2.5.1. Configure external port..... | 12 |
| 2.5.2. Configure management port | 12 |
| 2.6. Configuring DNS Server..... | 13 |
| 2.7. Set System time..... | 14 |
| 2.8. Software updates | 14 |
| 2.9. Software Version Verification | 16 |
| 2.9.1. Version verification via GUI..... | 16 |
| 2.9.2. Version verification via local console | 16 |
| 3. TOE configuration | 18 |
| 3.1. Prerequisites for TOE Configuration..... | 18 |
| 3.2. System Reboot | 18 |
| 3.3. Password Minimum Length Configuration | 18 |
| 3.4. Reset Password | 20 |
| 3.5. User Creation..... | 21 |
| 3.5.1. User Creation via GUI | 21 |
| 3.5.2. User Creation via Console | 22 |
| 3.6. Role Mapping..... | 23 |
| 3.7. Serial Console Access Control Configuration..... | 24 |
| 3.8. Logging into the Console | 25 |
| 3.9. Terminating a Local Console Session..... | 26 |
| 3.10. Administrative Banner Configuration | 26 |

- 3.11. Enable NDcPP mode 29
- 3.12. Disable NDcPP mode via the Console 32
- 3.13. Configure Inactivity Timeout Period 32
- 3.14. Terminating a GUI Session..... 33
- 3.15. Configuring authentication lockout 33
- 3.16. Import Trusted Client CA..... 34
- 3.17. Import Trusted Server CA..... 37
- 3.18. Device Certificates..... 38
 - 3.18.1. Generate RSA or ECC Certificate 39
- 3.19. Configure Secure Channel to Syslog Server 45
- 3.20. Import Client Auth Certificate..... 46
- 3.21. Configuring Syslog Server 47
 - 3.21.1. Configure Syslog Server for Event Log 47
 - 3.21.2. Configure Syslog Server for Admin Access Log 48
 - 3.21.3. Configure Syslog Server for User Access Log 48
- 3.22. Configure Syslog Server Parameters 49
- 3.23. CRL checking configuration 50
 - 3.23.1. Understanding CRL 50
 - 3.23.2. Enable CRL checking 52
- 3.24. Removing Cached CRL Entry of CA Chain 54
- 3.25. Delete CA Chain from Trusted Client CA..... 55
- 3.26. Delete CA Chain from Trusted Server CA 56
- 3.27. Zeroization process 57
- 4. Self-Test..... 58
- 5. Hash Functions..... 60
- 6. Keyed Hash Cryptographic Operation (Keyed Hash Algorithm) 61
- 7. Sample audit logs..... 62
 - 7.1. Audit log records 62
 - 7.2. Audit Data Generation..... 63
 - 7.2.1. Start-up and shutdown of the audit functions..... 63
 - 7.2.2. Administrative login and logout 63
 - 7.2.3. Console access 63
 - 7.2.4. Changes to TSF data related to configuration changes..... 64
 - 7.2.5. Generating/import of, changing, or deleting of cryptographic keys..... 64

- 7.2.6. Resetting passwords 65
- 7.3. NDCPP and FIPS mode 65
- 7.4. HTTPS session 67
- 7.5. Access banner configuration logs..... 67
- 7.6. Session inactivity time configuration log..... 67
- 7.7. Successful TLS session 67
- 7.8. Failure to establish a TLSC Session 67
 - 7.8.1. Failure due to Invalid extension 67
 - 7.8.2. Failure due to unsupported certificate type and protocols 68
 - 7.8.3. Failure due to CN and SAN 68
 - 7.8.4. Failure due to failed certificate path 69
 - 7.8.5. Failure due to expired certificate..... 69
- 7.9. Failure to establish a TLSS connection 69
- 7.10. Authentication failure parameters configuration log..... 69
- 7.11. Unsuccessful login attempts limit is met or exceeded 69
- 7.12. Successful and unsuccessful login attempts 70
 - 7.12.1. Remote connection 70
 - 7.12.2. Local connection 70
- 7.13. Configure/ modify audit behaviour logs 70
- 7.14. Unsuccessful attempt to validate a certificate 71
 - 7.14.1. Certificate revoked 71
 - 7.14.2. Invalid key..... 71
 - 7.14.3. Certificate verification failed..... 71
 - 7.14.4. Basic Constraints failure 71
- 7.15. CRL check logs..... 72
 - 7.15.1. Certificate CRL addition 72
 - 7.15.2. CA CRL download log 72
 - 7.15.3. CA CRL validation log 72
- 7.16. Initiation of update 72
 - 7.16.1. Update initiated 72
 - 7.16.2. Update completed successfully..... 73
 - 7.16.3. Update failed 73
- 7.17. Power-on Self-Test..... 73
- 8. Reference Documents..... 74

Common Criteria Configuration Instructions

Follow the instructions in this document to install Ivanti connect secure, and to make the configuration changes required after installation to bring the system into “Common Criteria mode”. This document is a guide to the Ivanti connect secure implementation of the Common Criteria Network Device Protection Profile v2.2e (NDcPP).

1. Introduction

1.1. Audience

This document is written for administrators configuring the TOE, specifically the Ivanti Connect Secure. To use this guide, you need a broad understanding of networks in general and the internet in particular, networking principles, and network configuration. All the Sections in the Document is written in a sequence based on what all steps administrator has to do when received a brand new Ivanti Connect Secure Device.

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 that are necessary to configure and maintain the TOE in the evaluated configuration as defined in the Security Target [Ivanti Connect Secure 22.2 Security Target]. This document does not mandate configuration settings for the features of the TOE that are outside the evaluation scope.

1.3. Supported TOE Platforms

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

| 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 Connect 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.

| 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 Security target [Ivanti Connect Secure 22.2 Security Target].

1. 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

- 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 with tampered 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 Secure 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 services.
- 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 of the TOE 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 if the needs arise.

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 Connect Secure <release version>
5. Enter **1** to install the Ivanti Connect 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 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:

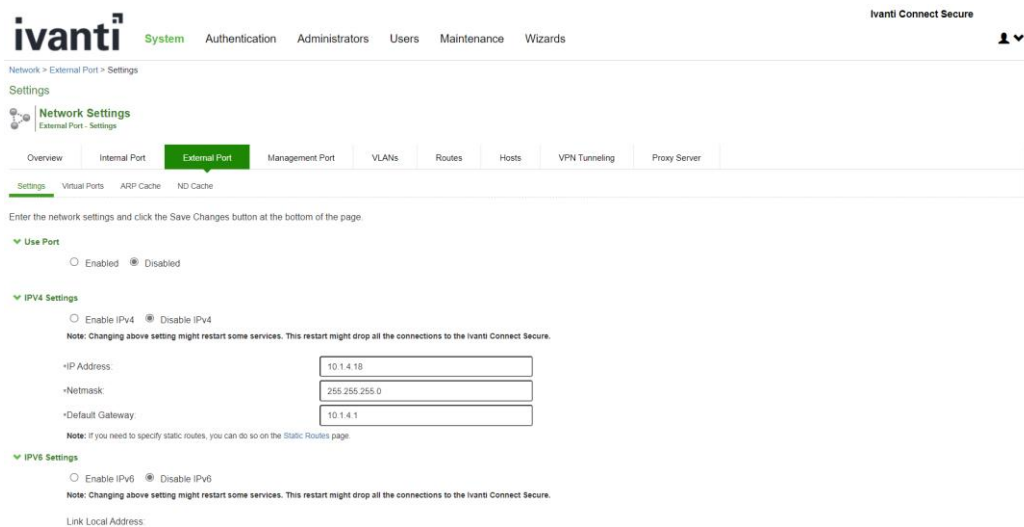
1. Launch a web browser from a laptop that is network connected.
2. Point the browser at the same IP address that was assigned to the internal port followed by /admin (for example, <https://a.b.c.d/admin>).
3. When prompted with the security alert to proceed without a signed certificate, click **Yes**. 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



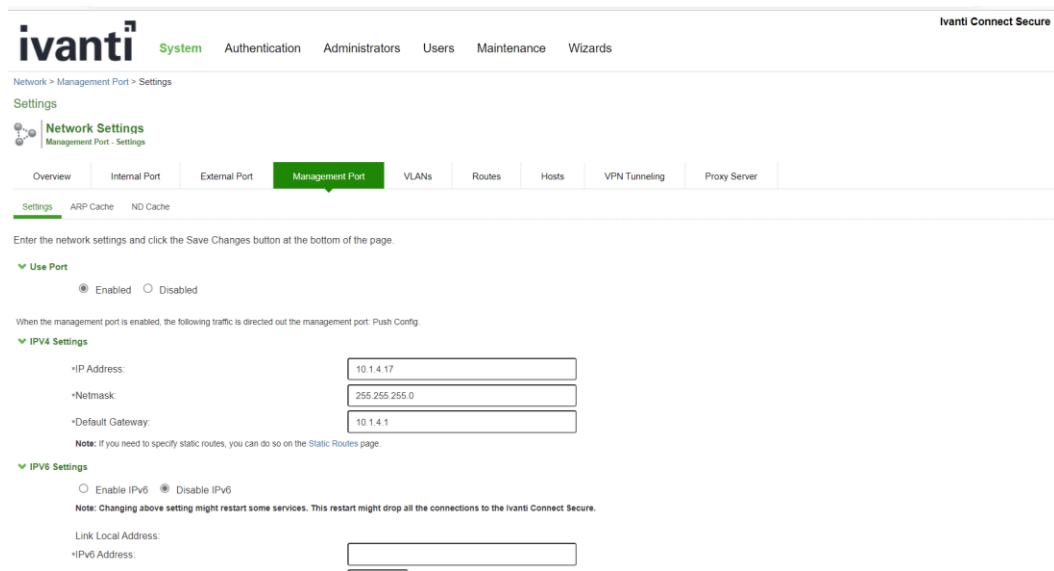
2.5.2. Configure management port

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**

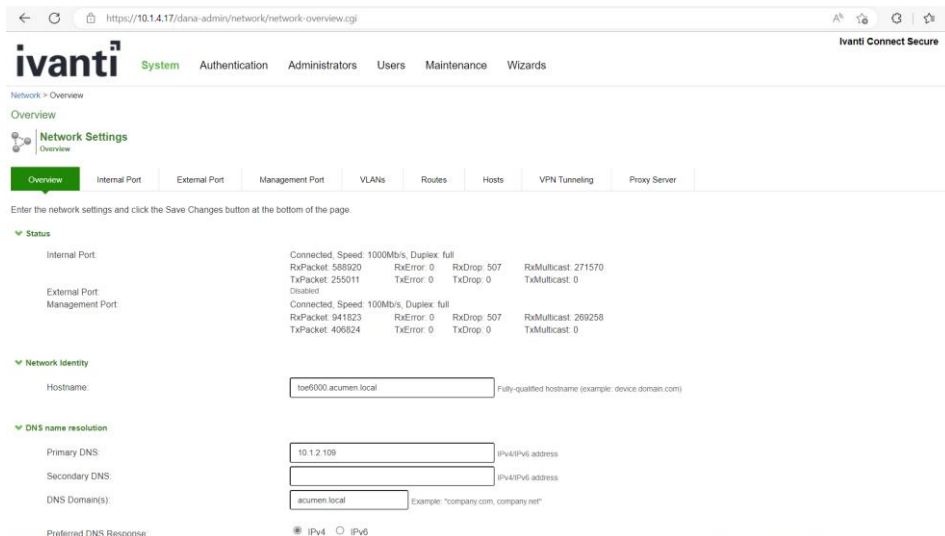
3. Enter IP address, Netmask, and Default Gateway



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 Maintenance Wizards Ivanti Connect Secure

Status > Overview > Date and Time

Date and Time

System Date 2/6/2023
System Time 1:03:56 PM
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)

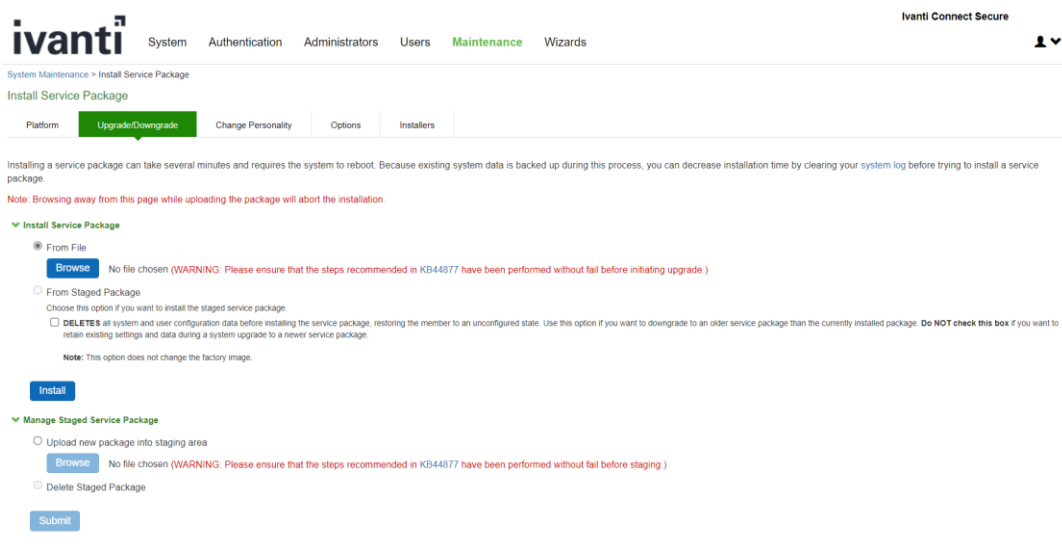
Note: Save Changes will result in restarting of services which will disconnect all the connected users.

2.8. Software updates

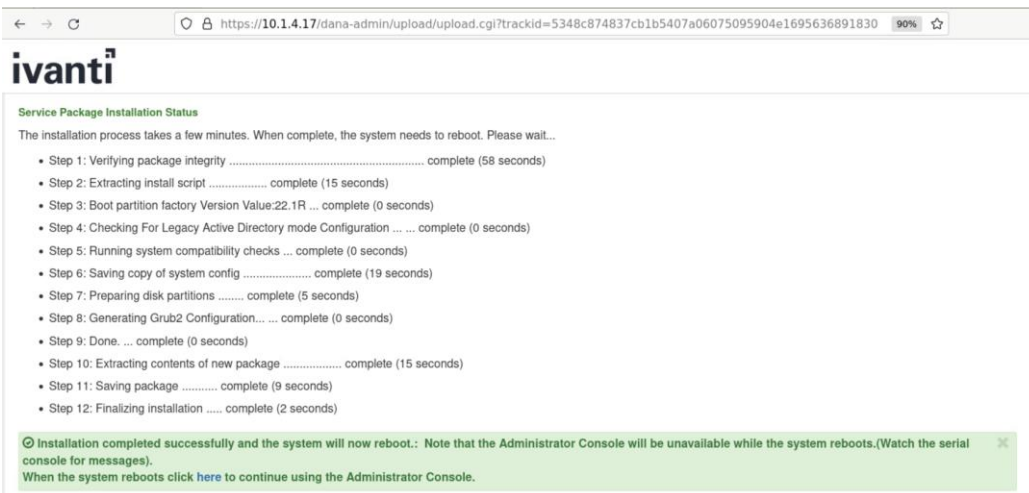
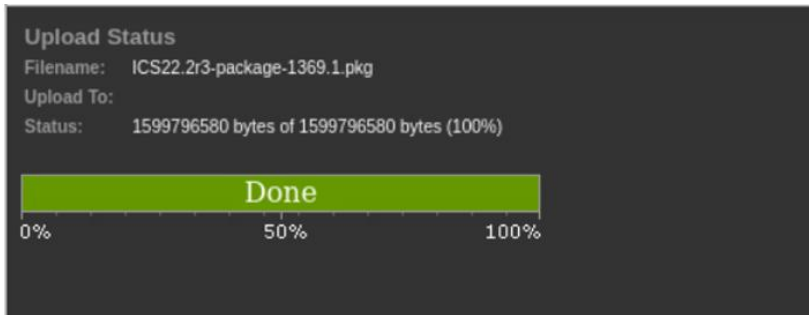
If a new NDcPP-compliant software package is available, follow the instructions in this section to update the software package on the TOE. The verification of the authenticity of the software package is performed by digital signature verification.

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

5. Click **Install** to start the installation process



6. Once package is uploaded, integrity check is done system validates the image, installation is completed.



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.

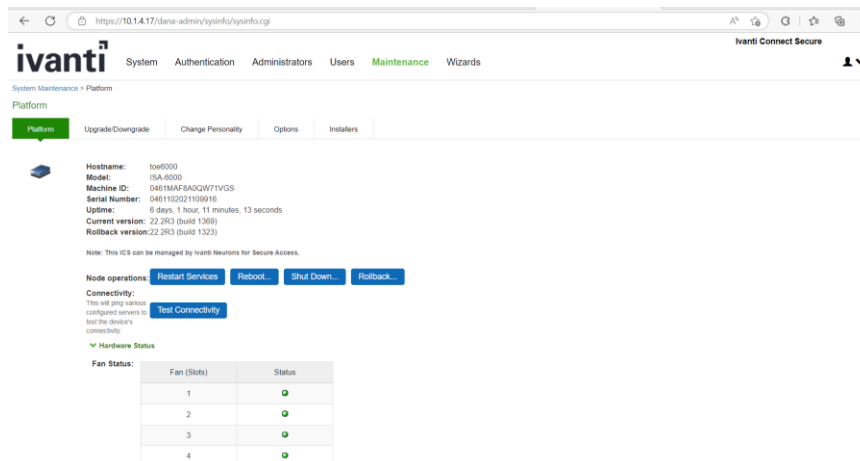
The public key is distributed as part of the firmware package. Ivanti Secure retains control over the private key used to sign firmware updates. If the signature check is successful, the TSF installs the update.

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. The following feature is used, Navigate to **Maintenance > Platform**



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 1459)  
Rollback version: 22.2R3 (build 1437)  
Reset version: 22.1R1 (build 421) Ivanti Connect Secure  
                22.1R1 (build 211) Ivanti Policy Secure  
  
Licensing Hardware ID: 0482M56LE04PO0PQS  
Serial Number: 0482032022100249  
  
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: 
```

3. TOE configuration

3.1. Prerequisites for TOE Configuration

- You've configured the TOE as per the instructions in [Commissioning the Appliance](#).
- 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 connect 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

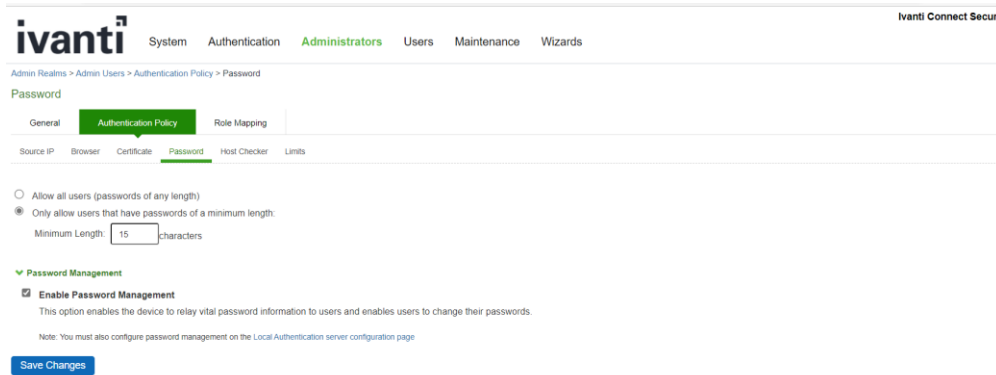
```
Please choose the operation to perform:
 1. Reboot this Ivanti Connect Secure
 2. Shutdown this Ivanti Connect Secure
 3. Restart services at this Ivanti Connect Secure
 4. Rollback this Ivanti Connect Secure
 5. Factory reset this Ivanti Connect Secure
 6. Clear all configuration data at this Ivanti Connect Secure
 7. Install self-signed certificate
21. Clear all session data at this Ivanti Connect Secure
22. Clear all Named Users at this Ivanti Connect Secure
24. Clear behavioral analytics database
31. Clean up diskspace on this Ivanti Connect 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 Connect Secure? (y/n) y
Doing reboot.
Reboot action message: user initiated, via serial console
```

3.3. Password Minimum Length Configuration

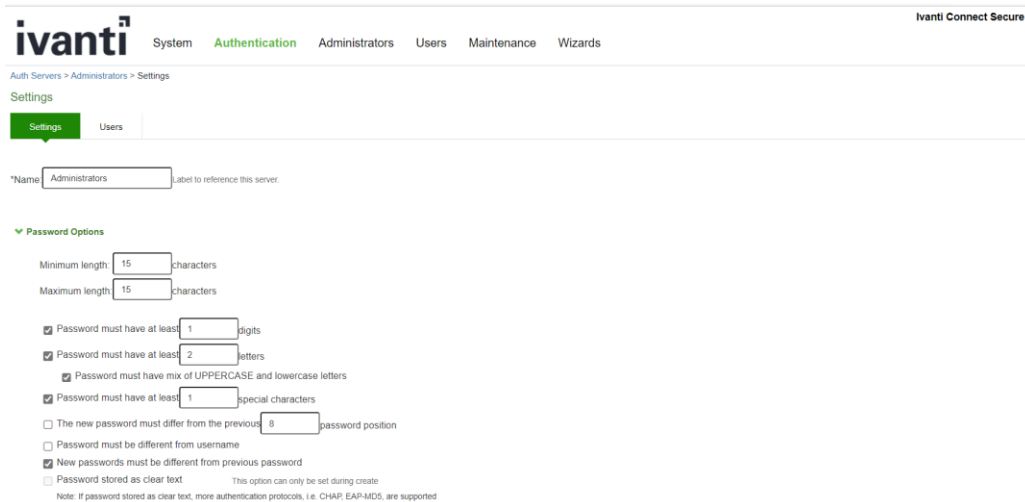
On Administrator Web Console, follow the below instruction to set the administrator minimum password length to 15.

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**

The screenshot shows the Ivanti Connect Secure web console interface. The breadcrumb navigation is "Auth Servers > Administrators > Users". The "Users" tab is active. Below the navigation, there are search and filter options: "Show users named" with an input field, "Show 200 users", and an "Update" button. There are also buttons for "New...", "Delete...", and "Unlock...". Below this is a table of users with columns for Username, Name, Console Access, Date&Time, IPAddress, Agent, and Status. The 'admin' user is highlighted.

| | Username | Name | Console Access | Last Sign-in Statistic | | | Status |
|-------------------------------------|-----------|------------------------|----------------|------------------------|-----------------|---|--------|
| | | | | Date&Time | IPAddress | Agent | |
| <input type="checkbox"/> | acumensec | Platform Administrator | Yes | 2023/02/15 08:11:46 | 192.168.228.46 | Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/110.0.0.0 Safari/537.36 Edg/110.0.1587.41 | |
| <input checked="" type="checkbox"/> | admin | Platform Administrator | Yes | 2023/02/24 13:07:25 | 192.168.254.203 | Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/110.0.0.0 Safari/537.36 Edg/110.0.1587.50 | |
| <input type="checkbox"/> | correct1 | correct1 | Yes | 2022/09/13 19:13:24 | | | |

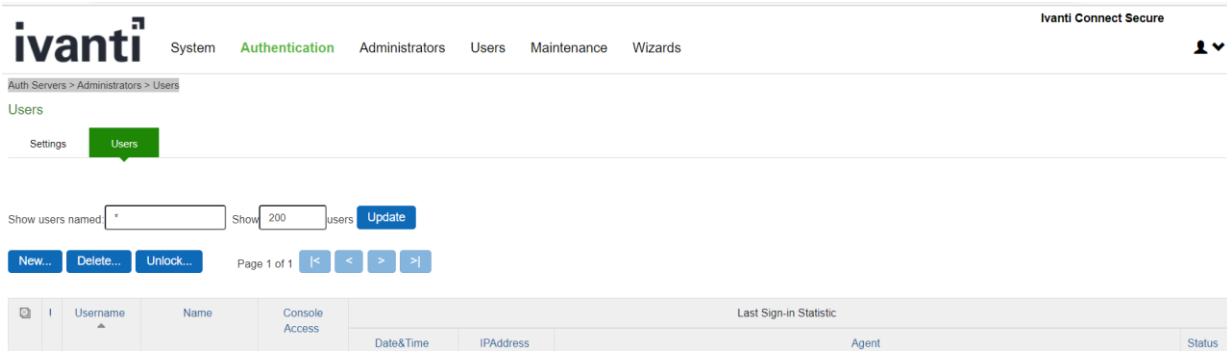
Select the username and click on **reset password** and click on save changes

The screenshot shows the "Update Administrator acumensec" configuration page in the Ivanti Connect Secure web console. The breadcrumb navigation is "Auth Servers > Administrators > Users > Update Administrator acumensec". The "Full Name" field contains "Platform Administrator" and "Authenticate using" is set to "Administrators". There are two radio button options: "Reset Password" (selected) and "Change Password". Below these are several checkboxes for user management settings: "One-time use (disable account after the next successful sign-in)", "Allow console access" (checked), "Allow access to REST APIs" (checked), "Enabled" (selected), "Disabled", "Quarantined", and "Require user to change password at next sign in". 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." A "Save Changes" button is at the bottom left.

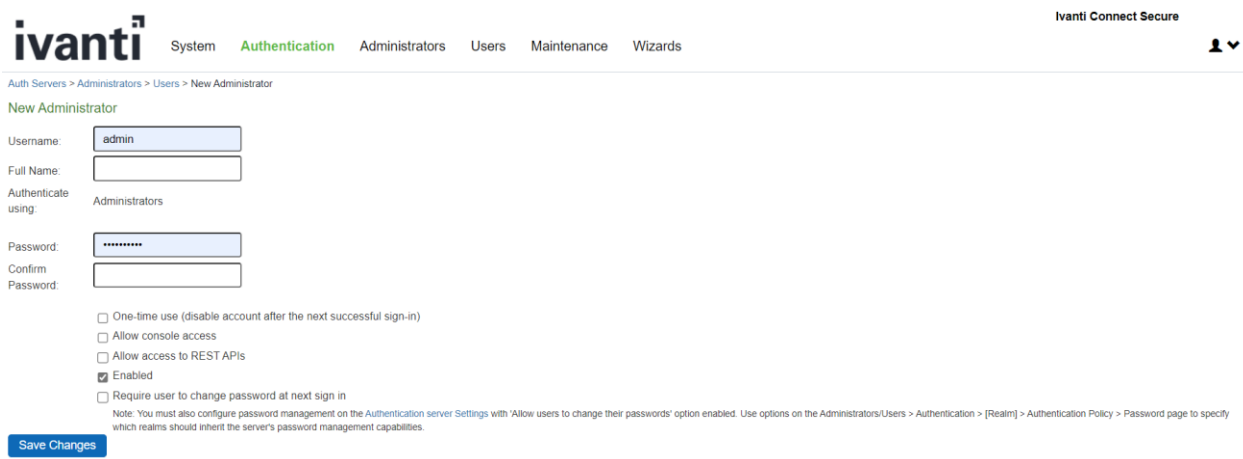
3.5. User Creation

3.5.1. User Creation via GUI

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



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



3.5.2. User Creation via Console

Login into the console

1. Select the option **2. Create admin username and password**

```
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 1433)
Rollback version: 22.2R3 (build 1369)
Reset version: 22.1R1 (build 421) Ivanti Connect Secure
                22.1R1 (build 211) Ivanti Policy Secure

Licensing Hardware ID: 0482M56LE04PO0PQS
Serial Number: 0482032022100249

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: 2

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

2. Mention username and password you want to create

```
11. Exit Serial Console Session
Choice: 2

Please create an administrator username and password.
Admin username: testadmin1

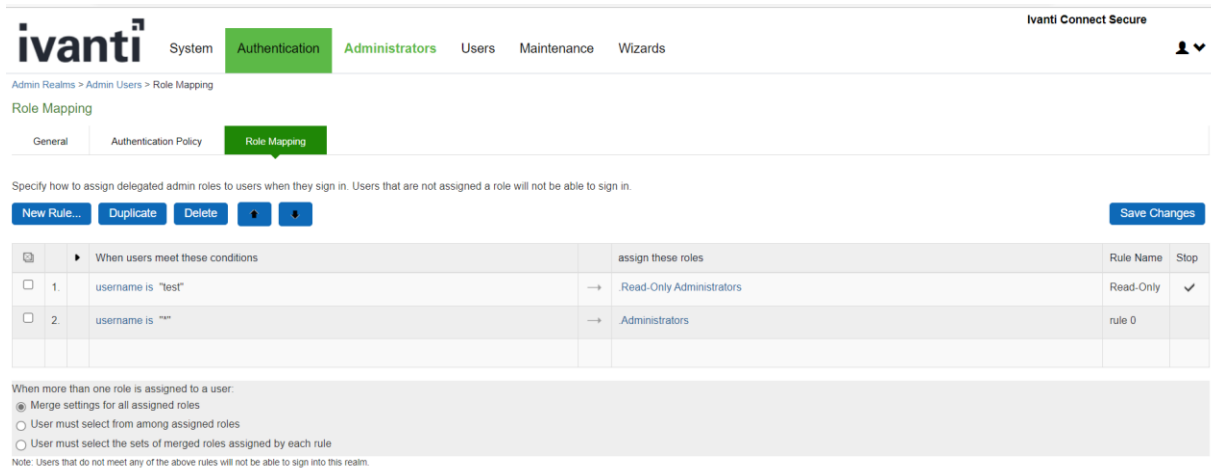
Password:
Confirm password:
Do you want to enable REST API access for this administrator (y/n): y

The administrator testadmin1 was successfully created.
```

3.6. Role Mapping

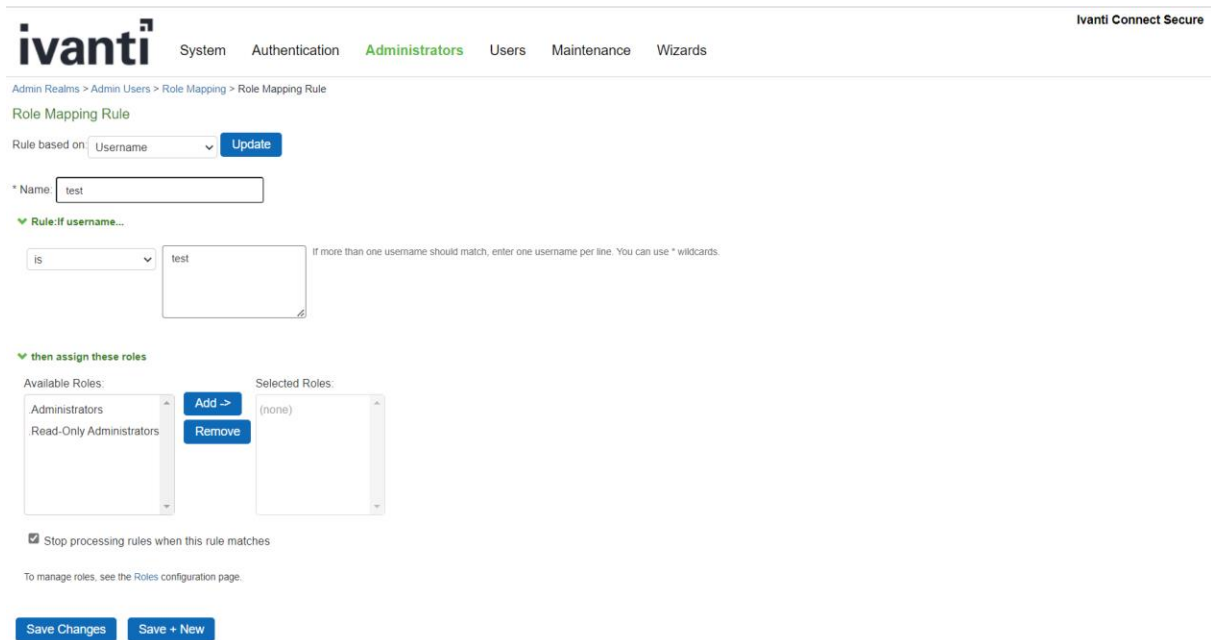
Assign privilege level to users using role mapping.

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



- 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



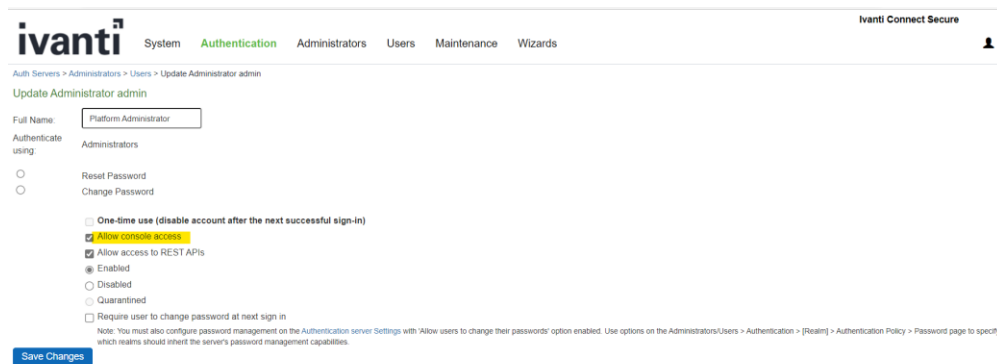
3.7. Serial Console Access Control Configuration

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

Step1, 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 [Initial Setup Through Serial Console](#)
5. Click on **Allow console access** checkbox
6. Click on **Save Changes**



Step2, 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 1369)
Rollback version: 22.2R3 (build 1323)
Reset version: 22.1R1 (build 421) Ivanti Connect Secure
                22.1R1 (build 211) Ivanti Policy Secure

Licensing Hardware ID: 0461MAF8A0QW71VGS
Serial Number: 0461102021109916

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: █
```

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 (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: █
```

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.

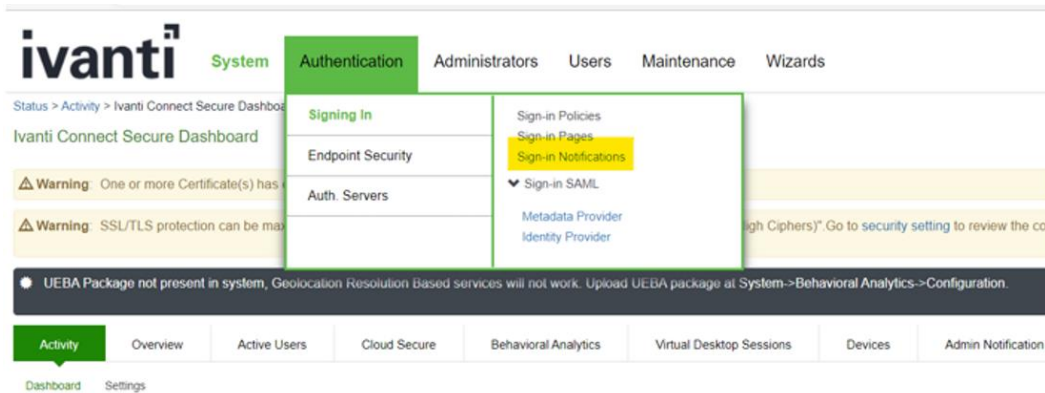
```
Please choose from among the following options:
 1. Network Settings and Tools
 2. Create admin username and password
 3. Display log/status
 4. System Operations
 5. Toggle password protection for the console (On)
 6. Create a Super Admin session
 7. System Maintenance
 8. Turn off NDcPP Mode and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

3.10. Administrative Banner Configuration

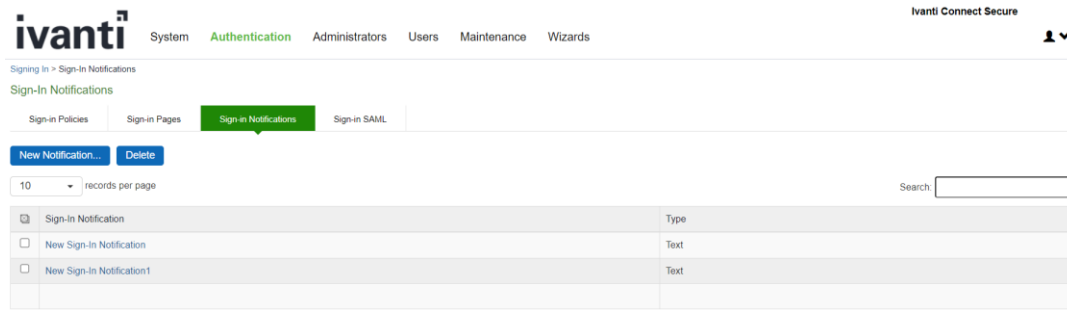
Configure administrator banner for the Administrator Web Console and the local serial console is a two- step process.

Step1, create a Sign-in notification. On Administrator Web Console:

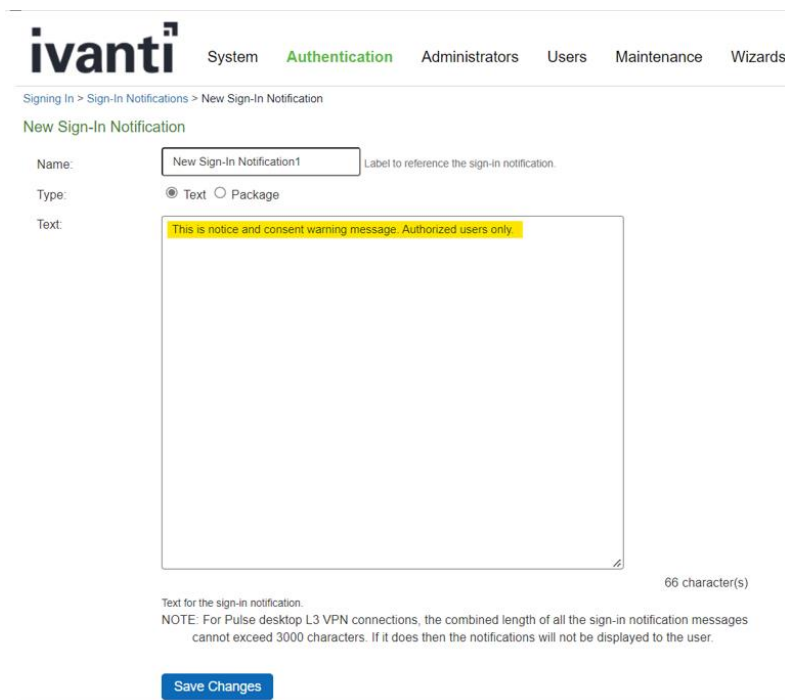
1. Navigate to **Authentication -> Signing In -> Sign-in Notifications**



2. This screen is shown



3. Click on **New Notification**



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.**

https://10.14.17/dana-admin/auth/signinPolicy.cgi

ivanti System **Authentication** Administrators Users Maintenance Wizards

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

*/admin/

User type: Users Administrators Authorization Only Access

Sign-in URL: Format: <host>/<path>/; Use * as wildcard in the beginning of the host name.

Description:

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.

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.

ivanti System **Authentication** Administrators Users Maintenance V

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 (page).

Available realms:

Selected realms:

Configure Fallback Uri

Fallback to next available url if auth server unreachable Supported Auth Servers: Active Directory and LDAP

Configure SignIn Notifications

Pre-Auth Sign-in Notification

Post-Auth Sign-in Notification

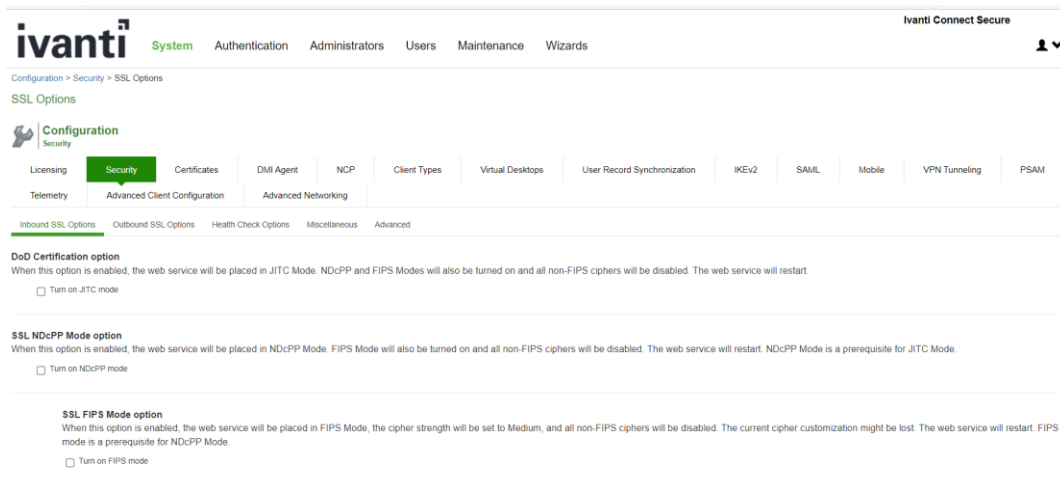
5. Click on **Save Changes**

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

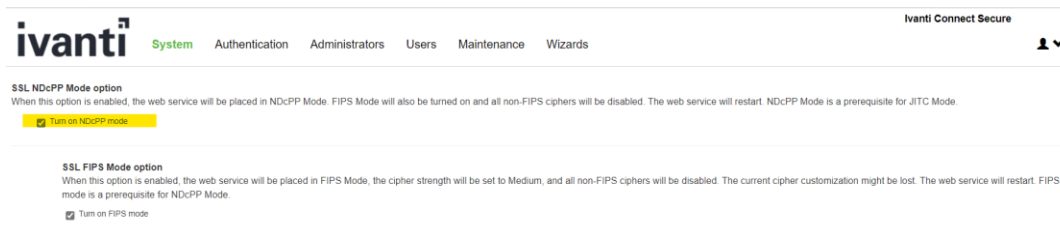
3.11. Enable NDcPP mode

On Administrator Web Console,

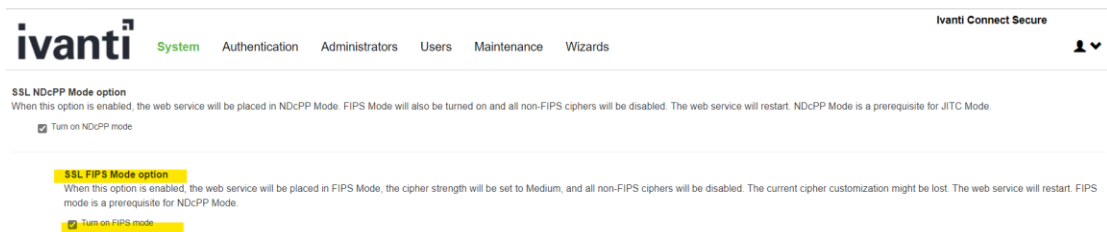
1. Navigate to **System -> Configuration > Security > Inbound SSL Options**



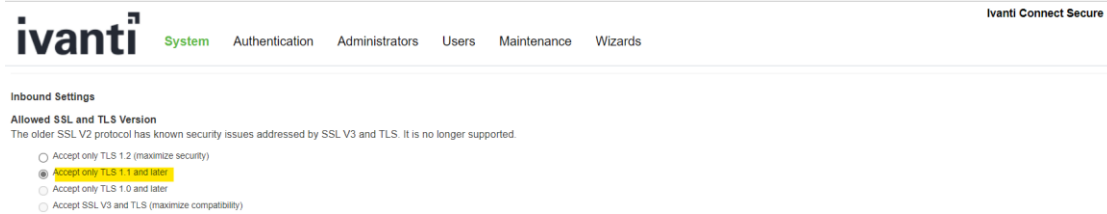
2. Click on **Turn on NDcPP mode** checkbox to make the TOE common criteria compliant



3. Once **Turn on NDcPP mode** is enabled, **Turn on FIPS mode** is also automatically enabled.

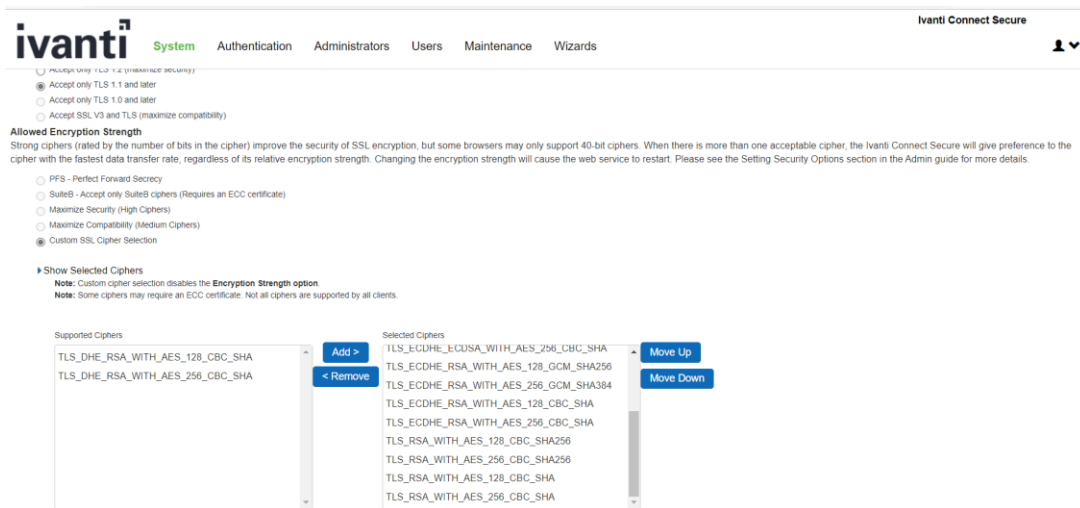


4. Once NDcPP mode is selected, **Accept only TLS 1.1 and later** is selected by default.



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

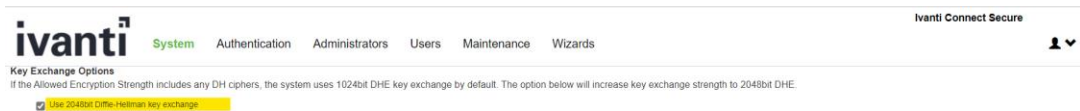
5. Custom SSL Cipher Selection Allowed Encryption Strength are automatically selected. Click on displays below 16 Ciphers in the right panel labelled **Selected Cipher**. **Show Selected Ciphers**



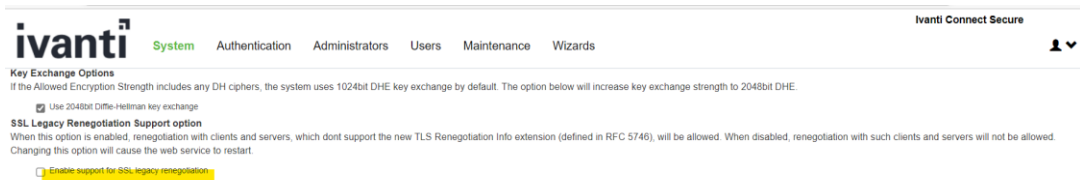
Select TLS_DHE_RSA_WITH_AES_128_CBC_SHA and TLS_DHE_RSA_WITH_AES_256_CBC_SHA on the right panel, and click “Remove” button to remove it from the “Selected Ciphers”.

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

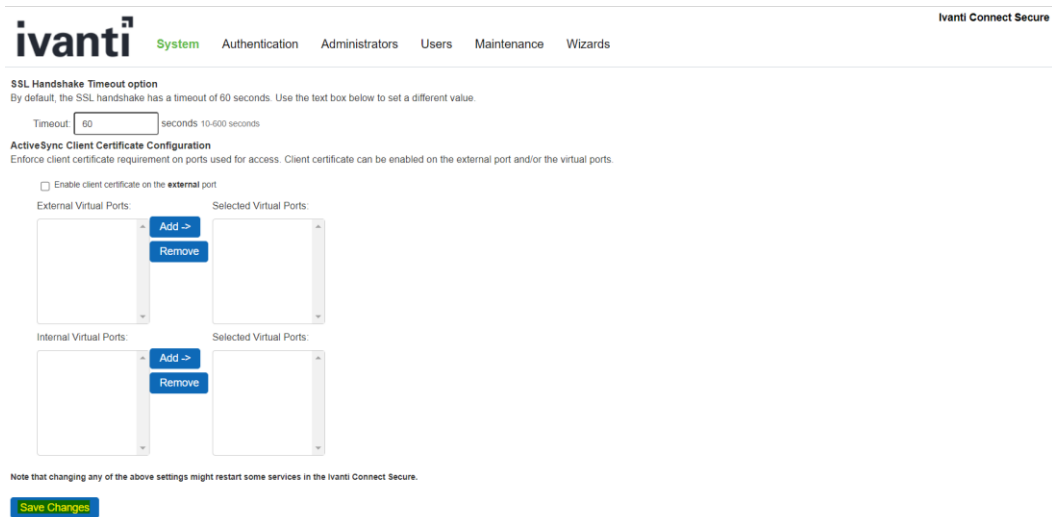
6. Enable **Use 2048 bit Diffie-Hellman key exchange checkbox**



7. Uncheck **SSL Legacy Renegotiation Support option**

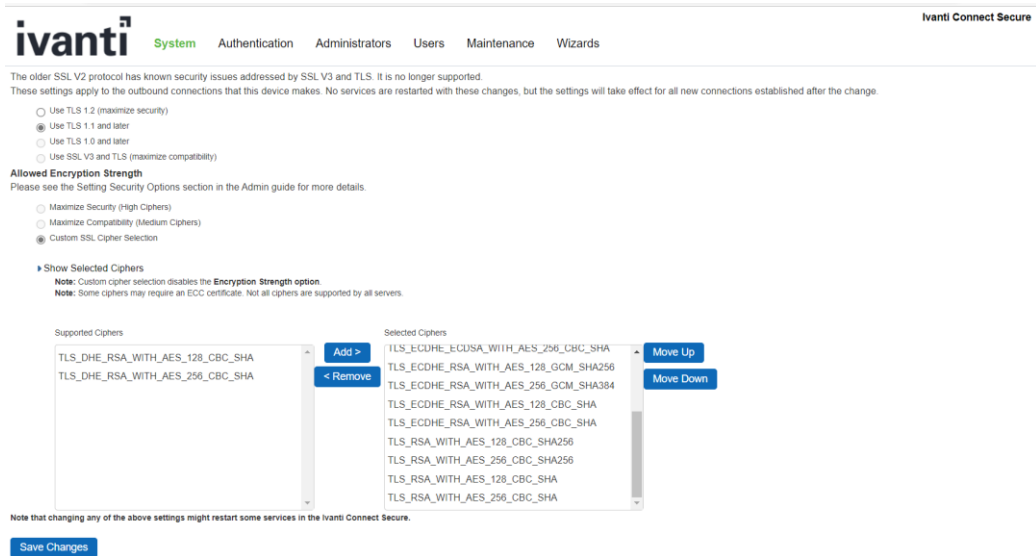


8. Click on **Save Changes**



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 below log to confirm NDcPP mode is enabled

- 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 1369)
Rollback version: 22.2R3 (build 1323)
Reset version: 22.1R1 (build 421) Ivanti Connect Secure
                22.1R1 (build 211) Ivanti Policy Secure

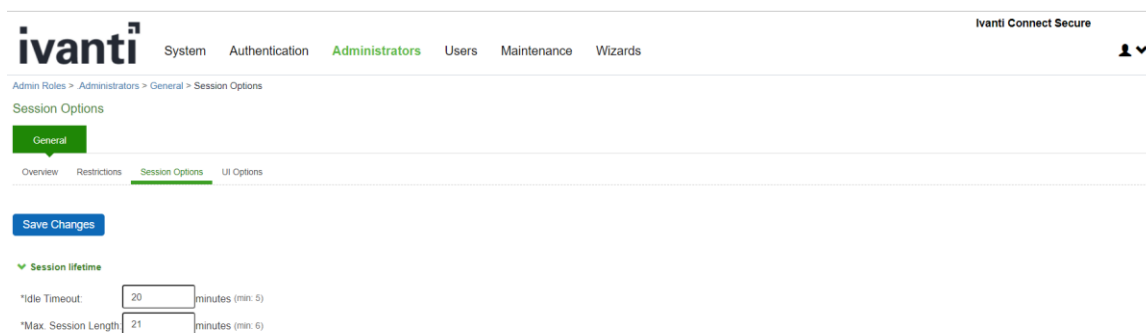
Licensing Hardware ID: 0461MAF8A0QW71VGS
Serial Number: 0461102021109916

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**



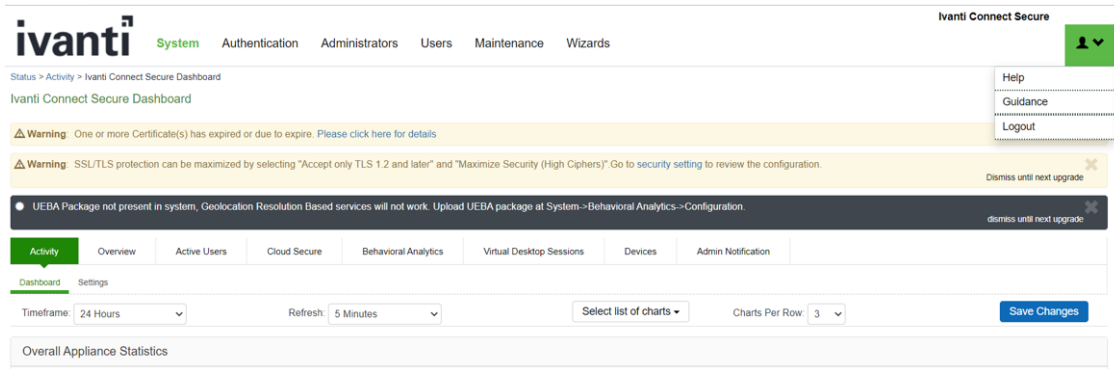
2. Under the 'Session lifetime' section, enter the Idle timeout in minutes.

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

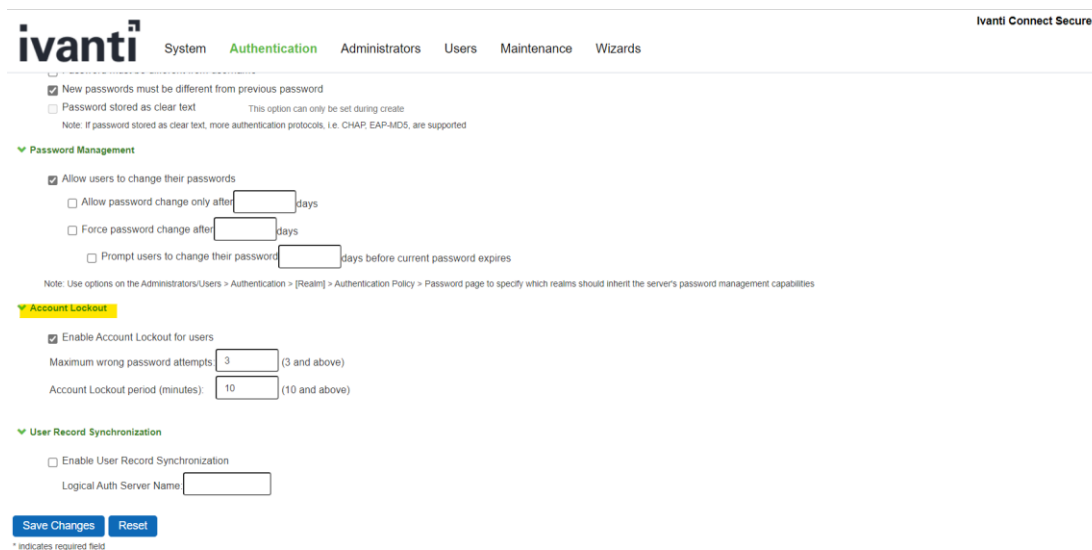
To log out of the web administrative session, on any screen click on the “Logout” link at the top right of the screen.



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.

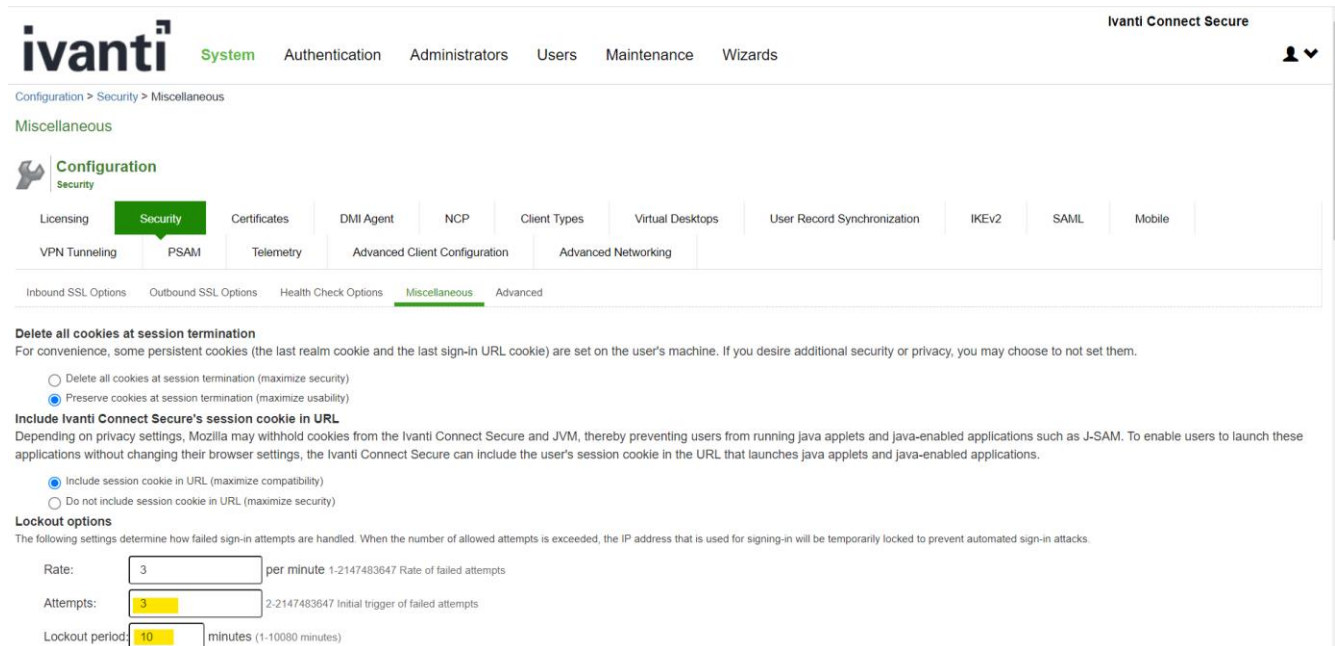
- Maximum wrong password attempts should be configured to be 3 and above (Max 10).
- If the user enters an incorrect password the configured number of times, the user is

locked out they cannot login through any remote interface on the TOE.

- 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 **Authentication > Auth Servers > Administrators > Settings**



The screenshot shows the Ivanti Connect Secure web console interface. The top navigation bar includes the Ivanti logo, 'System', and various menu items like 'Authentication', 'Administrators', 'Users', 'Maintenance', and 'Wizards'. The breadcrumb trail is 'Configuration > Security > Miscellaneous'. The 'Miscellaneous' configuration page is displayed, with a sidebar menu on the left containing 'Configuration' and 'Security'. The main content area has a grid of tabs: 'Licensing', 'Security' (selected), 'Certificates', 'DMI Agent', 'NCP', 'Client Types', 'Virtual Desktops', 'User Record Synchronization', 'IKEv2', 'SAML', and 'Mobile'. Below this is another row of tabs: 'VPN Tunneling', 'PSAM', 'Telemetry', 'Advanced Client Configuration', and 'Advanced Networking'. At the bottom of the grid are 'Inbound SSL Options', 'Outbound SSL Options', 'Health Check Options', 'Miscellaneous' (selected), and 'Advanced'. The 'Miscellaneous' section contains three main settings:

- Delete all cookies at session termination:** A heading followed by a note: 'For convenience, some persistent cookies (the last realm cookie and the last sign-in URL cookie) are set on the user's machine. If you desire additional security or privacy, you may choose to not set them.' Two radio buttons are present: 'Delete all cookies at session termination (maximize security)' (unselected) and 'Preserve cookies at session termination (maximize usability)' (selected).
- Include Ivanti Connect Secure's session cookie in URL:** A heading followed by a note: 'Depending on privacy settings, Mozilla may withhold cookies from the Ivanti Connect Secure and JVM, thereby preventing users from running java applets and java-enabled applications such as J-SAM. To enable users to launch these applications without changing their browser settings, the Ivanti Connect Secure can include the user's session cookie in the URL that launches java applets and java-enabled applications.' Two radio buttons are present: 'Include session cookie in URL (maximize compatibility)' (selected) and 'Do not include session cookie in URL (maximize security)' (unselected).
- Lockout options:** A heading followed by a note: '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.' Below this are three input fields: 'Rate' (3) per minute, 'Attempts' (3), and 'Lockout period' (10) minutes.

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

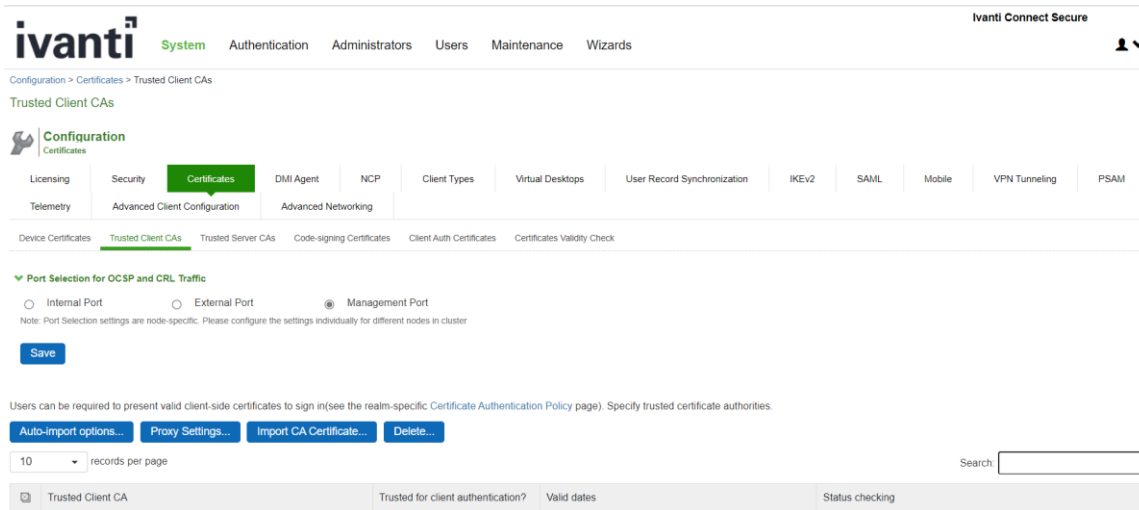
3.16. Import Trusted Client CA

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

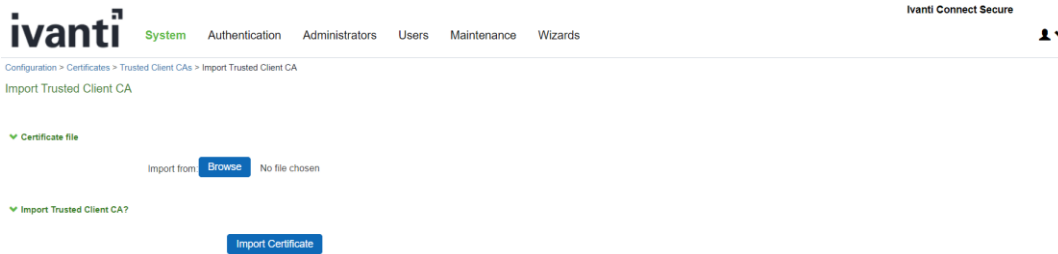
On Administrator Web Console,

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

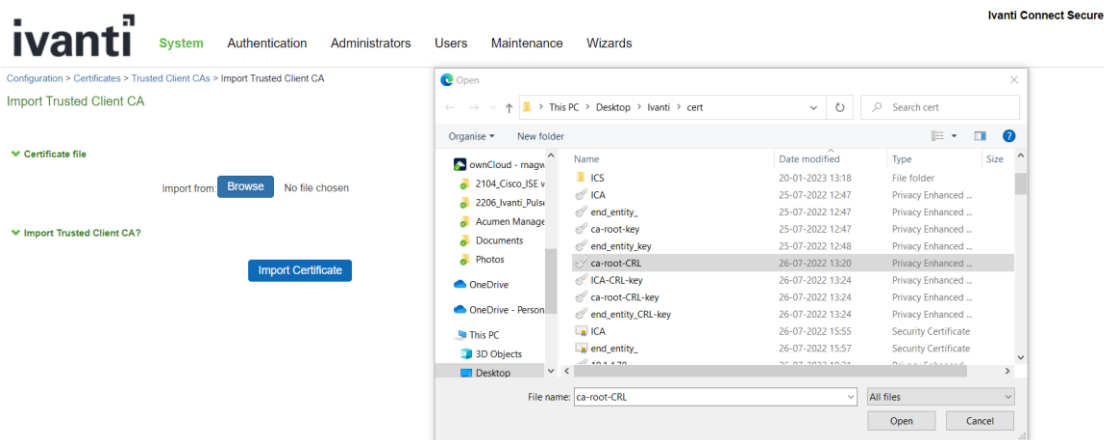
Ivanti Connect Secure v22.2 Common Criteria Configuration Guide



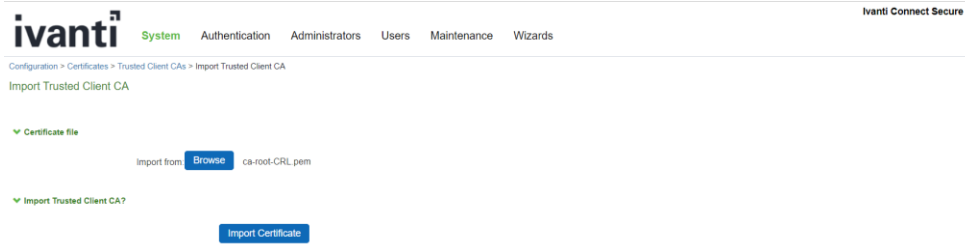
2. Click **Import CA Certificates...** to import CA or Chain of CAs one by one as explained below in different Screenshots



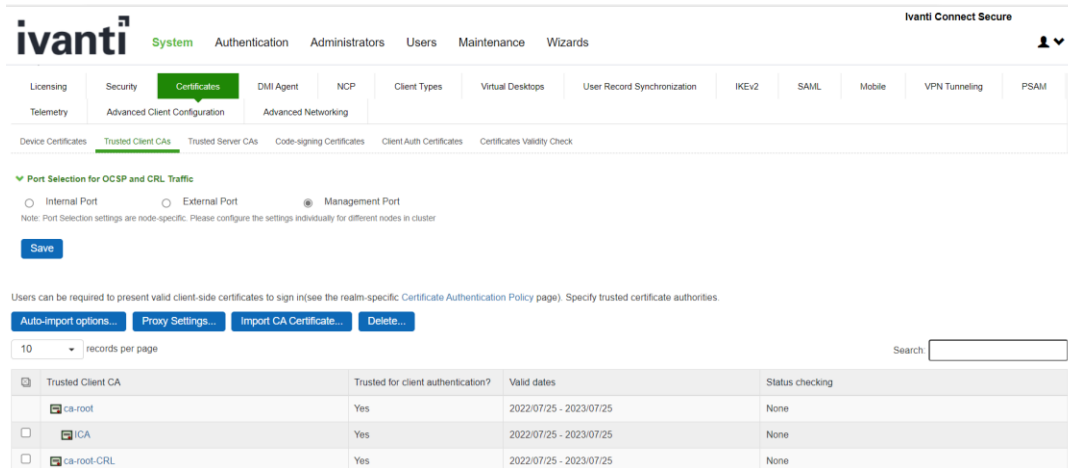
3. Click on **Browse** and select the certificate, then click on **Import Certificate**



Ivanti Connect Secure v22.2 Common Criteria Configuration Guide



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



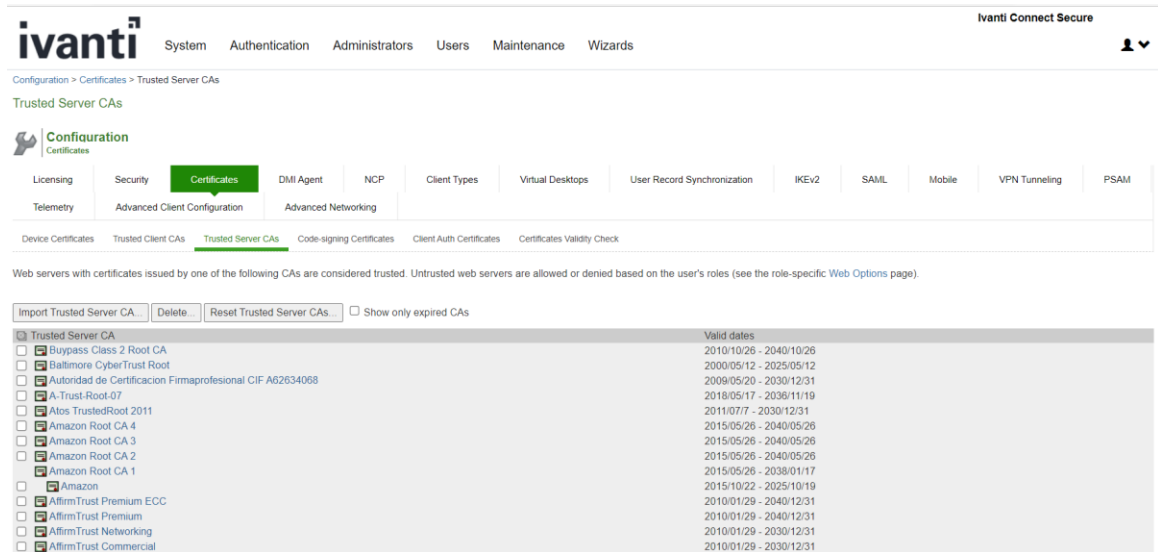
3.17. Import Trusted Server CA

Trusted Server CA is used in two situations:

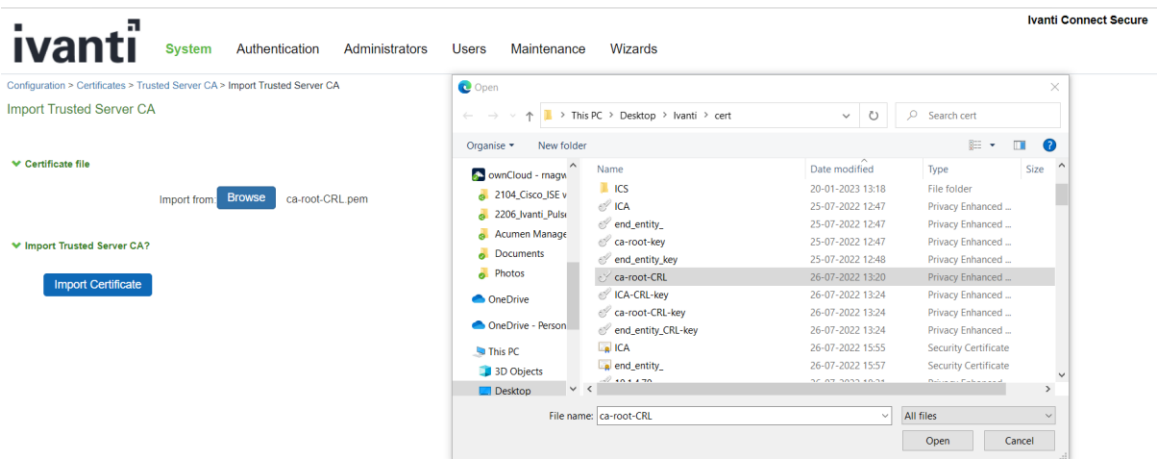
To validate the device certificate that is generated for TLS handshake when a TLS client is connecting to the TOE. To validate the server certificate received in TLS handshake when the TOE connects to syslog server.

On Administrator Web Console,

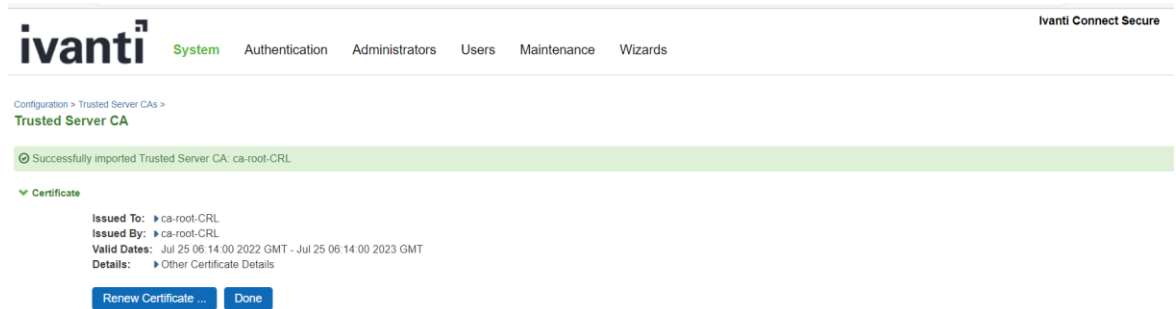
1. Navigate to **System > Configuration > Certificates > Trusted Server CAs.**



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

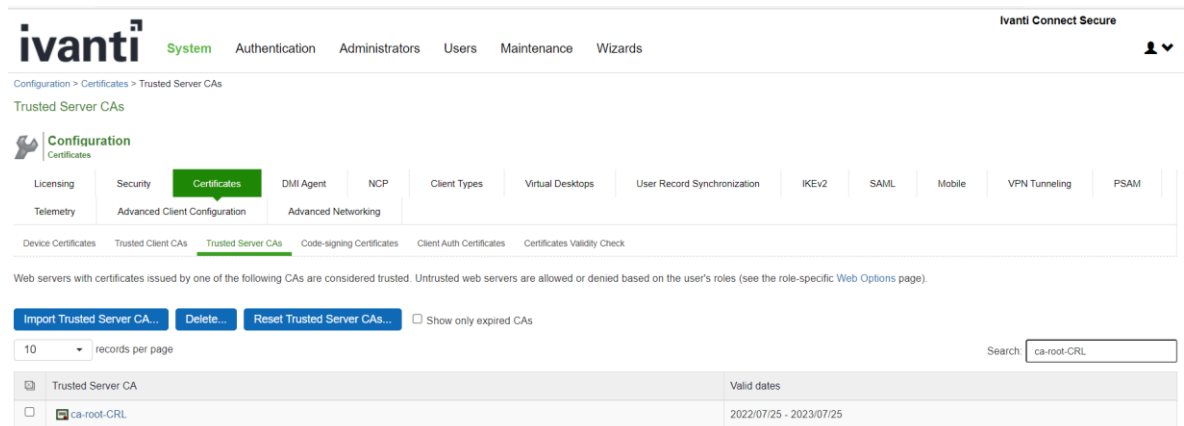


4. Once CA or CA Chain is Imported, click **Done**



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

5. 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**.



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:

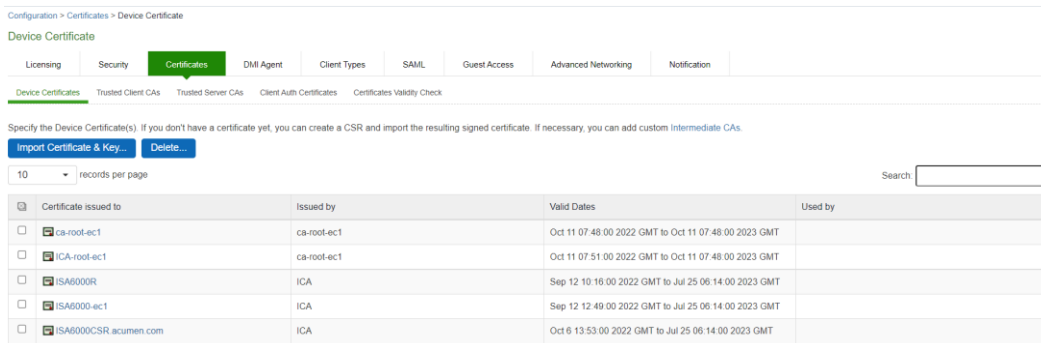
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

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 Certificates**



2. Click on **New CSR...**



3. Fill in CSR fields:

The screenshot shows the 'New Certificate Signing Request' form in the Ivanti System interface. The form is titled 'New Certificate Signing Request' and includes a breadcrumb trail: 'Configuration > Certificates > New Certificate Signing Request'. Below the title, there is a brief instruction: 'Use this page to create a new Certificate Signing Request (CSR) to send to your Certificate Authority of choice.' The form contains several input fields and a dropdown menu:

- Common Name:** (e.g., secure.company.com) - Input: secure.ivanti.com
- Organization Name:** (e.g., Company Inc.) - Input: acumensecurity.pvt.ltd
- Org. Unit Name:** (e.g., IT Group) - Input: CC
- Locality:** (e.g., SomeCity) - Input: Rockville
- State (fully spelled out):** (e.g., California) - Input: Maryland
- Country (2 letter code):** (i.e., US) - Input: US
- Email Address:** - Input: test@ivanti.com
- Key Type:** - Radio buttons for RSA (selected) and ECC
- Key Length:** - Dropdown menu with options 1024, 2048, and 3072 bits. The 2048 option is currently selected.
- Random Data:** (used for key generation) - Input: A field of asterisks representing random characters.

At the bottom of the form is a blue button labeled 'Create CSR'.

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. E.g.: acumensecurity.pvt.ltd

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

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

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

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

Email Address: The email address used to contact your organization. E.g.: 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:

4. Click on **Create CSR**

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: secure.ivanti.com
 Created: 10/21/2022 13:15:32
 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-----
MIIDIDCCAggCAQAwgZ4xCzAJBgNVBAYTAiVhbnRlcm9udC5jb20wDQYJKoZIhvcNAQEF
bGFuZDEZ
MBAGA1UEBwwJUm9ja3ZpbGxMR8wHQYDVQKDBZhy3VizW5zZWw1cmI
OeS5wdnQu
```

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

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

```
-----BEGIN CERTIFICATE REQUEST-----
MIIDIDCCAggCAQAwgZ4xCzAJBgNVBAYTAiVMTREwDwYDVQQIDAhNYXJ5
bGFuZDES
MBAGA1UEBwwJUm9ja3ZpbGxMR8wHQYDVQQKDBZlY3VtZW50ZWN1cmI
0eS5wdnQu
```

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

[New CSR...](#) [Delete...](#)

| <input type="checkbox"/> | Certificate Signing Requests | Created |
|--------------------------|---|---------------------|
| <input type="checkbox"/> | Pending CSR for secure.ivanti.com | 10/21/2022 13:15:32 |

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

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: [Browse](#) [secure.ivanti.com.crt](#)

[Import](#)

- Click on **Import**
- The new certificate is shown in **System > Configuration > Certificates > Device Certificates**

Configuration > Certificates > Device Certificate

Device Certificate

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

Specify the Device 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](#).

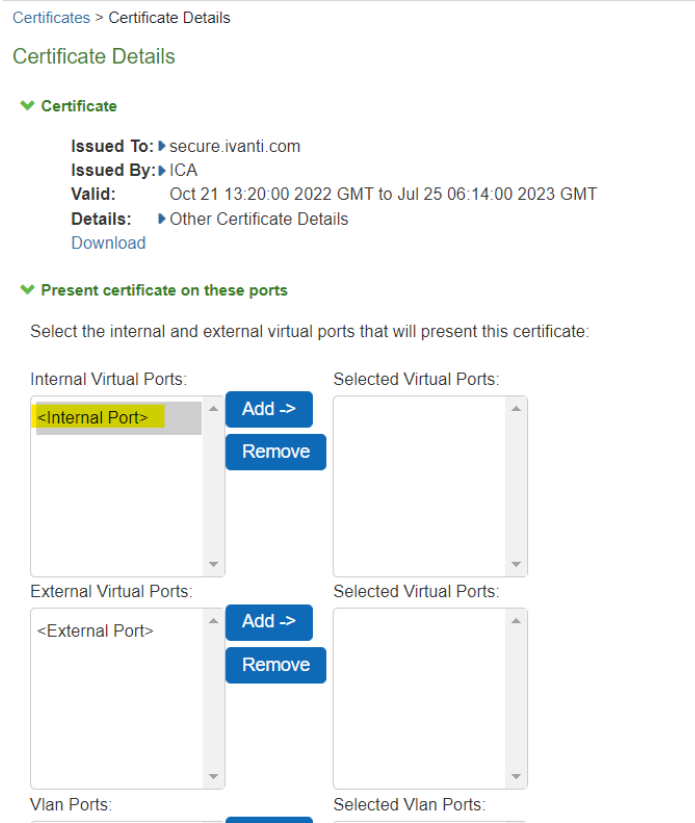
[Import Certificate & Key...](#) [Delete...](#)

10 records per page

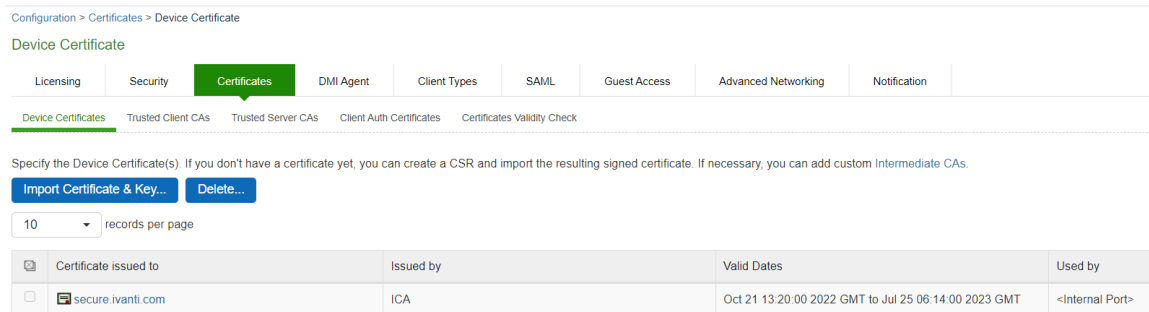
| <input type="checkbox"/> | Certificate issued to | Issued by | Valid Dates | Used by |
|--------------------------|-----------------------------------|-----------|--|---------|
| <input type="checkbox"/> | secure.ivanti.com | ICA | Oct 21 13:20:00 2022 GMT to Jul 25 06:14:00 2023 GMT | |

- 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.

12. 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.



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



NOTE: 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

[Certificates](#) > Certificate Details

Certificate Details

▼ Certificate

Issued To: ▶ secure.ivanti.com

Issued By: ▶ ICA

Valid: Oct 21 13:20:00 2022 GMT to Jul 25 06:14:00 2023 GMT

Details: ▶ Other Certificate Details

[Download](#)

▼ Present certificate on these ports

Select the internal and external virtual ports that will present this certificate:

| | | |
|--|---|---|
| Internal Virtual Ports: | | Selected Virtual Ports: |
| <div style="border: 1px solid #ccc; height: 100px; width: 100%;"></div> | Add -> Remove | <div style="border: 1px solid #ccc; padding: 5px;"><div style="background-color: yellow; padding: 2px;"><Internal Port></div></div> |
| External Virtual Ports: | | Selected Virtual Ports: |
| <div style="border: 1px solid #ccc; padding: 5px;"><External Port></div> | Add -> Remove | <div style="border: 1px solid #ccc; height: 100px; width: 100%;"></div> |

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

Internal Virtual Ports:

<Internal Port>

Add ->
Remove

Selected Virtual Ports:

External Virtual Ports:

<External Port>

Add ->
Remove

Selected Virtual Ports:

Vlan Ports:

Add ->
Remove

Selected Vlan Ports:

▼ Certificate status checking

Use CRLs (Certificate Revocation Lists)

Note: Certificate Revocation is supported only when the CDP is embedded in the device certificate and the CRL is hosted on a HTTP server.

Save Changes
Renew Certificate...

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. See 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. See the section [Import Client Auth Certificate](#).
- A trusted client CA must be imported to validate the client auth certificate. See 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.

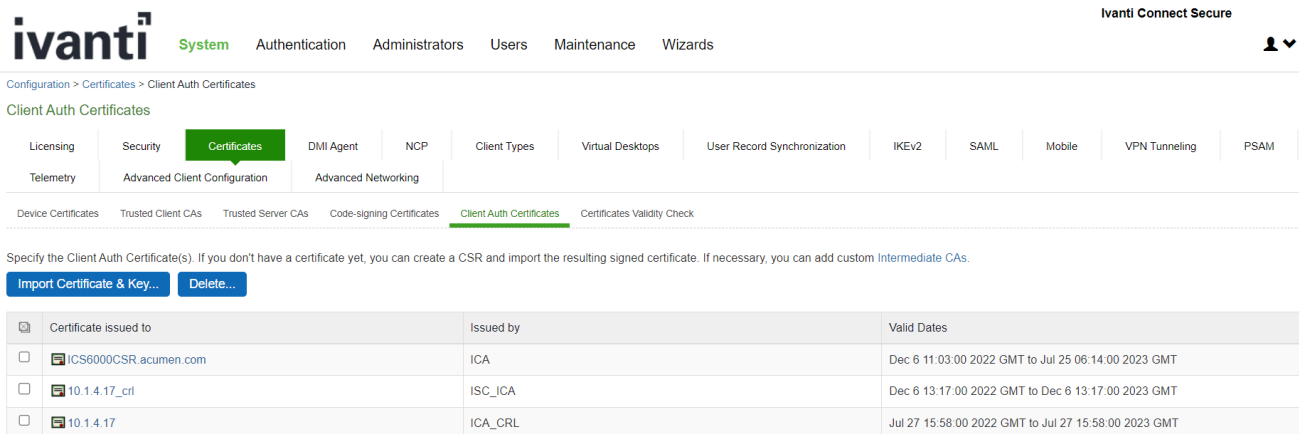
3.20. Import Client Auth Certificate

Client auth certificates are used for mutual authentication.

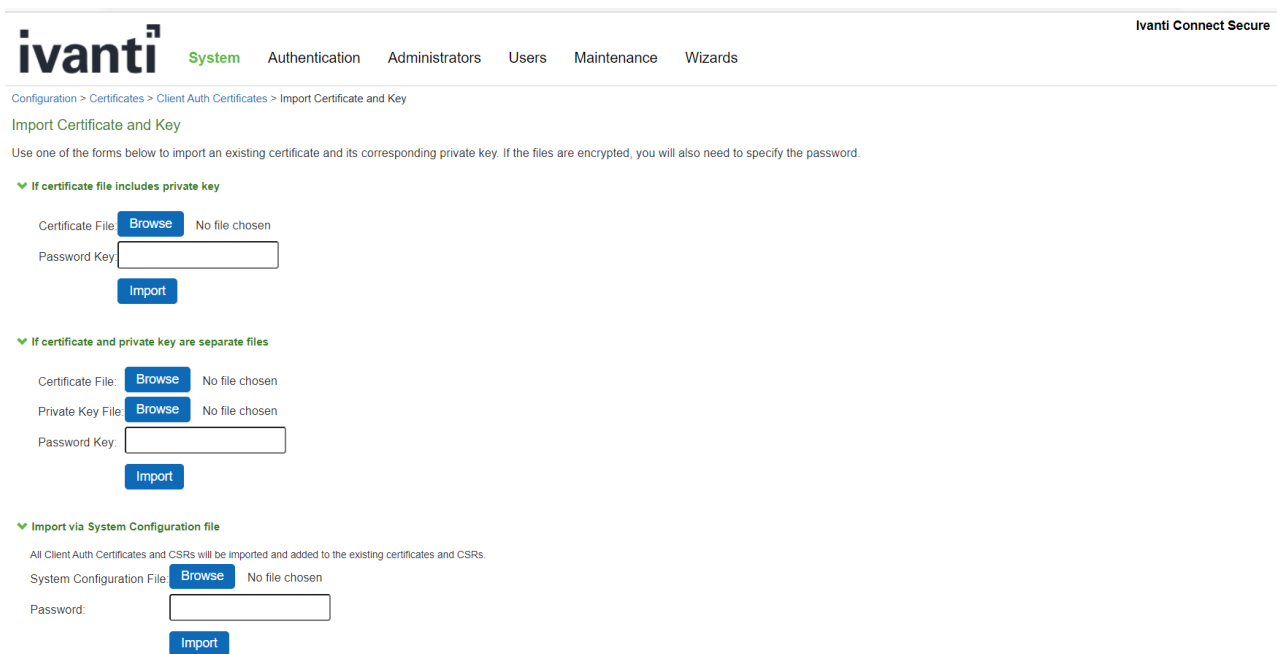
Follow instructions below to import a RSA 2048/3072 Client Auth Certificate into the TOE.

On Administrator Web Console,

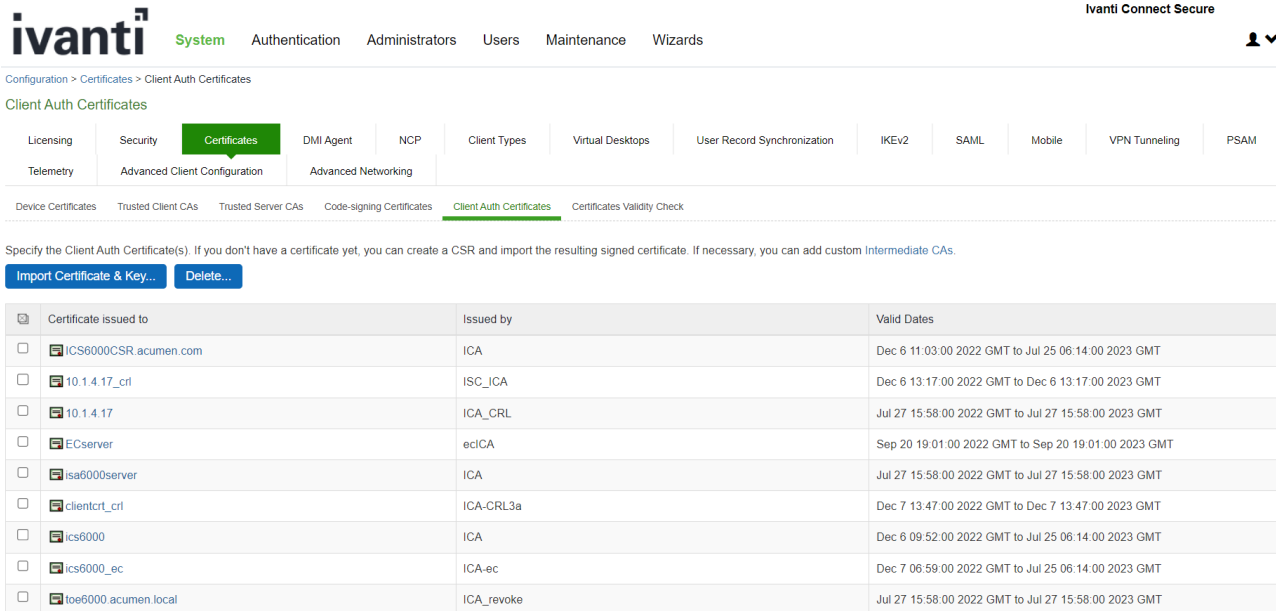
1. Navigate to **System > Configuration > Certificates > Client Auth Certificates**



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



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



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:

| 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 |

| PARAMETER | SELECTION |
|-----------------------|--|
| 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:

| 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:

| 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 |

| PARAMETER | SELECTION |
|----------------|--|
| 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

| 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 Ivanti Connect Secure web interface. At the top, there is a navigation menu with options: System, Authentication, Administrators, Users, Maintenance, and Wizards. Below the menu, there are several checked items: License Protocol Events, MDM API Trace, Ivanti Neurons for Secure Access Events, Profiler Events, and HTML5 Access Events. The 'Syslog Servers' section is expanded, showing a 'Delete' button and a table for configuring Syslog Servers. The table has the following columns: Server name/IP, Facility, Type, Client Certificate, Filter, and Source Interface. The first row in the table has the following values: an empty text box for Server name/IP, 'LOCAL0' for Facility, 'TLS' for Type, 'clientct_crl' for Client Certificate, 'Standard: Standard (default)' for Filter, and 'Management' for Source Interface. There is an 'Add' button at the bottom 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. The TSF divides the local audit storage between two audit files (active and inactive). When the current audit file reaches capacity; the TSF overwrites the inactive log file (if present). If the inactive log file is not present, then the TOE 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

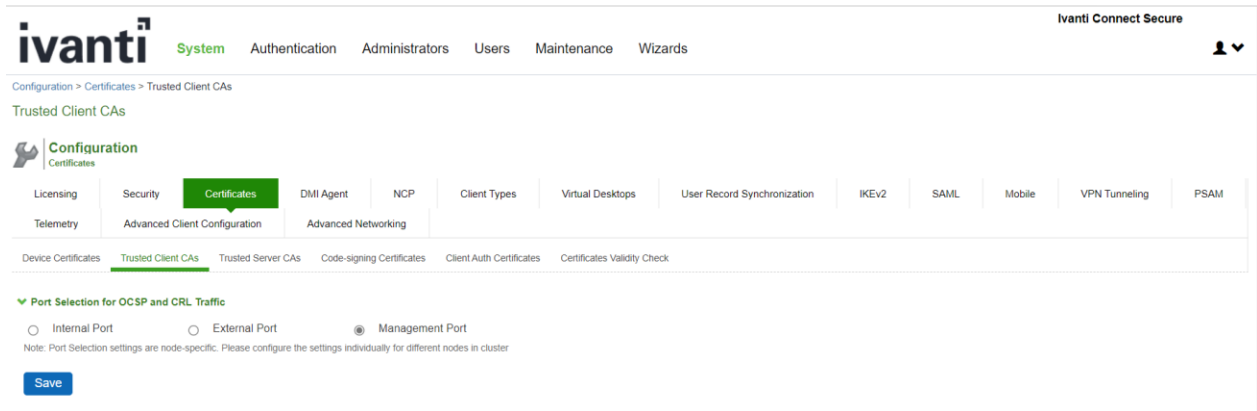
the certificate itself.) To ensure that it receives the most up-to-date CRL information, the system periodically contacts a CRL distribution point to get an updated list of CRLs. A CRL distribution point (CDP) is a location on an LDAP directory server or Web server where a CA publishes CRLs. The system 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:

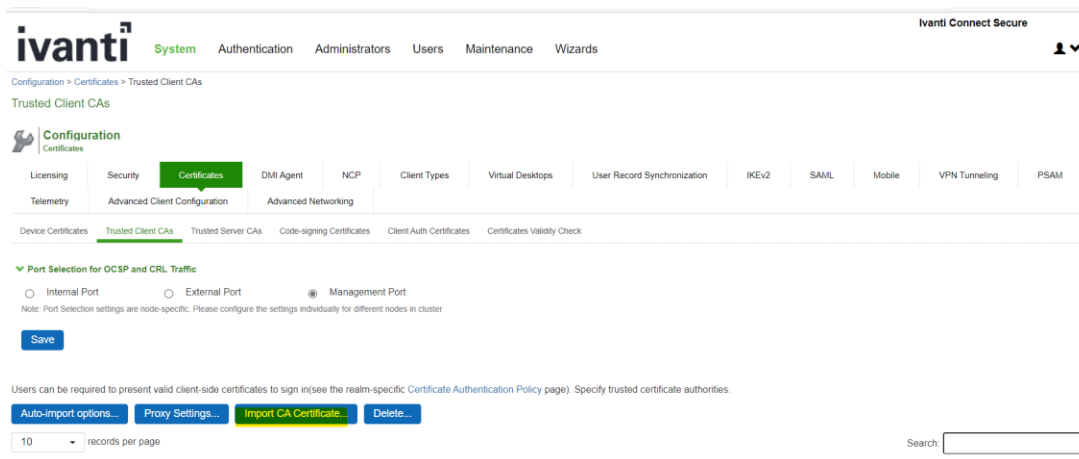
- Specify the CDP(s) in the CA certificate—When the CA issues a CA certificate, it might include an attribute specifying the location of the CDPs that the system should contact. If more than one CDP is specified, the system chooses the first one listed in the certificate and then fails over to subsequent 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

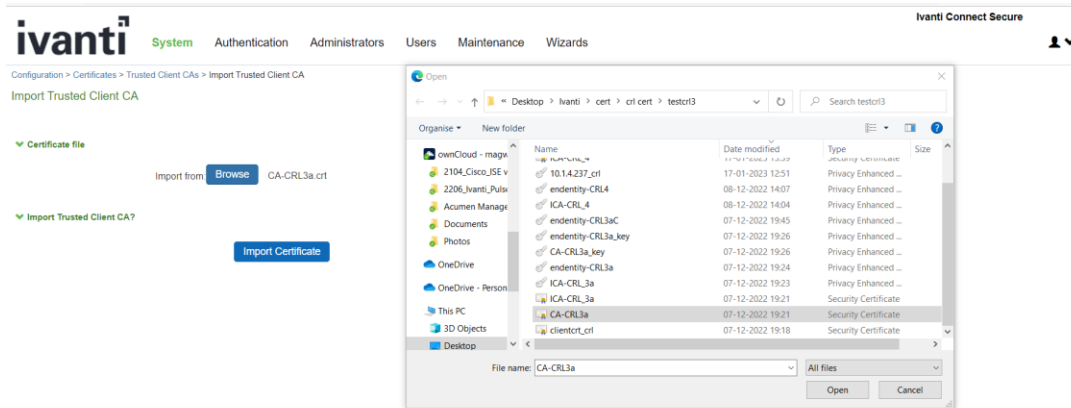


2. Click on **Import CA certificate**

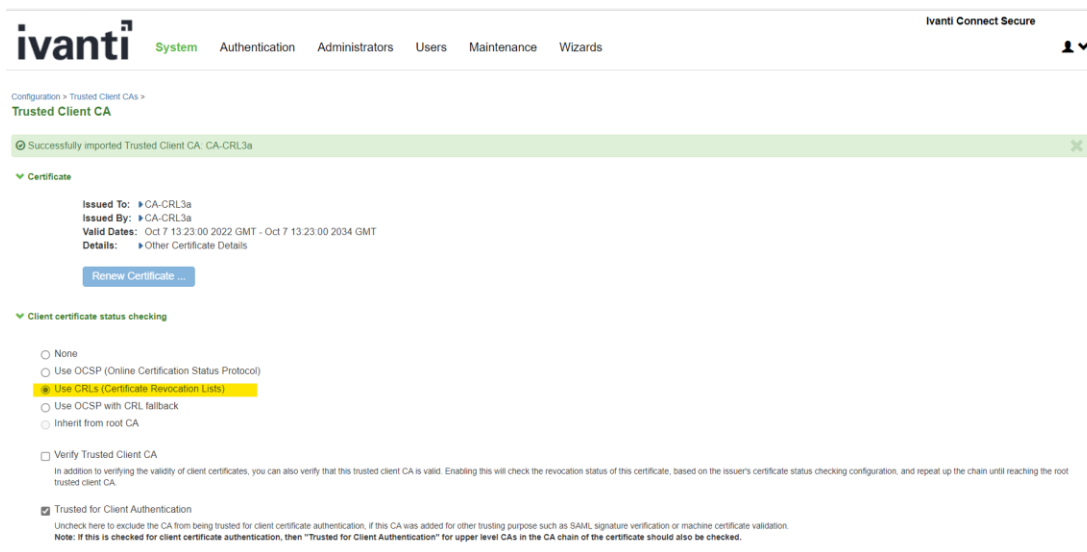


Ivanti Connect Secure v22.2 Common Criteria Configuration Guide

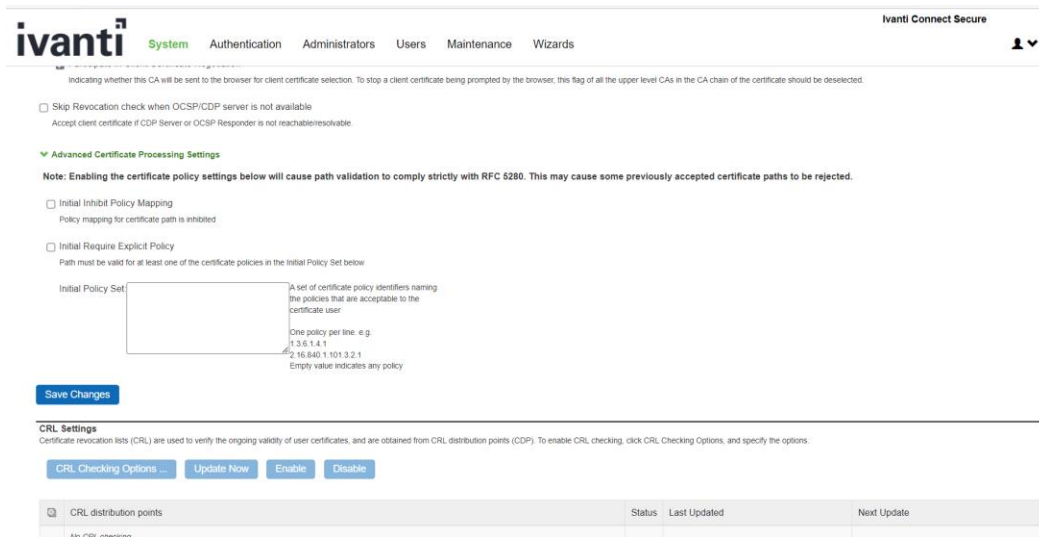
3. Click on Browse and select the certificate, click on **Import certificate**



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



5. Click on **Save changes**



- 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.
- 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 Connect 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**

Configuration > Certificates > Trusted Client CAs

Trusted Client CAs

Configuration
Certificates

Licensing Security **Certificates** DMI Agent NCP Client Types Virtual Desktops User Record Synchronization IKEv2 SAML Mobile VPN Tunneling PSAM

Telemetry Advanced Client Configuration Advanced Networking

Device Certificates **Trusted Client CAs** Trusted Server CAs Code-signing Certificates 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 |
|----------------------------------|------------------------------------|-------------------------|-----------------|
| <input type="checkbox"/> ca-root | Yes | 2022/07/25 - 2023/07/25 | None |
| <input type="checkbox"/> ICA | Yes | 2022/07/25 - 2023/07/25 | None |

2. Select CA Chain one by one and Click **Delete**

Configuration > Certificates > Trusted Client CAs

Trusted Client CAs

Configuration
Certificates

Licensing Security **Certificates** DMI Agent NCP Client Types Virtual Desktops User Record Synchronization IKEv2 SAML Mobile VPN Tunneling PSAM

Telemetry Advanced Client Configuration Advanced Networking

Device Certificates **Trusted Client CAs** Trusted Server CAs Code-signing Certificates 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 |
|---|------------------------------------|-------------------------|-----------------|
| <input type="checkbox"/> ca-root | Yes | 2022/07/25 - 2023/07/25 | None |
| <input checked="" type="checkbox"/> ICA | Yes | 2022/07/25 - 2023/07/25 | None |

3. 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**

Configuration > Certificates > Trusted Server CAs

Trusted Server CAs

Configuration Certificates

Licensing Security **Certificates** DMI Agent NCP Client Types Virtual Desktops User Record Synchronization IKEv2 SAML Mobile VPN Tunneling PSAM

Telemetry Advanced Client Configuration Advanced Networking

Device Certificates Trusted Client CAs **Trusted Server CAs** Code-signing Certificates Client Auth Certificates Certificates Validity Check

Web servers with certificates issued by one of the following CAs are considered trusted. Untrusted web servers are allowed or denied based on the user's roles (see the role-specific [Web Options](#) page).

Import Trusted Server CA... Delete... Reset Trusted Server CAs... Show only expired CAs

10 records per page Search:

| Trusted Server CA | Valid dates |
|--|-------------------------|
| <input type="checkbox"/> Bypass Class 2 Root CA | 2010/10/26 - 2040/10/26 |
| <input type="checkbox"/> Baltimore CyberTrust Root | 2000/05/12 - 2025/05/12 |
| <input type="checkbox"/> Autoridad de Certificacion Firmaprofesional CIF A62634068 | 2009/05/20 - 2030/12/31 |
| <input type="checkbox"/> A-Trust-Root-07 | 2018/05/17 - 2038/11/19 |
| <input type="checkbox"/> Atos TrustedRoot 2011 | 2011/07/7 - 2030/12/31 |
| <input type="checkbox"/> Amazon Root CA 4 | 2015/05/26 - 2040/05/26 |

2. Search CA by its Common Name in Search Bar to List the CA which needs to be deleted

Configuration > Certificates > Trusted Server CAs

Trusted Server 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

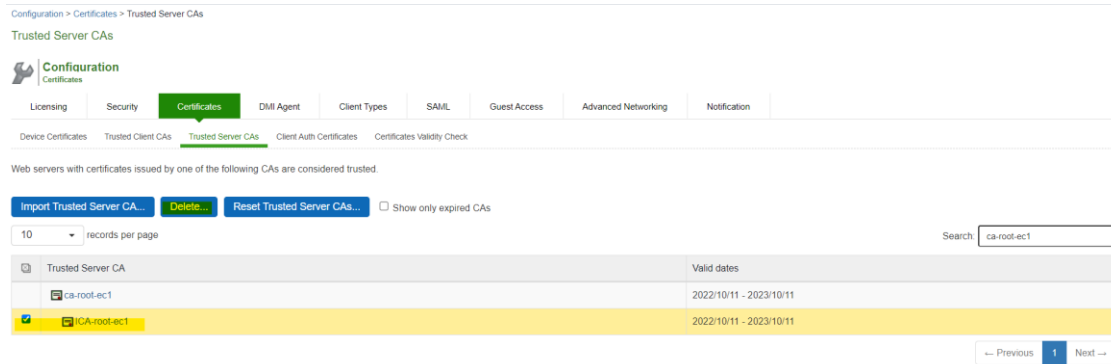
Web servers with certificates issued by one of the following CAs are considered trusted.

Import Trusted Server CA... Delete... Reset Trusted Server CAs... Show only expired CAs

10 records per page Search:

| Trusted Server CA | Valid dates |
|--|-------------------------|
| <input type="checkbox"/> ca-root-ect1 | 2022/10/11 - 2023/10/11 |
| <input type="checkbox"/> ICA-root-ect1 | 2022/10/11 - 2023/10/11 |

3. Select CA Chain one by one and Click **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 connect 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 connect 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 connect 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.

| 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 | 2023-02-10 07:57:51 - ive - [192.168.254.203] admin(Admin Users)[Administrators] - Login succeeded for admin/Admin Users from 192.168.254.203 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 2023-02-10 07:57:51

Node name is ive

Source IP is

192.168.254.203

User is admin

The **Realm** is Admin Users

Role is Administrators

The log **message** is Login succeeded for admin/Admin Users from 192.168.254.203 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

Minor SYS10306

| | | |
|-------|----------|---|
| Minor | SYS10306 | 2024-02-01 06:58:14 - ive - [127.0.0.1] Root::System() - Starting services: postgresd |
| Minor | SYS10306 | 2024-02-01 06:58:13 - ive - [127.0.0.1] Root::System() - Starting services: Logging |
| Minor | SYS10306 | 2024-02-01 06:58:13 - ive - [127.0.0.1] Root::System() - Starting services: Debuglog Server |
| Minor | SYS10306 | 2024-02-01 06:58:13 - ive - [127.0.0.1] Root::System() - Starting services: Event Service |
| Minor | SYS10306 | 2024-02-01 06:58:12 - ive - [127.0.0.1] Root::System() - Starting services: state server |

Shutdown of the audit function

Minor SYS10299

| | | |
|-------|----------|---|
| Minor | SYS10020 | 2024-02-01 06:58:12 - ive - [127.0.0.1] Default Network::System() - Changeset: Exceeded maxim |
| Minor | SYS10299 | 2024-02-01 06:54:55 - ive - [127.0.0.1] Root::System() - Server shutdown |
| Info | LIC31565 | 2024-02-01 06:17:04 - ive - [127.0.0.1] Root::System() - Applying Virtual Appliance license. |

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 | 2023-02-10 09:34:58 - ive - [192.168.254.203] admin(Admin Users)[Administrators] - Login succeeded for admin/Admin Users from 192.168.254.203 via management port. |
|------|----------|--|

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

| | | |
|------|----------|--|
| Info | ADM22671 | 2023-02-10 09:34:14 - ive - [192.168.254.203] admin(Admin Users)[Administrators][409f1660c9] - Logout from 192.168.254.203 |
|------|----------|--|

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 | 2022-12-16 09:54:08 - ive - [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 | 2022-12-16 09:53:39 - ive - [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 | 2020-05-12 23:00:01 - ive - [192.168.254.203] admin(Admin Users)[.Administrators][d9a1f29d20] - System date modified to May 12 23:00:00 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 | 2023-02-09 08:49:36 - ive - [192.168.254.203] admin(Admin Users)[.Administrators][2813037fd2] - Added CA Certificate 'CN=ca-root-CRL, 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 | 2023-02-10 10:05:02 - ive - [192.168.254.203] admin(Admin Users)[.Administrators][2f1857b2f5] - Removed CA Certificate 'ISC_ICA' |
|------|----------|--|

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>

Ivanti Connect Secure v22.2 Common Criteria Configuration Guide

| Date: Oldest to Newest | | |
|-------------------------|----------|---|
| Query: | | |
| Export Format: Standard | | |
| Severity | ID | Message |
| Info | ADM23081 | 2023-01-04 10:15:50 - ive - [192.168.228.49] admin(Admin Users)[Administrators][8b3c826343] - Created Certificate Signing Request. key size 2048. 'CN=toetest.acumen.local,OU=CC,O=acumen,L=rockville,ST=md,C=us,Email=admin' |

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

| Severity | ID | Message |
|----------|----------|--|
| Info | ADM23082 | 2023-01-03 13:29:20 - ive - [192.168.254.203] admin(Admin Users)[Administrators][4fad897fad] - Removed CSR 'test6000.acumen.local' |

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 | 2023-02-10 10:35:03 - ive - [192.168.254.203] admin(Admin Users)[Administrators][d4b7058133] - 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 | 2023-02-06 13:38:39 - ive - [192.168.254.203] admin(Admin Users)[Administrators][990ed9261f] - NDcPP Mode is now turned on. The web server will restart. |
|------|----------|--|

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

| | | |
|------|----------|---|
| Info | ADM30965 | 2023-02-06 13:38:39 - ive - [192.168.254.203] admin(Admin Users)[Administrators][990ed9261f] - FIPS Mode is now turned on. The web server 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>'

Ivanti Connect Secure v22.2 Common Criteria Configuration Guide

| | | |
|------|----------|--|
| Info | ADM31346 | 2023-02-06 13:45:07 - ive - [192.168.254.203] admin(Admin Users)[.Administrators][990ed9261f] - Changed outbound custom cipher for Allowed Encryption Strength from 'ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-SHA256:ECDHE-ECDSA-AES256-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:AES128-SHA256:AES256-SHA256:AES128-SHA:AES256-SHA:DHE-RSA-AES128-SHA:DHE-RSA-AES256-SHA' to 'ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-SHA256:ECDHE-ECDSA-AES256-SHA384:ECDHE-ECDSA-AES128-SHA:ECDHE-ECDSA-AES256-SHA:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-SHA:AES256-SHA:AES128-SHA256:AES256-SHA256:AES128-SHA:AES256-SHA' |
|------|----------|--|

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 | 2023-02-06 13:31:54 - ive - [192.168.254.203] admin(Admin Users)[.Administrators][990ed9261f] - 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 | 2023-02-06 13:31:54 - ive - [192.168.254.203] admin(Admin Users)[.Administrators][990ed9261f] - 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 | 2022-09-21 14:09:21 - ive - [10.1.4.115] System() - SSL negotiation failed while client at source IP '10.1.4.115' was trying to connect to '10.1.4.17'. 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 ADM23440 <current timestamp> <node name> <IP Address> <user id> <Realm> <Role>
 - Updated the sign-in policy <policy name>

| | | |
|------|----------|--|
| Info | ADM23440 | 2023-01-04 06:08:01 - ive - [192.168.254.203] admin(Admin Users)[_Administrators][eea6863d5c] - Updated the sign-in policy 'admin' |
| Info | ADM32011 | 2023-01-04 06:07:55 - ive - [127.0.0.1] System() - Triggered dynamic policy evaluation for realm: Users |
| Info | ADM30467 | 2023-01-04 06:04:04 - ive - [192.168.254.203] admin(Admin Users)[_Administrators][eea6863d5c] - Created new sign-in notification 'New Sign-In Notification1' |

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 | 2023-01-04 07:17:07 - ive - [192.168.254.203] admin(Admin Users)[_Administrators][70c2c5e4ca] - SESSION_IDLE_TIMEOUT in Role 'Administrators' is modified from [7] to [5] |
|------|----------|---|

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 | 2022-12-21 07:54:40 - ive - [127.0.0.1] System() - Successful syslog connection to peer: '10.1.4.115' |
|------|----------|---|

7.8. Failure to establish a TLSC Session

7.8.1. Failure due to Invalid extension

Ivanti connect secure configuration guide

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

| Severity | ID | Message |
|----------|----------|--|
| Major | SYS31377 | 2022-12-22 12:30:01 - Ive - [127.0.0.1] System()[] - 'Inbound Server' Certificate 'CN=10.1.4.115, OU=CC, O=acumen, C=US' issued by 'CN=ICA2, 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>

| Severity | ID | Message |
|----------|----------|---|
| Critical | SYS31439 | 2022-12-22 08:34:38 - Ive - [127.0.0.1] System()[] - SSL handshake with peer: 10.1.4.115 failed with Error message: 336134527: error:1409017F:SSL routines:ssl3_get_server_certificate:wrong certificate type |

| Severity | ID | Message |
|----------|----------|--|
| Critical | SYS31439 | 2022-12-22 09:12:43 - Ive - [127.0.0.1] System()[] - SSL handshake with peer: 10.1.4.115 failed with Error message: 336142584: error:140920F8:SSL routines:ssl3_get_server_hello:unknown cipher returned |

| Severity | ID | Message |
|----------|----------|--|
| Critical | SYS31439 | 2022-12-22 09:27:45 - Ive - [127.0.0.1] System()[] - SSL handshake with peer: 10.1.4.115 failed with Error message: 336142597: error:14092105:SSL routines:ssl3_get_server_hello:wrong cipher returned |

| Severity | ID | Message |
|----------|----------|--|
| Critical | SYS31439 | 2022-12-22 09:57:48 - Ive - [127.0.0.1] System()[] - SSL handshake with peer: 10.1.4.115 failed with Error message: 336122234: error:1408D17A:SSL routines:ssl3_get_key_exchange:wrong curve |

| Severity | ID | Message |
|----------|----------|--|
| Critical | SYS31439 | 2023-01-11 05:57:01 - Ive - [127.0.0.1] System()[] - SSL handshake with peer: 10.1.4.115 failed with Error message: 336032002: error:14077102:SSL routines:SSL23_GET_SERVER_HELLO:unsupported protocol |

| Severity | ID | Message |
|----------|----------|--|
| Critical | SYS31439 | 2022-12-22 10:27:53 - Ive - [127.0.0.1] System()[] - SSL handshake with peer: 10.1.4.115 failed with Error message: 336121979: error:1408D07B:SSL routines:ssl3_get_key_exchange:bad signature |

| Severity | ID | Message |
|----------|----------|--|
| Critical | SYS31439 | 2022-12-22 10:43:00 - Ive - [127.0.0.1] System()[] - SSL handshake with peer: 10.1.4.115 failed with Error message: 336117909: error:1408C095:SSL routines:ssl3_get_finished:digest check failed |

| Severity | ID | Message |
|----------|----------|--|
| Critical | SYS31439 | 2022-12-22 10:58:07 - Ive - [127.0.0.1] System()[] - SSL handshake with peer: 10.1.4.115 failed with Error message: 336150673: error:14094091:SSL routines:ssl3_read_bytes:data between ccs and finished |

| Severity | ID | Message |
|----------|----------|--|
| Critical | SYS31439 | 2022-12-22 11:13:11 - Ive - [127.0.0.1] System()[] - SSL handshake with peer: 10.1.4.115 failed with Error message: 336121979: error:1408D07B:SSL routines:ssl3_get_key_exchange:bad signature |

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>).

| Severity | ID | Message |
|----------|----------|---|
| Critical | SYS31051 | 2022-12-23 09:59:07 - Ive - [127.0.0.1] System()[] - Syslog TLS validation of server '10.1.4.115' with Client-Cert: 'ics6000'; Server-Cert: 'CN=10.1.4.69, OU=CC, O=acumen, C=US' failed (err: There is no SAN and the CN did not match the Configured Reference Identifier). |

| Severity | ID | Message |
|----------|----------|--|
| Critical | SYS31051 | 2022-12-23 10:14:09 - Ive - [127.0.0.1] System()[] - Syslog TLS validation of server '10.1.4.115' with Client-Cert: 'ics6000'; Server-Cert: 'CN=10.1.4.115, OU=CC, O=acumen, C=US' failed (err: None of the certificate's Subject Alternative Names(SAN) match the Configured Reference Identifier). |

| Severity | ID | Message |
|----------|----------|---|
| Critical | SYS31051 | 2022-12-23 06:55:30 - Ive - [127.0.0.1] System()[] - Syslog TLS validation of server 'foo.syslog.acumensec.local' with Client-Cert: 'ics6000'; Server-Cert: 'CN=foo.*.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 | 2022-12-23 07:10:17 - IVE - [127.0.0.1] System() - Syslog TLS validation of server 'foo.syslog.acumensec.local' with Client-Cert: 'ics6000', Server-Cert: '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).

| Severity | ID | Message |
|----------|----------|--|
| Critical | SYS31051 | 2022-12-09 08:44:00 - IVE - [127.0.0.1] System() - Syslog TLS validation of server '10.1.4.115' with Client-Cert: 'ics6000', Server-Cert: 'CN=10.1.4.115, 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 | 2022-12-09 08:54:58 - IVE - [127.0.0.1] System() - Syslog TLS validation of server '10.1.4.115' with Client-Cert: 'ics6000', Server-Cert: 'CN=10.1.4.115, 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 | 2022-12-14 10:19:44 - IVE - [10.1.4.115] System() - SSL negotiation failed while client at source IP '10.1.4.115' was trying to connect to '10.1.4.17' Reason: 'no shared cipher' |
|-------|----------|---|

| | | |
|-------|----------|--|
| Minor | AUT24604 | 2022-12-14 10:28:55 - IVE - [10.1.4.115] System() - SSL negotiation failed while client at source IP '10.1.4.115' was trying to connect to '10.1.4.17' Reason: 'digest check failed' |
|-------|----------|--|

| | | |
|-------|----------|---|
| Minor | AUT24604 | 2022-12-14 10:46:55 - IVE - [10.1.4.115] System() - SSL negotiation failed while client at source IP '10.1.4.115' was trying to connect to '10.1.4.17' 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 | 2023-01-05 08:37:24 - IVE - [192.168.254.203] admin(Admin Users)[Administrators][e4db2ea1b8] - Local Authentication server 'Administrators' Update the account lockout period from '11' minutes to '10' minutes |
| Info | ADM31781 | 2023-01-05 08:37:24 - IVE - [192.168.254.203] admin(Admin Users)[Administrators][e4db2ea1b8] - 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 | 2023-01-05 08:40:16 - IVE - [192.168.254.203] admin(Admin Users)[Administrators] - Login failed from 192.168.254.203 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 | 2022-12-16 09:50:15 - ive - [192.168.254.203] admin(Admin Users)[_Administrators]] - Login succeeded for admin/Admin Users from 192.168.254.203 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 | 2023-01-04 10:41:29 - ive - [192.168.254.203] 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 | 2022-12-16 09:54:08 - ive - [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 | 2022-12-16 09:53:39 - ive - [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 | 2022-09-07 15:47:45 - ive - [192.168.128.117] acumensec(Admin Users)[_Administrators][ec68573cbf] - Syslog server 10.1.4.224 (facility LOCAL0, filter Standard, type UDP, interface Management) 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 | 2023-01-04 11:03:39 - ive - [192.168.254.203] acumensec(Admin Users)[_Administrators][42b64d9898] - Syslog server my.syslogserv.com (facility LOCAL0, filter Standard, type TCP, interface Management) added for Events 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 | 2022-12-06 07:25:53 - Ive - [192.168.254.203] admin\Admin Users\Administrators[571186a082] - 'Server CA' 'CN=ICA-CRL3a, OU=CC, O=acumen, C=US' issued by 'CN=CA-CRL3a, 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 | 2022-12-08 09:17:40 - Ive - [127.0.0.1] System() - 'Server CA' Certificate 'CN=ICA-CRL_4, OU=CC, O=acumen, C=US' issued by 'CN=CA-CRL3a, 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 | 2022-12-06 10:12:04 - Ive - [127.0.0.1] System() - 'Inbound Server' Certificate 'CN=10.1.4.115, OU=CC, O=acumen, C=US' issued by 'CN=ICA, 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 | 2022-12-07 10:56:13 - Ive - [192.168.228.59] admin\Admin Users\Administrators[afd88fe101] - 'Trusted Server CA' Certificate 'CN=ICA-ec, OU=CC, O=acumen, C=US' issued by 'CN=ica-ec, 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 | 2022-12-06 10:04:28 - Ive - [127.0.0.1] System() - SSL handshake with peer: 10.1.4.115 failed with Error message: 336134278: error:14090086:SSL routines:ssl3_get_server_certificate:certificate verify failed |
|----------|----------|--|

| | | |
|----------|----------|--|
| Critical | SYS31439 | 2022-12-06 08:14:30 - Ive - [127.0.0.1] System() - SSL handshake with peer: 10.1.4.115 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 | 2022-12-07 11:09:45 - Ive - [192.168.228.59] admin\Admin Users\Administrators[afd88fe101] - 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 | 2023-02-14 07:19:33 - ive - [192.168.228.46] admin\Admin Users\Administrators[9f63393d67] - Added CDP 'URI:http://10.1.4.115/CA-CRL3a.der' for Trusted Server CA 'CA-CRL3a' |
|------|----------|---|

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 | 2022-12-08 06:50:43 - ive - [127.0.0.1] System()[][] - Downloaded new CRL (609 bytes) from 'http://10.1.4.115/CA-CRL3a.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 | 2022-12-08 06:53:18 - ive - [192.168.254.203] admin\Admin Users\Administrators[571185a082] - The X.509 certificate for 'CN=ICA-CRL3a, OU=CC, O=acumen, C=US' issued by CN=CA-CRL3a, 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 | 2023-02-01 14:29:32 - ive - [127.0.0.1] System()[][] - CRL checking started for certificate 'CN=ICA2, OU=CC, O=acumen, C=US' issued by CN=ca-root, 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 | 2022-12-07 09:29:01 - ive - [10.1.4.115] acumensec\Admin Users\Administrators[107e0a8643] - 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 | SYS20413 | 2022-12-12 09:44:29 - ive - [127.0.0.1] System()[] - Started system software version 22.2R3 (build 1369) successfully |
|------|----------|---|

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 | 2023-01-24 12:53:38 - ive - [10.1.4.115] admin\Admin Users\Administrators[d32c7b7bc1] - 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 | 2023-02-13 10:06:27 - ive - [127.0.0.1] System()[] - Server restart |
|-------|----------|---|

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

| | | |
|-------|----------|--|
| Minor | SYS10306 | 2023-02-13 10:07:00 - ive - [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 | 2023-02-13 10:07:00 - ive - [127.0.0.1] System()[] - Web server running in FIPS mode |
|------|----------|--|

8. Reference Documents

- Ivanti Secure Operational User Guidance and Preparative Procedures
- Ivanti Connect Secure Administration Guide:
https://help.ivanti.com/ps/help/en_US/ICS/22.x/ag/landingpage.htm
- Ivanti Connect Secure Supported Platforms Guide:
https://help.ivanti.com/ps/help/en_US/ICS/22.x/spg/Default.htm
- Ivanti Connect Secure 22.2 Security Target

=====END OF THE DOCUMENT=====