infraonSecuRA®

Powered by EverestIMS

A Secure Remote Access and Authentication System

Operations Guide

V1.1

Disclaimer

Information in this document is subject to change without prior notice. Companies, names and data used in examples herein are fictitious and for illustration purposes only, unless otherwise stated. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express permission of EverestIMS Technologies.

EverestIMS Technologies may have patents or pending patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. The furnishing of this document does not give external parties any license to these patents, trademarks, copyrights, or other intellectual property rights except as expressly provided in any written license agreement from EverestIMS Technologies.

EverestIMS Technologies and Everest are trademarks of EverestIMS Technologies Pvt. Ltd. All other brand and product names are trademarks or registered trademarks of their respective holders.

URL: http://www.everestims.com

Privacy Information

This document contains sensitive information. Access to this document or the content within should strictly be provided only to authorize users of SecuRA software on a need to know basis.

Any unauthorized use or sharing of information contained within this document will be considered as breach of respective confidentiality/copyright and shall be treated accordingly.

Table of Contents

1. Introduction

Infraon SecuRA, powered by EverestIMS is a Remote Access system for networks and servers (CLI based). It comes with built-in Authorization, Authentication and Job Scheduling modules to help the administrators secure the network's remote access.

SecuRA's web portal-based system enables the Network Administrator to control access of a user to a selected set of devices and manage the same by restricting activities that can be performed by the user within the system. Restrictions can be both time and command based. All user activities can be monitored in real-time and audited anytime.

In addition to the above features, SecuRA facilitates running scheduled Jobs and performing remote file management in a secured manner.

In this guide, SecuRA (Secure Remote Access and Authentication System) users will learn about

- Overview/Advantages of SecuRA
- SecuRA feature configurations
- User Interfaces and work flow
- Licensing information
- Other SecuRA documentation references to Python and Jinja2 Templates

Target Users/Audience

- SecuRA Administrator
- Network Administrator
- Network Operator
- Manager

2. Overview

SecuRA enables Network administrators to efficiently manage remote IT networks and IP enabled security devices from a centralized location.

Key benefits

- Distribute patch updates
- Provide role-based access control
- Report all Aspects of Network Device Configurations Changes
- Secured authentication and authorization access

Features of SecuRA are based on the editions – ***SecuRA Standard & SecuRA Pro***. Pro Version includes the all the features of Standard version in addition to:

- ✓ Bulk discovery
- ✓ Bulk Upload
- ✓ Temporary User Account
- ✓ Device Authorization Profile
- ✓ Configuration Templates
- ✓ File Management

In addition to the above features, SecuRA facilitates running scheduled Jobs and performing remote file management in a secured manner.

3. How to get started with SecuRA

Log into SecuRA

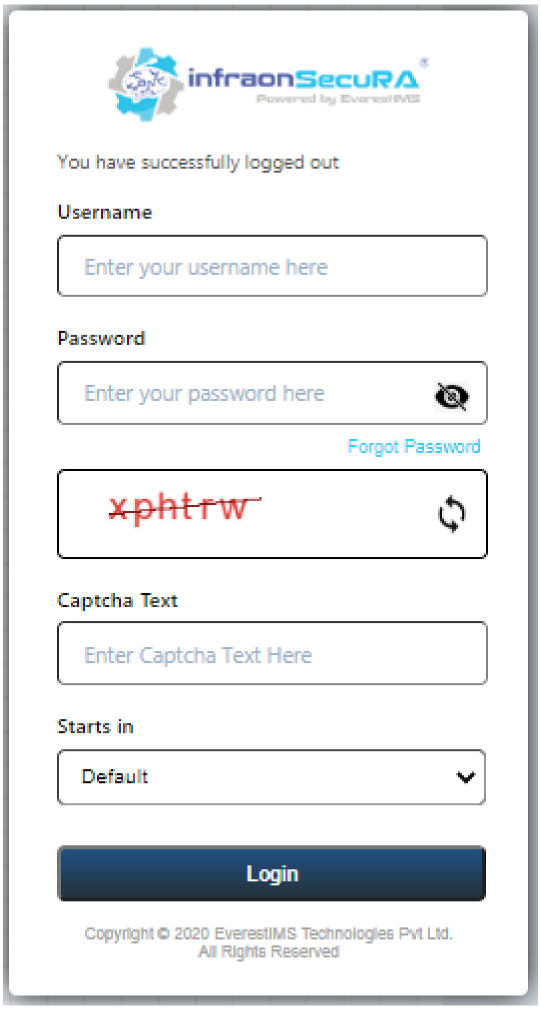
- SecuRA will be managed via "Internet Browsers" and is best viewed on latest version of Google chrome and Mozilla Firefox.
- To access SecuRA, go to the corresponding URL < http(s)://domain-name or server IP address >
- Enter the below given login credentials.

User Name: administrator
Password: admin
Captcha*: (code as displayed)*

Select the landing page (Start in) using the dropdown menu and click 'Login'.

Note: *If no page is selected, SecuRA will redirect the user to the Default Landing Page.*

For compliance purposes, please note that SecuRA would prompt the user to change the password, when logged in for the first time.



You have successfully logged out

Username

Enter your username here

Password

Enter your password here

Forgot Password

xphtrw

Captcha Text

Enter Captcha Text Here

Starts in

Default

Login

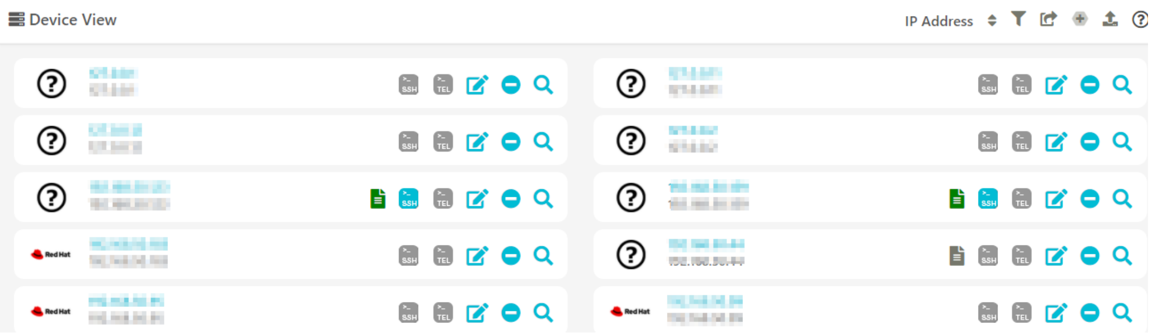
Copyright © 2020 EverestIMS Technologies Pvt Ltd.
All Rights Reserved

Note:

Browser cookie feature must be enabled for SecuRA domain URL to maintain the session details.

Clear the SecuRA Domain Browser cache when the SecuRA server is upgraded to next version.

On successful authentication, the user will be redirected to Device View Page.



Note: If the user session is inactive for an hour, SecuRA logs the user out. This can be configured from System Parameters page.

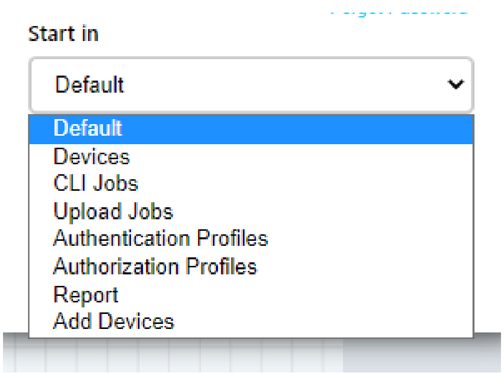
Online help for Infraon SecuRA and the same can be accessed by clicking ?, located on the top right corner of each page.

4. Default Login Page

SecuRA lets the user choose the Landing page, at the time of Login. If 'Default' or no Landing page is selected, SecuRA will redirect to the page, selected as default. There are two ways to configure 'Default' landing page.

- System Parameters
- User Accounts

Additionally, the user can use the dropdown menu to select the landing page (*Devices and Upload Jobs* at the time of Login.

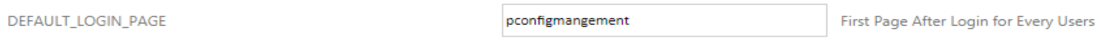


Start in

Default

System Parameters

From the top panel, click ⚙ and select 'System Parameters'.



DEFAULT_LOGIN_PAGE pconfigmangement First Page After Login for Every Users

Input default parameter for login page – Type-in page name. Click Save (Selected Process).

User Account

From the left panel, click 👤 select User Accounts -> 'Accounts'. Click the User ID to navigate to the edit page. Input 'Start In' page details and click Ok to save.

SecuRA default login page is derived from the below scenarios

- At the time of Logging in to SecuRA, if the user selects the 'Start In' page, SecuRA starts from the selected page.
- If 'Default' is selected and SecuRA takes the input from the user 'Accounts' page. If the user account 'Default Login page' is not configured, SecuRA takes the Login page specified in the 'System Parameters' page.
- If none of the above are configured, SecuRA redirects the user to 'Device View' page.

5. Navigation bar

Click on "Infraon SecuRA' logo on the top left corner of the page to view an expanded view of the menu. Navigation options from the left panel are as follows:

⏲	Dashboard	Device View of devices (includes SSO options and File Management modules) and Server Performance
☰	Devices	Also referred to as Device Grid page, displays Active/Current Device Inventory and quick Diagnosis tools (includes SSO options and File Management modules). Displays Archived/Deleted Devices Inventory details.
♻	Configuration Templates	Manage Configuration Templates, Configuration Profiles, Global Parameters and System Object ID's.
🤖	Jobs	Manage Upload Jobs and CLI Jobs/Sessions
🔍	Discovery	Discover devices on to SecuRA through Automatic and CSV Device Upload Discovery options or add an individual Device manually.

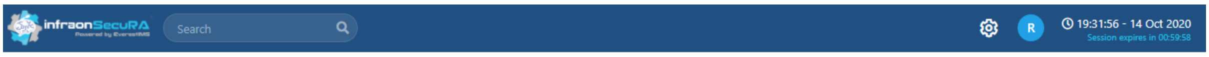
👤⚙	Account Management	Manage Password Policy, User Accounts, User Groups, User Roles, Device Groups, Device Credentials, Authentication & Authorization profiles, and Password Change.
✉	Notification	Configure Notifier, Methods/Channels, Monitor Messages and Email Server
▤	Diagnostics	Diagnosis Operations including Telnet & SSH, Ping, SNMP Walk and Trace Route.
◕	Reports	Configure, Schedule and view online Reports
☰	Audits	View SecuRA Configurations, User Activity including Device operation Audits

The below modules can be accessed directly from the Top panel:

⚙	Manage	Displays expanded view of modules like User Accounts, Account Management, Notification, Application details, Manage, Database and Process Config.

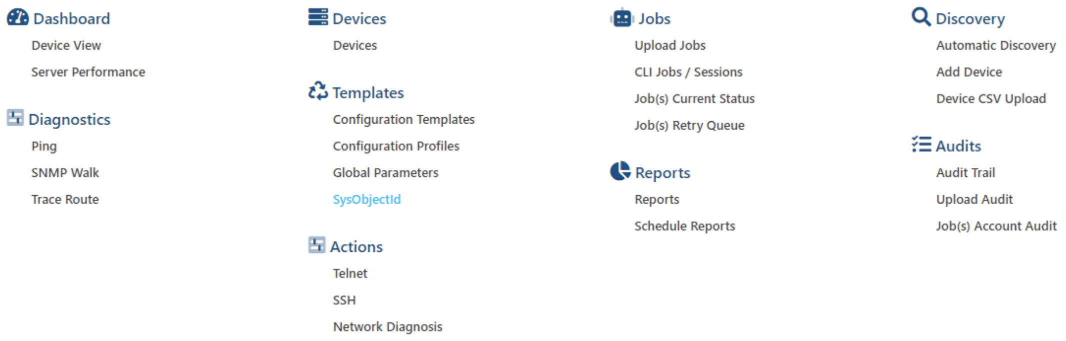
6. Title Bar

Title bar/Horizontal bar at the top of every page (other than the Pop-Up windows) depicts Product name, Global Device Search, and links to open My Approval page User Sign out from SecuRA session.



Menu:

Click on Infraon SecuRA logo on the top left corner to view an expanded form of the menus within SecuRA.

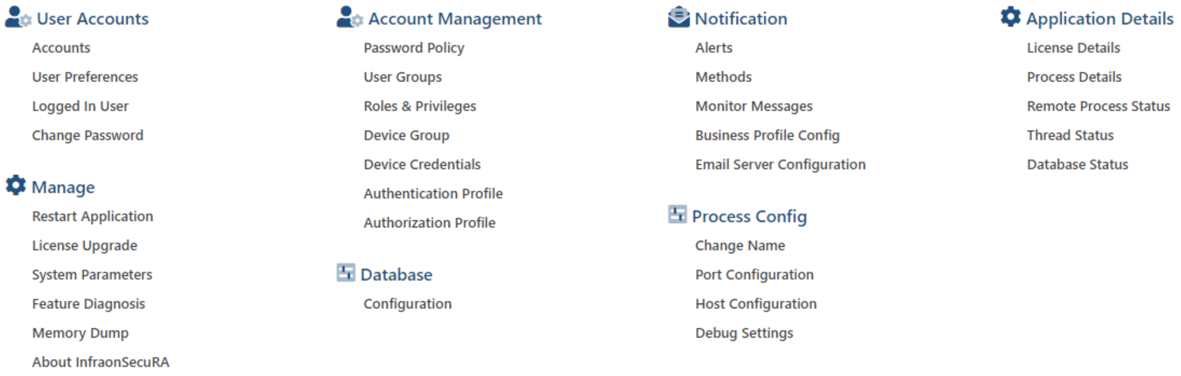


Search:

To locate a specific device or a group of devices from any page in SecuRA, enter node properties to search (use comma, semicolon, or single space separator) in the Textbox Search 🔍 and use “Enter” or Click 🔍. SecuRA will redirect the user to “Devices” page, listing the search result Devices.

Manage:

Click ⚙ to view Manage menu of SecuRA. Can be used to navigate to other modules.



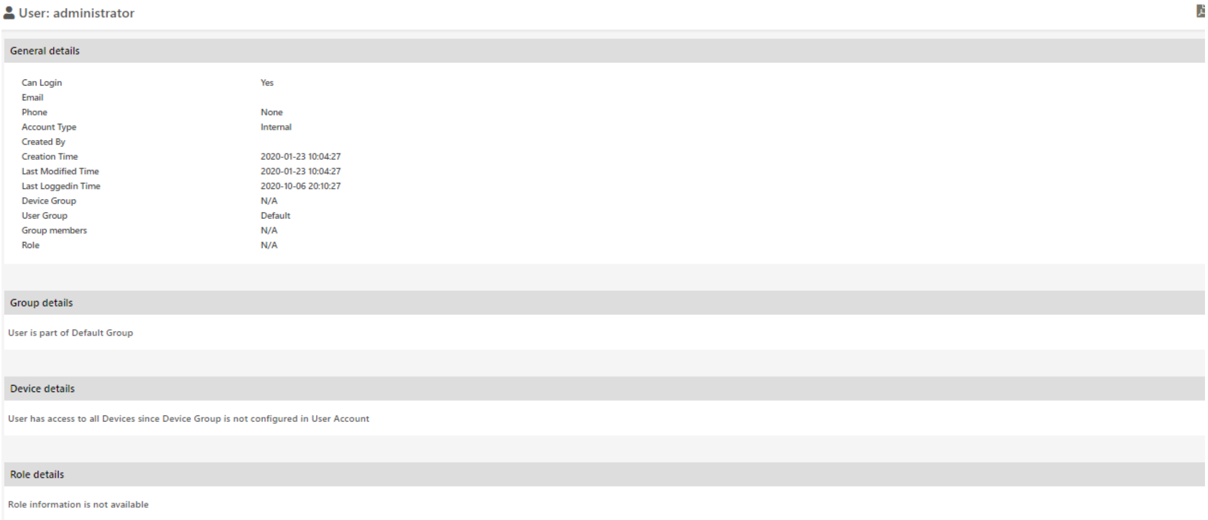
User Profile: Click the User Account icon A (usually the first alphabet of the Username) to view user profile related options within SecuRA.

Logout:

Click ⏻ Logout to exit the user session.

User Report:

Click User Report . This page displays User related information like General, Approval, Group, Device and Roles & Privileges Details. These details can be exported into PDF by clicking



User: administrator

General details

Can Login	Yes
Email	
Phone	None
Account Type	Internal
Created By	
Creation Time	2020-01-23 10:04:27
Last Modified Time	2020-01-23 10:04:27
Last Loggedin Time	2020-10-06 20:10:27
Device Group	N/A
User Group	Default
Group members	N/A
Role	N/A

Group details

User is part of Default Group

Device details

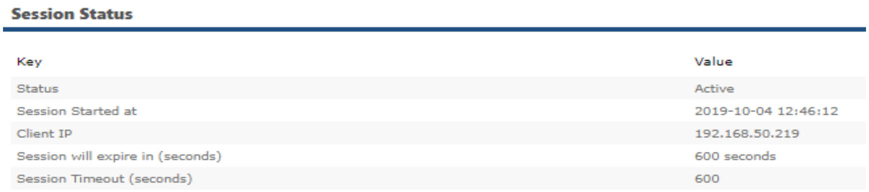
User has access to all Devices since Device Group is not configured in User Account

Role details

Role information is not available

Session Detail:

Click Username and select Session Detail . This Page displays details of the current session.

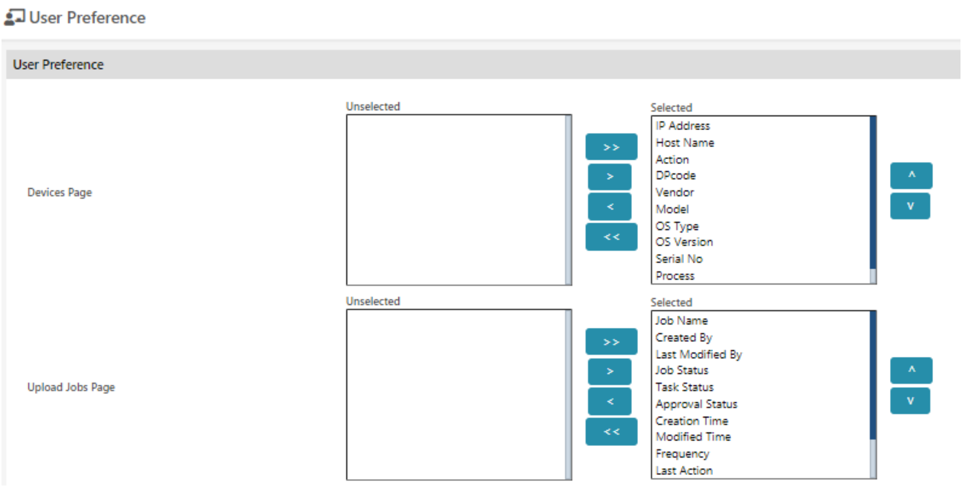


Session Status

Key	Value
Status	Active
Session Started at	2019-10-04 12:46:12
Client IP	192.168.50.219
Session will expire in (seconds)	600 seconds
Session Timeout (seconds)	600

User Preference:

Click User Name and select User Preference to change page view preferences of Devices, Upload Job and CLI Job pages. Remember to save the changes.



User Preference

User Preference

Devices Page

Unselected

Selected

IP Address
Host Name
Action
DPcode
Vendor
Model
OS Type
OS Version
Serial No
Process

Upload Jobs Page

Unselected

Selected

Job Name
Created By
Last Modified By
Job Status
Task Status
Approval Status
Creation Time
Modified Time
Frequency
Last Action

Set Default Page:

From any page within SecuRA, the user can click on the User Account icon A (usually the first alphabet of the Username) and Set Default Page to select the current page as the default landing page for the logges in user.

Default Page is updated successfully

Server Time:

On the Right side, SecuRA displays the current Server time along with session expiry time 13:06:29 - 24 Jun 2020 Session expires in 00:58:06 (when the page is queried). This is auto updated.

Note: *Please ensure that the server time is in sync with NTP servers.*

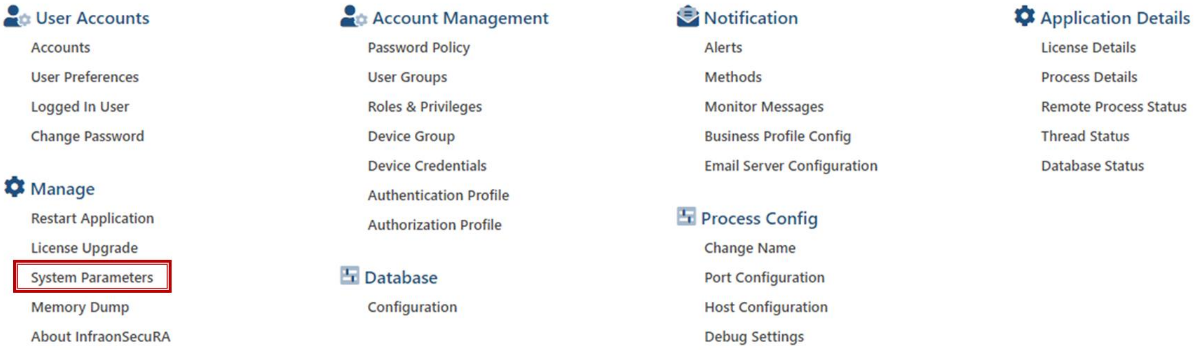
7. System Parameters

This is a Privilege based feature: The user will be able to access, view, add, edit, delete, execute & export, only if privileges have been given by the administrator. This will be defined under roles and privileges.

This menu is accessible only if the below privilege has been checked.

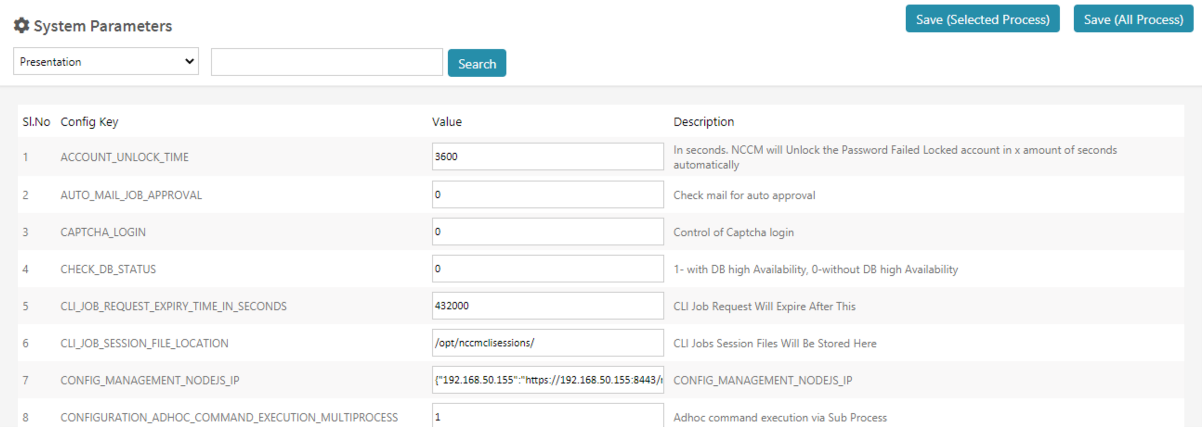
☑ System Administration

Click ⚙ on the top panel and select “System Parameters”.



'System Parameters' page displays name and value of parameters globally used by SecuRA. Though this is an open field, it is advised to 'Not Modify' the parameter value without knowing the parameter usage and impact. Parameters can be applied to a specific process or across all processes by using 'apply all' or 'apply specific' process button.

Click "System Parameters", to view the System configuration window.



Sl.No	Config Key	Value	Description
1	ACCOUNT_UNLOCK_TIME	3600	In seconds. NCCM will Unlock the Password Failed Locked account in x amount of seconds automatically
2	AUTO_MAIL_JOB_APPROVAL	0	Check mail for auto approval
3	CAPTCHA_LOGIN	0	Control of Captcha login
4	CHECK_DB_STATUS	0	1- with DB high Availability, 0-without DB high Availability
5	CLI_JOB_REQUEST_EXPIRY_TIME_IN_SECONDS	432000	CLI Job Request Will Expire After This
6	CLI_JOB_SESSION_FILE_LOCATION	/opt/nccmclisessions/	CLI Jobs Session Files Will Be Stored Here
7	CONFIG_MANAGEMENT_NODEJS_IP	{"192.168.50.155":"https://192.168.50.155:8443/	CONFIG_MANAGEMENT_NODEJS_IP
8	CONFIGURATION_ADHOC_COMMAND_EXECUTION_MULTIPROCESS	1	Adhoc command execution via Sub Process

System parameters can be configured based on the datacenter option, chosen using the dropdown menu.

Sl.No	Config Key	Value	Description
1	ACCOUNT_UNLOCK_TIME	60	In seconds. NCCM will Unlock the Password Failed Locked account in x amount of seconds automatically

2	CAPTCHA_LOGIN	1	Control of Captcha login
3	CHECK_DB_STATUS	0	1- with DB high Availability, 0-without DB high Availability
4	CLI_JOB_REQUEST_EXPIRY_TIME_IN_SECONDS	43200	CLI Job Request Will Expire After This
5	CLI_JOB_SESSION_FILE_LOCATION	/opt/nccmclisessions	CLI Jobs Session Files Will Be Stored Here
6	CLI_SESSION_IDLE_TIMEOUT	180	CLI Session Closing time for idle
7	CONFIG_MANAGEMENT_NODEJS_IP	{"192.168.50.167": "http://192.168.50.167:8080/everestnms/config"}	CONFIG_MANAGEMENT_NODEJS_IP
8	CONFIGURATION_ADHOC_COMMAND_EXECUTION_MULTIPROCESS	1	Adhoc command execution via Sub Process
9	CONFIGURATION_UPLOAD_MULTIPROCESS	1	Configuration Upload via Sub Process
10	CREATE_TEMP_DB_CONN	1	After Maximum connections allow creating new connection
11	DB_LOSS_NOTIFICATION_WAIT_TIME	300	This flag is to wait for 300 secs before sending the Database Connectivity Loss
12	DB_POOL_SIZE	20	Inital number of Database connections
13	DB_TIME_ZONE	Asia/Kolkata	Database Server Time Zone

14	DEBUG_MODULES	["General", "Poll", "SNMP"]	DEBUG_MODULES
15	DEFAULT_CHECKSUM_REFRESH	20000	In Milli Seconds
16	DEFAULT_LOGIN_PAGE	pconfigmangement	First Page After Login for Every Users
17	DEVICE_VIEW_CHECKSUM_REFRESH	1200000	In Milli Seconds
18	DO_API_DOWNLOAD	0	Configuration Download through API Module
19	DO_NCCM_PERFORMANCE_POLLING	0	NCCM Server Monitoring
20	FILE_MANAGEMENT_CLAM_AV_COMMAND	clamscan	To Scan the uploading files by clamAV
21	FILE_MANAGEMENT_F_SECURE_COMMAND	fsav	To Scan the uploading files by F-Secure
22	FILE_MANAGEMENT_SYMANTEC_COMMAND	/opt/Symantec/symantec_antivirus/./sav	To Scan the uploading files by Symantec
23	FPING_TIMEOUT	500	FPING_TIMEOUT
24	HA_OSIMAGE_SYNC	{}	High Availability TFTP Server IPs
25	HIDE_DEVICES_PAGE_COLUMNS	["DPcode"]	Hiding System Level device page column
26	INTERNATIONALIZATION_INSERT_FLAG	0	if set to 1, the new text in the UI will get inserted in the international.txt and mapping.py files.

27	INVALID_USER_RETRY_COUNT	2	INVALID_USER_RETRY_COUNT
28	KEEP_SAME_CLI_CONNECTION_OBJECT_UPLOAD_JOB	1	Same CLI Connection Object across Upload features
29	LICENSE_CHECK_INTERVAL	3600	License breach check time and the value should be in seconds
30	LOGIN_TIMEOUT	3600	In Seconds
31	MASTER1	master1	MASTER1
32	MASTER2	master2	MASTER2
33	MAX_DB_POOL_SIZE	50	Maximum number of Database connections
34	MAXIMUM_CONCURRENT_CONFIGURATION_UPLOAD_COUNT	10	Number of Concurrent Task Upload
35	MAXIMUM_CONCURRENT_CONFIGURATION_UPLOAD_IP_COUNT	25	Number of Concurrent Task IP Upload
36	NCCM_HTTP_PRESENTATION_URL	http://127.0.0.1:9000	NCCM HTTP URL for Sending Email for Command Authorization Execute and Notify
37	NO_OF_DATABASE_BACKUP_COPIES_TO_MAINTAIN	5	Number of Database Backup copies to maintain in the system
38	NO_OF_NOTIFICATION_WORKER_THREAD	1	Number of Thread count

39	NOTIFY_START_BASELINE_DIFFERENCE	0	To Notify Startup Baseline change
40	ODBC_CHECK_FREQUENCY	15	This flag is to sleep between each Database connectivity check if the database is down.
41	OS_CHECK_INTERVAL	3600	OS Version Check Interval Time
42	PASSWORD_RESET_LINK_EXPIRY	300	PASSWORD_RESET_LINK_EXPIRY
43	PASSWORD_RESET_URL	https://192.168.50.123	NCCM Presentation URL for Password Reset
44	PDF_FIRST_PAGE	1	PDF_FIRST_PAGE
45	PING_PACKETS_IN_BYTES	24	Implies 32 as 8 more bytes is added by Fping. :(
46	REMEDY_JOB_REQUEST_EXPIRY_TIME_IN_SECONDS	7776000	REMEDY Job Will Expire After This
47	RemoteProcessWaitTime	600	RemoteProcessWaitTime
48	SERVER_ZIP_FILE_START_TIME(HH:MM)	0.0423611	Fix JSON zip file start time
49	SMTP_local_hostname	localhost	update the result of socket.getfqdn() if facing any connectivity issue
50	SMTPTIMEOUT	10	10 sec

51	UPLOAD_JOB_REQUEST_EXPIRY_TIME_IN_SECONDS	7776000	UPLOAD Job Will Expire After This
52	WAIT_PERIOD_FOR_CONNECTION	1	no.of sec need to wait if all connections are being used.

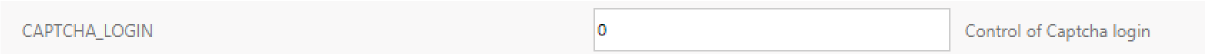
Click Save (Selected Process) to save the values for the current process or click Save (All Process) to save across all processes. Configuration Changes (applied newly) will be displayed. Scroll down and click Save Config to save.

Following Parameters must mandatorily be updated during SecuRA deployment or implementation

- CLI_JOB_SESSION_FILE_LOCATION
    - The folder location where CLI Session Audits will be stored on SecuRA DB Server
- CONFIG_MANAGEMENT_NODEJS_IP
    - CLI service installed server's IP (could be in DB Server IP Address) in dictionary format mentioned in above table

If Infraon SecuRA is integrated with NMS, the relevant sync should be enabled (can be found in system parameters with Sync keyword).

Additionally, the parameter for Captcha code can be managed here.



CAPTCHA_LOGIN	0	Control of Captcha login

If Captcha parameter is set to '1' captcha will be enabled in the below screens

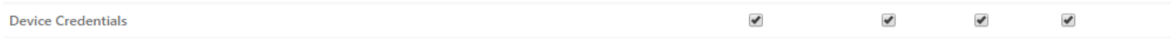
- Login page.

- Change Password
- Reset Password

8. Device Credentials

This is a Privilege based feature: The user will be able to access, view, add, edit, delete, execute & export, only if privileges have been given by the administrator. This will be defined under roles and privileges.

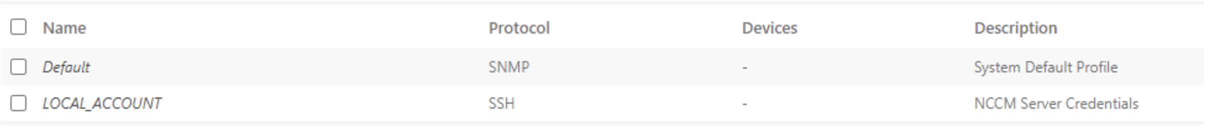
This menu is accessible only if the below privilege has been checked.



Device Credentials	☑	☑	☑	☑

Device Credentials module of Infraon SecuRA enables the administrator and user configure and store Device/Account information such as login credentials (user name, password, enable password) of a specific Connection Protocol across SNMP/SSH/TELNET/FTP/HTTP. Device Credentials are used in 'Discovery' and hence it is important to create before discovering the devices for management.

From the left panel, click ⚙ and select "Device Credentials".

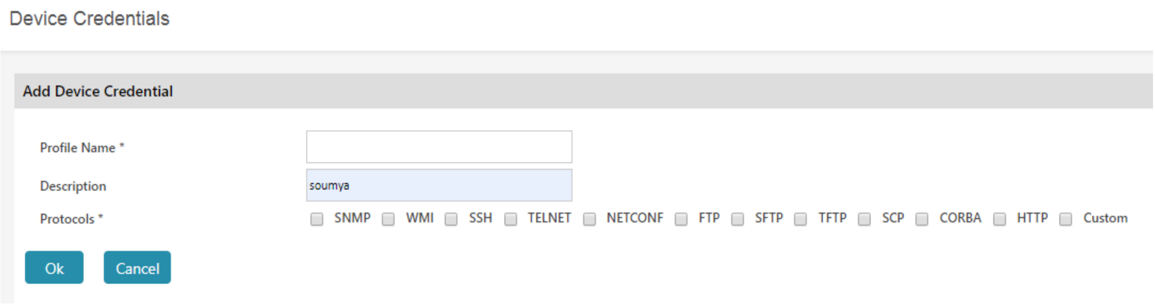


☐ Name	Protocol	Devices	Description
☐ *Default*	SNMP	-	System Default Profile
☐ *LOCAL_ACCOUNT*	SSH	-	NCCM Server Credentials

+ − × Add/Edit/Delete actions can be performed using the action icons.

8.1. Add Device Credentials

- Click + to add a new Device Credential profile.
- Add a Profile Name* and Description.
- Check the relevant communication protocol, applicable to the device.



Device Credentials

Add Device Credential

Profile Name *

Description: soumya

Protocols * ☐ SNMP ☐ WMI ☐ SSH ☐ TELNET ☐ NETCONF ☐ FTP ☐ SFTP ☐ TFTP ☐ SCP ☐ CORBA ☐ HTTP ☐ Custom

Additional options to add the parameters as per the selected protocol would be displayed.

- Add credentials for the selected protocol.

Click Ok to save the profile. Repeat steps until the profiles for all the devices are added.

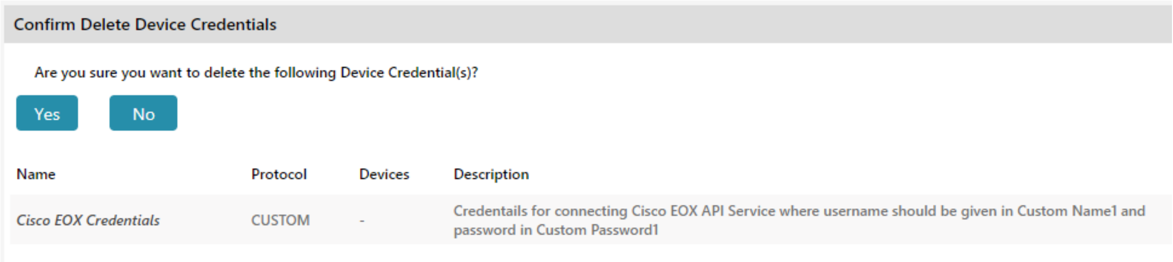
Note: *Appropriate device communication protocol needs to be selected while configuring device credential to build successful connectivity.*

8.2. Edit Device Credentials

Select any profile and click ⊖ to make changes. Once done, click Ok to save the changes.

8.3. Delete Device Credentials

Select a profile and click ⊗ to delete the device credential(s).



Confirm Delete Device Credentials

Are you sure you want to delete the following Device Credential(s)?

Yes No

Name	Protocol	Devices	Description
Cisco EOX Credentials	CUSTOM	-	Credentails for connecting Cisco EOX API Service where username should be given in Custom Name1 and password in Custom Password1

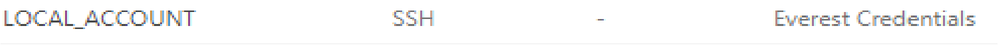
Click Yes to delete the device credentials.

Click No to cancel the delete operation.

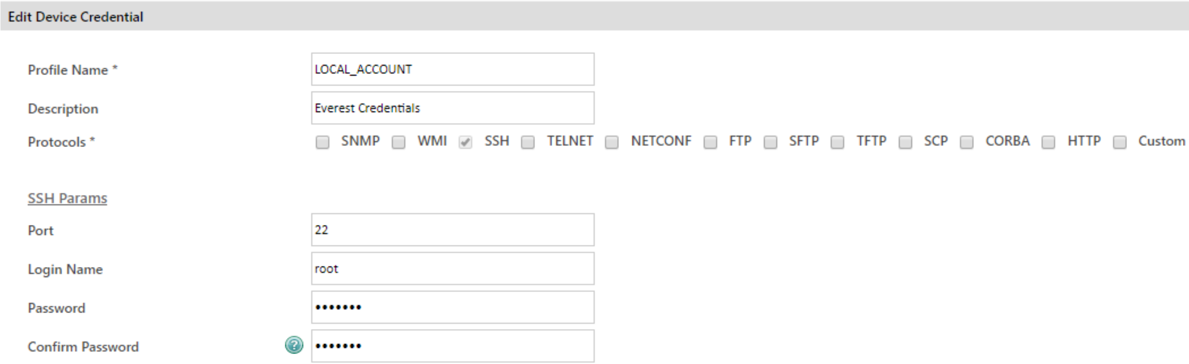
8.4. Default Credentials

1. Local Account

This profile is used by all SecuRA Processes for connecting SecuRA DB Server to upload Configuration into TFTP Repository and DB Backup process triggering.



LOCAL_ACCOUNT	SSH	-	Everest Credentials



Edit Device Credential

Profile Name *	LOCAL_ACCOUNT
Description	Everest Credentials
Protocols *	□ SNMP □ WMI ☑ SSH □ TELNET □ NETCONF □ FTP □ SFTP □ TFTP □ SCP □ CORBA □ HTTP □ Custom

SSH Params

Port	22
Login Name	root
Password	•••••••
Confirm Password	•••••••

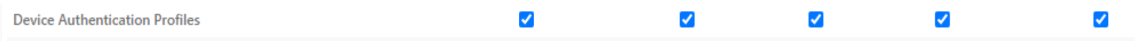
Description:

- In SSH Login Name, mention SecuRA DB Server SSH root account name.
- In SSH Password, mention SecuRA DB Server SSH root account password.
- In SSH Confirm Password field, mention SecuRA DB Server SSH root account password.

9. Authentication Profile

This is a Privilege based feature: The user will be able to access, view, add, edit, delete, execute & export, only if privileges have been given by the administrator. This will be defined under roles and privileges.

This menu is accessible only if the below privilege has been checked.



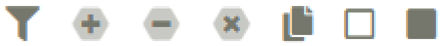
Device Authentication Profiles	☑	☑	☑	☑	☑

'Device Authentication Profile' enables authentication of user/user groups (verifying user identity) to access devices through CLI session.

From the left panel, click and select 'Authentication Profile'.

9.1. Action Icons – Authentication Profile Page

Multiple action icons are displayed on the top right corner of the page.



Icons	Label	Actions
▼	Filter	Click to use filter options to search
⊕	Add	Click to add 'Authentication Profile'
⊖	Edit	Click to edit the Authentication Profile
⊗	Delete	Click to delete an Authentication Profile
⧉	Clone	Click to clone an 'Authentication Profile'
☐	Enable	Click to enable the Authentication Profile
■	Disable	Click to disable the Authentication Profile

9.2. Authentication Profile Filter

User can search through authentication profiles using the below filters

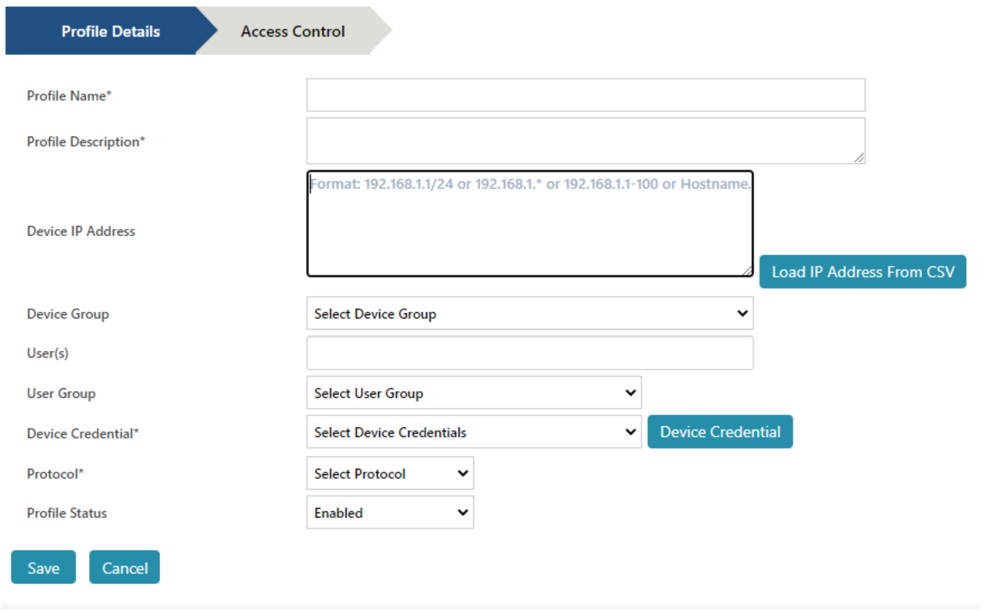
- Profile Name
- Device IP Address
  - Input can be a single Device IP Address or “list of Device IP Address separated by comma or semicolon or single space” or Device IP address in CIDR format.
- Device Group
- User Name
- User Group
- Device Credentials
- Protocol
- Status

Click Search to filter the authentication based on the filter applied.

9.3. Add Authentication Profile

Click ⊕ to add a Device Authentication profile. There are two tabs in ‘Add Device Authentication Profile’ page.

Add the below information in ‘Profile Details’ tab.



Profile Name*

Profile Description*

Device IP Address: Format: 192.168.1.1/24 or 192.168.1.* or 192.168.1.1-100 or Hostname.

Device Group: Select Device Group

User(s)

User Group: Select User Group

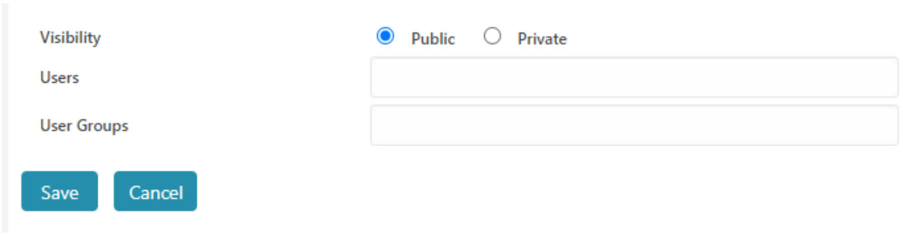
Device Credential*: Select Device Credentials

Protocol*: Select Protocol

Profile Status: Enabled

- Define a Profile Name* and Description.
- Provide the IP address(s) in the given textbox
  - Input can be a single Device management IP Address or "list of Device Management IP Address separated by comma or semicolon or single space" or Device IP address in CIDR format. Click Load IP Address From CSV to add IPs using CSV.
- Alternatively, select Device Group using the dropdown menu.
- Select user or user groups to authenticate.
- Select Device credentials, as applicable (Click Device Credential to edit credentials)
- Select Protocol using the dropdown menu (SSH/Telnet/or both)
- Select Profile status (enabled/disabled).

Click Access Control and add the below information.



Visibility: ● Public ○ Private

Users

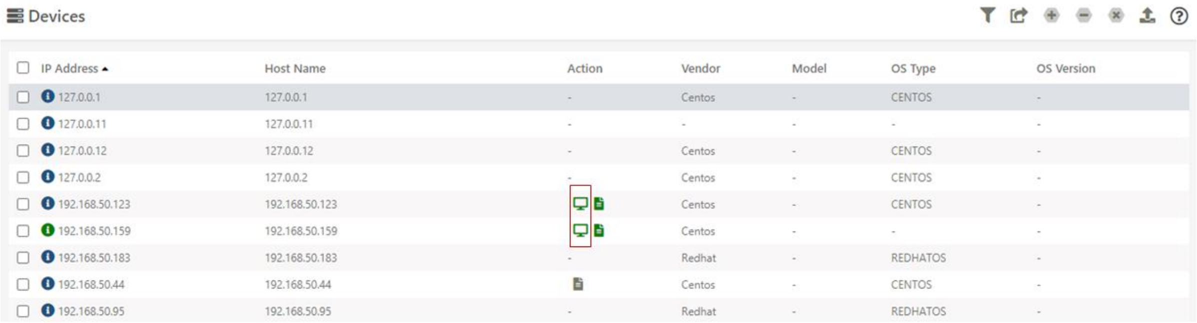
User Groups

- Select Profile visibility

    - Note: If the visibility is “Private”, User and User group dropdown will be enabled, and selected user and administrator will only be able view and manage the authentication profile.

- Select User(s).
- Select User group(s).
- Click Save to save the authentication profile.

When a user is authenticated, 🖥 icon will be enabled in the Devices & Device View page. User can click on this icon to sign-in (SSH or Telnet as selected by the admin) without prompting for Username/Password authentication. Please note that only Google Chrome (browser) supports Single Sign-On.



Devices

☐	IP Address ▲	Host Name	Action	Vendor	Model	OS Type	OS Version
☐	127.0.0.1	127.0.0.1	-	Centos	-	CENTOS	-
☐	127.0.0.11	127.0.0.11	-	-	-	-	-
☐	127.0.0.12	127.0.0.12	-	Centos	-	CENTOS	-
☐	127.0.0.2	127.0.0.2	-	Centos	-	CENTOS	-
☐	192.168.50.123	192.168.50.123	🖥 🗎	Centos	-	CENTOS	-
☐	192.168.50.159	192.168.50.159	🖥 🗎	Centos	-	-	-
☐	192.168.50.183	192.168.50.183	-	Redhat	-	REDHATOS	-
☐	192.168.50.44	192.168.50.44	🗎	Centos	-	CENTOS	-
☐	192.168.50.95	192.168.50.95	-	Redhat	-	REDHATOS	-

Note:

1. Multiple users can be authenticated for a single IP, enabling multiple users to access the same IP.
2. Duplicate authentication profiles cannot be created for the same user.

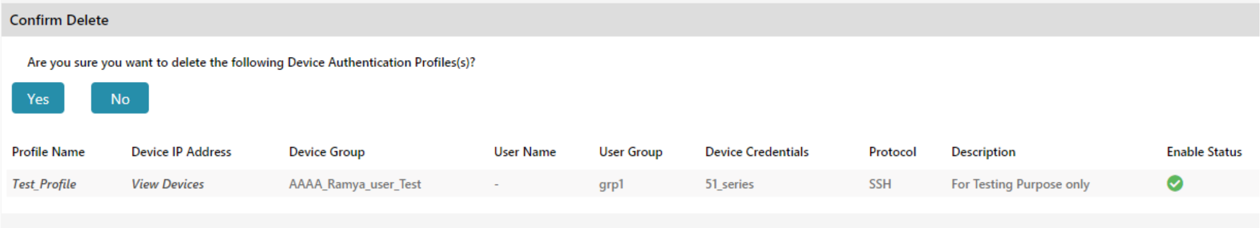
9.4. Edit Authentication Profile

Select a profile and click ⊖ to make the necessary changes and click Save to save the changes.

Note*: - Procedure to ‘Edit’ is similar to Add operation.*

9.5. Delete Authentication Profile

Select a profile and click ⊗ to delete.



Confirm Delete

Are you sure you want to delete the following Device Authentication Profiles(s)?

Profile Name	Device IP Address	Device Group	User Name	User Group	Device Credentials	Protocol	Description	Enable Status
Test_Profile	*View Devices*	AAAA_Ramya_user_Test	-	grp1	51_series	SSH	For Testing Purpose only	✓

Click Yes to delete.

Click No to cancel the delete operation.

9.6. Clone Authentication Profile

Clone Profile option can be used to copy a profile i.e. to duplicate an existing profile with minimal changes in the profile. Select a profile and click ⧉

Add Authentication Profile page appears with details pre-filled. Change inputs, as applicable and click Save to add a Profile.

9.7. Enable Authentication Profile

Select a Profile and click ☐ to change the enable the profile. Profiles will be marked with ✓

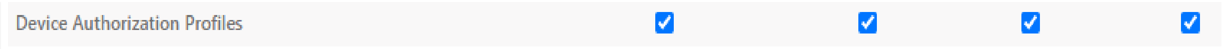
9.8. Disable Authentication Profile

Select a Profile and click ■ to 'Disable. Profiles will be marked with ✖.

10. Authorization Profile (SecuRA Pro)

This is a Privilege based feature: The user will be able to access, view, add, edit, delete, execute & export, only if privileges have been given by the administrator. This will be defined under roles and privileges.

This menu is accessible only if the below privilege has been checked.



Device Authorization Profiles	☑	☑	☑	☑

Device Authorization Profile enables authorizing user/user groups (controlling level of access) to perform actions on devices through CLI session.

From the left panel, click 👤 and select 'Authentication Profile'.

10.1. Action Icons – Authentication Profile Page

Multiple action icons are displayed on the top right corner of the page.

Icons	Label	Actions
▼	Filter	Click to use filter options to search
⊕	Add	Click to add 'Authorization Profile'
⊖	Edit	Click to edit the Authorization Profile
⊗	Delete	Click to delete an Authorization Profile
⧉	Clone	Click to clone an 'Authorization Profile'
□	Enable	Click to enable the Authorization Profile
■	Disable	Click to disable the Authorization Profile

10.2. Authorization Profile Filter

User can search through Authorization profiles using the below filters

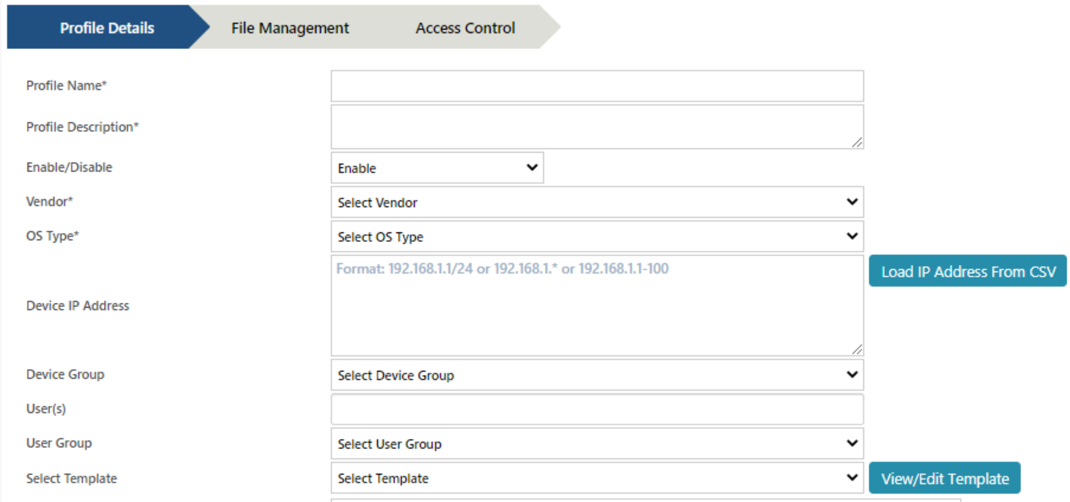
- Profile Name
- Vendor
- OS Type
- Device IP Address
  - Input can be a single Device IP Address or “list of Device IP Address separated by comma or semicolon or single space” or Device IP address in CIDR format.
- Device Group
- User Name
- User Group
- Permit Commands
- Deny Commands
- Ignore Commands
- Grant
- Status

Click Search to filter the authorization job based on the filter applied.

10.3. Add Authorization Profile

Click + to add a Device Authorization profile. There are three tabs in ‘Add Device Authorization Profile’ page.

Add the below information in ‘Profile Details’ tab.



Profile Name*	
Profile Description*	
Enable/Disable	Enable
Vendor*	Select Vendor
OS Type*	Select OS Type
Device IP Address	Format: 192.168.1.1/24 or 192.168.1.* or 192.168.1.1-100
Device Group	Select Device Group
User(s)	
User Group	Select User Group
Select Template	Select Template

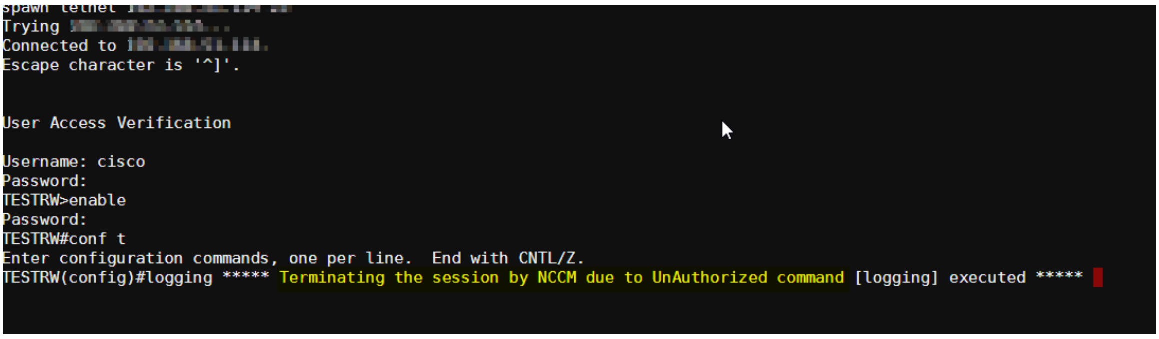
- Define a Profile Name* and Description.
- Select Vendor and OS Type using the dropdown menu.
- Provide the IP address(s) in the given textbox
  - Input can be a single Device management IP Address or “list of Device Management IP Address separated by comma or semicolon or single space” or Device IP address in CIDR format. Click Load IP Address From CSV to add IPs using CSV.
- Alternatively, select Device Group using the dropdown menu.
- Select user or user groups to authorize.
- Select Authorization Template using the dropdown menu. ***This option will be enabled only if an Authorization template has been created in the Configuration Templates section.*** Click View/Edit Template to view and edit existing templates.

- Input permit/Deny/Ignore commands in the respective textboxes.

Infraon SecuRA accepts command input in regex pattern only. Command inputs are split into three sections:

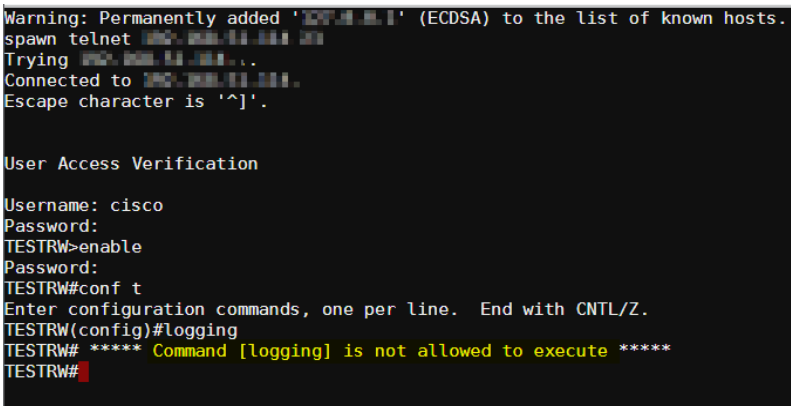
  - **Permit Commands** – Command (sets) that are permitted for execution by the User/User Group. Commands that are not added in the 'Permit' section will be blocked at the time of execution.
  - **Deny Commands** - Command (sets) that are denied for execution by the User/User Group. When a user tries to execute commands, which are mentioned in this section, SecuRA terminates the session or blocks the user and/or triggers a notification, as defined by the administrator.
  - **Ignore Commands** – used to ignore inputs like password and other User credential input. For example: When a user tries to execute a Command, that requires authentication by the system, the user is prompted by the system to provide additional information. In this case, the system prompt must be added in the 'Ignore' section. If not, system runs the command through the Permit command list and may end up blocking the command/command set.

- Select Grant* using the dropdown menu. Grant is used to define actions when the user inputs 'Deny' commands in the CLI session.
  - Terminate Session – Terminates the CLI Session immediately.



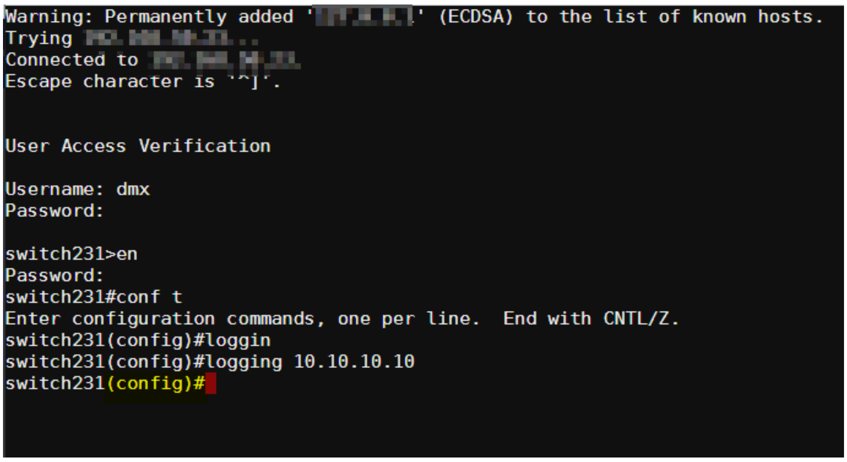
```
spawn telnet [redacted]
Trying [redacted]...
Connected to [redacted].
Escape character is '^]'.


User Access Verification

Username: cisco
Password:
TESTRW>enable
Password:
TESTRW#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
TESTRW(config)#logging ***** Terminating the session by NCCM due to UnAuthorized command [logging] executed *****
```

  - Block Command – Blocks the command from being executed.



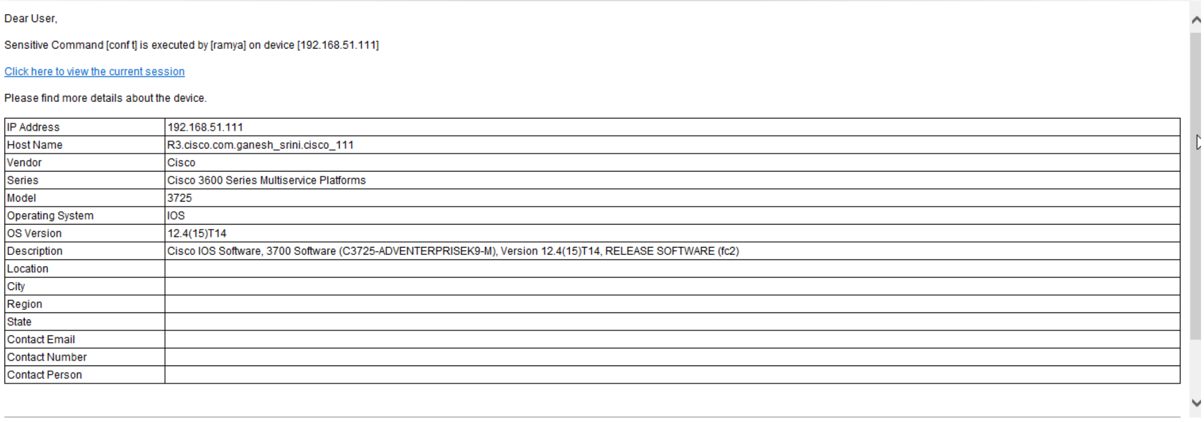
```
Warning: Permanently added '[redacted]' (ECDSA) to the list of known hosts.
spawn telnet [redacted]
Trying [redacted]...
Connected to [redacted].
Escape character is '^]'.


User Access Verification

Username: cisco
Password:
TESTRW>enable
Password:
TESTRW#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
TESTRW(config)#logging
TESTRW# ***** Command [logging] is not allowed to execute *****
TESTRW#
```

- ○ Execute and Notify – Executes the given command and triggers a notification about the action. If this option is selected, select Notifier (user) using the dropdown menu.



```
Warning: Permanently added '[redacted]' (ECDSA) to the list of known hosts.
Trying [redacted]...
Connected to [redacted].
Escape character is '^]'.


User Access Verification

Username: dmx
Password:

switch231>en
Password:
switch231#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
switch231(config)#loggin
switch231(config)#logging 10.10.10.10
switch231(config)#
```

- Select 'Notifier' (user) to be notified for 'Execute & Notify' option of grant command. Selected user receives a notification as displayed below, when the specified command is executed by the user.



Dear User,

Sensitive Command [conf t] is executed by [ramya] on device [192.168.51.111]

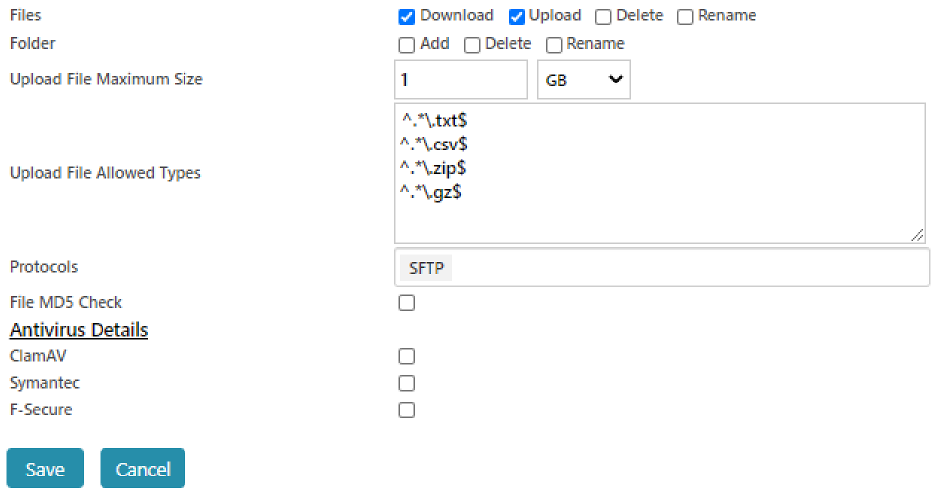
Click here to view the current session

Please find more details about the device.

IP Address	192.168.51.111
Host Name	R3.cisco.com.ganesh_srini.cisco_111
Vendor	Cisco
Series	Cisco 3600 Series Multiservice Platforms
Model	3725
Operating System	IOS
OS Version	12.4(15)T14
Description	Cisco IOS Software, 3700 Software (C3725-ADVENTERPRISEK9-M), Version 12.4(15)T14, RELEASE SOFTWARE (fc2)
Location	
City	
Region	
State	
Contact Email	
Contact Number	
Contact Person	

- Enable the check boxes to block 'Up/Down' keys and horizontal tab keys on the CLI session.

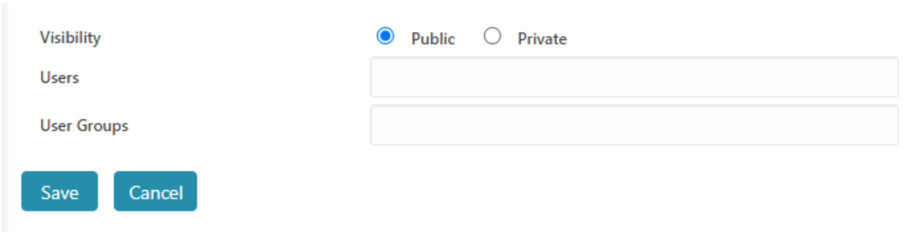
Click File Management. Authorization for the File management module can be selected here.



Files	☑ Download ☑ Upload □ Delete □ Rename
Folder	□ Add □ Delete □ Rename
Upload File Maximum Size	1 GB
Upload File Allowed Types	^.*\.txt$ ^.*\.csv$ ^.*\.zip$ ^.*\.gz$
Protocols	SFTP
File MD5 Check	□
Antivirus Details	
ClamAV	□
Symantec	□
F-Secure	□

- Use checkboxes to enable access to Download, Upload, Delete and Rename operations on files. Only selected actions will be enabled for the user.
- Use checkboxes to enable access to Add, Delete and Rename operations on folders. Only selected actions will be enabled for the user.
- Select file size limit for upload actions.
- Provide file extensions that can be allowed for upload by the user.
- Add Protocols (SFTP)
- Check 'File MD5' check key to enable MD5 hash key verification for file uploads.
- Select antivirus (Clam AV, Symantec, F-Secure) to scan the selected files/folders.

Click Access Control and add the below information.



Visibility	● Public ○ Private
Users	
User Groups	

- Select Profile visibility
  - Note: If the visibility is "Private", User and User group dropdown will be enabled, and selected user and administrator will only be able view and manage the authorization profile.

- Select User(s).
- Select User group(s).
- Click Save to save the authorization profile.

Note:

1. Multiple users can be authorized for a single IP, enabling multiple users to access the same IP.
2. Duplicate authorization profiles cannot be created for the same user.

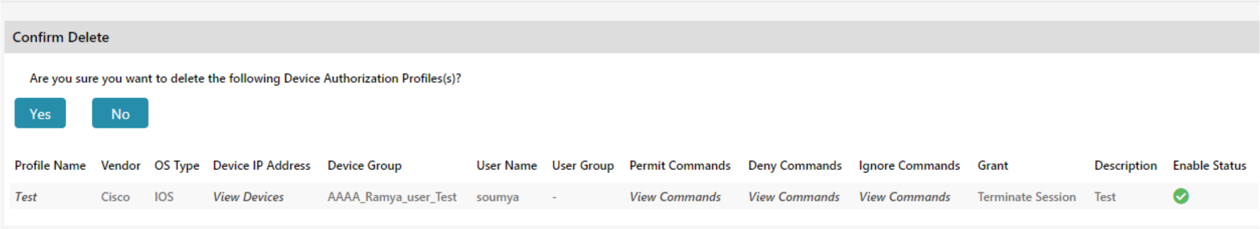
10.4. Edit Authorization Profile

Select a profile and click ⊖ to make the necessary changes and click Save to save the changes.

Note: *- Procedure to 'Edit' is similar to Add operation.*

10.5. Delete Authorization Profile

Select a profile and click ⊗ to delete.



Confirm Delete

Are you sure you want to delete the following Device Authorization Profiles(s)?

Yes No

Profile Name	Vendor	OS Type	Device IP Address	Device Group	User Name	User Group	Permit Commands	Deny Commands	Ignore Commands	Grant	Description	Enable Status
Test	Cisco	IOS	*View Devices*	AAAA_Ramya_user_Test	soumya	-	*View Commands*	*View Commands*	*View Commands*	Terminate Session	Test	✓

Click Yes to delete.

Click No to cancel the delete operation.

10.6. Clone Authorization Profile

Clone Profile option can be used to copy a profile i.e. to duplicate an existing profile with minimal to no changes in the profile. Select a profile and click ⧉

Add Authorization Profile page appears with details pre-filled. Change inputs, as applicable and click Save to add a Profile.

10.7. Enable Authorization Profile

Select a Profile and click □ to change the enable the profile. Profiles will be marked with ✓

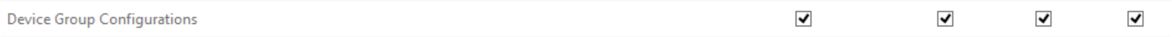
10.8. Disable Authorization Profile

Select a Profile and click ■ to ‘Disable. Profiles will be marked ⊗.

11. Device Group

This is a Privilege based feature: The user will be able to access, view, add, edit, delete, execute & export, only if privileges have been given by the administrator. This will be defined under roles and privileges.

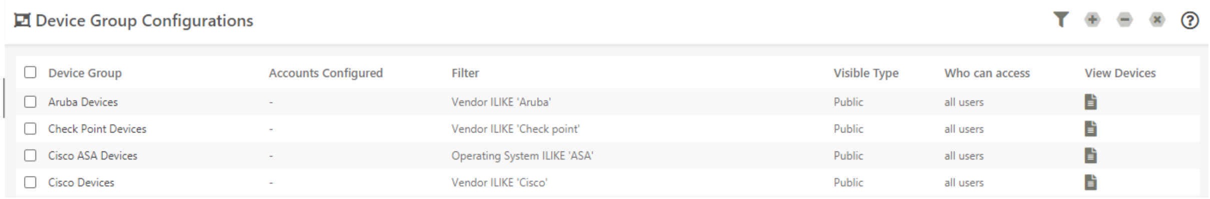
This menu is accessible only if the below privilege has been checked.



Device Group Configurations	☑	☑	☑	☑

From the left panel, click 👤 and select ‘Device Group’.

Device Group is a way of grouping devices under a profile based on Vendor, Configuration Profile, State, City, Location, and Device Type etc. This Device Group profile can be applied in User Group (for Controlling User login to access devices only on specific Device Group Profile), Reports, Dashboards, Upload Job Device Selection, Device Grid pages for filtering purpose etc.

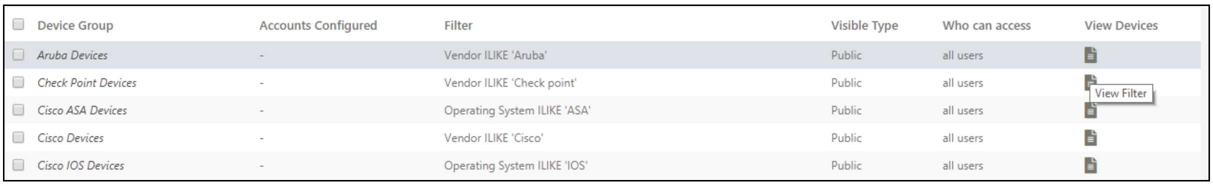


Device Group Configurations

□ Device Group	Accounts Configured	Filter	Visible Type	Who can access	View Devices
□ Aruba Devices	-	Vendor ILIKE 'Aruba'	Public	all users	🗎
□ Check Point Devices	-	Vendor ILIKE 'Check point'	Public	all users	🗎
□ Cisco ASA Devices	-	Operating System ILIKE 'ASA'	Public	all users	🗎
□ Cisco Devices	-	Vendor ILIKE 'Cisco'	Public	all users	🗎

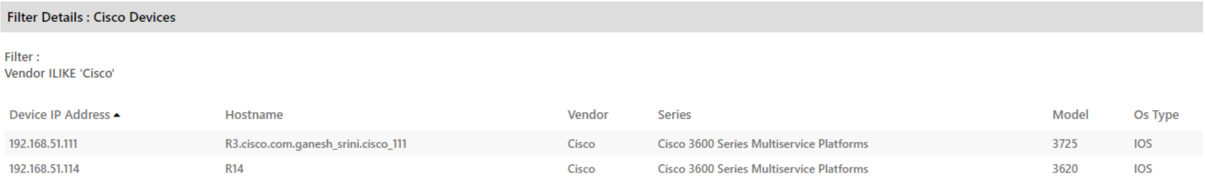
Add Edit and Delete operations of Device Group Profile are done from this page.

▼ (Filter) is used to search (Regex Pattern Search) Device Group profile based on Device Group Name and Device Group Filter condition.



□ Device Group	Accounts Configured	Filter	Visible Type	Who can access	View Devices
□ *Aruba Devices*	-	Vendor ILIKE 'Aruba'	Public	all users	🗎
□ *Check Point Devices*	-	Vendor ILIKE 'Check point'	Public	all users	🗎
□ *Cisco ASA Devices*	-	Operating System ILIKE 'ASA'	Public	all users	🗎
□ *Cisco Devices*	-	Vendor ILIKE 'Cisco'	Public	all users	🗎
□ *Cisco IOS Devices*	-	Operating System ILIKE 'IOS'	Public	all users	🗎

The **View Filter** option on each Device Group Profile row displays the Devices based on Group created. This will help confirm the Device Group Profile conditions are working before applying on other features.



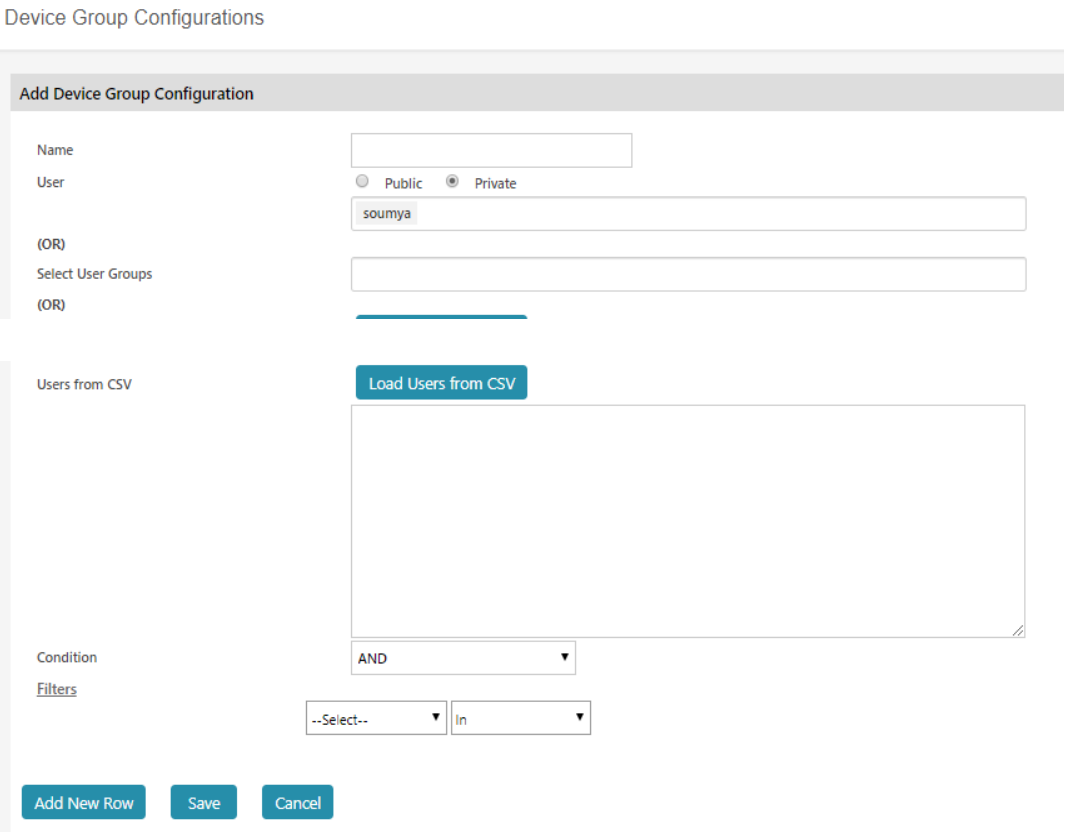
Filter Details : Cisco Devices

Filter :
Vendor ILIKE 'Cisco'

Device IP Address ▴	Hostname	Vendor	Series	Model	Os Type
192.168.51.111	R3.cisco.com.ganesh_srini.cisco_111	Cisco	Cisco 3600 Series Multiservice Platforms	3725	IOS
192.168.51.114	R14	Cisco	Cisco 3600 Series Multiservice Platforms	3620	IOS

11.1. Add Device group

Click + to add a device profile.



Device Group Configurations

Add Device Group Configuration

Name	
User	○ Public ● Private soumya
(OR)	
Select User Groups	
(OR)	
Users from CSV	Load Users from CSV
Condition	AND ▾
Filters	--Select-- ▾ In ▾

- Input the Device Group Profile Name in the Name textbox.
- Choose the User Visibility (Public or Private) using User Radio button.

Note: *If the visibility is "Private" then User dropdown will be shown. Users selected in the list and administrator user will only be able to use or see this Device Group profile.*

- If "Private" Select using the dropdown.
- Select User Groups using the dropdown menu or use the 'Load users from CSV' option.

- Select the condition (AND/OR) using the dropdown. When more than one Filter is selected then the condition value will be used to define how the conditions should be joined.
- In the Filters section, Select the Device Column/Property; choose the operator and the value for the Device Column/Property as per the requirement.
- SecuRA Support the following Device Column/Property.
    - Region
    - State
    - City
    - Location
    - Country
    - Host Name (Device Name)
    - IP Address (Device IP Address)
    - Vendor
    - Category
    - Product Type
    - Service Type
    - Series
    - Model
    - Device Type
    - Operating System
    - OS Version
    - MAC Address
    - Image File Name
    - End of Life
    - End of Support
    - Asset ID

- Owner
- Address
- Domain
- SysObjectID
- Priority
- Client
- Poller
- Configuration Profile

SecuRA Support the following Conditional Operator

- IN
- NOT IN
- Or
- Equal (=)
- Not Equal (!=)
- Like
- NOT ILIKE
- Greater (>)
- Greater or Equal (>=)
- Lesser (<)
- Lesser or Equal (<=)

Click Add New Row to add multiple filter conditions. Click Save to save the Device Group Profile or click Cancel to abort the operation.

Note:

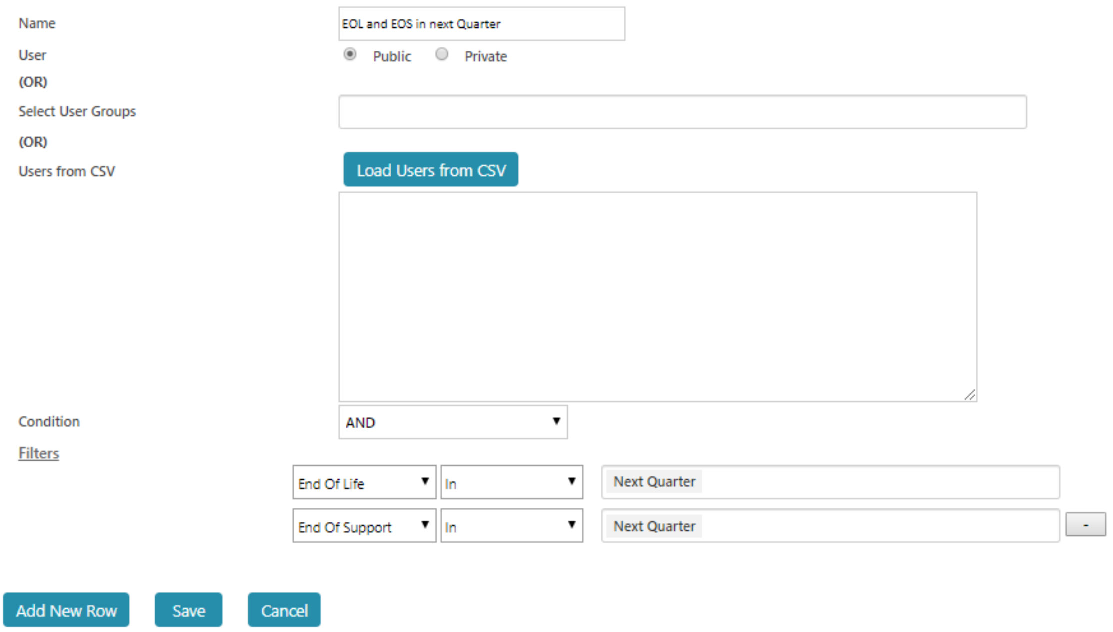
Bulk IP Copy Paste action will be allowed rather than selecting the IP's one by one.

The following formats are supported in device group

In Device Group IP address, the following formats we support

- 192.168.50.1 192.168.50.2 192.168.50.3 (space separator)
- 192.168.50.1,192.168.50.2,192.168.50.3 (comma separated IPs)
- 192.168.50. * (CIDR format)
- 192.168.50,1-3 (Range of IPs)
- All the above with a Comma separator

Given below is a sample Device Group Profile for Finding Cisco Devices which all End of Life and End of Support due in the next quarter.



Name: EOL and EOS in next Quarter

User: ● Public ○ Private

(OR)

Select User Groups

(OR)

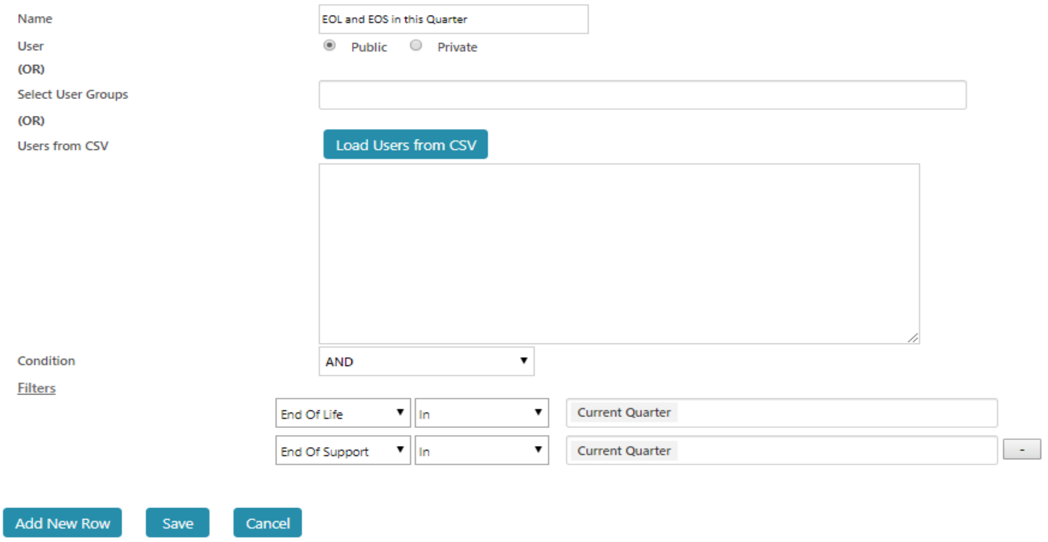
Users from CSV: Load Users from CSV

Condition: AND

Filters

End Of Life	In	Next Quarter
End Of Support	In	Next Quarter

Sample Device Group Profile for Finding Cisco Devices which all End of Life and End of Support happens in Current quarter



Name: EOL and EOS in this Quarter

User: ● Public ○ Private

(OR)

Select User Groups

(OR)

Users from CSV: Load Users from CSV

Condition: AND

Filters

End Of Life	In	Current Quarter
End Of Support	In	Current Quarter

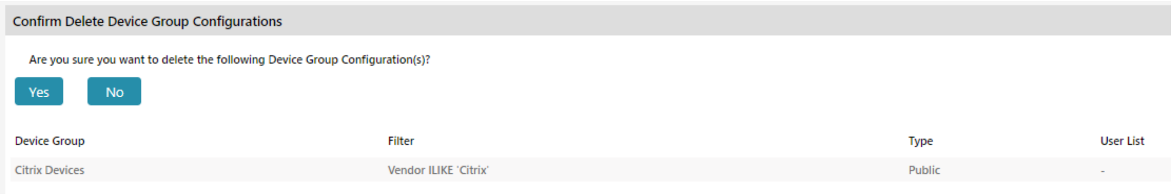
11.2. Edit Device Group

Select a Device Group profile and click ⊖ to make the necessary changes and click Save to save the changes.

***Note**: - Procedure to 'Edit' is similar to Add operation. Multiple configuration edit is not supported. Please select single configuration to edit.*

11.3. Delete Device Group

Select a Device Group profile and click ✖ to delete the device group(s) profile.



Confirm Delete Device Group Configurations

Are you sure you want to delete the following Device Group Configuration(s)?

Yes No

Device Group	Filter	Type	User List
Citrix Devices	Vendor ILIKE 'Citrix'	Public	-

Click Yes to delete the device group.

Click No to cancel the delete operation.

***Note**: - Make sure Device Group Profile selected for Deletion is not used in "User Group" for limiting user to access Specific Devices, Upload Jobs Device Group, Reports or Offline Reports.*

12. Discovery

This is a Privilege based feature: The user will be able to access, view, add, edit, delete, execute & export, only if privileges have been given by the administrator. This will be defined under roles and privileges.

This menu is accessible only if the below privilege has been checked.

Discovery ☑

Discovery is the process of boarding devices into SecuRA through SNMP and PING protocol. SecuRA supports all version of SNMP including v1, v2c and v3.

***Note:** - SNMP is mandatory on all devices and if SNMP is not running on devices SecuRA still board those devices (at least if reachable through PING) with zero inventory details of the device (including Hostname, Vendor, Series, Model, Serial Number, Device Type, Interfaces and every basic details).*

SecuRA supports four ways of Discovering Devices from network.

- Automatic Discovery *(SecuRA Pro)*
- CSV Upload Discovery *(SecuRA Pro)*
- Add Device

Discovery options can be accessed through the Discovery menu 🔍 on the left panel.

Note: SecuRA Standard version does not support Automatic Discovery & Device CSV Upload options.

Note for Auto Discovery:

1. IP address and Host Name uniqueness should be maintained throughout the application. Device managing through dynamic IP Address is not recommendable.

2. SecuRA Discovery module does not allow adding same Device more than once through other IPs of same Device, meaning when a Device is already added through Loopback IP, the same Device cannot be added through any of its Network IP.

3. Duplicate Discovery of IPs are not recommended.

12.1. Automatic Discovery

Automatic Discovery is the simplest way of discovering devices on network, due to minimal input to Discovery. IP Address is alone enough to initiate the discovery and all other inputs will come from System Default Parameters.

From the left panel, click 🔍 and select 'Automatic Discovery'.

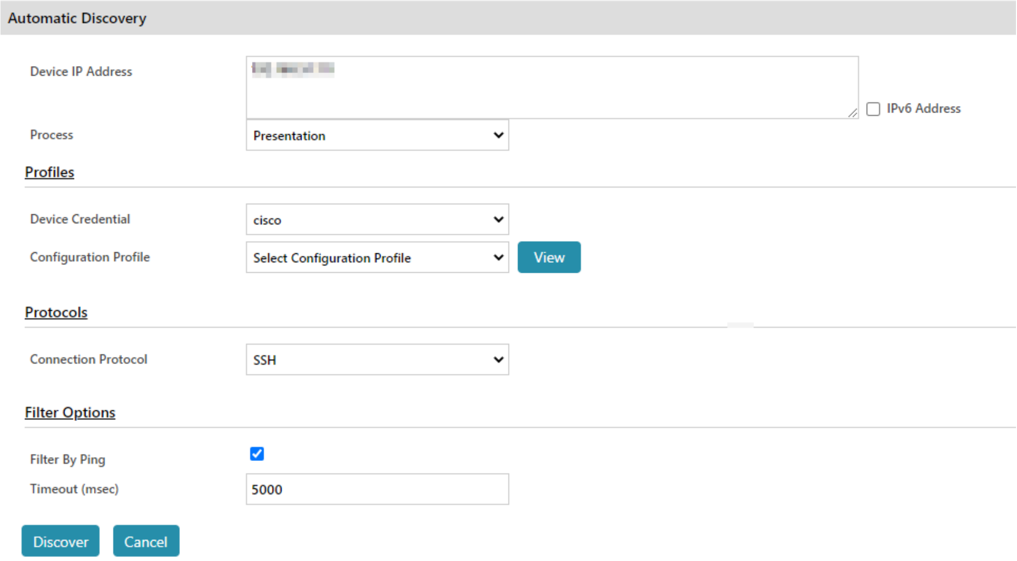
Follow the below steps to initiate Discovery

- Provide the IP address(s) in the given textbox
    - Input can be a single Device management IP Address or "list of Device Management IP Address separated by comma or semicolon or single space" or Device IP address in CIDR format.
- Select the SecuRA Process where it must be managed
    - Manage includes Device Inventory and Configuration Upload.
- Select Device credential Profile (only if the Range of Input Devices has same credential to manage) or keep it as Select Device Credential profile. SecuRA will automatically find the right profile for each device during discovery.
- Select Configuration profile (only if the Range of Input Devices can have the same profile to manage) or keep it as 'Select Configuration Profile'. SecuRA will automatically find the right Profile for each device during discovery.
- Select the Connection Protocol for the devices that are to be discovered.

- Select or deselect filter by ping.
    - If Filter by Ping is enabled, SecuRA will filter the PING response devices and send those Devices for Discovery process.
    - If Filter by ping is not selected, SecuRA will send all devices IP to Discovery process for SNMP Scan. Discovery could take more time when it discovery's not PING devices.

- Select Ping Time (in seconds). This will be used only when Filter by Ping is enabled.

Click 'Discover' to start the process immediately. Click 'Cancel' to abort the operation.



Automatic Discovery

Device IP Address [redacted] □ IPv6 Address

Process: Presentation

Profiles

Device Credential: cisco

Configuration Profile: Select Configuration Profile

Protocols

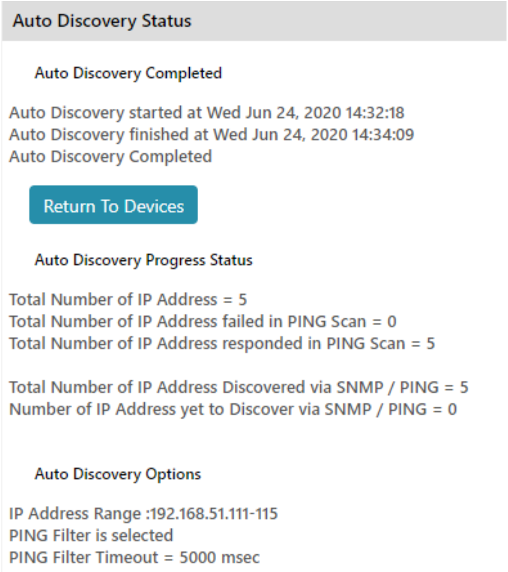
Connection Protocol: SSH

Filter Options

Filter By Ping ☑

Timeout (msec): 5000

Discovery Progress and completion summary reports the count of Success and Failure devices.



Auto Discovery Status

Auto Discovery Completed

Auto Discovery started at Wed Jun 24, 2020 14:32:18
Auto Discovery finished at Wed Jun 24, 2020 14:34:09
Auto Discovery Completed

Auto Discovery Progress Status

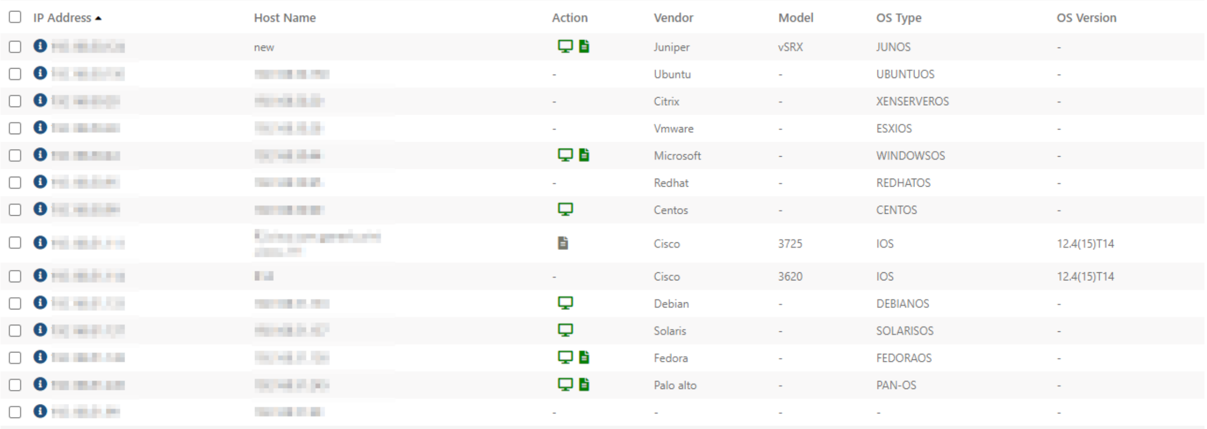
Total Number of IP Address = 5
Total Number of IP Address failed in PING Scan = 0
Total Number of IP Address responded in PING Scan = 5

Total Number of IP Address Discovered via SNMP / PING = 5
Number of IP Address yet to Discover via SNMP / PING = 0

Auto Discovery Options

IP Address Range :192.168.51.111-115
PING Filter is selected
PING Filter Timeout = 5000 msec

Device Grid page will list out all discovered Devices with inventory and configuration details.



□	IP Address ▲	Host Name	Action	Vendor	Model	OS Type	OS Version
□	ⓘ [redacted]	new	🖥 📄	Juniper	vSRX	JUNOS	-
□	ⓘ [redacted]	[redacted]	-	Ubuntu	-	UBUNTUOS	-
□	ⓘ [redacted]	[redacted]	-	Citrix	-	XENSERVEROS	-
□	ⓘ [redacted]	[redacted]	-	Vmware	-	ESXIOS	-
□	ⓘ [redacted]	[redacted]	🖥 📄	Microsoft	-	WINDOWSOS	-
□	ⓘ [redacted]	[redacted]	-	Redhat	-	REDHATOS	-
□	ⓘ [redacted]	[redacted]	🖥	Centos	-	CENTOS	-
□	ⓘ [redacted]	[redacted]	📄	Cisco	3725	IOS	12.4(15)T14
□	ⓘ [redacted]	[redacted]	-	Cisco	3620	IOS	12.4(15)T14
□	ⓘ [redacted]	[redacted]	🖥	Debian	-	DEBIANOS	-
□	ⓘ [redacted]	[redacted]	🖥	Solaris	-	SOLARISOS	-
□	ⓘ [redacted]	[redacted]	🖥 📄	Fedora	-	FEDORAOS	-
□	ⓘ [redacted]	[redacted]	🖥 📄	Palo alto	-	PAN-OS	-
□	ⓘ [redacted]	[redacted]	-	-	-	-	-

12.2. Device CSV Upload

Device CSV Upload Discovery is another advanced form of Automatic Discovery where in administrator can input more options to the Discovery process individually at device level.

Device CSV Upload allows administrator to discover a bulk of devices with additional device information like Device Location (State, City, Address), User managing the device (contact details), Type of Service, product Type, Priority of Device, Device managing Process etc.

Note: *Discovery and output process is the same as Auto discovery. Through Device CSV upload administrator can also perform edit/delete operations on the existing Device Properties in bulk manner.*

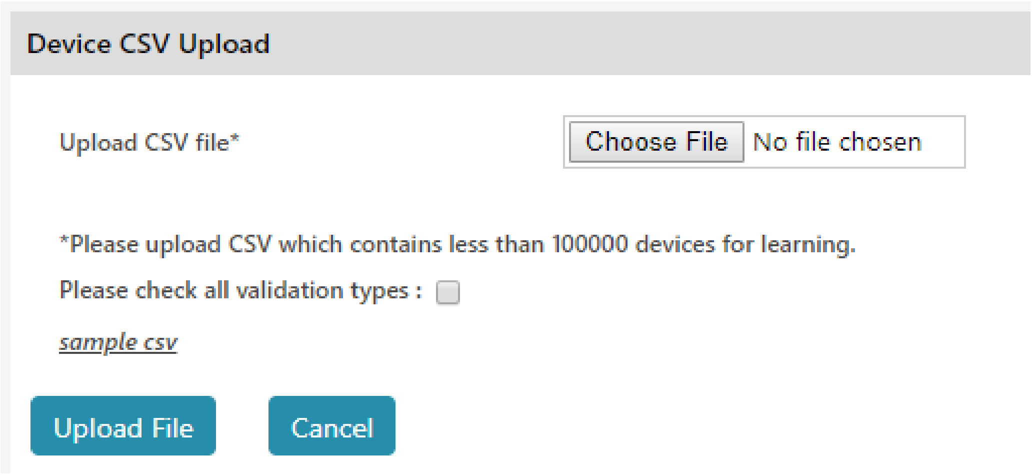
From the left panel, click 🔍 and select 'Device CSV Upload'.

Follow the below instructions to initiate Discovery of devices

- ○ Input all columns of Upload CSV file (IP Address, Flag, Process are the mandatory).

- To 'Add/Discover' new device(s) into SecuRA, Flag value should be "1".
- To 'Edit' an existing device(s) from SecuRA, Flag value should be "2".
- To 'Delete' an existing device(s) from SecuRA, Flag value should be "3".
- Click Choose File to select the CSV file.
- Check the Validation type checkbox to know the Error types.

- Click on sample csv to download a sample upload CSV file.
- Click Upload File to upload the selected CSV file to discover the bulk IPs.
- Click Cancel to discard the action.



Device CSV Upload

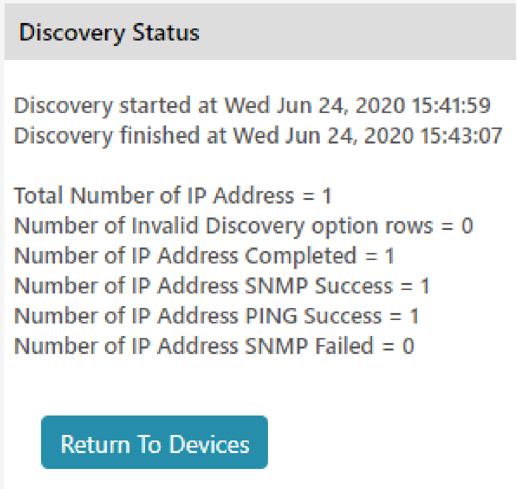
Upload CSV file* Choose File No file chosen

*Please upload CSV which contains less than 100000 devices for learning.

Please check all validation types : □

sample csv

Result page will be displayed like below



Discovery Status

Discovery started at Wed Jun 24, 2020 15:41:59
Discovery finished at Wed Jun 24, 2020 15:43:07

Total Number of IP Address = 1
Number of Invalid Discovery option rows = 0
Number of IP Address Completed = 1
Number of IP Address SNMP Success = 1
Number of IP Address PING Success = 1
Number of IP Address SNMP Failed = 0

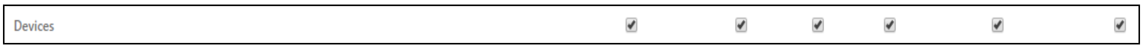
Note:

- *IP Address uniqueness should be maintained throughout the application.*
- *Edit and Delete Operations is also performed based on the IP address while uploading the CSV.*

12.3. Add Device

This is a Privilege based feature: The user will be able to access, view, add, edit, delete, execute & export, only if privileges have been given by the administrator. This will be defined under roles and privileges.

This menu is accessible only if the below privilege has been checked.



Devices	☑	☑	☑	☑	☑	☑

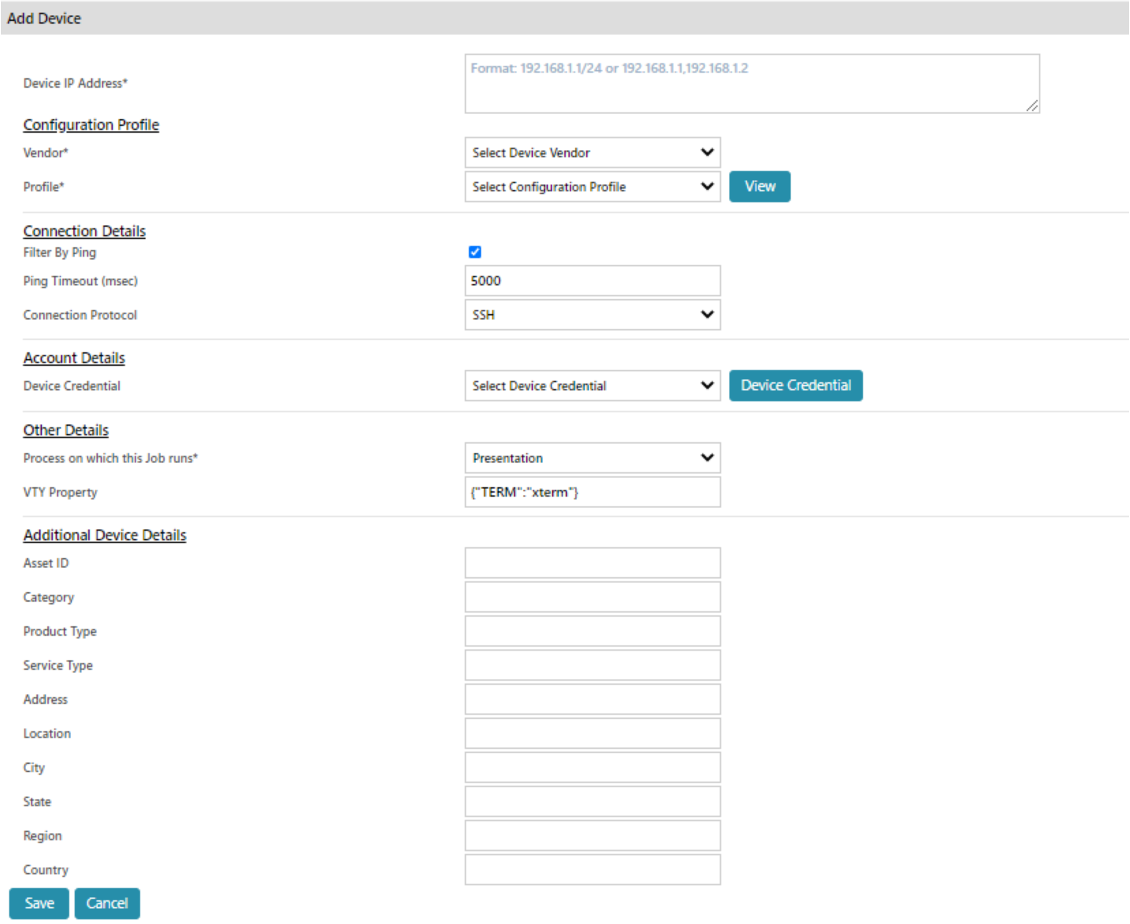
Add Device operation will add a Single or Multiple Devices directly into SecuRA without going through SNMP Discovery. This operation is mainly followed by devices which do not support SNMP protocol.

Some of critical Inventory information like Device Series, Model, System Contact, Location and Interfaces, Environment (hardware components), Topology will not be available for a Device if the device is not added using SNMP protocol.

From the left panel, click 🔍 and select 'Add Device'.

Follow the below steps to Add device(s)

- Provide the IP address(s) in the given textbox
    - Input can be a single Device management IP Address or "list of Device Management IP Address separated by comma or semicolon or single space" or Device IP address in CIDR format
- Select the Device Vendor
- Select the Configuration profiles
- Select the Connection Protocol for the devices that are to be discovered.
- Select or deselect filter by ping
    - If Filter by Ping is enabled, SecuRA will filter the PING response devices and send those Devices for Discovery process.
    - If Filter by ping is not selected, SecuRA will send all devices IP to Discovery process for SNMP Scan. Discovery could take more time when it discovery's not PING devices.
- Select Ping Time (in seconds). This will be used only when Filter by Ping is enabled.
- Select proper Device credentials
- Select the SecuRA Process where it must be managed.
    - Manage includes Device Inventory and Configuration Upload.
- Input Additional details of device in the Additional Device Details Segment.
- Click 'Save' to add the devices manually and immediately.
- Click 'Cancel' to abort the operation.



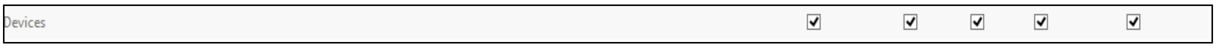
Add Device

Device IP Address*	Format: 192.168.1.1/24 or 192.168.1.1,192.168.1.2
Configuration Profile	
Vendor*	Select Device Vendor
Profile*	Select Configuration Profile
Connection Details	
Filter By Ping	☑
Ping Timeout (msec)	5000
Connection Protocol	SSH
Account Details	
Device Credential	Select Device Credential
Other Details	
Process on which this Job runs*	Presentation
VTY Property	{"TERM":"xterm"}
Additional Device Details	
Asset ID	
Category	
Product Type	
Service Type	
Address	
Location	
City	
State	
Region	
Country	

13. Devices

This is a Privilege based feature: The user will be able to access, view, add, edit, delete, execute & export, only if privileges have been given by the administrator. This will be defined under roles and privileges.

This menu is accessible only if the below privilege has been checked.

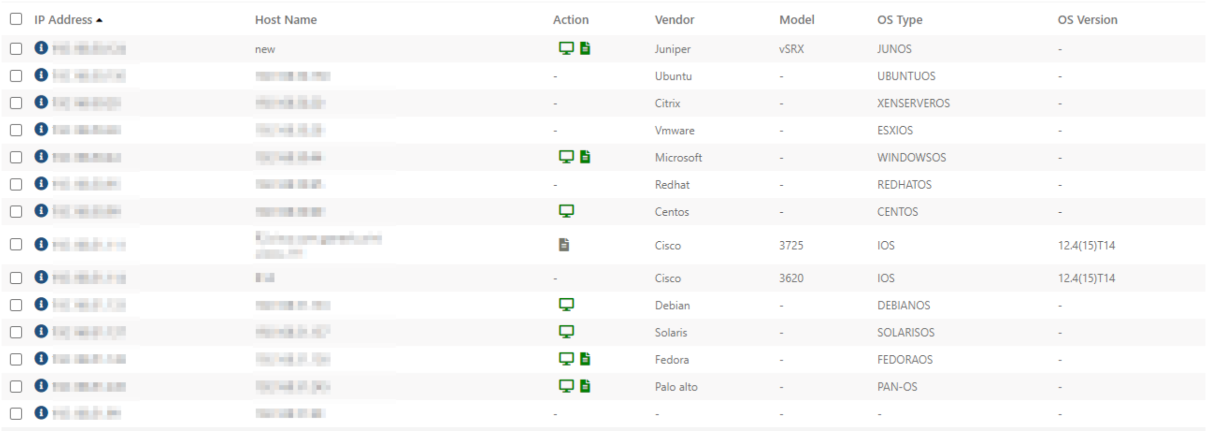


Devices	☑	☑	☑	☑	☑

"Devices" page (also known as Device Grid Page) displays all active devices (given below) that are being monitored. Device basic inventories (IP Address, Hostname, Vendor, Model, OS Type, OS Version, and Serial Number).

Process through which the device is managed. Device Actions (SSH and Telnet).

From the left panel, click ☰ and select 'Devices'.



□	IP Address ▲	Host Name	Action	Vendor	Model	OS Type	OS Version
□	ⓘ [redacted]	new	🖥 📄	Juniper	vSRX	JUNOS	-
□	ⓘ [redacted]	[redacted]	-	Ubuntu	-	UBUNTUOS	-
□	ⓘ [redacted]	[redacted]	-	Citrix	-	XENSERVEROS	-
□	ⓘ [redacted]	[redacted]	-	Vmware	-	ESXIOS	-
□	ⓘ [redacted]	[redacted]	🖥 📄	Microsoft	-	WINDOWSOS	-
□	ⓘ [redacted]	[redacted]	-	Redhat	-	REDHATOS	-
□	ⓘ [redacted]	[redacted]	🖥	Centos	-	CENTOS	-
□	ⓘ [redacted]	[redacted]	📄	Cisco	3725	IOS	12.4(15)T14
□	ⓘ [redacted]	[redacted]	-	Cisco	3620	IOS	12.4(15)T14
□	ⓘ [redacted]	[redacted]	🖥	Debian	-	DEBIANOS	-
□	ⓘ [redacted]	[redacted]	🖥	Solaris	-	SOLARISOS	-
□	ⓘ [redacted]	[redacted]	🖥 📄	Fedora	-	FEDORAOS	-
□	ⓘ [redacted]	[redacted]	🖥 📄	Palo alto	-	PAN-OS	-
□	ⓘ [redacted]	[redacted]	-	-	-	-	-

13.1. Action Icons – Devices Page

Multiple action icons are displayed on the top right corner of the page.

▼ ↗ ⊕ ⊖ ⊗ ⤒ ?

Icons	Label	Actions
▼	Filter	Click to use filter options to search
↗	Script Execute	Click to add an 'Upload Job'.
⊕	Add	Click to add a Device.
⊖	Edit	Click to edit a Device.
⊗	Delete	Click to delete a Device.
⤒	Inventory CSV upload	Click to upload inventories (devices) using the CSV file.

13.2. Device Action

From the device Result List page, scroll right to view the 'Actions Column. This column has three additional action icons:

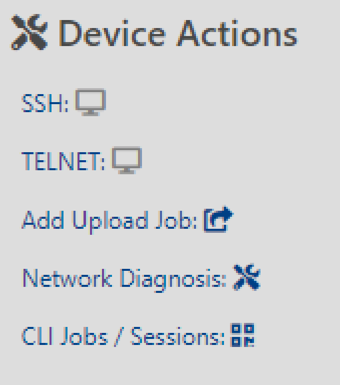
ⓘ 🖥 🖥 📄

Icons	Label	Actions
ℹ	View Details	Click to view device details and Device Actions
🖥	SSH	Click to iniate SSH session (Single Sign On)
🖥	Telnet	Click to iniate Telnet session (Single Sign On)
📄	File Management	Click to perform File Management actions on the device.

🖥 (Single Sign-On icons) and 📄 (File Management icon) are enabled only for users, authenticated to access through SSH/Telnet or both.

13.2.1. Actions

Click ℹ to view perform additional action on the device.



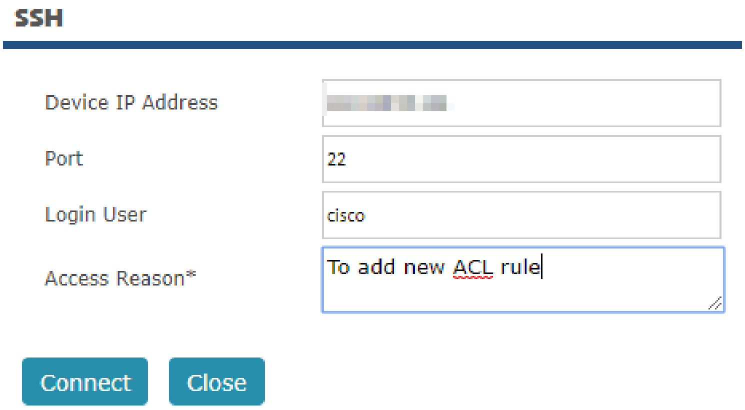
Note: *If device Authentication has been configured, two additional icons (to enable SSO) SSH and Telnet will be displayed and upon clicked will log the user in automatically.*

SSH:

Click SSH: 🖥 to open the SSH Session Page.

Note: SSH "*Access and Execute*" privilege must be enabled (for the user's Role) for accessing SSH CLI Job.

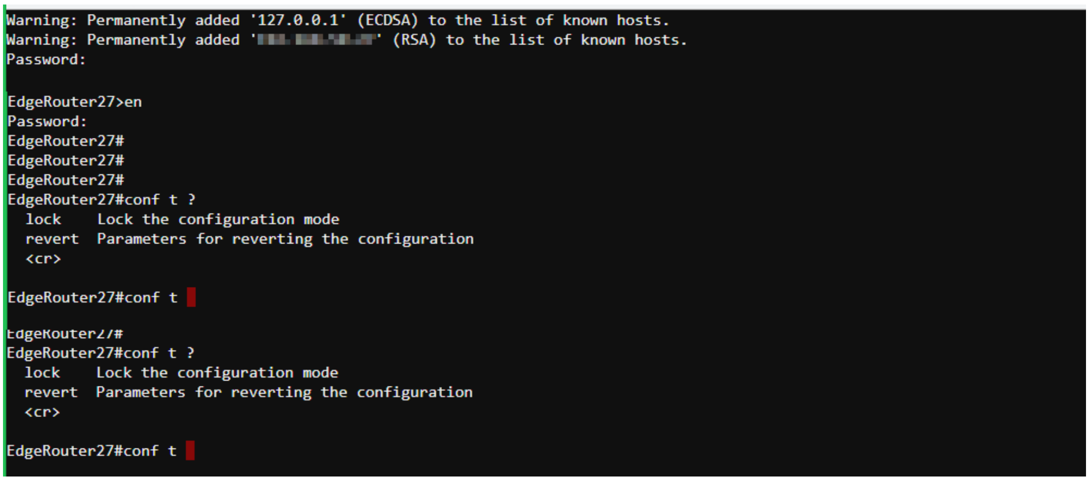
- Provide the Login User, Access Reason values and click Connect



SSH

Device IP Address	[redacted]
Port	22
Login User	cisco
Access Reason*	To add new ACL rule

SSH CLI Session is connected for configuration activity.

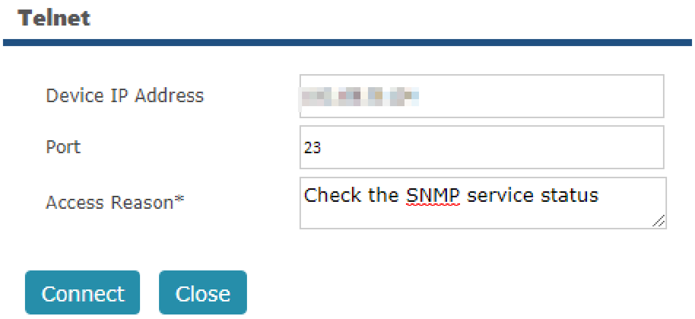


```
Warning: Permanently added '127.0.0.1' (ECDSA) to the list of known hosts.
Warning: Permanently added '[redacted]' (RSA) to the list of known hosts.
Password:

EdgeRouter27>en
Password:
EdgeRouter27#
EdgeRouter27#
EdgeRouter27#
EdgeRouter27#conf t ?
  lock     Lock the configuration mode
  revert   Parameters for reverting the configuration
  <cr>

EdgeRouter27#conf t 

EdgeRouter27#
EdgeRouter27#conf t ?
  lock     Lock the configuration mode
  revert   Parameters for reverting the configuration
  <cr>

EdgeRouter27#conf t 
```

Telnet:

Click TELNET: to open Telnet diagnosis window.

- Mention the Access Reason and click Connect.

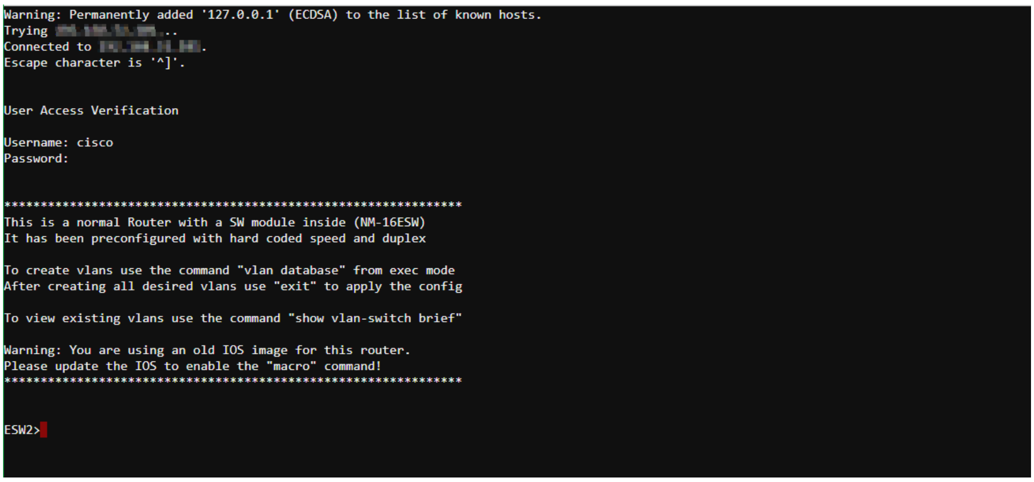


Telnet

Device IP Address	[redacted]
Port	23
Access Reason*	Check the SNMP service status

Note: *Telnet "Access and Execute"* privilege must be enabled (for the user's Role) for accessing Telnet *CLI Job.*

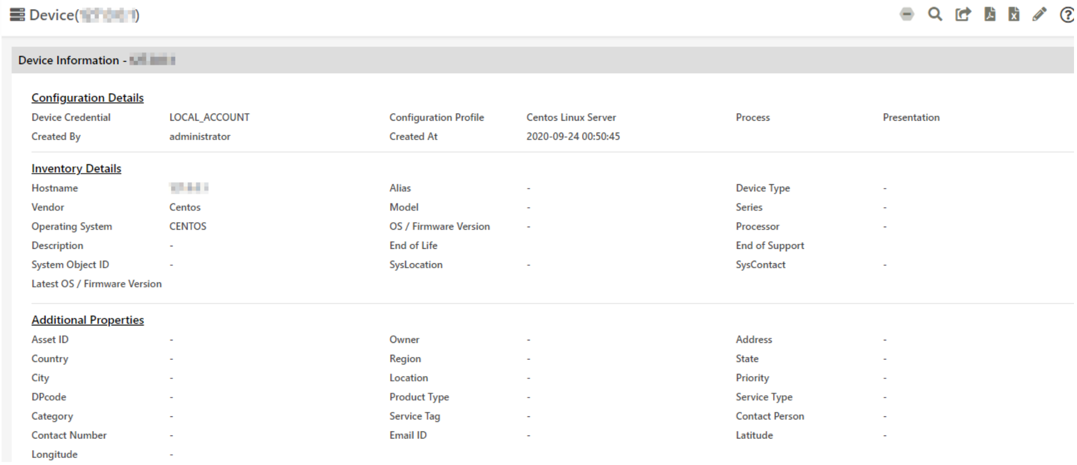
Telnet CLI Session is connected for configuration activity



```
Warning: Permanently added '127.0.0.1' (ECDSA) to the list of known hosts.
Trying [redacted]...
Connected to [redacted].
Escape character is '^]'.


User Access Verification

Username: cisco
Password:

***************************************************************
This is a normal Router with a SW module inside (NM-16ESW)
It has been preconfigured with hard coded speed and duplex

To create vlans use the command "vlan database" from exec mode
After creating all desired vlans use "exit" to apply the config

To view existing vlans use the command "show vlan-switch brief"

Warning: You are using an old IOS image for this router.
Please update the IOS to enable the "macro" command!
***************************************************************


ESW2>
```

13.3. Edit Device IP Address

From the Device Grid Page, select the specific Device and click the Host Name.



Device([redacted])

Device Information - [redacted]

Configuration Details

Device Credential	LOCAL_ACCOUNT	Configuration Profile	Centos Linux Server	Process	Presentation
Created By	administrator	Created At	2020-09-24 00:50:45		

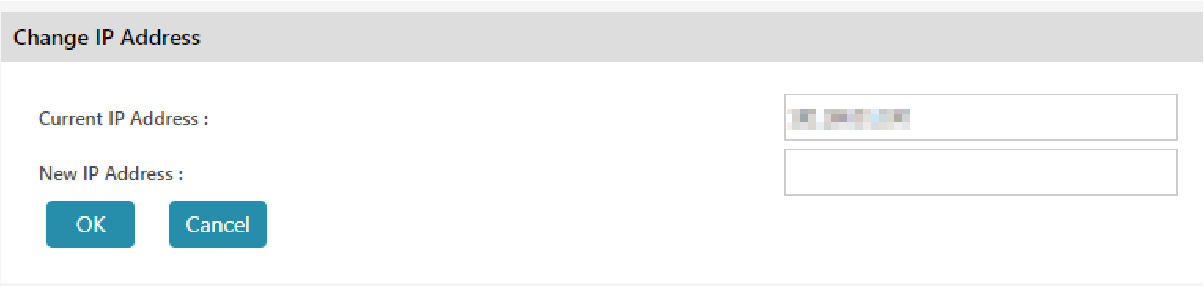
Inventory Details

Hostname	[redacted]	Alias	-	Device Type	-
Vendor	Centos	Model	-	Series	-
Operating System	CENTOS	OS / Firmware Version	-	Processor	-
Description	-	End of Life		End of Support	
System Object ID	-	SysLocation	-	SysContact	-
Latest OS / Firmware Version					

Additional Properties

Asset ID	-	Owner	-	Address	-
Country	-	Region	-	State	-
City	-	Location	-	Priority	-
DPcode	-	Product Type	-	Service Type	-
Category	-	Service Tag	-	Contact Person	-
Contact Number	-	Email ID	-	Latitude	-
Longitude	-				

Click ✎ to edit.



Change IP Address

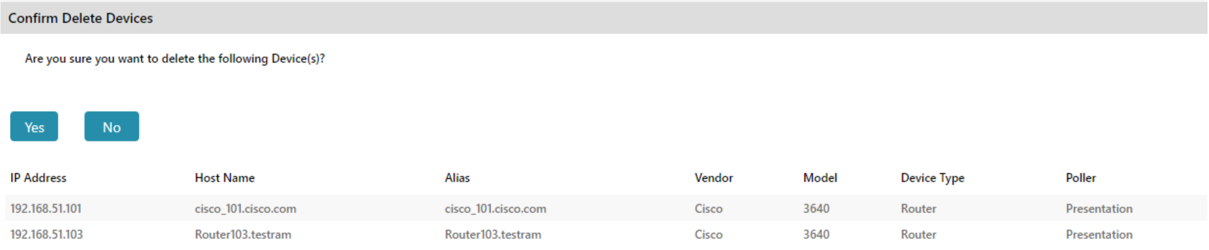
Current IP Address : [redacted]

New IP Address :

Input the New IP Address. Click Ok to save the changes or click Cancel to discard the changes.

13.4. Delete Device

Select the device and click ✖ to remove the devices from SecuRA management. (Multiple devices can be selected).



Confirm Delete Devices

Are you sure you want to delete the following Device(s)?

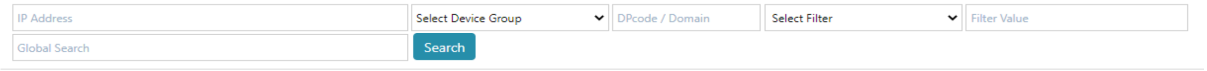
IP Address	Host Name	Alias	Vendor	Model	Device Type	Poller
192.168.51.101	cisco_101.cisco.com	cisco_101.cisco.com	Cisco	3640	Router	Presentation
192.168.51.103	Router103.testram	Router103.testram	Cisco	3640	Router	Presentation

Click Yes to remove the device or click No to cancel the device removal.

Note: *Upload Jobs/Audits, CLI Jobs will also get deleted from System along with Node deletion.*

13.5. Device Page filter

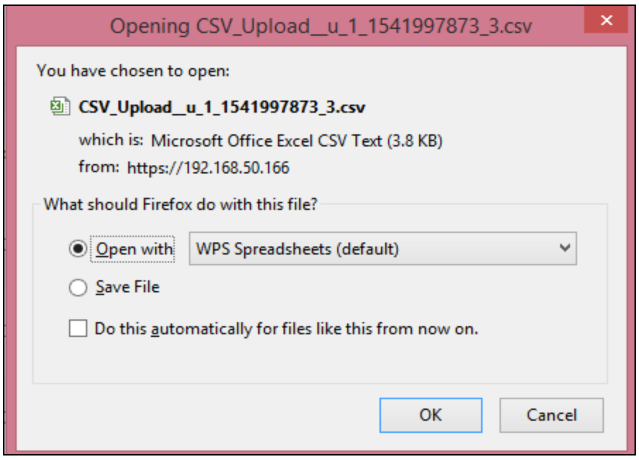
Click ▼ to enable Device filter.



- Select the IP Address.
  - IP Address can be a single Device management IP Address or “list of Device Management IP Address separated by comma, semicolon or single space” or Device IP address in CIDR format.
- Select the Device group using the dropdown.
- Select the Filter column using the dropdown.
- Based on selected filter column, input the filter keyword in the search Textbox.
- Click Search to search for specific devices.

13.5.1. Download the Device CSV (Devices)

Click 🗎 to download all or selected the device(s) listed on Device Grid Page.



Opening CSV_Upload_u_1_1541997873_3.csv

You have chosen to open:

CSV_Upload_u_1_1541997873_3.csv

which is: Microsoft Office Excel CSV Text (3.8 KB)

from: https://192.168.50.166

What should Firefox do with this file?

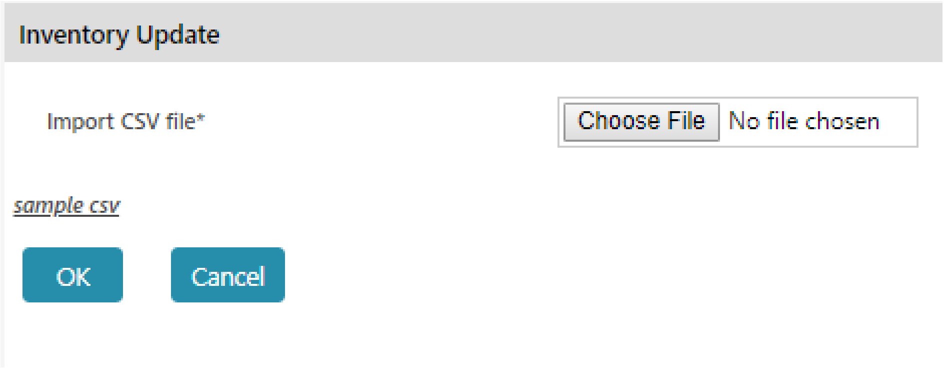
● Open with WPS Spreadsheets (default)

○ Save File

□ Do this automatically for files like this from now on.

13.5.2. Inventory CSV Upload

Click Inventory update icon to upload a CSV file containing Devices Properties, to be modified.



Inventory Update

Import CSV file* Choose File No file chosen

- Choose the Inventory CSV that needs to be imported, using the browse button
  - For reference, “sample.csv” has been given.
- Click Ok to upload the CSV.
- Click Cancel to abort the operation.

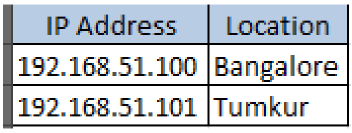
Note:

Device IP Address is a mandatory column while all other columns are optional.
To ignore a device property column, specify value as null.

If updating specific details about the inventories, the user can either remove other columns or specify the value as ‘null’ (Refer below example):
Scenario:

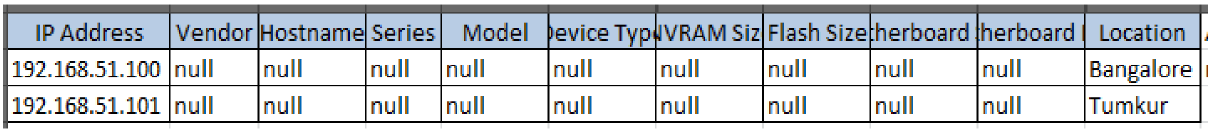
Update location details of an inventory.

Example 1 – Remove other columns.



IP Address	Location
192.168.51.100	Bangalore
192.168.51.101	Tumkur

Example 2 – Change column values to 'null'.



IP Address	Vendor	Hostname	Series	Model	)evice Typ	VRAM Siz	Flash Size	:herboard	:herboard I	Location
192.168.51.100	null	null	null	null	null	null	null	null	null	Bangalore
192.168.51.101	null	null	null	null	null	null	null	null	null	Tumkur

Warning Note: *Uploading the CSV file with blank columns will result in clearing the Inventory's detail from the system.*

13.6. Device Detail Page

From Devices page, click Host Name to open the detailed Device page. This page contains complete information of the Device.

13.6.1. Action Icons – Device Detail Page

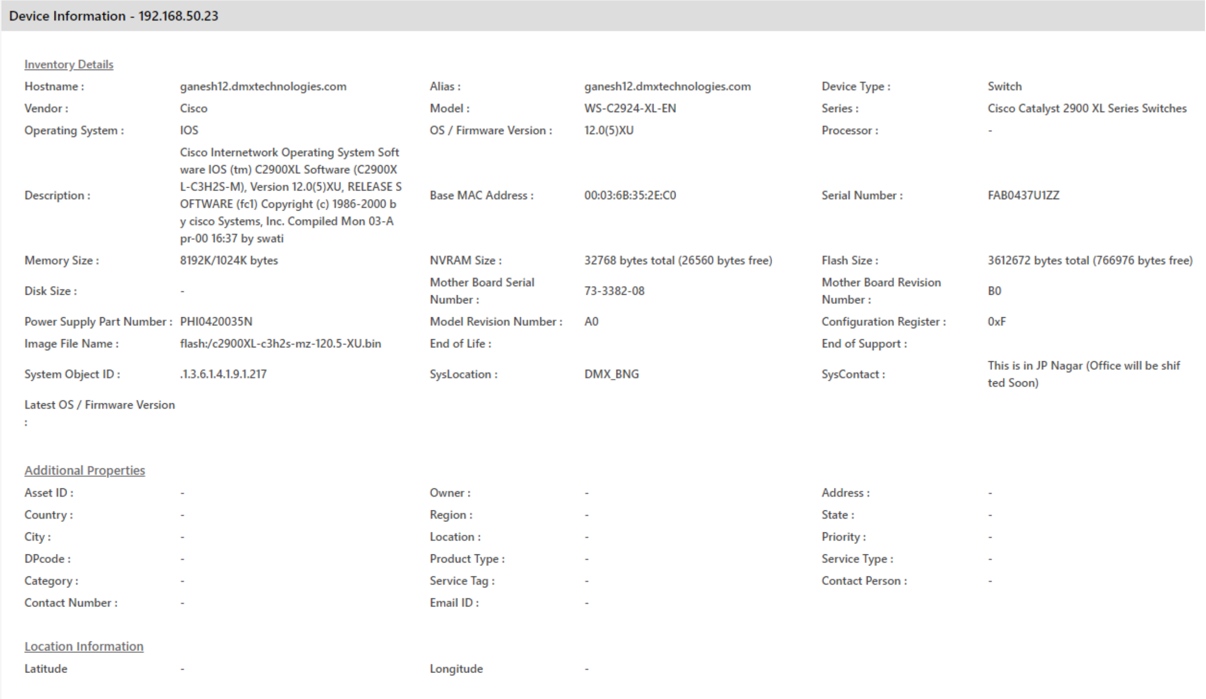
Multiple action icons are displayed on the top right corner of the page.

⊖ 🔍 ↪ 📄 📄 ✎

Icons	Label	Actions
⊖	Edit Node	Click to edit node information of the Device
🔍	Re-Scan	Re Scan the selected Device
↪	Script Execution	Click to add 'Upload Job' for the Device
📄	PDF	Click to export Device data in a PDF format.
📄	Excel	Click to export Device data in a Excel format.
✎	Edit IP Address	Click to Edit IP Address of the device

13.6.2. Device Information

Device information section contains Inventory details, Additional properties and Location Information.



Device Information - 192.168.50.23

Inventory Details

Hostname :	ganesh12.dmxtechnologies.com	Alias :	ganesh12.dmxtechnologies.com	Device Type :	Switch
Vendor :	Cisco	Model :	WS-C2924-XL-EN	Series :	Cisco Catalyst 2900 XL Series Switches
Operating System :	IOS	OS / Firmware Version :	12.0(5)XU	Processor :	-
Description :	Cisco Internetwork Operating System Software IOS (tm) C2900XL Software (C2900XL-C3H2S-M), Version 12.0(5)XU, RELEASE SOFTWARE (fc1) Copyright (c) 1986-2000 by cisco Systems, Inc. Compiled Mon 03-Apr-00 16:37 by swati	Base MAC Address :	00:03:6B:35:2E:C0	Serial Number :	FAB0437U1ZZ
Memory Size :	8192K/1024K bytes	NVRAM Size :	32768 bytes total (26560 bytes free)	Flash Size :	3612672 bytes total (766976 bytes free)
Disk Size :	-	Mother Board Serial Number :	73-3382-08	Mother Board Revision Number :	B0
Power Supply Part Number :	PHI0420035N	Model Revision Number :	A0	Configuration Register :	0xF
Image File Name :	flash:/c2900XL-c3h2s-mz-120.5-XU.bin	End of Life :		End of Support :	
System Object ID :	.1.3.6.1.4.1.9.1.217	SysLocation :	DMX_BNG	SysContact :	This is in JP Nagar (Office will be shifted Soon)
Latest OS / Firmware Version :					

Additional Properties

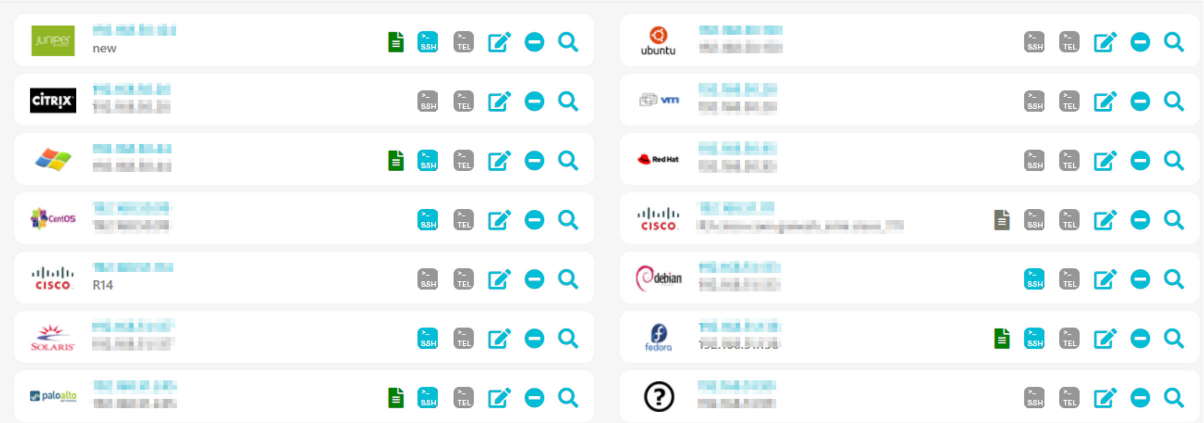
Asset ID :	-	Owner :	-	Address :	-
Country :	-	Region :	-	State :	-
City :	-	Location :	-	Priority :	-
DPcode :	-	Product Type :	-	Service Type :	-
Category :	-	Service Tag :	-	Contact Person :	-
Contact Number :	-	Email ID :	-		

Location Information

Latitude	-	Longitude	-

14. Device View

Device View is the default landing page on Infraon SecuRA and acts as a simple dashboard for Devices.



Click from the left panel and select ‘Device View’.

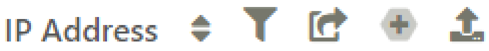
- Click on the IP Address to view/edit node configuration details.
- Click on the Hostname to view Node related information.
- If the user is authenticated for Single Sign-on by the administrator, the respective icon will be enabled SSH TEL

- If the user is authorized to perform file management actions, 📄 icon will be enabled on selected devices.
    - ⟳ Icon is visible when CLI Session is in progress.
- If the user is not authenticated, the user will be able to connect using the login credentials.

Note: For users of SecuRA Pro, the CLI Job requests will be subjected to approval.

14.1. Quick Action Icon

The below quick action icons are placed at the top right corner of the page.

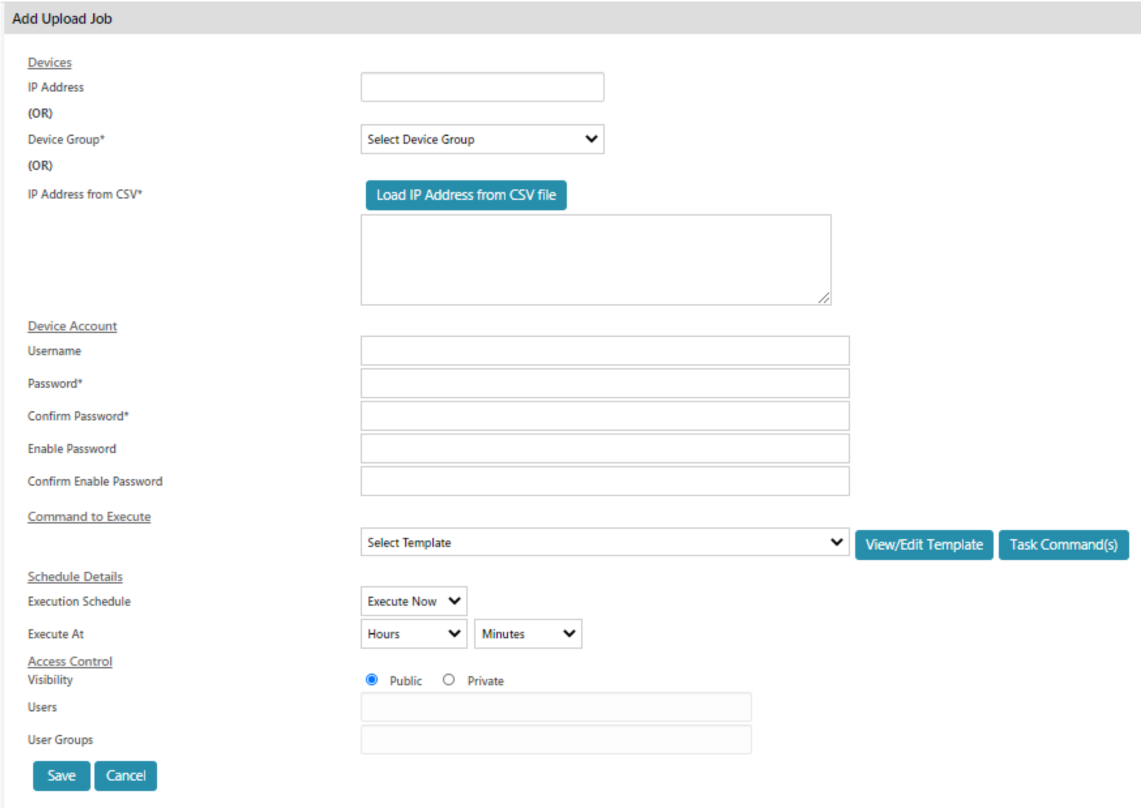


Icons	Label	Actions
⇕	Sort	Use the sort button to sort Device View based on IP Address or Hostname
▼	Filter	Click to use filter options to search
↗	Script Execute	Click to add an 'Upload Job'.
⊕	Add	Click to add a Device.
⭱	Inventory CSV upload	Click to upload inventories (devices) using the CSV file.

14.2. Script Execute

Click Script Execute to navigate to ‘Add Upload Job’ page. Update the below information

- Provide Device detail – Either an IP address or a Device Group or add addresses using a CSV.
- Provide the Username and Password details to establish device connection.
- Select Commands (using template) or Task Command(s)
- Select Schedule details
- Select Visibility (Public or Private) accordingly.
- Click Save



Add Upload Job

Devices

IP Address

(OR)

Device Group*: Select Device Group

(OR)

IP Address from CSV*: Load IP Address from CSV file

Device Account

Username

Password*

Confirm Password*

Enable Password

Confirm Enable Password

Command to Execute

Select Template | View/Edit Template | Task Command(s)

Schedule Details

Execution Schedule: Execute Now

Execute At: Hours | Minutes

Access Control

Visibility: ● Public ○ Private

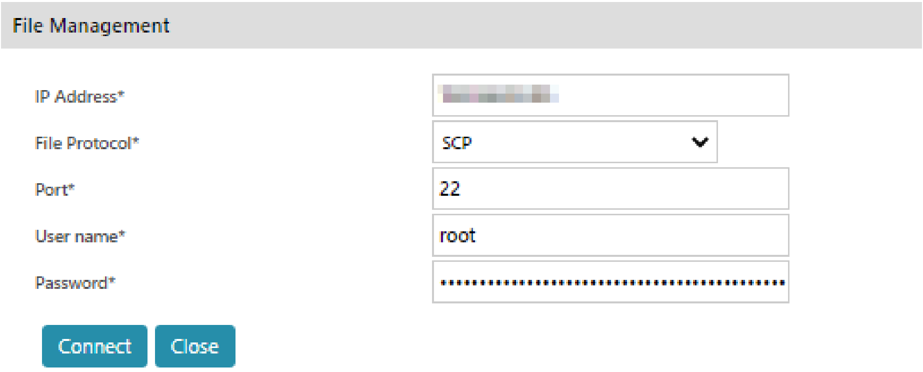
Users

User Groups

Save | Cancel

15. File Management

File management module on SecuRA enables the user to perform file management actions like Add. Edit and delete files and folders on the selected device. All actions that are performed through SSH clients can be performed using File Management module of SecuRA. From Device View page, click 🗎. The below pop-up appears.



File Management

IP Address*: [redacted]

File Protocol*: SCP

Port*: 22

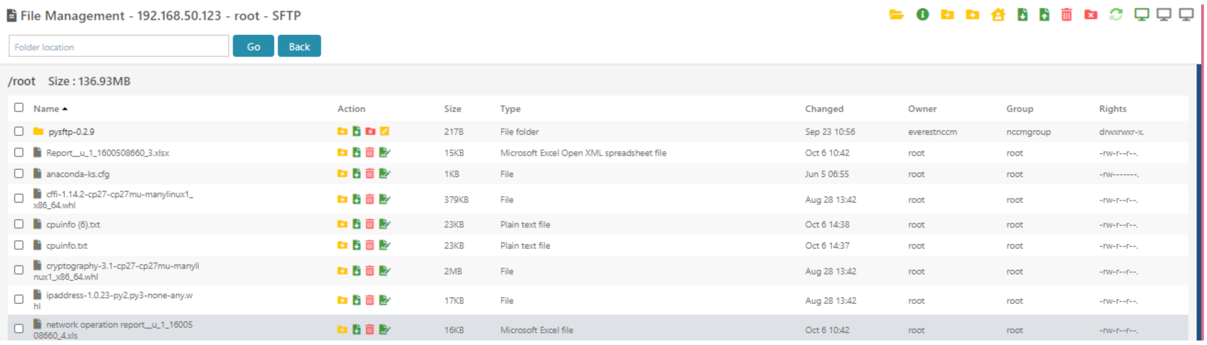
User name*: root

Password*: •••

Connect | Close

Click ‘Connect’. File Management window appears as below.

Note: *Access to File Management is based on user privileges (File Management tab of Authorization Profile).*



File Management - 192.168.50.123 - root - SFTP

Folder location | Go | Back

/root Size : 136.93MB

☐	Name ▲	Action	Size	Type	Changed	Owner	Group	Rights
☐	pysftp-0.2.9		217B	File folder	Sep 23 10:56	everestnccm	nccmgroup	drwxrwxr-x.
☐	Report__u_1_1600508660_3.xlsx		15KB	Microsoft Excel Open XML spreadsheet file	Oct 6 10:42	root	root	-rw-r--r--.
☐	anaconda-ks.cfg		1KB	File	Jun 5 06:55	root	root	-rw-------.
☐	cffi-1.14.2-cp27-cp27mu-manylinux1_x86_64.whl		379KB	File	Aug 28 13:42	root	root	-rw-r--r--.
☐	cpuinfo (6).txt		23KB	Plain text file	Oct 6 14:38	root	root	-rw-r--r--.
☐	cpuinfo.txt		23KB	Plain text file	Oct 6 14:37	root	root	-rw-r--r--.
☐	cryptography-3.1-cp27-cp27mu-manylinux1_x86_64.whl		2MB	File	Aug 28 13:42	root	root	-rw-r--r--.
☐	ipaddress-1.0.23-py2.py3-none-any.whl		17KB	File	Aug 28 13:42	root	root	-rw-r--r--.
☐	network operation report__u_1_1600508660_4.xls		16KB	Microsoft Excel file	Oct 6 10:42	root	root	-rw-r--r--.

Warning Note: *Actions performed within the File Management module cannot be undone.* ***All operations must be done with utmost care.***

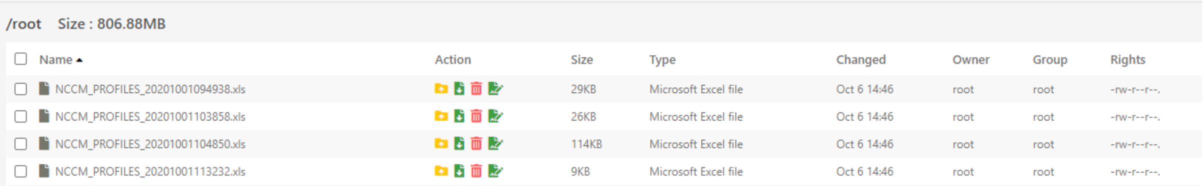
15.1. Action Icons – File Management Page

Multiple action icons are displayed on the top right corner of the page.

📂 ℹ 📁 📁 🏠 ⬇ ⬆ 🗑 ☒ 🔄 🖥 🖥

Icons	Label	Actions
📂	Toggle Open Folder	Click to perform folder search
ℹ	File System Disk space	Click to view Disk space details of the selected device
📁	Add Folder	Click to add a new folder in the destination folder
📁	Parent Directory	Click to navigate to the Parent Directory
🏠	User Home Directory	Click to navigate to the User's Home Directory
⬇	Download File	Click to download file from the selected folder
⬆	Upload File	Click to upload file to the selected folder
🗑	Delete File	Click to delete the seected file
☒	Delete Folder	Click to delete the selected folder
🔄	Refresh	Click to refresh page
🖥	SSO SSH	Click to SSO through SSH Protocol
🖥	SSH	Click to establish CLI session through SSH Protocol

In addition to the above, action icons are available on each line item in the File Management page.



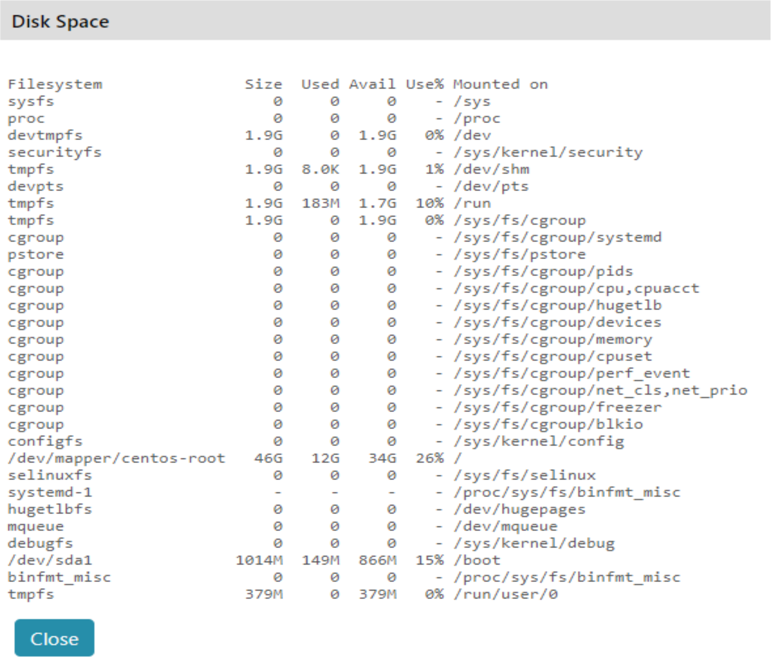
/root Size : 806.88MB

☐	Name ▲	Action	Size	Type	Changed	Owner	Group	Rights
☐	NCCM_PROFILES_20201001094938.xls	📁 ⬇ 🗑 ✎	29KB	Microsoft Excel file	Oct 6 14:46	root	root	-rw-r--r--.
☐	NCCM_PROFILES_20201001103858.xls	📁 ⬇ 🗑 ✎	26KB	Microsoft Excel file	Oct 6 14:46	root	root	-rw-r--r--.
☐	NCCM_PROFILES_20201001104850.xls	📁 ⬇ 🗑 ✎	114KB	Microsoft Excel file	Oct 6 14:46	root	root	-rw-r--r--.
☐	NCCM_PROFILES_20201001113232.xls	📁 ⬇ 🗑 ✎	9KB	Microsoft Excel file	Oct 6 14:46	root	root	-rw-r--r--.

Icons	Label	Actions
📁	Parent Directory	Click to navigate to the Parent Directory of the selected file
⬇	Download File	Click to download file from the selected folder
🗑	Delete File	Click to delete the seected file
✎	Rename File	Click to edit File name

15.2. File System Disk Space

Click ⓘ to view details related to the Disk space.

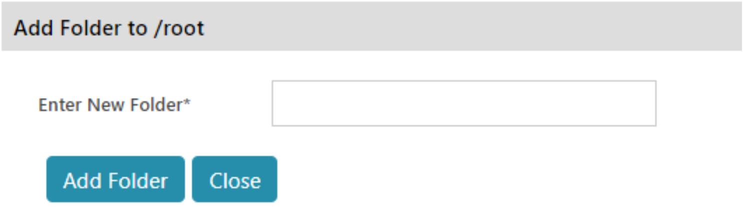


Disk Space

```
Filesystem               Size  Used Avail Use% Mounted on
sysfs                       0     0     0    - /sys
proc                        0     0     0    - /proc
devtmpfs                 1.9G     0  1.9G   0% /dev
securityfs                  0     0     0    - /sys/kernel/security
tmpfs                    1.9G  8.0K  1.9G   1% /dev/shm
devpts                      0     0     0    - /dev/pts
tmpfs                    1.9G  183M  1.7G  10% /run
tmpfs                    1.9G     0  1.9G   0% /sys/fs/cgroup
cgroup                      0     0     0    - /sys/fs/cgroup/systemd
pstore                      0     0     0    - /sys/fs/pstore
cgroup                      0     0     0    - /sys/fs/cgroup/pids
cgroup                      0     0     0    - /sys/fs/cgroup/cpu,cpuacct
cgroup                      0     0     0    - /sys/fs/cgroup/hugetlb
cgroup                      0     0     0    - /sys/fs/cgroup/devices
cgroup                      0     0     0    - /sys/fs/cgroup/memory
cgroup                      0     0     0    - /sys/fs/cgroup/cpuset
cgroup                      0     0     0    - /sys/fs/cgroup/perf_event
cgroup                      0     0     0    - /sys/fs/cgroup/net_cls,net_prio
cgroup                      0     0     0    - /sys/fs/cgroup/freezer
cgroup                      0     0     0    - /sys/fs/cgroup/blkio
configfs                    0     0     0    - /sys/kernel/config
/dev/mapper/centos-root   46G   12G   34G  26% /
selinuxfs                   0     0     0    - /sys/fs/selinux
systemd-1                   -     -     -    - /proc/sys/fs/binfmt_misc
hugetlbfs                   0     0     0    - /dev/hugepages
mqueue                      0     0     0    - /dev/mqueue
debugfs                     0     0     0    - /sys/kernel/debug
/dev/sda1               1014M  149M  866M  15% /boot
binfmt_misc                 0     0     0    - /proc/sys/fs/binfmt_misc
tmpfs                    379M     0  379M   0% /run/user/0
```

15.3. Add Folder

Click 📁 to add a new folder within the root.

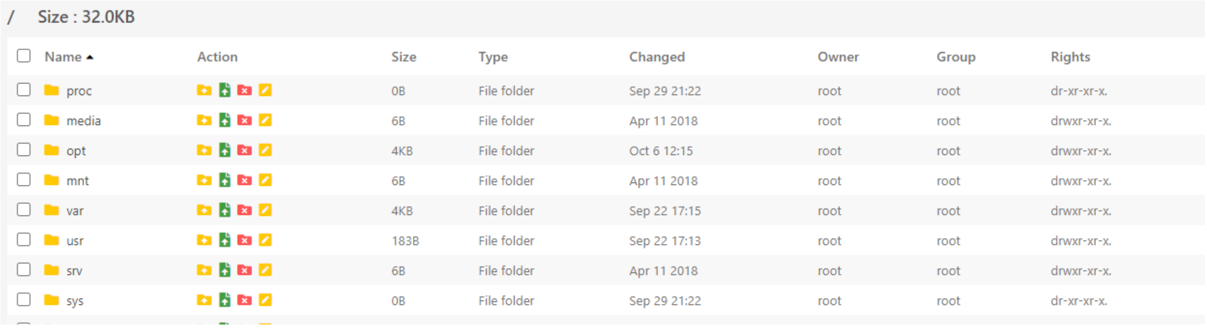


Add Folder to /root

Enter New Folder*

15.4. Parent Directory

Click to navigate to the parent directory of the selected file/folder.

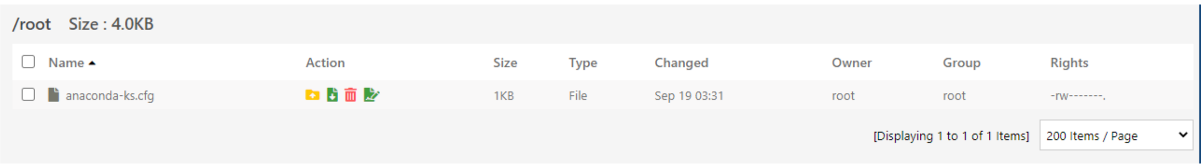


/ Size : 32.0KB

□	Name ▲	Action	Size	Type	Changed	Owner	Group	Rights
□	proc		0B	File folder	Sep 29 21:22	root	root	dr-xr-xr-x.
□	media		6B	File folder	Apr 11 2018	root	root	drwxr-xr-x.
□	opt		4KB	File folder	Oct 6 12:15	root	root	drwxr-xr-x.
□	mnt		6B	File folder	Apr 11 2018	root	root	drwxr-xr-x.
□	var		4KB	File folder	Sep 22 17:15	root	root	drwxr-xr-x.
□	usr		183B	File folder	Sep 22 17:13	root	root	drwxr-xr-x.
□	srv		6B	File folder	Apr 11 2018	root	root	drwxr-xr-x.
□	sys		0B	File folder	Sep 29 21:22	root	root	dr-xr-xr-x.

15.5. User Home Directory

Click to navigate to the User's Home directory (as defined).



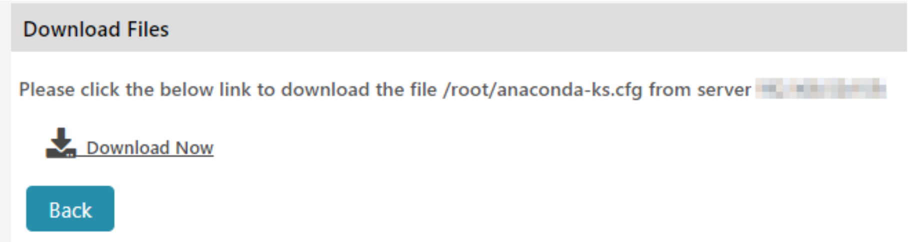
/root Size : 4.0KB

□	Name ▲	Action	Size	Type	Changed	Owner	Group	Rights
□	anaconda-ks.cfg		1KB	File	Sep 19 03:31	root	root	-rw-------.

[Displaying 1 to 1 of 1 Items] 200 Items / Page

15.6. Download File

Click to download the selected file.

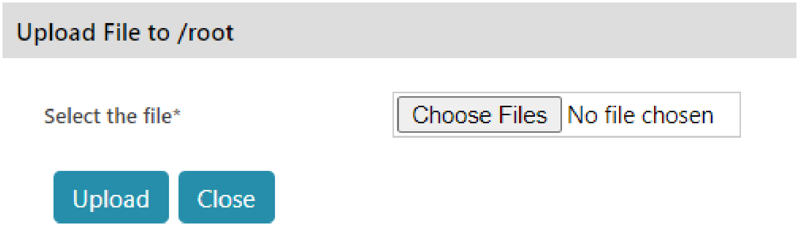


Download Files

Please click the below link to download the file /root/anaconda-ks.cfg from server [redacted]

15.7. Upload File

Click to upload a file to the root. Click 'Choose Files' to browse through the system and select a file.



Upload File to /root

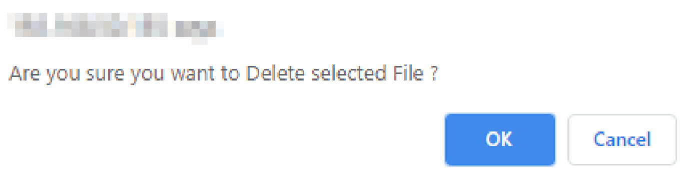
Select the file*

Note:

- *If the administrator has enabled MD5 check within 'Authorization Profile', the user must give the MD5 Hash Key to upload.*
- *If the user tries to upload a duplicate file or a file which has the same name as an existing file, SecuRA prompts the user that uploading the selected file will overwrite the existing file.*

15.8. Delete File

Click to delete the selected file.



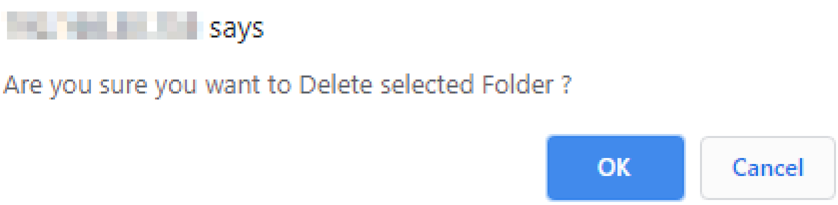
[redacted]

Are you sure you want to Delete selected File ?

Click 'Ok' to delete or 'Cancel' to cancel delete operation.

15.9. Delete Folder

Click to delete the selected folder.



[redacted] says

Are you sure you want to Delete selected Folder ?

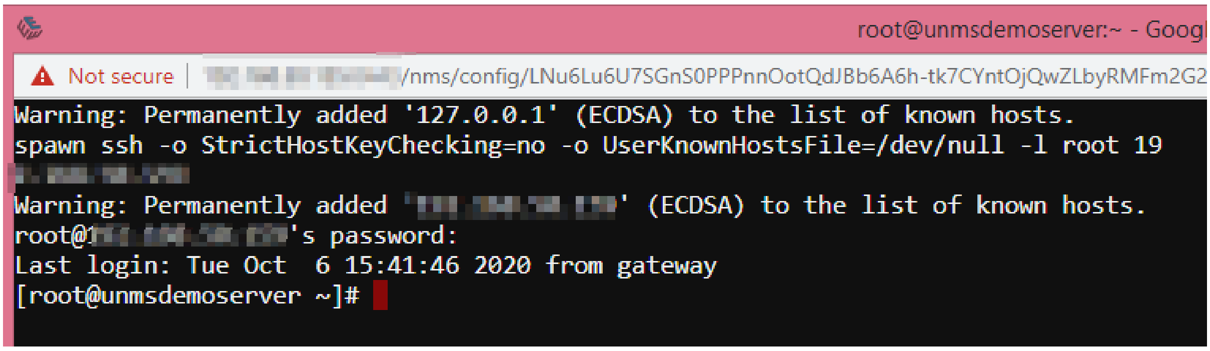
Click ‘Ok’ to delete or ‘Cancel’ to cancel delete operation.

15.10. Refresh

Click 🔄 to refresh page.

15.11. SSO SSH

Click 🖥 to SSO (Single Sign On) using SSH. CLI session (SSH) is established immediately.

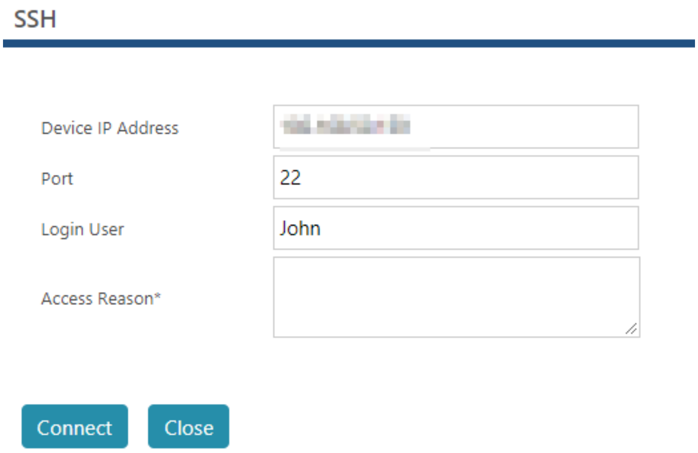

root@unmsdemoserver:~ - Googl
Not secure
[redacted]/nms/config/LNu6Lu6U7SGnS0PPPnnOotQdJBb6A6h-tk7CYntOjQwZLbyRMFm2G2

```
Warning: Permanently added '127.0.0.1' (ECDSA) to the list of known hosts.
spawn ssh -o StrictHostKeyChecking=no -o UserKnownHostsFile=/dev/null -l root 19
[redacted]
Warning: Permanently added '[redacted]' (ECDSA) to the list of known hosts.
root@[redacted]'s password:
Last login: Tue Oct  6 15:41:46 2020 from gateway
[root@unmsdemoserver ~]#
```

15.12. SSH

Click 🖥 to establish CLI using SSH. This option is used when the user is not authorised to SSO into to a specific device.

The user is requird to specify reason to access and click ‘Connect’.

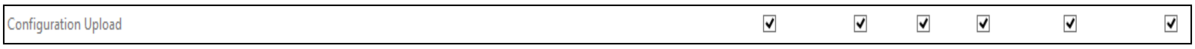

SSH

Device IP Address	[redacted]
Port	22
Login User	John
Access Reason*	

16. Upload Job

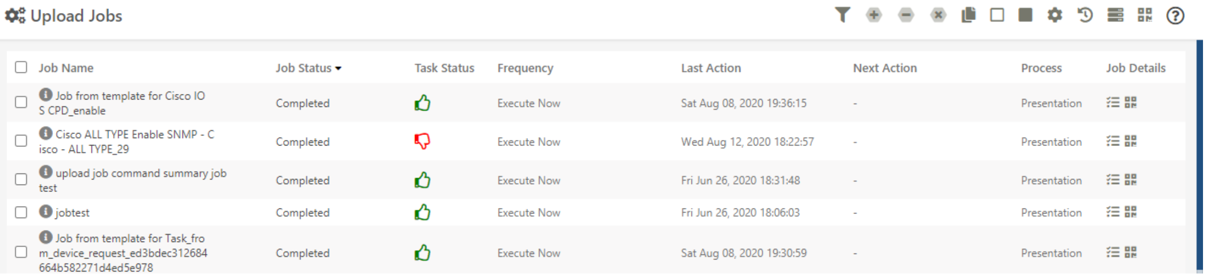
This is a Privilege based feature: The user will be able to access, view, add, edit, delete, execute & export, only if privileges have been given by the administrator. This will be defined under roles and privileges.

This menu is accessible only if the below privilege has been checked.



Configuration Upload	☑	☑	☑	☑	☑	☑

Upload Job is a controlled way of changing the Device Configuration. From the left panel, click and select ‘Upload Jobs’.



Upload Jobs

□	Job Name	Job Status	Task Status	Frequency	Last Action	Next Action	Process	Job Details
□	Job from template for Cisco IO S CPD_enable	Completed	👍	Execute Now	Sat Aug 08, 2020 19:36:15	-	Presentation	
□	Cisco ALL TYPE Enable SNMP - C isco - ALL TYPE_29	Completed	👎	Execute Now	Wed Aug 12, 2020 18:22:57	-	Presentation	
□	upload job command summary job test	Completed	👍	Execute Now	Fri Jun 26, 2020 18:31:48	-	Presentation	
□	jobtest	Completed	👍	Execute Now	Fri Jun 26, 2020 18:06:03	-	Presentation	
□	Job from template for Task_from_device_request_ed3bdec312684664b582271d4ed5e978	Completed	👍	Execute Now	Sat Aug 08, 2020 19:30:59	-	Presentation	

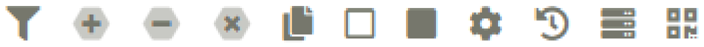
Upload Jobs Grid page displays

- Upload Job Name (Click to edit Job)
  - Unique Name to identify the Job.
- Created By
- Last Modified by
- Job Status
  - Active
  - Expired
  - Completed
- Task Status
  - Waiting for Execution 🕓
  - Success 👍
  - Failed 👎
  - Previous Task Failed 👎

- Creation Time
- Modified Time
- Frequency
    - Execute Now
    - Execute at
    - At Every
    - Weekly
    - Daily
    - Monthly
- Last Action Time
- Next Action Time
- Process Name
    - The Upload Job on which the Process runs.
- Job Details
    - Task Result
        - To view the task results
    - Job Audit
        - To view the audit trail of Upload Job

16.1. Action Icons – Upload Job Page

Multiple action icons are displayed on the top right corner of the page.

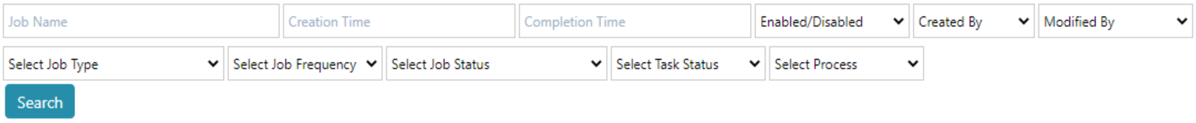


Icons	Label	Actions
▼	Filter	Click to use filter options to search
↗	Script Execute	Click to add an 'Upload Job'.
⊕	Add	Click to add a Device.
⊖	Edit	Click to edit a Device.
⊗	Delete	Click to delete a Device.
⤓	Download Now	Click to initiate 'Device Configuration' immediately.

🗎	Export Configuration	Click to export a particular 'Device Configuration'.
⚙	View Download Jobs	Click to view Download Jobs.
☰	View Download Results	Click to view results of download jobs.
🗎	Download Device CSV	Click to Download 'Devices' in a CSV format.
⬆	Inventory CSV upload	Click to upload inventories (devices) using the CSV file.

16.2. Upload Job Filter

Click ▼ to view Upload filter panel.



- Upload Job name
  - Exact match and Pattern match is supported
- Choose Time from Calendar and time filter will get applied to Job Creation Time
- Job Completion Time
- Job Live status
- Created By (users)
- Last Modified By (users)
- Job Type
- Job Frequency
- Job Status
- Task Status
- Process

Click Search to perform the search based on the filter applied.

16.3. Add Upload Job

From the Upload Job page, click ⊕ to add an Upload Job. The 'Add Upload' page contains four additional tabs. They are:

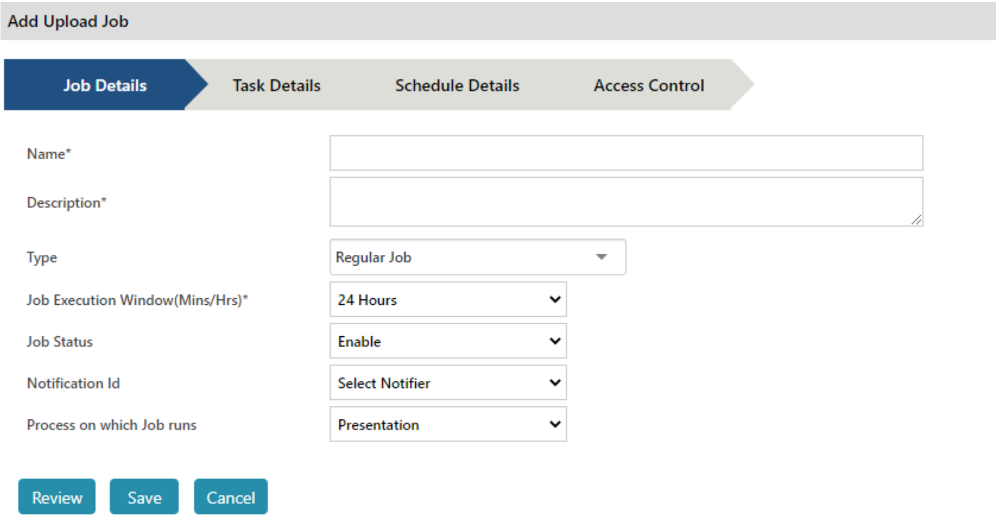
- Job Details
- Task Details

- Schedule Details
- Access Control

16.3.1. Job Details

Update the below information

- Provide a Name.
- Provide a brief Description
- Select Job Type using the dropdown menu.
- Select Job Execution window (mins/hrs) using the dropdown menu.
- Select Job status (enable/disable) using the dropdown menu.
- Select the Notifier using the dropdown (those to be notified).
- Select the Process on which the Job must RUN.



Add Upload Job

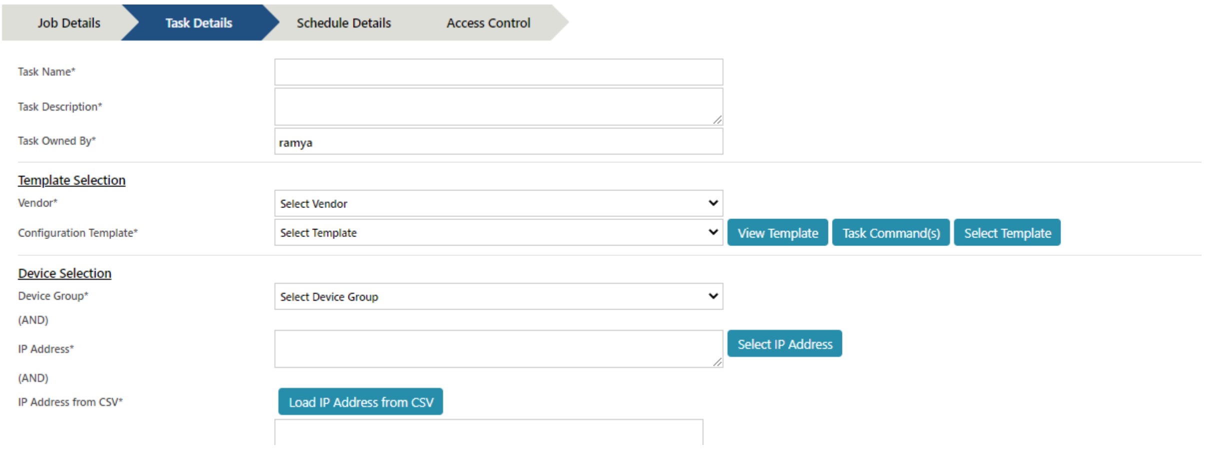
Name*	
Description*	
Type	Regular Job
Job Execution Window(Mins/Hrs)*	24 Hours
Job Status	Enable
Notification Id	Select Notifier
Process on which Job runs	Presentation

16.3.2. Task Details

Each Job has one or more tasks to be executed in a specific order, as defined. Task is the smallest unit where command execution on Devices is defined. Every task will have its own Configuration Template and the Devices to RUN with Runtime object input. Each Task supports multiple command execution with multiple parameter substitutions at the same time for individual location devices. Every Task gets Device Credentials from User while creation.

Each task requires following inputs from User

- Task Name.
- Task Description.
- Task Owned By
- Vendor.
- Configuration Template (Based on the Vendor).
    - View Template - used to view the selected template.
    - Task Command(s) - Command(s) can be added in runtime
    - Select Template - used to select the template from the collection of templates(s).
- Device group and IP Address and IP Address from CSV - Using the dropdown or IP Address(s) in textbox or IP address from the CSV by using Load IP Address from CSV



Task Name*	
Task Description*	
Task Owned By*	ramya

Template Selection

Vendor*	Select Vendor
Configuration Template*	Select Template

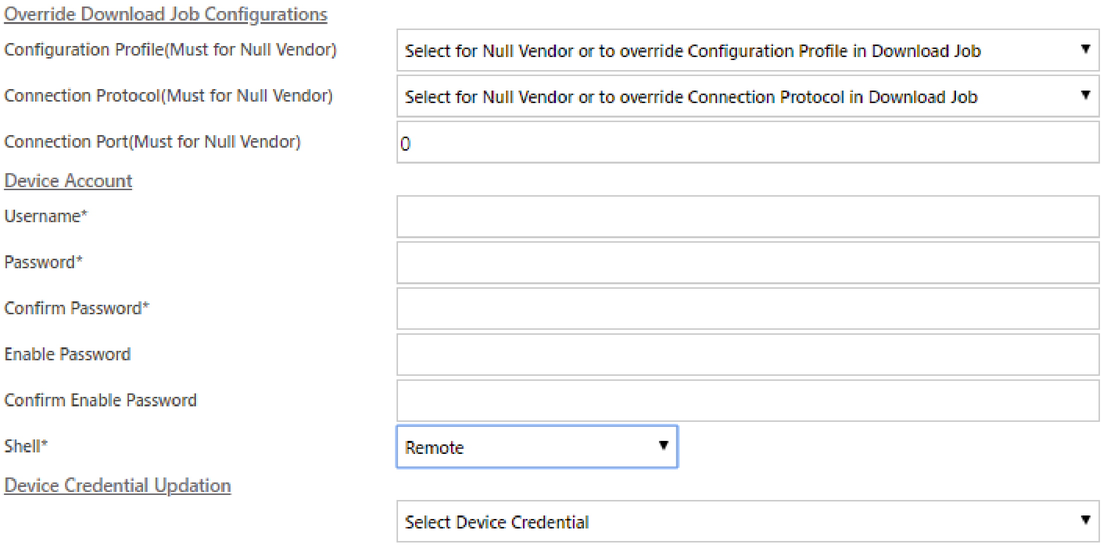
Device Selection

Device Group*	Select Device Group
(AND)	
IP Address*	
(AND)	
IP Address from CSV*	

- Configuration profile (Mandatory for null vendor)
- Configuration protocol (Mandatory for null vendor)
- Connection Port (Mandatory for null vendor)
- Device Username
- Device Password
- Confirm Password

- Enable Password
- Confirm Enable Password
- Select if Shell must be installed remotely or locally.
- Update Device credential using the dropdown menu.

This option is for performing password rotation:



Override Download Job Configurations

Configuration Profile(Must for Null Vendor)	Select for Null Vendor or to override Configuration Profile in Download Job ▾
Connection Protocol(Must for Null Vendor)	Select for Null Vendor or to override Connection Protocol in Download Job ▾
Connection Port(Must for Null Vendor)	0

Device Account

Username*	
Password*	
Confirm Password*	
Enable Password	
Confirm Enable Password	
Shell*	Remote ▾

Device Credential Updation

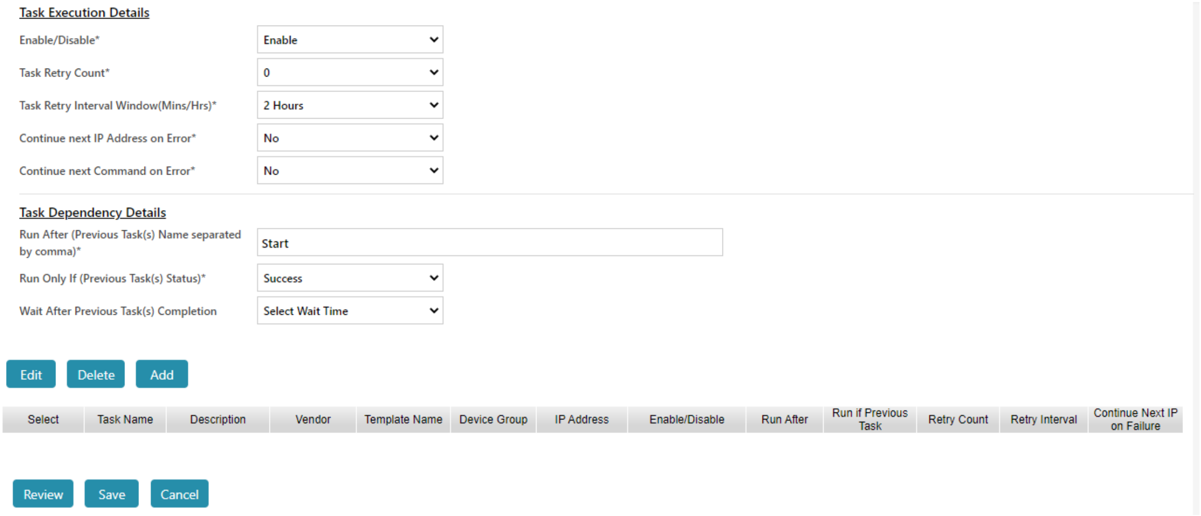
Select Device Credential ▾

- Task Enabled/Disabled
- Task retry count
- Task retry interval window (mins/hrs)
- Continue next IP Address on Error
- Continue next Command on Error
- Run after (Previous Task(s) Name)
- Run only (Previous Task(s)) Status)
- Wait After Previous Task(s) Completion in seconds

Click Add to Add the Task into Upload Job Execution Queue.

- In order to Edit the Added Task, select the Task and click Edit
- Select the Task and click Delete to remove the Task from the upload job.
- Clicking on ^ will move the task up.

- Clicking on v will move the task down.



Task Execution Details

Enable/Disable* Enable

Task Retry Count* 0

Task Retry Interval Window(Mins/Hrs)* 2 Hours

Continue next IP Address on Error* No

Continue next Command on Error* No

Task Dependency Details

Run After (Previous Task(s) Name separated by comma)* Start

Run Only If (Previous Task(s) Status)* Success

Wait After Previous Task(s) Completion Select Wait Time

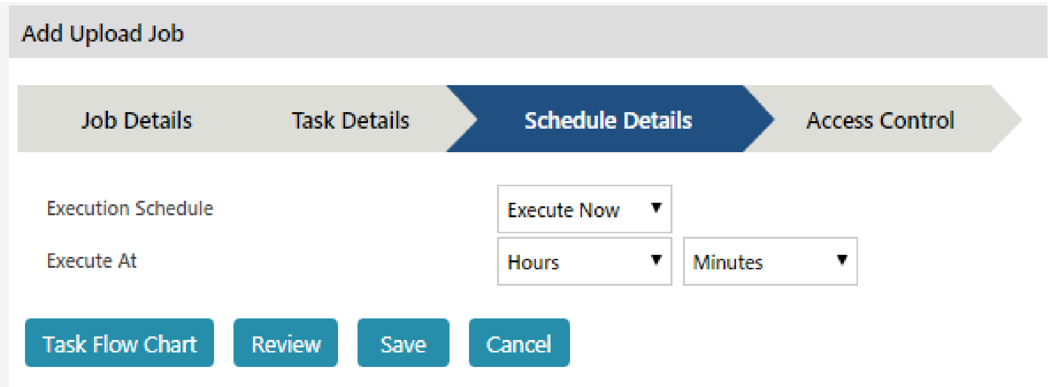
Select	Task Name	Description	Vendor	Template Name	Device Group	IP Address	Enable/Disable	Run After	Run if Previous Task	Retry Count	Retry Interval	Continue Next IP on Failure

Note: Task is limited to one per Job. However, it is possible to upgrade license to include multiple task(s) for each Upload Job.

16.3.3. Schedule Details

Click Schedule Details Tab. Update the below information

- Select the execution schedule option.
  - Daily
  - Weekly
  - Monthly
- Select the Hours and Minutes from the Execute



Add Upload Job

Execution Schedule Execute Now

Execute At Hours Minutes

16.3.4. Access Control

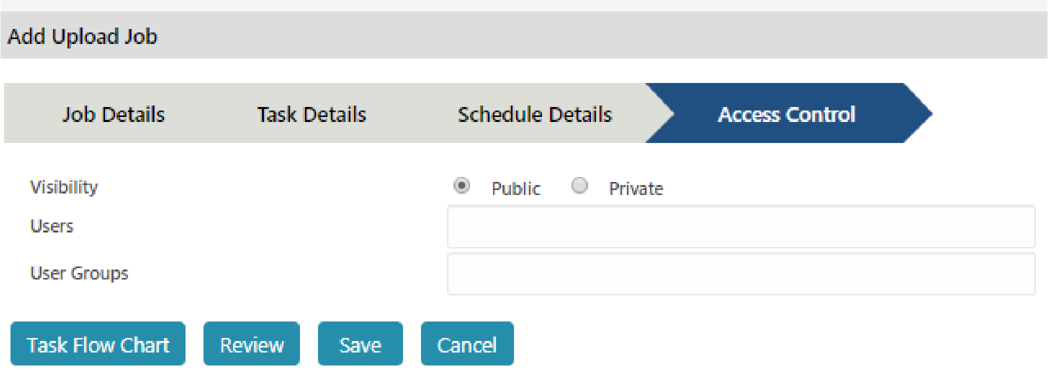
Click Access Control tab.

- Choose the visibility using the Radio button

  If visibility is "Private", User and User group dropdown will be enabled.

  - Select User(s) using dropdown.
  - Select User group(s) using dropdown.

If Upload job is private, only selected users and User groups would be able to view the job.



Visibility ● Public ○ Private

Users

User Groups

16.3.5. Review Job

Click Review to Review the Upload job.

- Review process displays all Tasks and their definition and completed details including commands to execute before saving the job.
- Review result could be exported into Excel and CSV.

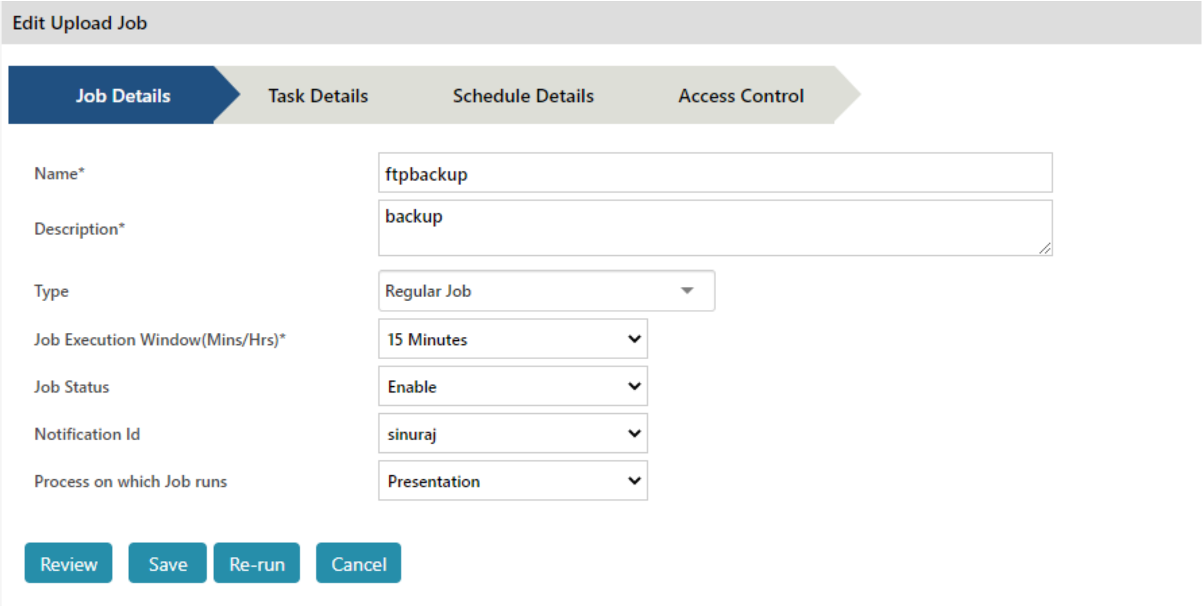
Click Save to configure the Upload job. Click Cancel to abort the job.

Note:

- *Task waiting Period will suspend the execution of the next Task execution until end of period and then the Task execution resumes.*
- *If the device(s) vendor is not identified (due to SNMP not being reachable), then the upload Job must be selected with Profile, Protocol and Port to override null entries.*
- *If any particular task has failed, the task will execute it again based on the Retry count and interval before the dependent task execution.*
- *If first task has failed, second task will get executed after the completing whole retry interval of previous task.*
- *If a task has multiple IP(s) configured and at the time of execution, if any of the IP(s) fail, the next retry will happen only for the failed IP's.*

16.4. Edit Upload Job

To edit an upload job, select an existing job and click −



Edit Upload Job

Name*	ftpbackup
Description*	backup
Type	Regular Job
Job Execution Window(Mins/Hrs)*	15 Minutes
Job Status	Enable
Notification Id	sinuraj
Process on which Job runs	Presentation

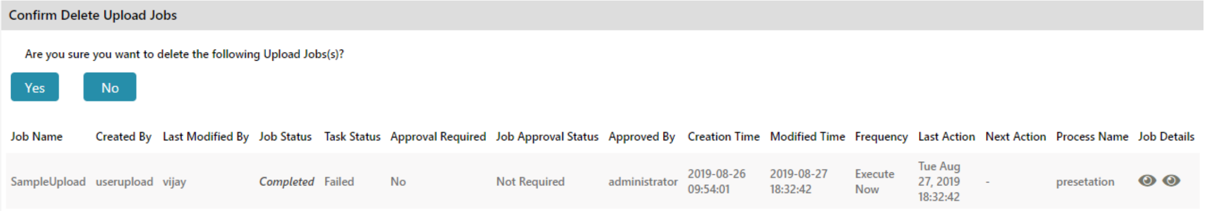
Follow the same procedure as ‘Add job’ to edit.

Note:

- *Once the job execution has been completed, we can Re-run the same job.*
- *Re-Run options aren’t available in the below scenarios*
    - *Active Jobs*
- *Re-Run and Save options aren’t available in the below scenarios*
    - *Schedule Jobs*

16.5. Delete Upload Job

To delete an upload job(s), Select the job(s) and click ✖



Confirm Delete Upload Jobs

Are you sure you want to delete the following Upload Jobs(s)?

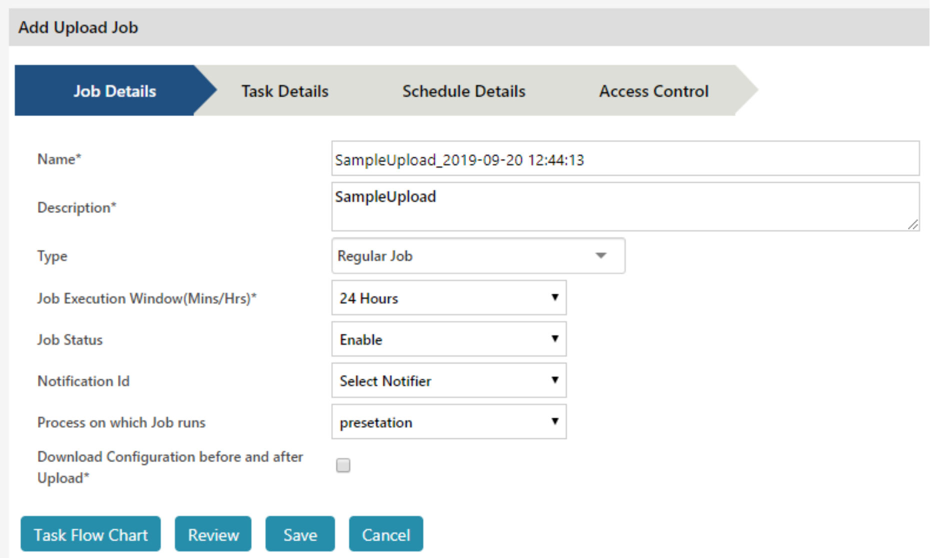
Job Name	Created By	Last Modified By	Job Status	Task Status	Approval Required	Job Approval Status	Approved By	Creation Time	Modified Time	Frequency	Last Action	Next Action	Process Name	Job Details
SampleUpload	userupload	vijay	*Completed*	Failed	No	Not Required	administrator	2019-08-26 09:54:01	2019-08-27 18:32:42	Execute Now	Tue Aug 27, 2019 18:32:42	-	presetation	👁 👁

Clicking Yes will remove the upload job, whereas clicking No will cancel the operation.

16.6. Copy Upload Job

Copy Upload Job option can be used to copy a Job i.e. to duplicate an existing upload. Select a Job and click ⧉

Add Upload Job page appears with details pre-filled. Change the inputs, as applicable and click Save to add a Job.



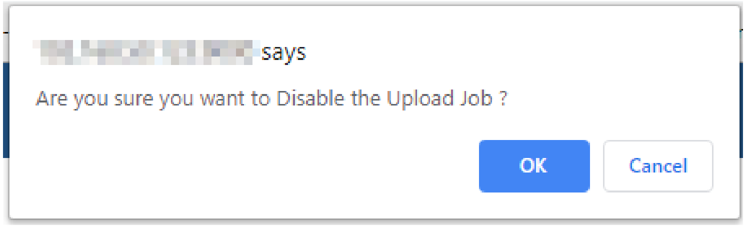
Add Upload Job

Name*	SampleUpload_2019-09-20 12:44:13
Description*	SampleUpload
Type	Regular Job
Job Execution Window(Mins/Hrs)*	24 Hours
Job Status	Enable
Notification Id	Select Notifier
Process on which Job runs	presetation
Download Configuration before and after Upload*	□

16.7. Disable Upload Job

To disable an upload job(s), Select the job(s) and click ■

Once upload is disabled, job will go to disabled state which means, the job won’t RUN until it is enabled.

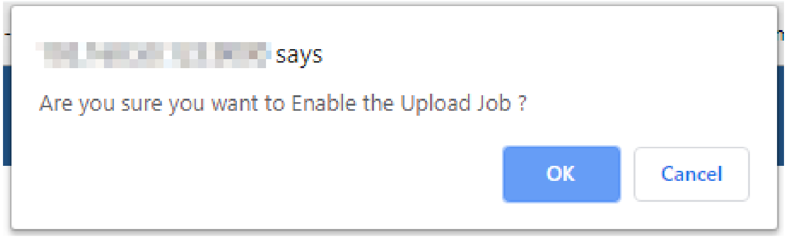


[redacted] says

Are you sure you want to Disable the Upload Job ?

16.8. Enable Upload Job

To enable an upload job(s), select the job(s) and click □. Disabled jobs will be activated and will be executed based on the scheduled time.

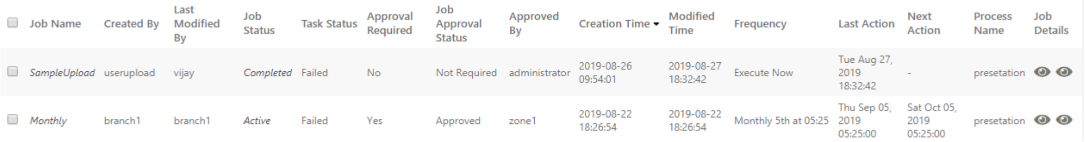


[redacted] says

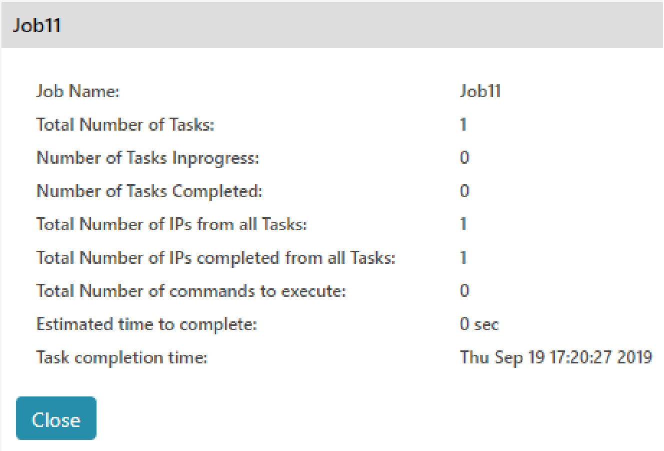
Are you sure you want to Enable the Upload Job ?

16.9. Upload Job Execution Time

To know the time taken for Upload Job execution, click ‘Job Status’ of the corresponding job entry.



□	Job Name	Created By	Last Modified By	Job Status	Task Status	Approval Required	Job Approval Status	Approved By	Creation Time ▾	Modified Time	Frequency	Last Action	Next Action	Process Name	Job Details
□	*SampleUpload*	userupload	vijay	*Completed*	Failed	No	Not Required	administrator	2019-08-26 09:54:01	2019-08-27 18:32:42	Execute Now	Tue Aug 27, 2019 18:32:42	-	presetation	👁 👁
□	*Monthly*	branch1	branch1	*Active*	Failed	Yes	Approved	zone1	2019-08-22 18:26:54	2019-08-22 18:26:54	Monthly 5th at 05:25	Thu Sep 05, 2019 05:25:00	Sat Oct 05, 2019 05:25:00	presetation	👁 👁



Job11

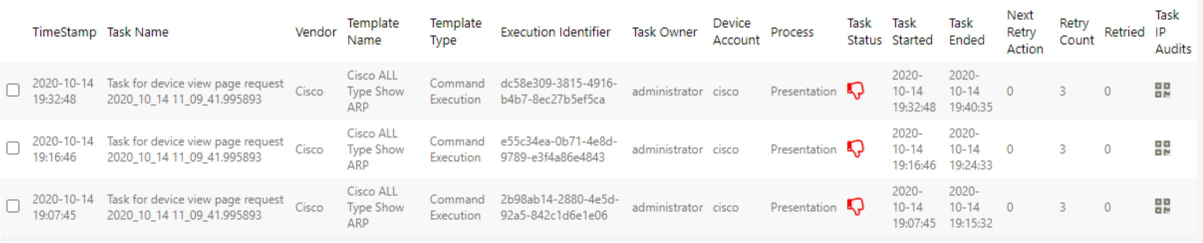
Job Name:	Job11
Total Number of Tasks:	1
Number of Tasks Inprogress:	0
Number of Tasks Completed:	0
Total Number of IPs from all Tasks:	1
Total Number of IPs completed from all Tasks:	1
Total Number of commands to execute:	0
Estimated time to complete:	0 sec
Task completion time:	Thu Sep 19 17:20:27 2019

- Job Name
- Total no. of tasks
- No. of Tasks In progress
- No of Tasks Completed
- Total no. of IP’s from all tasks
- Total no. of IP’s completed from all tasks
- Total no. of commands to execute
- Estimated time to complete the job
- Task completion time

Click Close will close the window.

16.10. Task Results

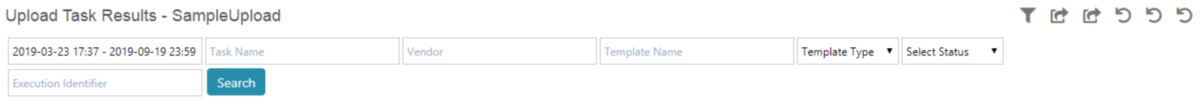
To know the Task Result summary, click available in the Job details column for each Job.



	TimeStamp	Task Name	Vendor	Template Name	Template Type	Execution Identifier	Task Owner	Device Account	Process	Task Status	Task Started	Task Ended	Next Retry Action	Retry Count	Retried	Task IP Audits
□	2020-10-14 19:32:48	Task for device view page request 2020_10_14 11_09_41.995893	Cisco	Cisco ALL Type Show ARP	Command Execution	dc58e309-3815-4916-b4b7-8ec27b5ef5ca	administrator	cisco	Presentation	👎	2020-10-14 19:32:48	2020-10-14 19:40:35	0	3	0	▦
□	2020-10-14 19:16:46	Task for device view page request 2020_10_14 11_09_41.995893	Cisco	Cisco ALL Type Show ARP	Command Execution	e55c34ea-0b71-4e8d-9789-e3f4a86e4843	administrator	cisco	Presentation	👎	2020-10-14 19:16:46	2020-10-14 19:24:33	0	3	0	▦
□	2020-10-14 19:07:45	Task for device view page request 2020_10_14 11_09_41.995893	Cisco	Cisco ALL Type Show ARP	Command Execution	2b98ab14-2880-4e5d-92a5-842c1d6e1e06	administrator	cisco	Presentation	👎	2020-10-14 19:07:45	2020-10-14 19:15:32	0	3	0	▦

16.10.1. Search Task

Click to open the search options.



Upload Task Results - SampleUpload

2019-03-23 17:37 - 2019-09-19 23:59

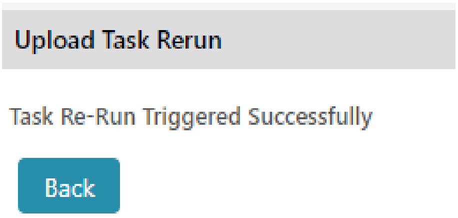
- Select the time from calendar options.
- Input Task Name in textbox.
- Input Vendor in textbox.
- Input Template Name in textbox.
- Select Template Type using the dropdown menu.
- Select status using the dropdown menu.

Click Search to perform the search, based on the filter applied.

16.10.2. Re-Run Tasks

Select one of the Tasks and click (Re-run icon) to Re-execute the selected Task. Task Re-run will be executed for all or only for the failed tasks (Devices).

Click Re-Run all Devices to Re-Run all devices or Re-Run Failed Devices to Re-Run the tasks only for failed Devices.

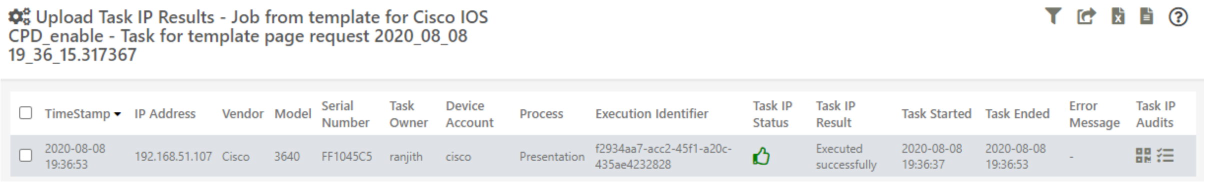


Upload Task Rerun

Task Re-Run Triggered Successfully

16.10.3. Task IP Audits

Click (Task IP Audit) to open Task Device IP execution result window. Task IP results can be exported to Excel and CSV format.

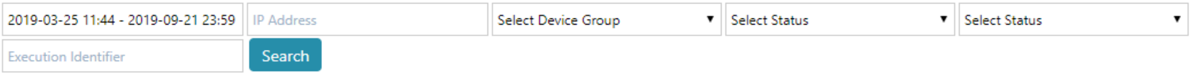


Upload Task IP Results - Job from template for Cisco IOS CPD_enable - Task for template page request 2020_08_08 19_36_15.317367

□	TimeStamp ▾	IP Address	Vendor	Model	Serial Number	Task Owner	Device Account	Process	Execution Identifier	Task IP Status	Task IP Result	Task Started	Task Ended	Error Message	Task IP Audits
□	2020-08-08 19:36:53	192.168.51.107	Cisco	3640	FF1045C5	ranjith	cisco	Presentation	f2934aa7-acc2-45f1-a20c-435ae4232828	👍	Executed successfully	2020-08-08 19:36:37	2020-08-08 19:36:53	-	

Task Search:

Click to open the search options.

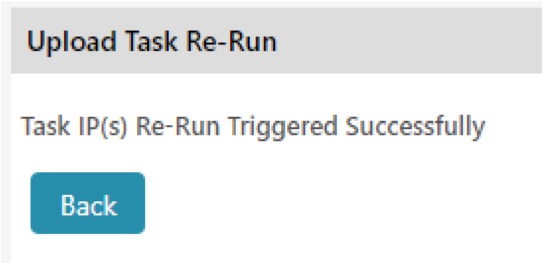


2019-03-25 11:44 - 2019-09-21 23:59 | IP Address | Select Device Group ▾ | Select Status ▾ | Select Status ▾
Execution Identifier | Search

- Select the Device IP execution Time from calendar options.
- Input IP Address in textbox.
- Select Device Group using the dropdown menu.
- Select execution status using the dropdown menu.
- Select Status Summary using the dropdown menu.
- Click Search to perform the search based on the applied filter.

Task Re-Run

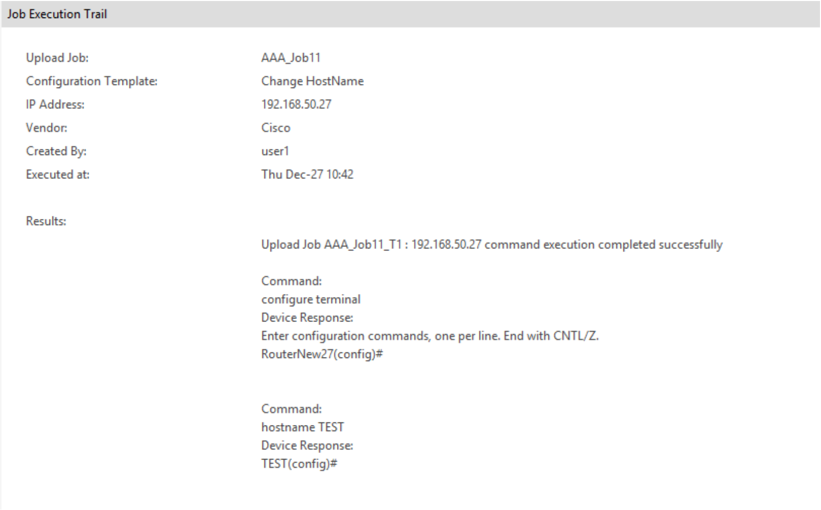
Select the Device IP entry and click (Task IP re-run icon) to re-execute the task IP(s).



Task IP(s) Re-Run Triggered Successfully

View Trails

Click ⊞ , available in the Task IP audits column to audit the command sent and device response for all configuration commands.



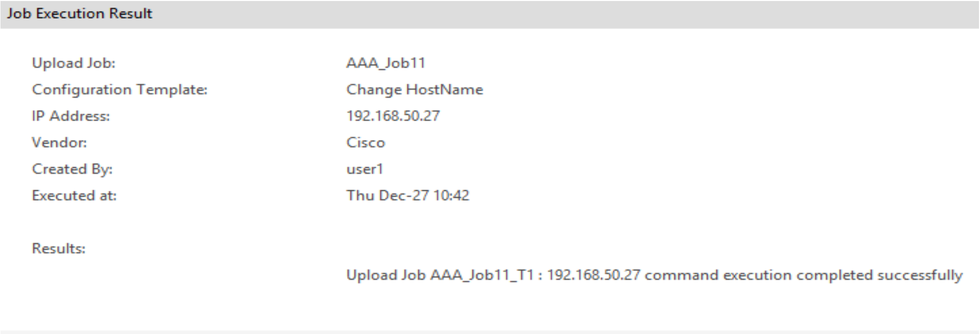
Upload Job:	AAA_Job11
Configuration Template:	Change HostName
IP Address:	192.168.50.27
Vendor:	Cisco
Created By:	user1
Executed at:	Thu Dec-27 10:42

Results:

```
Upload Job AAA_Job11_T1 : 192.168.50.27 command execution completed successfully

Command:
configure terminal
Device Response:
Enter configuration commands, one per line. End with CNTL/Z.
RouterNew27(config)#


Command:
hostname TEST
Device Response:
TEST(config)#
```

View Results

Click ⊞ (View Results icon) to know the Task IP audits execution status.



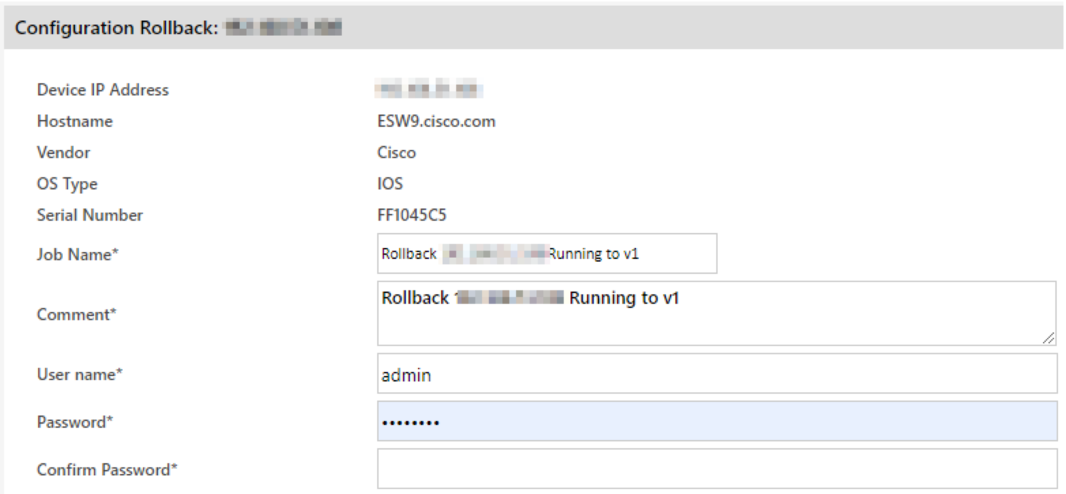
Upload Job:	AAA_Job11
Configuration Template:	Change HostName
IP Address:	192.168.50.27
Vendor:	Cisco
Created By:	user1
Executed at:	Thu Dec-27 10:42

Results:

```
Upload Job AAA_Job11_T1 : 192.168.50.27 command execution completed successfully
```

Configuration Rollback

Click ↺ (Configuration rollback icon), available in Task IP audits columns to open rollback job window.



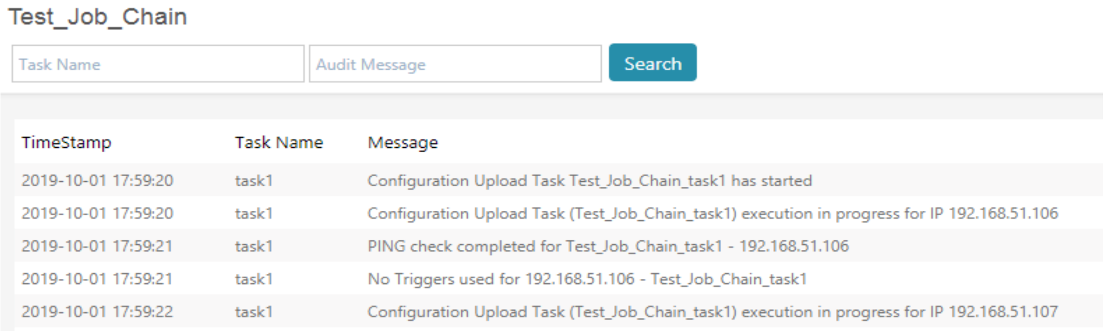
Configuration Rollback: [redacted]

Device IP Address	[redacted]
Hostname	ESW9.cisco.com
Vendor	Cisco
OS Type	IOS
Serial Number	FF1045C5
Job Name*	Rollback [redacted] Running to v1
Comment*	Rollback [redacted] Running to v1
User name*	admin
Password*	••••••••
Confirm Password*	

Input Device Credentials, Upload Protocol and Rollback Configuration version. Click Add Upload Job to save a new Roll Back Upload job.

16.11. View Job Audits

To know the Task Result summary, click ⊞ available in the Job details column for each Job.



Test_Job_Chain

TimeStamp	Task Name	Message
2019-10-01 17:59:20	task1	Configuration Upload Task Test_Job_Chain_task1 has started
2019-10-01 17:59:20	task1	Configuration Upload Task (Test_Job_Chain_task1) execution in progress for IP 192.168.51.106
2019-10-01 17:59:21	task1	PING check completed for Test_Job_Chain_task1 - 192.168.51.106
2019-10-01 17:59:21	task1	No Triggers used for 192.168.51.106 - Test_Job_Chain_task1
2019-10-01 17:59:22	task1	Configuration Upload Task (Test_Job_Chain_task1) execution in progress for IP 192.168.51.107

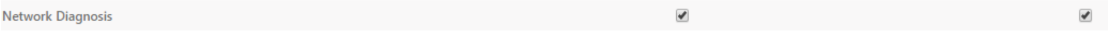
Search

- Input Task Name in textbox.
- Input Audit Message in textbox.
- Click Search to perform the search based on the applied filter.

17. Network Diagnosis

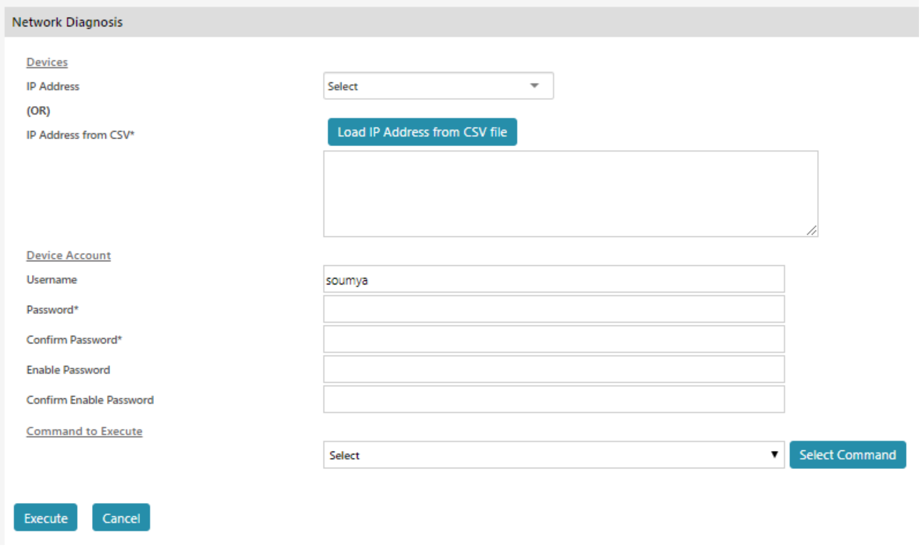
This is a Privilege based feature: The user will be able to access, view, add, edit, delete, execute & export, only if privileges have been given by the administrator. This will be defined under roles and privileges.

This menu is accessible only if the below privilege has been checked.



Network Diagnosis ☑ ☑

This is used to diagnose the device directly by using defined "Network diagnosis" template. Commands will be executed, and result will be shown in the same page. From the "Actions" menu on the left panel select "Network Diagnosis". Network diagnosis window will be displayed.



Network Diagnosis

Devices

IP Address: Select

(OR)

IP Address from CSV*: Load IP Address from CSV file

Device Account

Username: soumya

Password*

Confirm Password*

Enable Password

Confirm Enable Password

Command to Execute

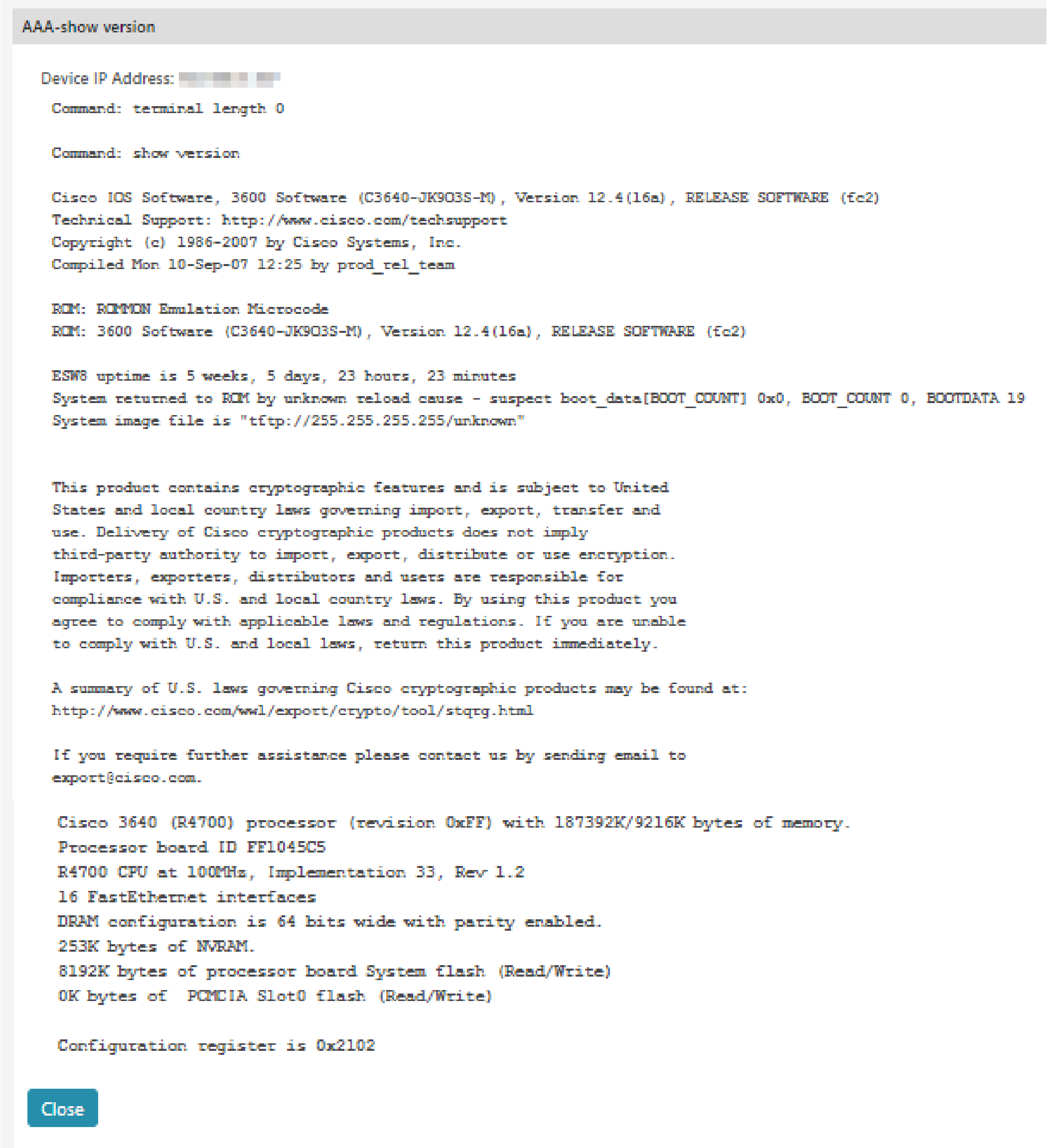
Select | Select Command

Execute | Cancel

- Select the IP Address using the dropdown menu or
- Load the IP Address using Load IP Address from CSV file option, to upload the CSV file *(This is based on the license).*
- Input Username in the textbox.
- Input Password in the textbox.
- Input Confirm Password in the textbox.
- Input Enable Password in the textbox.
- Input Confirm Enable Password in textbox.
- Clicking Select Command will open the configuration template window to select the template for the diagnosis.
- Select the template using the dropdown menu.

Click Execute to execute the script or click Cancel to abort the Operation.

The Result page will be displayed as below. This result can be exported using



Device IP Address: [redacted]

```
Command: terminal length 0

Command: show version

Cisco IOS Software, 3600 Software (C3640-JK9O3S-M), Version 12.4(16a), RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Mon 10-Sep-07 12:25 by prod_rel_team

ROM: ROMMON Emulation Microcode
ROM: 3600 Software (C3640-JK9O3S-M), Version 12.4(16a), RELEASE SOFTWARE (fc2)

ESW8 uptime is 5 weeks, 5 days, 23 hours, 23 minutes
System returned to ROM by unknown reload cause - suspect boot_data[BOOT_COUNT] 0x0, BOOT_COUNT 0, BOOTDATA 19
System image file is "tftp://255.255.255.255/unknown"


This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.

 Cisco 3640 (R4700) processor (revision 0xFF) with 187392K/9216K bytes of memory.
 Processor board ID FF1045C5
 R4700 CPU at 100MHz, Implementation 33, Rev 1.2
 16 FastEthernet interfaces
 DRAM configuration is 64 bits wide with parity enabled.
 253K bytes of NVRAM.
 8192K bytes of processor board System flash (Read/Write)
 0K bytes of  PCMCIA Slot0 flash (Read/Write)

 Configuration register is 0x2102
```

18. CLI Jobs/Session

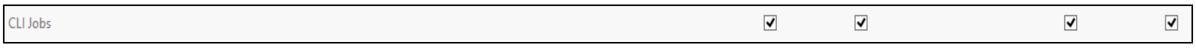
CLI Jobs in SecuRA are used to make direct CLI session (Either SSH or TELNET) between the Device and User through SecuRA application. By using CLI Job user can write direct commands on devices similar to putty application.

User will request CLI connection by inputting Device IP Address, Device account username (in case of SSH) and the reason for connection. Based on the user's role (administrator privileged or CLI white listed or normal user) CLI job will either open direct connection to the device or put the CLI request into **Request Queue** for Change Approval process.

CLI Job will audit all the commands executed by users on devices including device response.

This is a Privilege based feature: The user will be able to access, view, add, edit, delete, execute & export, only if privileges have been given by the administrator. This will be defined under roles and privileges.

This menu is accessible only if the below privilege has been checked.

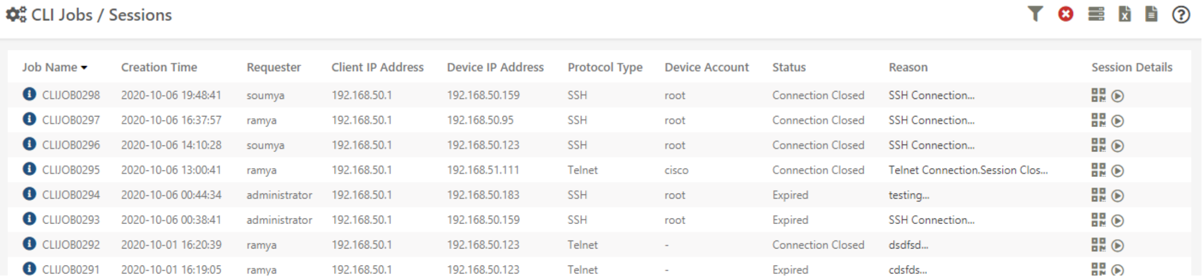


CLI Jobs ☑ ☑ ☑ ☑

User will be white listed for CLI operations (no need of Approval) only If 'CLI Job Pre-Approved' permission in enabled in Account Roles and Privileges.

From the left panel, click and select 'CLI Jobs/Sessions'

All CLI Jobs including history connection and live session is listed with its active status.

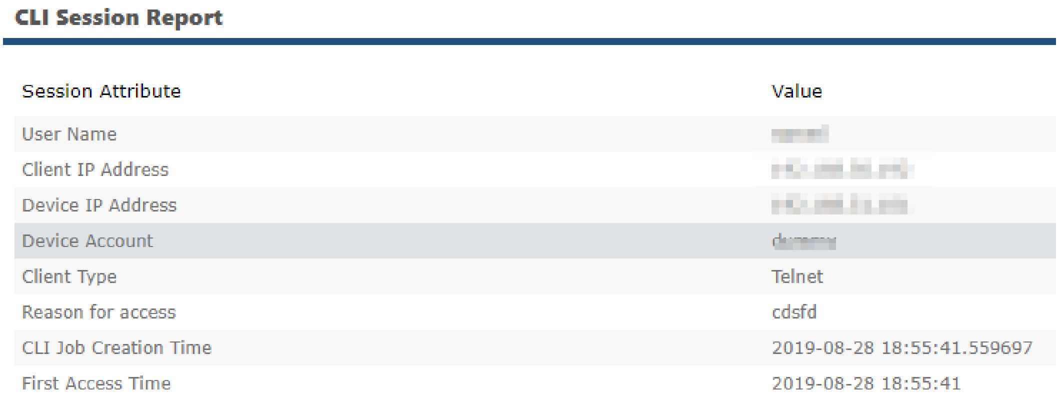


CLI Jobs / Sessions

Job Name	Creation Time	Requester	Client IP Address	Device IP Address	Protocol Type	Device Account	Status	Reason	Session Details
CLIJOB0298	2020-10-06 19:48:41	soumya	192.168.50.1	192.168.50.159	SSH	root	Connection Closed	SSH Connection...	
CLIJOB0297	2020-10-06 16:37:57	ramya	192.168.50.1	192.168.50.95	SSH	root	Connection Closed	SSH Connection...	
CLIJOB0296	2020-10-06 14:10:28	soumya	192.168.50.1	192.168.50.123	SSH	root	Connection Closed	SSH Connection...	
CLIJOB0295	2020-10-06 13:00:41	ramya	192.168.50.1	192.168.51.111	Telnet	cisco	Connection Closed	Telnet Connection.Session Clos...	
CLIJOB0294	2020-10-06 00:44:34	administrator	192.168.50.1	192.168.50.183	SSH	root	Expired	testing...	
CLIJOB0293	2020-10-06 00:38:41	administrator	192.168.50.1	192.168.50.159	SSH	root	Expired	SSH Connection...	
CLIJOB0292	2020-10-01 16:20:39	ramya	192.168.50.1	192.168.50.123	Telnet	-	Connection Closed	dsdfsd...	
CLIJOB0291	2020-10-01 16:19:05	ramya	192.168.50.1	192.168.50.123	Telnet	-	Expired	cdsfds...	

Clicking the session details icon will display live audits.

Note: CLI Jobs requested by Non-Whitelisted users will be submitted for approval and will be executed only when approved. However, Whitelisted user's CLI Jobs will be executed without approval process.



CLI Session Report

Session Attribute	Value
User Name	[redacted]
Client IP Address	[redacted]
Device IP Address	[redacted]
Device Account	[redacted]
Client Type	Telnet
Reason for access	cdsfd
CLI Job Creation Time	2019-08-28 18:55:41.559697
First Access Time	2019-08-28 18:55:41

Using this audit, administrator can find the changes, the user responsible for the changes and the time of change.

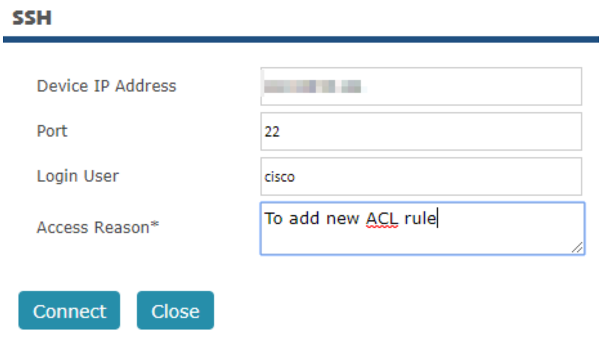
****Applicable for SecuRA Pro only:*** CLI Jobs that are not approved within the expiry time will get to Expired State and the expiry duration can be configured from System Parameters.

18.1. How to take CLI Connection

From **Device Grid** Page, click ⓘ (action icon) of the specific device to access Device Action window.

SSH:

Click SSH: 🖥 to open the SSH Connection window.

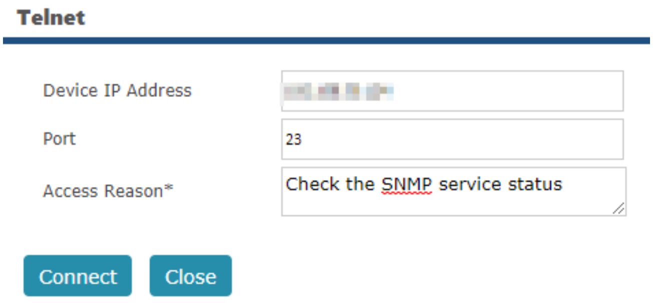


SSH

Device IP Address	[redacted]
Port	22
Login User	cisco
Access Reason*	To add new ACL rule

Telnet:

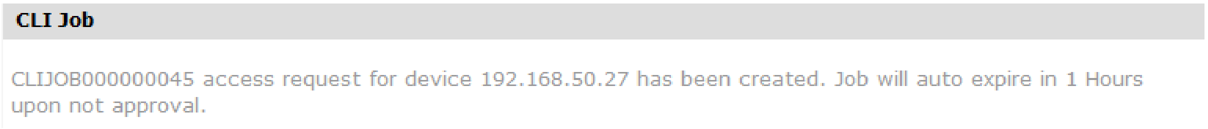
Click TELNET: 🖥 to open Telnet Connection window.



Telnet

Device IP Address	[redacted]
Port	23
Access Reason*	Check the SNMP service status

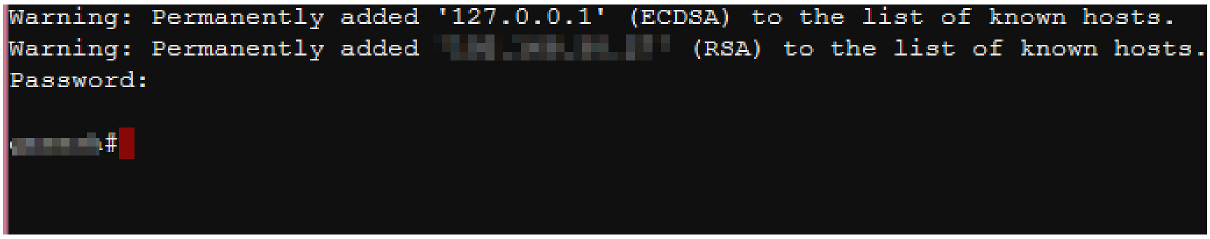
If the user is a Non-whitelisted user, the below message will be displayed.



CLI Job

CLIJOB000000045 access request for device 192.168.50.27 has been created. Job will auto expire in 1 Hours upon not approval.

For White listed user, session will start immediately (as shown below).

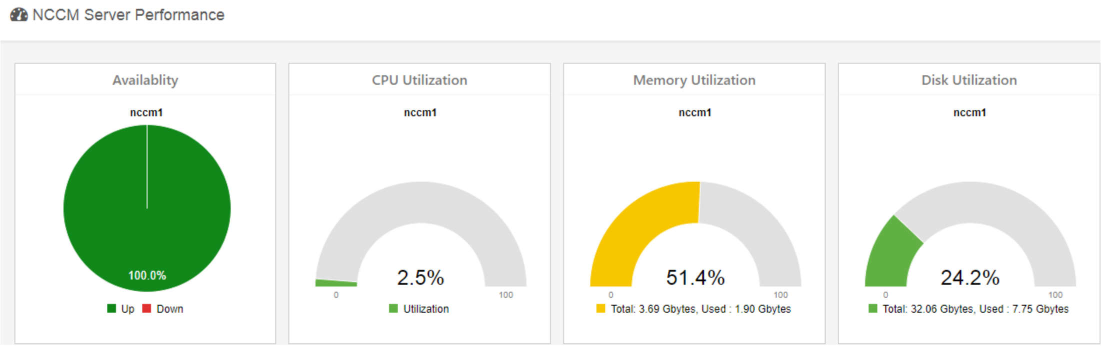


```
Warning: Permanently added '127.0.0.1' (ECDSA) to the list of known hosts.
Warning: Permanently added [redacted] (RSA) to the list of known hosts.
Password:

[redacted]#
```

19. Server Performance

This self-monitoring page helps to track the usage of SecuRA installed servers.

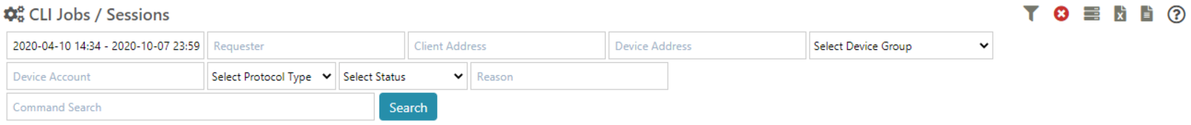
From the left panel, click and select ‘Server Performance’.



This illustrates the detailed information of CPU utilization, Memory utilization and Disk utilization of the server(s) where SecuRA installed.

CLI Jobs/Sessions Search

Click to enable the filter.



- Select the time from calendar options.
- Input the Requester Name in the textbox
- Input Client IP Address in textbox.
- Input Device IP Address in textbox.
- Select Device Group using the dropdown menu.
- Input Device Account in the textbox
- Select ‘Protocol Type’ using the dropdown menu.
- Select Status using the dropdown menu.
- Select ‘Approval Type’ using the dropdown menu.

- Input ‘Approver Name’ in the textbox.
- Input the Reason in the textbox.
- Input the command in the textbox.
- Click Search to perform the search.

Click ☰ from the CLI Jobs page to navigate to ‘Devices’ page.

CLI Job Export

CLI Jobs can be exported into excel by using 🗎 or into CSV by using 🗎.

20. Configuration Template (SecuRA Pro)

Configuration changes like “Provisioning”, “Service Creation”, “Service Deactivation” and “any change” on Networking Devices can be done using Configuration Templates.

Template Execution

- Template is a **Collection of commands** (one or more) with zero or more variables to be executed on devices for specific operations (like ACL Modification, Route ADD, Interface NAC configuration, Interface IP Change, Interface Enable Disable, SNMP/LLDP/CDP enable or Disabling, OS Upgrade). By substituting different values (to variables) for different Devices, user can reuse the same template for similar operations on multiple devices. Device Credentials, Device Interface Name/IP Address, command inputs will become a variable portion in command template.

- Templates are vendor and OS Type specific, which means, separate templates are required to be built for the same operation on two different vendor devices or for two different OS Types of same vendor. This is due to a difference in the command syntax and command formats for the same operation on two vendor devices.

- Apart from command portion, Templates also contain information of Vendor, OS Type, Series and Model where template can RUN, along with ACL configuration which defines who all can manage the Templates.

- Once the Configuration Template is built, user can execute the Templates on devices using the Upload Job functionality.

- Configuration Template (Network Diagnosis type) can be used in Network Diagnosis functionality for Checking the Device's operational data and for doing simple configurations like Crypto cache clearing, daily diagnosis check etc., (Which does not affect and is not a part of the Device Configuration).

- Configuration Template command portion should be written in **XML format.**

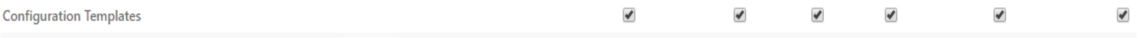
- Configuration Template inherits Jinja2 **Templating** standards where user gets all benefits of Jinja2 Template such as Data Types (Integer, Boolean, List), Control Statement (If – elif – else, For Loop, while Loop), Operator condition (=, != , >, <, >=, <= etc.).

Note: Same Template framework and fundamental is followed in

- Configuration Profile - Used by Configuration upload Job to add/remove/modify the services on devices
- CLI (Command Line Interface) Job
  - User will be given Direct CLI (SSH or Telnet) access to the Devices from SecuRA Application (like a Gateway process) for changing configurations.

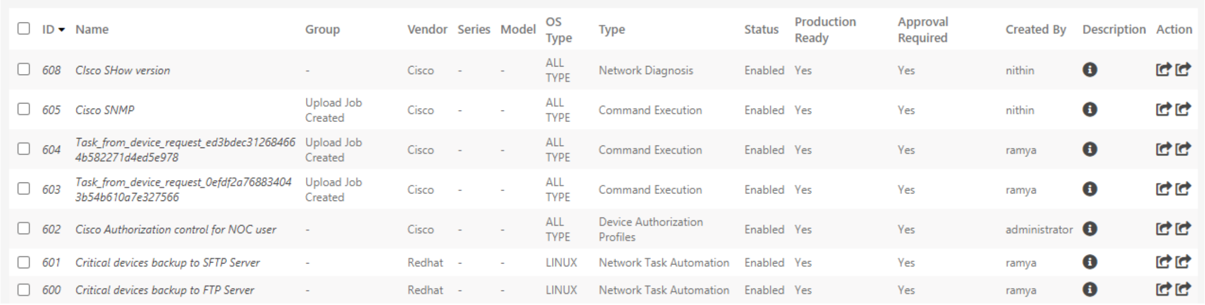
This is a Privilege based feature: The user will be able to access, view, add, edit, delete, execute & export, only if privileges have been given by the administrator. This will be defined under roles and privileges.

This menu is accessible only if the below privilege has been checked.



Configuration Templates	☑	☑	☑	☑	☑	☑

From the left panel, click ♻ and select 'Configuration Templates'.



☐	ID ▾	Name	Group	Vendor	Series	Model	OS Type	Type	Status	Production Ready	Approval Required	Created By	Description	Action
☐	608	CIsco SHow version	-	Cisco	-	-	ALL TYPE	Network Diagnosis	Enabled	Yes	Yes	nithin	ℹ	
☐	605	Cisco SNMP	Upload Job Created	Cisco	-	-	ALL TYPE	Command Execution	Enabled	Yes	Yes	nithin	ℹ	
☐	604	Task_from_device_request_ed3bdec31268466 4b582271d4ed5e978	Upload Job Created	Cisco	-	-	ALL TYPE	Command Execution	Enabled	Yes	Yes	ramya	ℹ	
☐	603	Task_from_device_request_0efdf2a76883404 3b54b610a7e327566	Upload Job Created	Cisco	-	-	ALL TYPE	Command Execution	Enabled	Yes	Yes	ramya	ℹ	
☐	602	Cisco Authorization control for NOC user	-	Cisco	-	-	ALL TYPE	Device Authorization Profiles	Enabled	Yes	Yes	administrator	ℹ	
☐	601	Critical devices backup to SFTP Server	-	Redhat	-	-	LINUX	Network Task Automation	Enabled	Yes	Yes	ramya	ℹ	
☐	600	Critical devices backup to FTP Server	-	Redhat	-	-	LINUX	Network Task Automation	Enabled	Yes	Yes	ramya	ℹ	

Configuration Template Grid page lists down all templates created by the user and also the templates which are assigned to the same user by admin or template management full privileged user.

The **Access Control List** feature in this module lets the admin privileged users to decide who can view, edit or delete any specific templates in SecuRA.

Configuration Template Grid shows

- Template ID - To know the creation sequence (recently created or old).
- Name of Template – Name will be unique and will be referred in other features while using the Template.
- Vendor – The Vendor Device where this template can RUN (Vendor Specific).
- OS Type – The Vendor Device OS Type where this Template can only RUN (OS specific).
    - In case the Template can RUN on all OS Type of same Vendor, Input OS Type as '**ALL TYPE'.**
    - **Example: CISCO IOS, IOS XE, NXOS, IOSXR, ASA** may take **different** command syntax for same operation.
- Type of Template – SecuRA Supports 9 Types of Templates and each of them will be explained in detail, in the following sections.
- Active Status – Enabled/Disabled – During execution, this flag does not impact those Jobs that are set as Disabled (template disabled) but is already assigned to an Upload Job. On the other hand, Disabled Templates will not be allowed to be used in New Upload Job Creation.
- Execution ready or Production Status – Should be in Ready State to use in Upload Job for configuration change.
- Approval Required Flag - The value will be always Yes (Approval is always required).
- Actions – There are two action icons displayed here – Execute & Quick Execute.

Note: - *When the Template is used in Upload Job by a white listed user or Approver, Approval Process will be by-passed, and Job will go for execution directly****.***

- Created User – User who created the Template.
- Description – Template description which defines the operation purpose.

How to write Command Portion in Template:

SecuRA supports two ways of writing commands in Template

1) Plain command format (Writing Device Command as it is)

    a. In plain command format, user writes the device commands as it is defined by the vendor. This format will be used only inside **Command Execution & Network Diagnosis template** type

b. Though it is a simple way to write the template, it is not a recommended format, since additional information to command such as command timeout, response prompt, error check condition on response cannot be used.

c. The Timeout for each command using plain command format is always 30 seconds and each command takes the full 30 seconds even if the execution is completed before.

2) XML Command Format

a. In XML command format, each command is enclosed in XML node and additional input to the command like command timeout, prompt, expected pattern, previous match, action will be added in XML node properties.

b. XML command format is the recommended format across all features of SecuRA including Upload and Diagnosis purpose.

Sample command portion for changing Device hostname in plain text format and XML format:

Plain Format	XML Format
conf t	<command prompt=”#” timeout=”10”>conf t</command>
hostname newname	<command prompt=”#” timeout=”10”>hostname newname</command>
exit	<command prompt=”#” timeout=”10” action=”exit”>exit</command>

In the above example, the plain format takes device command as it is the same way the command is executed using Putty or xtrem application, but in XML Format each device command will be placed inside XML node "Data" section and other information in XML node property section.

XML Command Syntax

<command property1=”value” property2=”value”> **Device Command** </command >

Command Properties Actual Command

XML Command Sample

```
<command prompt=”#” timeout=”10”> hostname newname</command>
```

The device command for every device will be inside the Data portion of XML Node and the additional properties or information will be inside XML’s property portion. Property value must always be inside Double quotes character.

SecuRA supports the following properties

1) timeout - value (in seconds). Every command execution is considered as complete either till the prompt pattern value is matched or till the timeout second count is reached.

2) prompt - is generally the last character of **command response** that informs the command execution completion of a Device. When the response from Device is not matching the prompt, command execution is considered as COMMAND ERROR.

   ```
   prompt=”#”
   ```

   a. The prompt can be a single character or a word or a line.

      ```
      prompt=” #”
      prompt=”Router27#”
      prompt=”[Are you confirm the reboot action]?”
      ```

   b. The prompt value is always a regex pattern and it can be escaped using \ to make exact match. Below example. (Dot) regex character is escaped with \ to consider it literally as ‘.’ (Dot) and not as regex pattern.

      ```
      prompt=”\.”
      ```

Follow the URL https://regex101.com/ to verify or check the regex pattern before saving the template.

   c. The prompt also supports multiple patterns (multiple single characters or multiple words) to match the command execution completion

      ```
      prompt=”[#,>,\$]”
      ```

      ```
      prompt=”[Username, login, User]”
      ```

d. When the given prompt is not matched within the specified timeout seconds, SecuRA will declare it as Command error and stop or continue the execution based on Task IP/Command continuation input from Upload Job task input.

3) "action" property is used to

a. Inform SecuRA that exit command is executed and to not wait for prompt.

action="exit"

b. Inform SecuRA to store the result of command for storing the configuration output of device and also to copy the command output for Trigger parsing.

action="output-to-store"

4) "shell" property is used to Inform SecuRA to open a remote session (TELNET or SSH) from a Device for further command executions.

shell="remote"

<Of Courcommand shell="remote" prompt="Password"> ssh -o StrictHostKeyChecking=no -o UserKnownHostsFile=/dev/null {{Profile.ssh_loginname}}@{{Device.IPaddress}} -p {{Profile.ssh_port}} </command>

5) "error_pattern" property is used to check the command response; if the pattern values match the command response, command execution is considered as COMMAND ERROR. Similar to prompt property, error_pattern can take multiple values. **NOTE: -** Prompt property is used to check for command completion however error_pattern property is for checking whether the Response is as per the expectation.

error_pattern="[Unknown command, Invalid Command]"

Example: when "copy tftp" command is not supported by a device, response will be %Error opening tftp and the error_pattern to catch the error will be

error_pattern="[%Error opening tftp]"

The below properties also follow the same principle as error_pattern .

6) "expected_pattern" property is used to check the command response; if the pattern value does not match the command response, command execution is considered as COMMAND ERROR.

expected_pattern="[bgp is enabled]"

7) “expected_any_response” property is used to check the command response; if the device does not respond to any data, command execution is considered as COMMAND ERROR. The value of property is not required and hence input can be empty double quotes

   expected_any_response=""

8) “expected_empty_response” property is used to check the command response; if the device responds with any data, command execution is considered as COMMAND ERROR. The value of property is not required and hence, input can be empty double quotes

   expected_empty_response=""

9) “expected_count_response” property is used to check the command response; if the device response line is not equal to count value data, command execution is considered as COMMAND ERROR. The value of property is the response line count. The count can be any number

   expected_count_response="5"

   SecuRA expects a 5 line response.

10) “expected_count_response” property is used to check the command response; if the device response line is not equal to the count value data, command execution is considered as COMMAND ERROR. The value of property is response line count. The count can be any number.

    expected_count_response="!5"

    SecuRA expects the response to be anything other than 5 lines.

11) “expected_count_response” property is used to check the command response; if the device response line is less than 6, command execution is considered as COMMAND ERROR. The value of property is count of line. The count can be any number.

    expected_count_response=">5"

    SecuRA expects the response to be greater than 5 lines.

12) “expected_count_response” property is used to check the command response; if the device response line is greater than 4, command execution is considered as COMMAND ERROR. The value of property is count of line. The count can be any number.

    expected_count_response="<5"

    SecuRA expects the response to be less than 5 lines.

13)“expected_count_response” property is used to check the command response; if the device response line is less than 5, command execution is considered as COMMAND ERROR. The value of property is count of line. The count can be any number.

```
expected_count_response=">=5"
```

SecuRA expects the response to be more than 4 lines.

14)“expected_count_response” property is used to check the command response; if the device response line is greater than 5, command execution is considered as COMMAND ERROR. The value of property is count of line. The count can be any number.

```
expected_count_response="<=5"
```

SecuRA expects the response to be less than 6 lines

15)“type” property is used to store the command response under property value. SecuRA stores the command output in **Operation Data store**.

For example:

If the output of the command, show IP interface brief is required to store in SecuRA as **Interface Brief**, XML command should be written as

<command prompt=”#” timeout=”5” type=”**Interface Brief**”> show IP interface brief</command>

Sample command to shut down an interface in plain text and XML format.

Plain Format	XML Format
conf t int Gi 0/0 shutdown exit	<command prompt=”#” timeout=”10”>conf t</command> <command prompt=”#” timeout=”10”> int Gi 0/0 </command> <command prompt=”#” timeout=”10”>shutdown</command> <command prompt=”#” timeout=”10” action=”exit”>exit</command>

Sample command to enable syslog in plain text format and XML format.

Plain Format	XML Format

conf t	<command prompt="#" timeout="10">conf t</command>
logging source-interface Loopback100	<command prompt="#" timeout="10"> logging source-interface Loopback100 </command>
end	<command prompt="#" timeout="10">end</command>
write memory	<command prompt="#" timeout="10" action="exit">write memory</command>

Below are some sample commands to replace the Device configuration file from SecuRA server.

```
<command prompt="\]\?">copy tftp: running-config</command>
<command prompt="\]\?">{{Global.managementIP}}</command>
<command prompt="\]\?">{{Job.uploadfilename}}</command>
<command prompt="[\],#]" timeout="300">running-config</command>
<command previous_match="\]" prompt="#" timeout="300">yes</command>
<command action="exit" prompt="">exit</command>
```

Note: *Plain text command cannot be written since the timeout of some commands are more than 30 seconds.*

SecuRA also supports writing of Comments inside the command portion, for better understanding of commands. To define a line as a comment, add # character at the beginning of a line.

Example for writing Comments inside commands:

```
# Make Terminal Len 0
<command prompt="#" timeout="60">terminal length 0</command>

# Copy the Image to Flash
<command prompt="]\?" timeout="60">copy tftp flash:</command>

# Remove boot system
<command prompt="#" timeout="60">no boot system</command>
```

Note: *At the time of execution, SecuRA ignores all lines starting with # (comment lines)*

SecuRA Variable Substitution

SecuRA follows **Jinja2 Template engine** for converting **command templates** into actual commands. Jinja2 Template engine provides features like

- Variable substitution
    - For substituting specific values for specific Devices
- Variable declaration
- Data structures like Integer, Boolean, List, and Dictionary
- Loop Statements like
    - For
    - While
    - Do while
- Conditional Statements like
    - If
    - If else
    - If elif else
- Conditional operators like
    - =
    - !=
    - in
    - not in
    - > and >=
    - < and <=

Variable Substitution:

Variables are **command inputs** given by a user dynamically during the execution time.

For example, if the user wants to change the hostname in Cisco devices, the command syntax will be

> #**hostname** <New Hostname>
> **hostname is the command and** <New hostname> is the variable or input portion to **hostname** command

Through variable substitution, single template is enough to change hostname of all devices same Vendor and OS Type configured in template; else each device requires a separate template.

To substitute a variable, follow the below steps, based on the condition applicable:

1) Use “Double Curly Brackets” before and after the variable {{ }}, only if variable is not inside Jinja2 statements

    <command prompt=”#” timeout=“5”>hostname {*{Runtime.hostame}}* *</command>*

    Runtime is a substitution object.

2) Directly writing variable, if variable is inside Jinja2 expression statement **{% %}**

{% if *Runtime.hostname. == “router27”* %}

SecuRA Substitution Objects in Template:

SecuRA supports 10 types of **substitution objects** for Variable substitution within configuration template

1. Runtime object

   Runtime object will be used in Configuration Upload and Network Diagnosis activities. Runtime object variables will be converted into user input form to get values while configuring upload task or Network Diagnosis creation.

   Ex {{Runtime.hostname}}

2. Global object

   All Global parameters configured in SecuRA are available through Global object for Variable substitution.

   Ex {{Global.managementIP}}

3. Type object

   Defines the field, based on the variable type specified such as Text Area, Text field, DropDown, Multi DropDown.

   Ex : Type.Speed=DropDown

4. Default object

   The default value for Type Object I defined here.

   Ex: Default.Speed=10,100,1000

5. Remark object

   Displays the Text on mouse hover on the Variable Name.

   Ex: Remark.Speed=enter speed of interface

6. Optional object

   If variable is declared ‘Optional’, the input for the field is not mandatory.

   Ex: Optional.VariableName

7. Check object

Ensures that the Input format matches the defined format.

Ex: In Textfield, it should allow only 1 to 255

^([1-9]|[1-9][0-9]|[1-2][0-5][0-5])$

8. LOCAL_SHELL object

LOCAL_SHELL object gets values from LOCAL_ACCOUNT profile, configured in Device credential for Variable substitution.

Ex {{LOCAL_SHELL.username}}

9. Device object

Device object gets values from **Device database** of corresponding Device where command execution takes place.

Ex {{Device.IPaddress}}

10. Interface object

Interface object gets values from **Device Interface database** of the corresponding Device where command execution takes place.

Ex {{Interface.name}}

Ex {{Interface.description}}

11. Job object

Job object gets values from Job Database (Upload Job) of corresponding Device where command execution takes place.

Ex {{Job.name}}

12. Profile object

Profile object gets values from Profile Database (Configuration Profile) of corresponding Device where command execution takes place.

*Ex {{*Profile*.user_name}}*

13. Trigger object:

Trigger object gets values from Configuration Trigger Database of corresponding Trigger name used in Configuration Template.

Ex {{Trigger.triggername}}

Note: *A template can have more than one Trigger variable.*

14. Profile object:

Profile object gets values from Device Credential Database of corresponding Device (Device Credential) where command execution will take place.

Ex {{Profile.ssh_loginname}}

15. Time object:

Time object gets values from SecuRA server based on current time which is for substituting time values in a template during execution

Ex {{Time.now}} – Time in unix epoc format

{{Time.YYYYMMDD}} – Time in YYYY MM DD format

{{Time.uniquestring}} – Unique string

Conditioning in Template:

SecuRA supports condition-based Templating using "if", "if else" and "if elif else" conditional statements

A. ”If” Condition:

```
{% if Runtime.interface_name == "GigabitEthernet0/0" %}
        IP address 192.168.1.1 255.0.0.0
        no shutdown
{% endif %}
```

B. ”If else” Condition:

```
{% if Runtime.interface_name == "GigabitEthernet0/0" %}
        IP address 192.168.1.1 255.0.0.0
        no shutdown
{% else %}
        IP address 192.168.2.1 255.0.0.0
        no shutdown
{% endif %}
```

C. ”If elif else” Condition:

```
{% if Runtime.interface_name == "GigabitEthernet0/0" %}
        IP address 192.168.1.1 255.0.0.0
        no shutdown
{% elif Runtime.interface_name == "GigabitEthernet0/1" %}
        IP address 192.168.1.1 255.0.0.0
        no shutdown
{% else %}
        IP address 192.168.2.1 255.0.0.0
        no shutdown
```

```
{% endif %}
```

Looping in Template:

SecuRA supports loop based Templating using “for” loop statements

”For Loop” Condition:

```
{% for interface_name in Runtime.interface_names %}
        {% if {{interface_name}} == "GigabitEthernet0/0" %}
                IP address 192.168.1.1 255.0.0.0
                no shutdown
        {% endif %}
{% endfor %}
```

Guidelines for Configuration Template:

#Substitution, Conditioning, Looping in Template should be in Jinja2 standard. Refer http://jinja.pocoo.org/docs/2.10/ for more tutorials.

Points to Remember

Always enclose the commands within **{% %}** for "if" and "for", "while" conditional statements

Always enclose the variables inside **{{ }}** for substitution

Sample Template Configuration

Example 1: Create an Empty List and add values into List and DO a simple ‘For Loop’

```
# Declaring a string variable to store value from Runtime or user.  Default (“”) function will make variable empty string till USER input
{%   set myinput = Runtime.interface_list | default(“”)   %}


# Converting User Input to a list using Split function
{%  set mylist = myinput .split(",")  %}

#Doing for Loop or Looping of Each Item
 i{% for each_interface in mylist %}
    <command prompt="#">int {{each_interface}}</command>
    <command prompt="#">shutdown</command>
# for requires endfor to close the section
{% endfor %}
```

<u>Example 2:</u> Conditions (if case elif Case and else case)

```
{%  for each_interface in mylist  %}
        {% if each_interface == "Gi0/1"  %}
               <command prompt="#">int {{each_interface}}</command>
               <command prompt="#">shutdown</command>
        {% elif each_interface == "Gi0/2"  %}
               <command prompt="#">int {{each_interface}}</command>
               <command prompt="#">no shutdown</command>
        {% else %}
               <command prompt="#">I dont know</command>
       {% endif %}
{% endfor %}
```

<u>Example 3</u>: Taking List Input from a Trigger

#**down_interface_list_cisco_ios** is a Trigger in Configuration Trigger

```
{%  set mylist1 = Trigger.down_interface_list_cisco_ios | default([])   %}

{% for each_interface in mylist1 %}
   <command prompt="#">int {{each_interface}}</command>
   <command prompt="#">shutdown</command>
{% endfor %}
```

<u>Example 4:</u> Disable the Interface named ‘Ether’

# String Manipulation startswith, endswith, find, lower, upper, strip

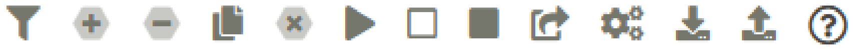
```
{% set myinput = Runtime.InterfaceNames | default ("") %}

{% set mylist = myinput.split(",")  %}

{%   for each_item  in  mylist  %}
   {%  if each_item.lower().startswith("ether")    %}
      <command prompt="#">int {{each_item}}</command>
      <command prompt="#">shutdown</command>
  {% endif %}
{% endfor %}
```

<u>Example 5:</u> Taking First Element from the Trigger

```
{% set mylist = Trigger.down_interface_list_cisco_ios | default ([])  %}
{% if mylist  %}
  <command timeout ="10" prompt ="#" >config t</command>
  <command timeout ="10" prompt ="#" >interface {{mylist[0]}}  </command>
   <command timeout="10" prompt ="#" >IP address 172.17.230.2 255.255.255.252</command>
   <command timeout ="10" prompt ="#" >no shut</command>
{% endif %}
```

20.1. Action Icons – Configuration Template

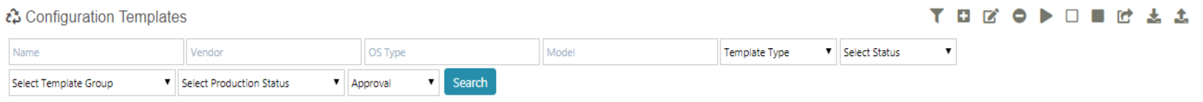
Multiple action icons are displayed on the top right corner of the page.



Icons	Label	Actions
▼	Filter	Click to use filter options to search
⊕	Add	Click to add a 'Configuration Template'
⊖	Edit	Click to edit a Template
⧉	Clone	Click to Clone a Configuration Template
⊗	Delete	Click to delete a Template
▶	Production Ready	Click to mark the template ready for Production
□	Enable	Click to enable Template
■	Disable	Click to disable Template
↗	Simple Script Execution	Click to add a Quick 'Upload Job'
⚙	Advanced Script Execution	Click to add an 'Upload Job'
⤓	Import	Click to import Template
⤒	Export	Click to export Template

20.2. Configuration Template Filter

Click ▼ to open the filter panel



Configuration Templates

Name | Vendor | OS Type | Model | Template Type ▾ | Select Status ▾

Select Template Group ▾ | Select Production Status ▾ | Approval ▾ | Search

SecuRA allows filtering the Configuration Templates based on the following columns.

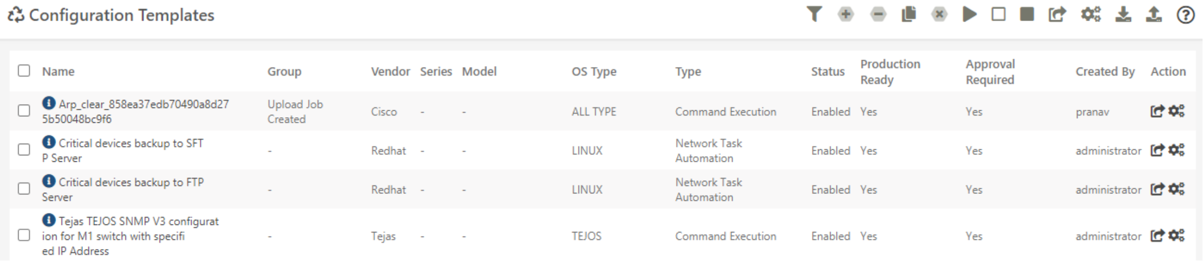
- Template Name
- Vendor
- OS Type
- Model
- Template type
- Active Status
- Template Group
- Production Status
- Approval State

Click Search to perform the filter-based search on filter columns selection.

Note: *SecuRA supports full match and pattern match for user input fields.*

20.3. Add Template

Click + to add a Configuration Template.



Configuration Templates

□	Name	Group	Vendor	Series	Model	OS Type	Type	Status	Production Ready	Approval Required	Created By	Action
□	Arp_clear_858ea37edb70490a8d27 5b50048bc9f6	Upload Job Created	Cisco	-	-	ALL TYPE	Command Execution	Enabled	Yes	Yes	pranav	
□	Critical devices backup to SFT P Server	-	Redhat	-	-	LINUX	Network Task Automation	Enabled	Yes	Yes	administrator	
□	Critical devices backup to FTP Server	-	Redhat	-	-	LINUX	Network Task Automation	Enabled	Yes	Yes	administrator	
□	Tejas TEJOS SNMP V3 configurat ion for M1 switch with specifi ed IP Address	-	Tejas	-	-	TEJOS	Command Execution	Enabled	Yes	Yes	administrator	

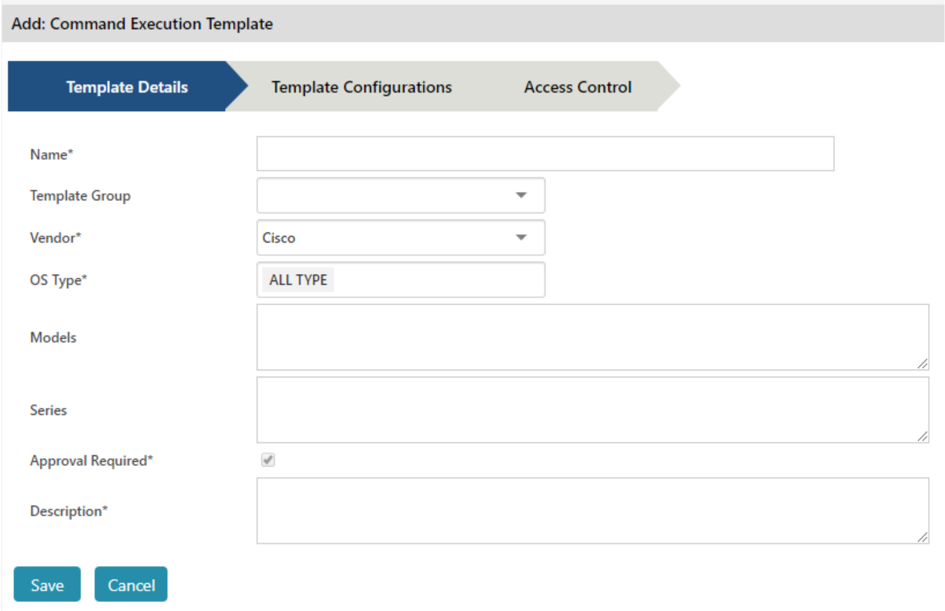
SecuRA supports six different types of Templates and each type is used for specific requirement. They are

- Command Execution
- Configuration Merge
- Configuration Replace
- Network Task Automation
- Network Diagnosis
- Device Authorization Profiles

20.3.1. Command Execution

Command Execution is used to execute a series of command (one by one) on devices, which is similar the user executing commands through putty application for configuration changes. This template type should be used for changing small set of configurations which does not roll back to previous ones.

Click ● Command Execution and click Ok to proceed further.



Add: Command Execution Template

Template Details | Template Configurations | Access Control

Name*

Template Group

Vendor* Cisco

OS Type* ALL TYPE

Models

Series

Approval Required* ☑

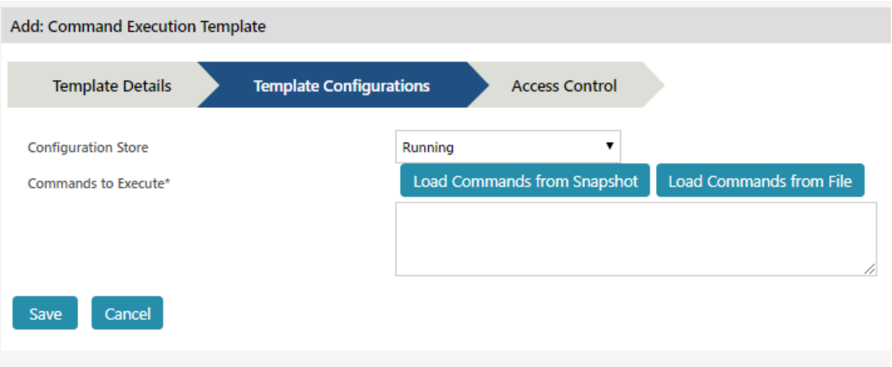
Description*

Save | Cancel

- Input the Template Name
    - Template Name should be unique.
- Select the Template Group using the dropdown menu.
- Select Vendor using the dropdown menu.
    - This is mandatory since Template commands are specific to vendor device.
- Select the OS Type
    - This is mandatory since Template commands are specific to vendor device OS types. In case of commands being executable on all devices of vendor then input as ALL TYPE.
- Input the Model details.
- Input the Series details.

- Approval Required Checkbox is mandatory, and hence the user cannot uncheck it. (**This is a compliance requirement**).
- Input the Template Description.

Click Template Configurations panel.



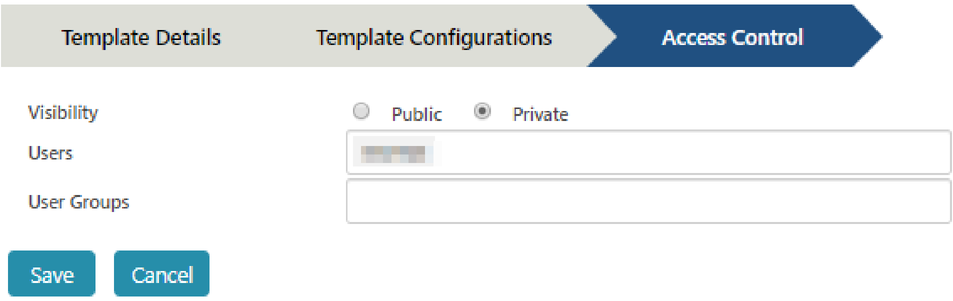
Add: Command Execution Template

Configuration Store: Running ▾

Commands to Execute*

- Select the Configuration Type or Store using the dropdown menu.
  - Supported Types are Startup, Running and Candidate.
  - This value does not impact the operation but acts as a label for type of configuration that is required to be changed.
- Click Load Commands from File to load configuration
  - User can load the configuration commands from a text file.
  - After loading the configuration commands, user has to make device specific changes and create variables, to be filled by SecuRA at the time of device execution.

Click Access Control panel



Visibility: ○ Public ● Private

Users: [redacted]

User Groups

- Select the visibility
  - Note: If the visibility is “Private”, User and User group dropdown will be enabled, and selected user and administrator will only be able to manage this template.

- Select the User(s).
- Select the User group(s).
- Click Save to save the template with given input.
- Click Cancel to abort the Template creation.

Example for Command Execution:

<command prompt=”#”>conf t</command>

<command prompt=”#”>hostname {{Rumtime.xxxx}} </command>

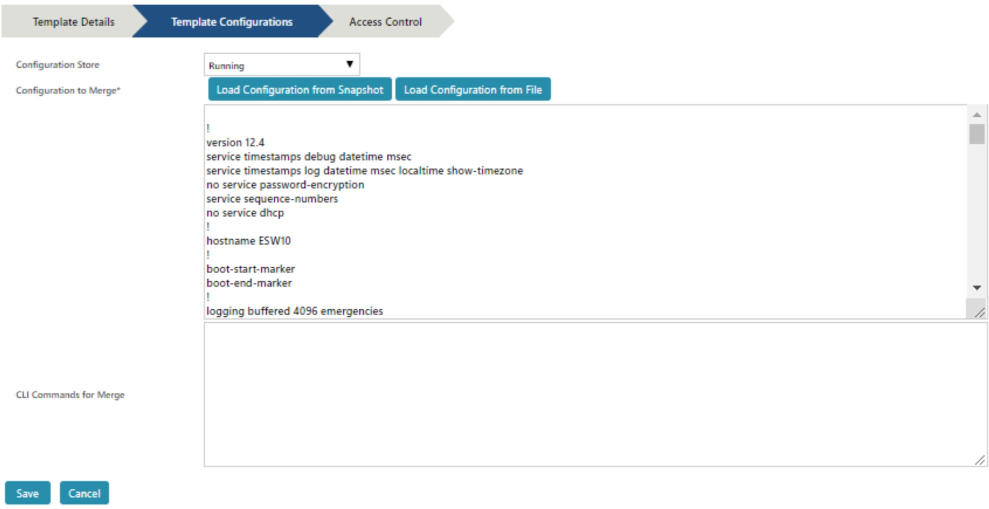
20.3.2. Configuration Merge

Configuration Merge is used to upload or merge a command block into Device. This type should be used for creating or merging a configuration block into device.

Click ● Configuration Merge and click Ok to proceed further.

Input the “Configurations to Merge” by directly typing or ‘Loading from Snapshot’ or from a file.

Input the “CLI Commands to Merge”. The CLI Commands will merge the new Configurations into Device Configuration.



Configuration Store: Running

Configuration to Merge*:

```
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec localtime show-timezone
no service password-encryption
service sequence-numbers
no service dhcp
!
hostname ESW10
!
boot-start-marker
boot-end-marker
!
logging buffered 4096 emergencies
```

CLI Commands for Merge

Example Commands to Merge:

<command prompt="\]\?">copy tftp: running-config</command>

<command prompt="\]\?">{{Global.managementIP}}</command>

```
<command prompt="\]\?">{{Job.uploadfilename}}</command>
<command previous_match="confirm\]" prompt="#" timeout="300">yes</command>
<command action="exit" prompt="">exit</command>
```

Note: SecuRA will auto fill the “Configurations to merge commands” into Job object *uploadfilename variable*.

The rest of the inputs are similar to “Add Command Execution”.

20.3.3. Configuration Replace

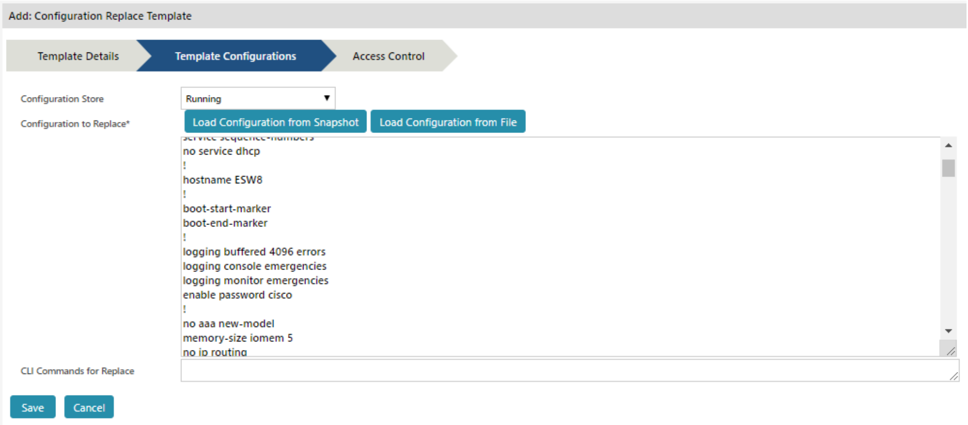
Configuration Replace is used to replace a full configuration into device. This should be used for replacing default or configuration discrepancies with backed up configuration version.

Click ● Configuration Replace and click Ok to proceed further.

- Input the “Configurations to Replace” by directly typing or Loading from Snapshot or from a file.
- Input the “CLI Commands to Replace”. The CLI Commands will replace the new full Configurations into Device Configuration.

Example Commands to Replace:

```
<command prompt="[\],#]" timeout="300">configure replace
tftp://{{Global.managementIP}}/{{Job.uploadfilename}}</command>

    <command previous match="confirm\]" prompt="#"
    timeout="300">y</command>

   <command action="exit" prompt="">exit</command>
```



Add: Configuration Replace Template

Template Details
Template Configurations
Access Control

Configuration Store: Running ▾

Configuration to Replace*

Load Configuration from Snapshot
Load Configuration from File

```
service sequence-numbers
no service dhcp
!
hostname ESW8
!
boot-start-marker
boot-end-marker
!
logging buffered 4096 errors
logging console emergencies
logging monitor emergencies
enable password cisco
!
no aaa new-model
memory-size iomem 5
no ip routing
```

CLI Commands for Replace

Note: *SecuRA will auto fill the "Configurations to Replace commands" into Job object uploadfilename variable.*

The rest of the inputs are similar to "Add Command Execution".

20.3.4. Network Task Automation

Network Task Automation is similar to Command Execution Template which executes a series of commands, one by one.

This template should be used for Network Automation tasks like Health Check, Trace Route, backing up important data, finding device service configurations like "SNMP Status, BGP Status, SSH Status, TFTP reachability" regularly.

Click ○ Network Task Automation and click Ok to proceed further.

The rest of the inputs are similar to "Add Command Execution".

Example:

If we must check important application server's availability from core router on a daily basis, write the below command in the template.

<command prompt="#" timeout=30>ping 192.168.50.235</command>

20.3.5. Network Diagnosis

This is similar to Command Execution Template which executes a series of commands, one by one. This template should only be used for Network Diagnosis tasks like Health Check, Trace Route, finding device service configurations like "SNMP Status, BGP Status, SSH Status" on an adhoc basis.

Click ● Network Diagnosis and click Ok to proceed further.

- Input the Commands for Diagnosis.

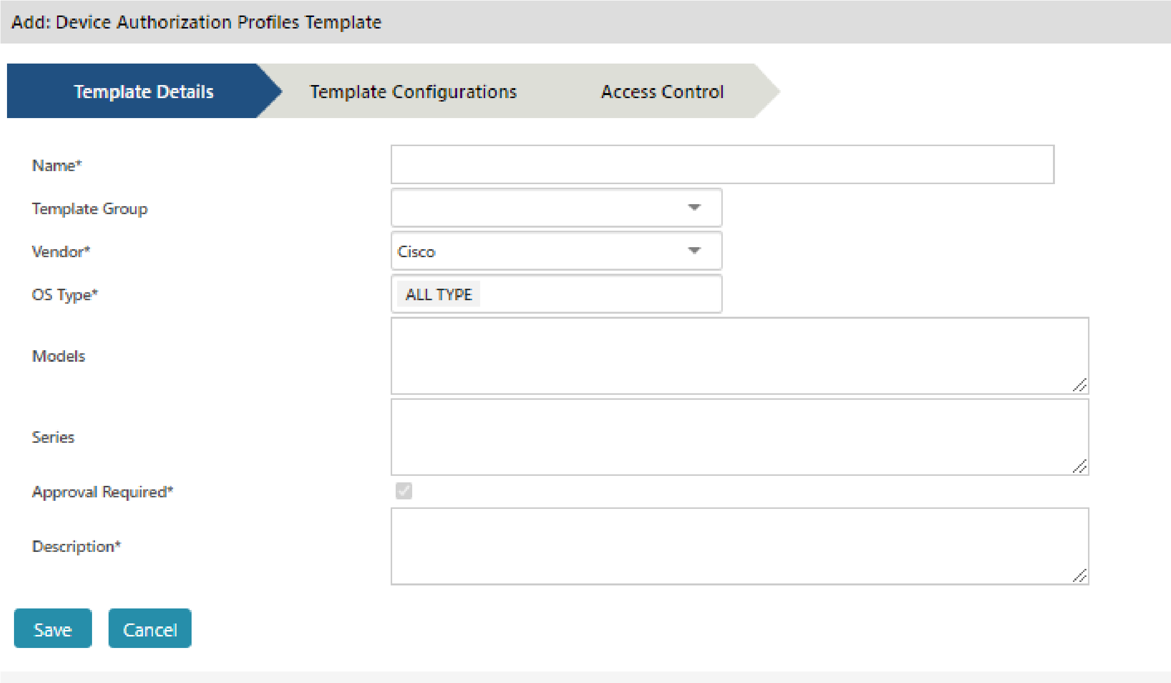
The rest of the inputs are similar to "Add Command Execution".

Note: *Network Diagnosis Template will be used in "Network Diagnosis feature" by service engineers.*

20.3.6. Device Authorization Profile

This feature will be used to define set of commands that can be executed/denied execution by a specific user/user group on Infraon SecuRA. Administrators can also restrict/permit command execution authorization based on device models.

Click ● Device Authorization Profiles and click Ok to proceed further.



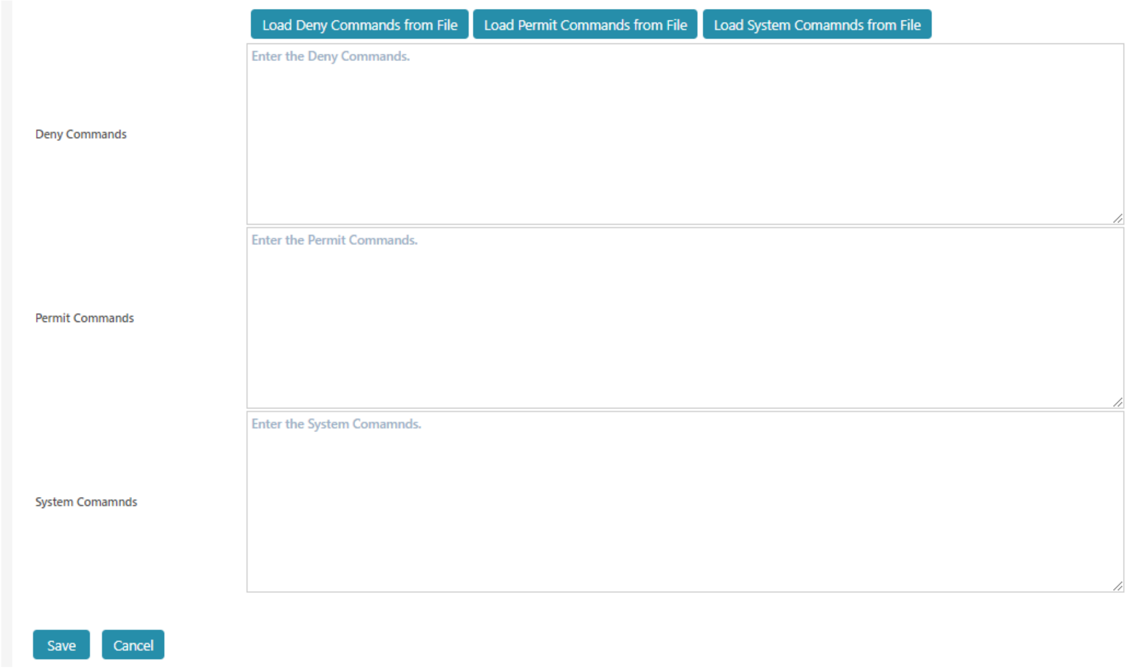
Add: Device Authorization Profiles Template

Name*	
Template Group	
Vendor*	Cisco
OS Type*	ALL TYPE
Models	
Series	
Approval Required*	☑
Description*	

- Input the Template Name
  - Template Name must be unique.
- Select the Template Group using the dropdown menu.
- Select Vendor using the dropdown menu.
  - This is mandatory since Template commands are specific to vendor device.
- Select the OS Type
  - This is mandatory since Template commands are specific to vendor device OS types. In case of commands being executable on all devices of vendor then input as ALL TYPE.
- Input the Model details.
- Input the Series details.

- Approval Required Checkbox is mandatory, and hence the user cannot uncheck it. (**This is a compliance requirement**).
- Input the Template Description.

Click Template Configurations panel.


Load Deny Commands from File
Load Permit Commands from File
Load System Comamnds from File
Deny Commands
Enter the Deny Commands.
Permit Commands
Enter the Permit Commands.
System Comamnds
Enter the System Comamnds.
Save
Cancel

Infraon SecuRA accepts command input in regex pattern only. Command inputs are split into three sections:

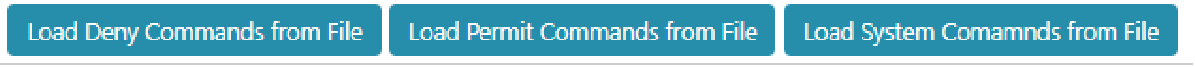
Permit Commands – Command (sets) that are permitted for execution by the User/User Group. Commands that are not added in the 'Permit' section will be blocked at the time of execution.

Deny Commands - Command (sets) that are denied for execution by the User/User Group. When a user tries to execute commands, which are mentioned in this section, SecuRA terminates the session or blocks the user and/or triggers a notification, as defined by the administrator.

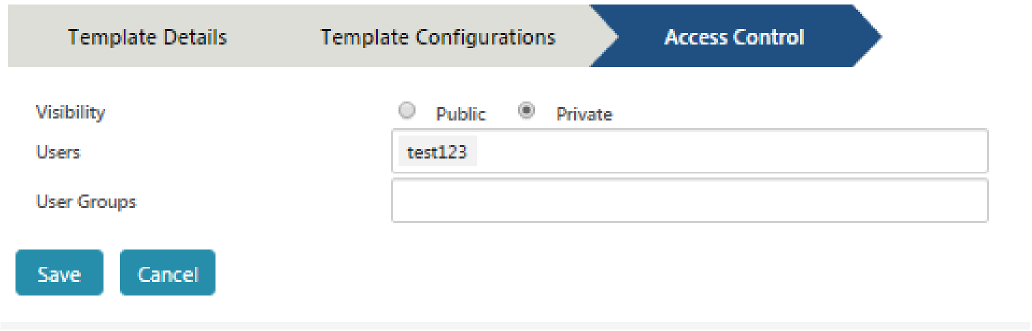
System Commands - used to ignore inputs like password and other User credential input. For example: When a user tries to execute a Command, that requires authentication by the system, the user is prompted by the system to provide additional information. In this case, the system prompt must be added in the 'System Commands' section. If not, system runs the command through the Permit command list and may end up blocking the command/command set.

There are two ways to input commands:

1. Adding commands in the respective text boxes.
2. Importing saved commands from a file. To import commands, click on the respective button- Permit/Deny/Ignore.


Load Deny Commands from File
Load Permit Commands from File
Load System Comamnds from File

Click Access Control panel



Visibility ○ Public ● Private

Users test123

User Groups

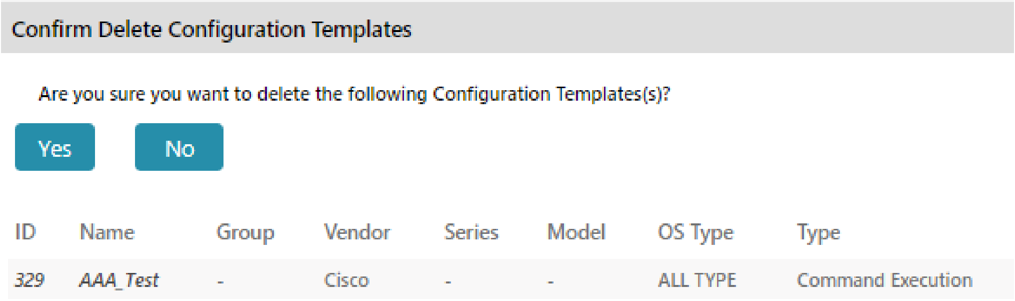
- Select the visibility
  - ***Note:*** If the visibility is "Private", User and User group dropdown will be enabled, and selected user and administrator will only be able to manage this template.
- Select the User(s).
- Select the User group(s).
- Click Save to save the template with given input.

20.4. Edit Template

Select an existing template and click ⊖ to edit. Edit operation follows the same steps as 'Add Template'. Other than Template Type all other fields on template can be modified.

20.5. Delete Template

Select the Template(s) and click ⊗ to the delete the Template



Confirm Delete Configuration Templates

Are you sure you want to delete the following Configuration Templates(s)?

ID	Name	Group	Vendor	Series	Model	OS Type	Type
329	AAA_Test	-	Cisco	-	-	ALL TYPE	Command Execution

Click Yes to delete the Template or No to cancel the delete operation.

20.6. Enable Template

Select Template(s) and click □ to enable the template i.e. to move the template state to active. Only Active Templates will be used in Upload job and Network Diagnosis.

20.7. Disable Template

Select Template(s) and click ■ to disable the template. Disabled templates will not be used in Upload job and Network Diagnosis.

20.8. Production Ready

Select Template(s) and click ▶ to change the templates' Production status to active. Only Active production Templates will be used in Upload job and Network Diagnosis. Templates manually created by user will be saved in Production

Ready and Enabled State. In case of Import Templates, Production Ready status will be in 'Disabled' state.

Note: Templates imported into SecuRA using excel must be changed manually to 'Production Ready' state.

20.9. Simple Script Execution

Click ↗ to execute a simple script. A quick upload page appears where the user can input details like Device IP/Device Group, account credentials, Schedule and Access details and execute the script.

20.1. Simple Script Execution

Click ⚙ to execute the template, which will redirect to 'Add an Upload Job'.

20.2. Template Import

Click ⬇ to upload/Import the template file (Only .xls file format is supported).

20.3. Template Export

Click ⬆ to export SecuRA's configured Templates to the XLS file. Click ⬆ to Download/Export the templates into excel file.

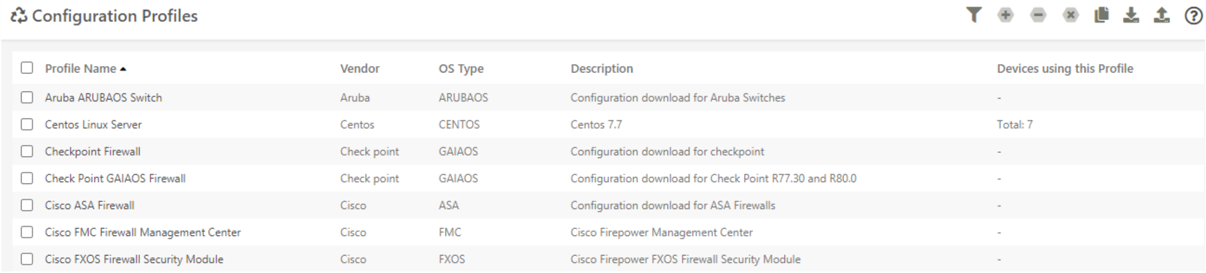
21. Configuration Profile

This is a Privilege based feature: The user will be able to access, view, add, edit, delete, execute & export, only if privileges have been given by the administrator. This will be defined under roles and privileges.

This menu is accessible only if the below privilege has been checked.

Configuration Profiles ☑ ☑ ☑ ☑ ☑

From the left panel, click ♻ and select 'Configuration Profiles'.



Configuration Profiles

□ Profile Name ▲	Vendor	OS Type	Description	Devices using this Profile
□ Aruba ARUBAOS Switch	Aruba	ARUBAOS	Configuration download for Aruba Switches	-
□ Centos Linux Server	Centos	CENTOS	Centos 7.7	Total: 7
□ Checkpoint Firewall	Check point	GAIAOS	Configuration download for checkpoint	-
□ Check Point GAIAOS Firewall	Check point	GAIAOS	Configuration download for Check Point R77.30 and R80.0	-
□ Cisco ASA Firewall	Cisco	ASA	Configuration download for ASA Firewalls	-
□ Cisco FMC Firewall Management Center	Cisco	FMC	Cisco Firepower Management Center	-
□ Cisco FXOS Firewall Security Module	Cisco	FXOS	Cisco Firepower FXOS Firewall Security Module	-

21.1. Quick Action Icons

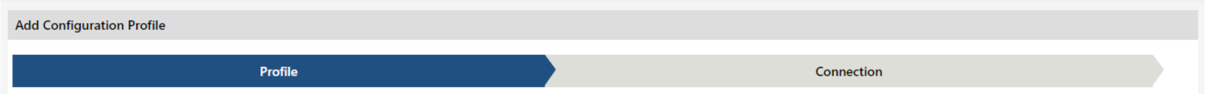
The below quick action icons are placed at the top right corner of Configuration Profile page

Icons	Label	Actions
▼	Filter	Click to use filter options to search
⊕	Add	Click to add 'Configuration Profile'
⊖	Edit	Click to edit a Configuration Profile

✖	Delete	Click to delete a Configuration Profile
⎘	Copy	Click to copy a Configuration Profile
⤓	Import	Click to import Configuration Profiles
⤒	Export	Click to export Configuration Profiles

21.2. Add Configuration Profile

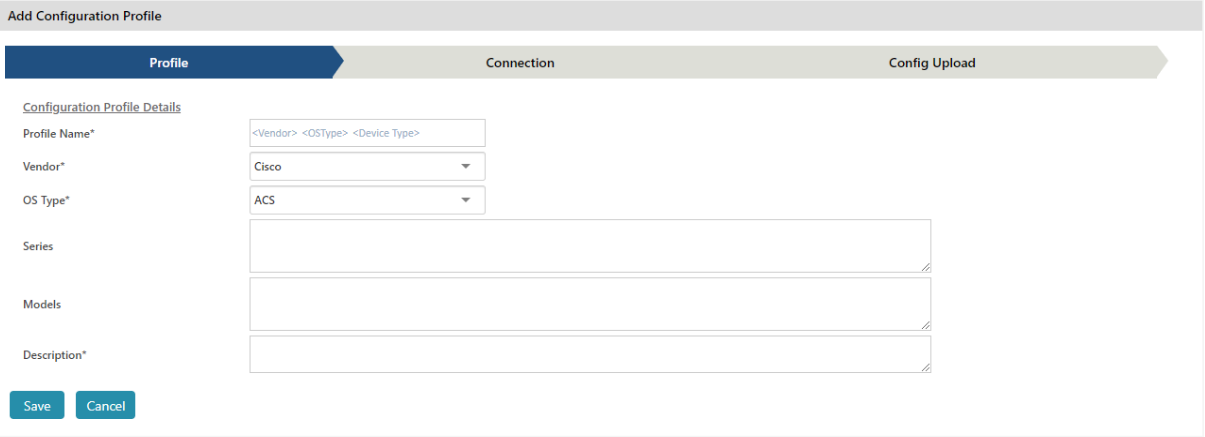
Click ⊕ to redirect to the Add Profile window. Update the below details in the ‘Profile' Tab.



There are multiple tabs in the ‘Add Configuration Profile’ page. They are:

- Profile
- Connection

21.2.1. Profile



Configuration Profile Details

Profile Name* <Vendor> <OSType> <Device Type>

Vendor* Cisco

OS Type* ACS

Series

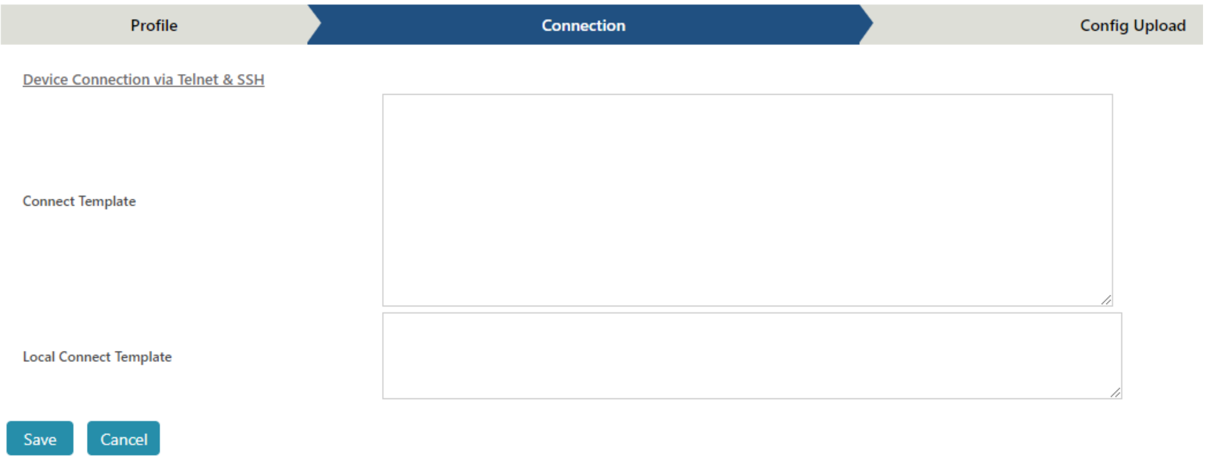
Models

Description*

- Input the Profile Name in the textbox.
- Select Vendor using the dropdown menu.
- Select OS Type using the dropdown menu.
- Input the Series in the textbox.
- Input the Models in the textbox.
- Input the Description in the textbox.

Click Connection tab to proceed.

21.2.2. Connection



- Input the Connect Details in textbox (SSH and Telnet Connection commands)
- Input the below Local Connect command in the given textbox.

```
<command prompt="[[Pp]assword,[Pp]ass,assword:,assword]">ssh -o StrictHostKeyChecking=no -o UserKnownHostsFile=/dev/null {{LOCAL_SHELL.ssh_loginname}}@127.0.0.1 -p {{LOCAL_SHELL.ssh_port}}</command>
<command prompt="[>,#]">{{LOCAL_SHELL.ssh_password}}</command>
```

For Example:

```
{% if Job.connection_protocol == "SSH" %}

<command shell="remote" prompt="[[Pp]assword,[Pp]ass,assword:,assword]">ssh -o StrictHostKeyChecking=no -o UserKnownHostsFile=/dev/null {{Profile.ssh_loginname}}@{{Device.IPaddress}} -p {{Profile.ssh_port}}</command>

 <command prompt="[#,>]">{{Profile.ssh_password}}</command>

{% endif %}
```

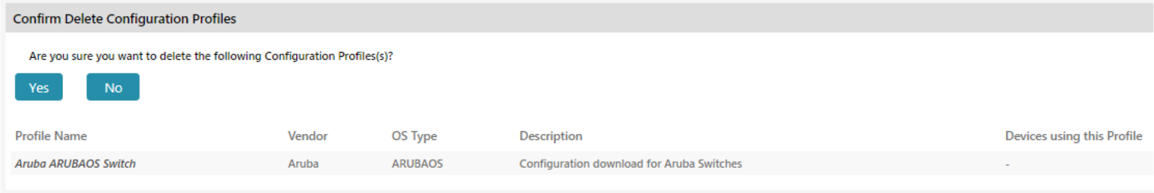
Click Save

21.3. Edit Configuration Profile

To edit a profile, select any of the existing profile and click ⊖. Make changes as necessary and save the changes.

21.4. Delete Configuration Profile

To delete Profile, select the profile(s) and click ✖



Confirm Delete Configuration Profiles

Are you sure you want to delete the following Configuration Profiles(s)?

Yes No

Profile Name	Vendor	OS Type	Description	Devices using this Profile
Aruba ARUBAOS Switch	Aruba	ARUBAOS	Configuration download for Aruba Switches	-

Click Yes to delete the Configuration Profile or click No to cancel the operation.

21.5. Copy Configuration Profile

To Copy a profile, select any existing profile and click ⧉. Follow the same procedure as Add Profile to copy the profile with minimal changes.

21.6. Profile Import

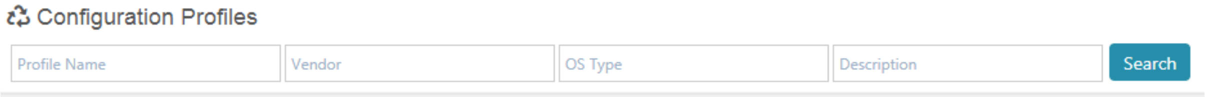
Click ⬇ to redirect to the upload window, to import the template file (.xls supported).

21.7. Profile Export

Click ⬆ to export SecuRA's configured Profiles to the XLS file.

21.8. Configuration Profile Search

Click ▼ icon to open the search options.



- Input Profile Name in the textbox.
- Input the Vendor in the textbox.
- Input OS Type in the textbox.
- Input Description in the textbox.

Click Search to search based, on the applied filter.

22. Account Management

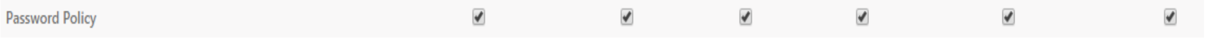
The Account Management module available in SecuRA allows the Administrator to create new user accounts, categorize it under roles/groups based on the privileges. This is done by assigning unique username and password for each user. This module plays a vital role in the security aspects of the entire system.

22.1. Password Policy

This page is used to set rules for the user passwords (applicable either at the time of creating account or to reset passwords). This can be configured to match internal and external compliances.

This is a Privilege based feature: The user will be able to access, view, add, edit, delete, execute & export, only if privileges have been given by the administrator. This will be defined under roles and privileges.

This menu is accessible only if the below privilege has been checked.



Password Policy	☑	☑	☑	☑	☑	☑

From the left panel, click 👤⚙ and select ‘Password Policy’.

22.1.1. Quick Action Icons

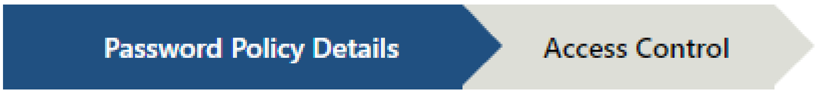
The below quick action icons are placed at the top right corner of the page.

▼ ⊕ ⊖ ⊗ 👤 ?

Icons	Label	Actions
▼	Filter	Click to use filter options to search
⊕	Add	Click to add a 'Password Policy'
⊖	Edit	Click to edit Password Policy
⊗	Delete	Click to delete Password Policy
👤	Accounts	Click to navigate to the Accounts Page

22.1.2. Add Password Policy

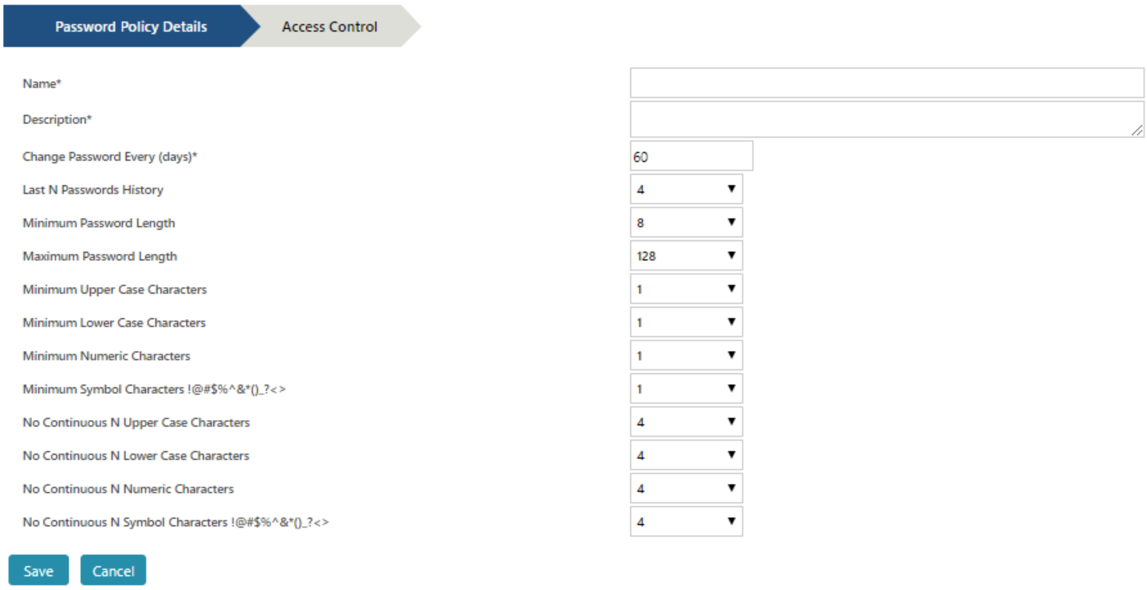
Click ⊕ to redirect to the add Password Policy window.



Password Policy contains 2 tabs

- Password Policy Details
- Access Control

Password Policy Details

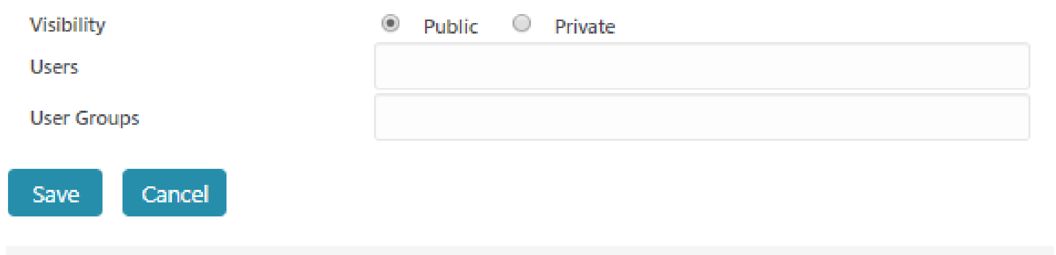


Name*	
Description*	
Change Password Every (days)*	60
Last N Passwords History	4
Minimum Password Length	8
Maximum Password Length	128
Minimum Upper Case Characters	1
Minimum Lower Case Characters	1
Minimum Numeric Characters	1
Minimum Symbol Characters !@#$%^&*()_?<>	1
No Continuous N Upper Case Characters	4
No Continuous N Lower Case Characters	4
No Continuous N Numeric Characters	4
No Continuous N Symbol Characters !@#$%^&*()_?<>	4

- Provide a name for the password Policy.
- Provide a brief description about the Policy.
- Mention the frequency (no. of days) for password change.
- Select the number of passwords (Passwords History) to maintain as history.
- Select options from the below criteria (to customize passwords)
    - Select Minimum Password length.
    - Select Maximum Password Length.
    - Select Minimum Upper-Case Characters
    - Select Minimum Lower-Case Characters
    - Select Numeric Characters

- Select Minimum Symbol Characters
- Select no. of Upper-Case characters (to restrict continuous occurrence of characters).
- Select no. of Lower-Case characters (to restrict continuous occurrence of characters).
- Select no. of Numeric characters (to restrict continuous occurrence of characters).
- Select no. of Symbols characters (to restrict continuous occurrence of characters).

Click **Access Control**



Visibility ● Public ○ Private

Users

User Groups

- Select Password Policy (Public/Private). If Private, select the user(s)/User Groups.

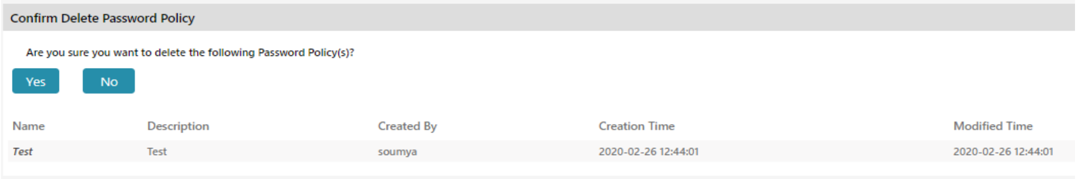
Click **Save** to add the group or click **Cancel** to abort the operation.

22.1.3. Edit Policy

Select Policy and click ⊖ to redirect to Edit Window. Make changes as necessary and click **Save** to save the changes.

22.1.4. Delete Policy

Select the Policy and click ⊗ to redirect to delete confirmation window.



Confirm Delete Password Policy

Are you sure you want to delete the following Password Policy(s)?

Name	Description	Created By	Creation Time	Modified Time
Test	Test	soumya	2020-02-26 12:44:01	2020-02-26 12:44:01

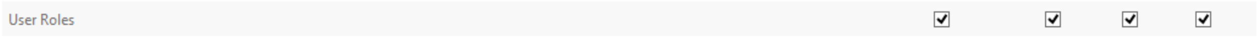
Click Yes to delete or click No to cancel the delete operation.

22.2. Roles and Privileges

This page is used to create roles and select the privileges for the role. Defining a role is mandatory, before creating an account.

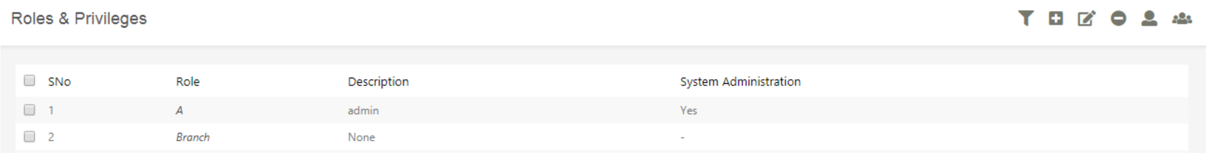
This is a Privilege based feature: The user will be able to access, view, add, edit, delete, execute & export, only if privileges have been given by the administrator. This will be defined under roles and privileges.

This menu is accessible only if the below privilege has been checked.



User Roles ☑ ☑ ☑ ☑

From the left panel, click and select ‘Roles and Privileges’.



Roles & Privileges

□ SNo	Role	Description	System Administration
□ 1	*A*	admin	Yes
□ 2	*Branch*	None	-

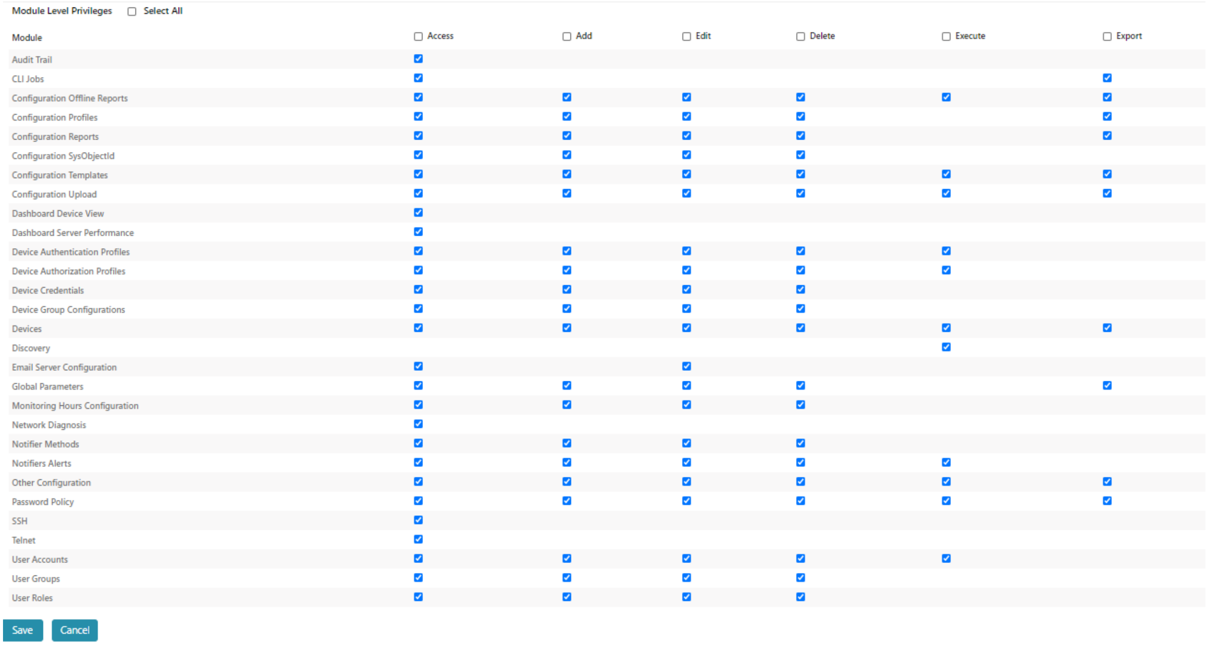
22.2.1. Quick Action Icons

The below quick action icons are placed at the top right corner of the page.

Icons	Label	Actions
▼	Filter	Click to use filter options to search
⊕	Add	Click to add a 'Role'
⊖	Edit	Click to edit a Role
⊗	Delete	Click to delete a Role
👤	Accounts	Click to navigate to the Accounts Page
👥	Groups	Click to navigate to the User Groups Page

22.2.2. Add Role

Click ➕ to redirect to the add role window.



Module Level Privileges ☐ Select All

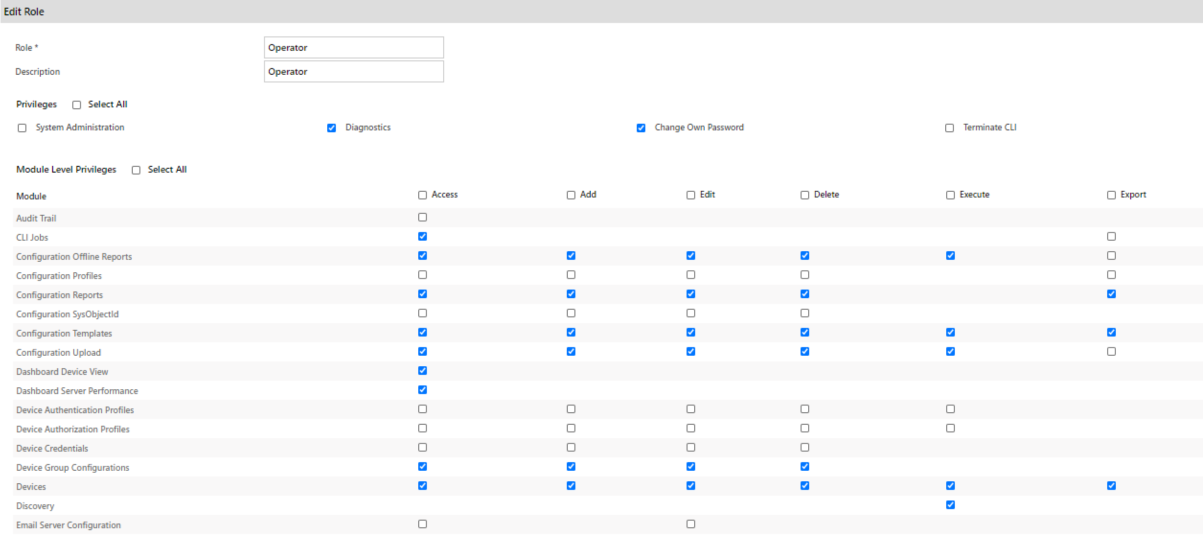
Module	☐ Access	☐ Add	☐ Edit	☐ Delete	☐ Execute	☐ Export
Audit Trail	☑					
CLI Jobs	☑					☑
Configuration Offline Reports	☑	☑	☑	☑	☑	☑
Configuration Profiles	☑	☑	☑	☑		☑
Configuration Reports	☑	☑	☑	☑		☑
Configuration SysObjectId	☑	☑	☑	☑		
Configuration Templates	☑	☑	☑	☑	☑	☑
Configuration Upload	☑	☑	☑	☑	☑	☑
Dashboard Device View	☑					
Dashboard Server Performance	☑					
Device Authentication Profiles	☑	☑	☑	☑	☑	
Device Authorization Profiles	☑	☑	☑	☑	☑	
Device Credentials	☑	☑	☑	☑		
Device Group Configurations	☑	☑	☑	☑		
Devices	☑	☑	☑	☑	☑	☑
Discovery					☑	
Email Server Configuration	☑		☑			
Global Parameters	☑	☑	☑	☑		☑
Monitoring Hours Configuration	☑	☑	☑	☑		
Network Diagnosis	☑					
Notifier Methods	☑	☑	☑	☑		
Notifiers Alerts	☑	☑	☑	☑	☑	
Other Configuration	☑	☑	☑	☑	☑	☑
Password Policy	☑	☑	☑	☑	☑	☑
SSH	☑					
Telnet	☑					
User Accounts	☑	☑	☑	☑	☑	
User Groups	☑	☑	☑	☑		
User Roles	☑	☑	☑	☑		

- Input Role Name in textbox.
- Input Description in textbox.
- Select privileges from the given option (Diagnostics, Change Own Password and SecuRA Administration) or select ‘All” to give all privileges to the new role.
- Privileges can be selected at individual module level i.e. Privileges can be given either to only access the modules, or privileges to add/edit/delete, or to execute and export, or all the above mentioned.
- Once all the module privileges have been selected, click to save the role with selected privileges.

Click Save to add the Group or click Cancel to abort the operation.

22.2.3. Edit Role

Select role and click − to redirect to Edit Role window. Make changes as necessary and click Save to save the changes.



Edit Role

Role * Operator

Description Operator

Privileges ☐ Select All

☐ System Administration ☑ Diagnostics ☑ Change Own Password ☐ Terminate CLI

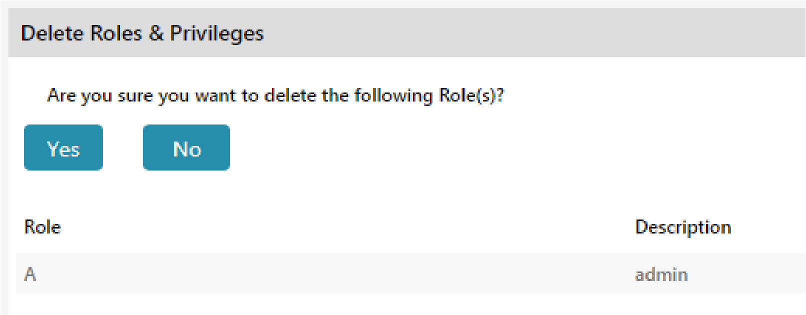
Module Level Privileges ☐ Select All

Module	☐ Access	☐ Add	☐ Edit	☐ Delete	☐ Execute	☐ Export
Audit Trail	☐					
CLI Jobs	☑					☐
Configuration Offline Reports	☑	☑	☑	☑	☑	☐
Configuration Profiles	☐	☐	☐	☐		☐
Configuration Reports	☑	☑	☑	☑		☑
Configuration SysObjectId	☐	☐	☐	☐		
Configuration Templates	☑	☑	☑	☑	☑	☑
Configuration Upload	☑	☑	☑	☑	☑	☐
Dashboard Device View	☑					
Dashboard Server Performance	☑					
Device Authentication Profiles	☐	☐	☐	☐	☐	
Device Authorization Profiles	☐	☐	☐	☐	☐	
Device Credentials	☐	☐	☐	☐		
Device Group Configurations	☑	☑	☑	☑		
Devices	☑	☑	☑	☑	☑	☑
Discovery					☑	
Email Server Configuration	☐		☐			

Note: *Role name cannot be edited.*

22.2.4. Delete Role

Select the Role(s) and click ✖ to redirect to delete confirmation window.



Delete Roles & Privileges

Are you sure you want to delete the following Role(s)?

Role	Description
A	admin

Click Yes to delete the Role or click No to cancel the delete operation.

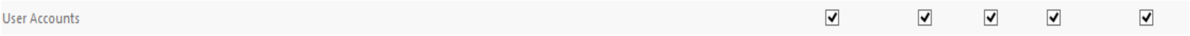
Note: *If Role has already been assigned to a User, administrator will not be able to delete the role.*

22.3. User Accounts

This is a Privilege based feature: The user will be able to access, view, add, edit, delete, execute & export, only if privileges have been given by the administrator. This will be defined under roles and privileges.

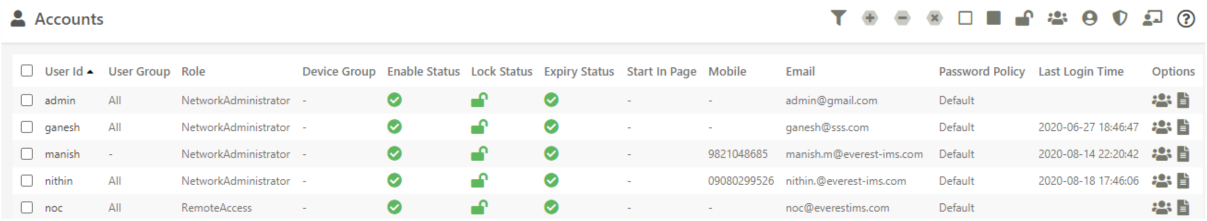
The ‘User Accounts’ module of SecuRA has been modified to enable ‘Hierarchy Level Approval’ privileges.

This menu is accessible only if the below privilege has been checked.



User Accounts ☑ ☑ ☑ ☑ ☑

From the left panel, click 👤 and select 'User Accounts -> Accounts.



Accounts

□	User Id ▲	User Group	Role	Device Group	Enable Status	Lock Status	Expiry Status	Start In Page	Mobile	Email	Password Policy	Last Login Time	Options
□	admin	All	NetworkAdministrator	-	✓	🔓	✓	-	-	admin@gmail.com	Default		👥 📄
□	ganesh	All	NetworkAdministrator	-	✓	🔓	✓	-	-	ganesh@sss.com	Default	2020-06-27 18:46:47	👥 📄
□	manish	-	NetworkAdministrator	-	✓	🔓	✓	-	9821048685	manish.m@everest-ims.com	Default	2020-08-14 22:20:42	👥 📄
□	nithin	All	NetworkAdministrator	-	✓	🔓	✓	-	09080299526	nithin.@everest-ims.com	Default	2020-08-18 17:46:06	👥 📄
□	noc	All	RemoteAccess	-	✓	🔓	✓	-	-	noc@everestims.com	Default		👥 📄

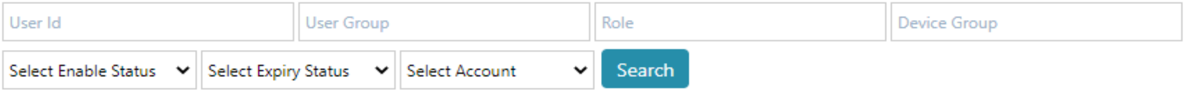
22.3.1. Quick Action Icons

The below quick action icons are placed at the top right corner of the page.

Icons	Label	Actions
▼	Filter	Click to use filter options to search
⊕	Add	Click to add a 'User Account'
⊖	Edit	Click to edit an Account
⊗	Delete	Click to delete an Account
□	Enable	Click to Enable the Account
■	Disable	Click to Disable the Account
🔓	Unlock	Click to Unlock an Account
👥	Groups	Click to navigate to the User Groups Page
👤	Roles	Click to navigate to the Roles & Priveliges Page
🛡	Password Policy	Click to navigate to the Password Policy Page
🖥	User Preference	Click to navigate to User Preference Page

22.3.2. User Account Search

User Accounts can be searched using one of the below fields.

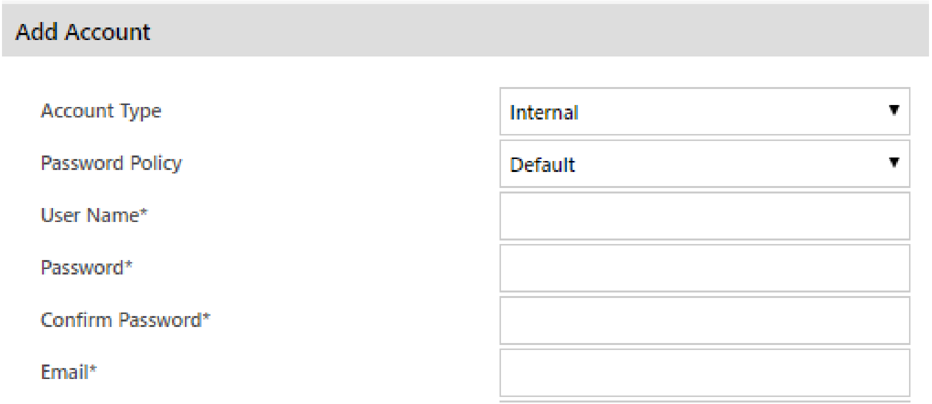


- User ID
- User Group
- Role
- Device Group
- Enable Status
- Expiry Status
- Account
- Account Type
- Click Search to perform the search, based on the applied filter.

22.3.3. Add Account

Click + to redirect to the Add Account window.

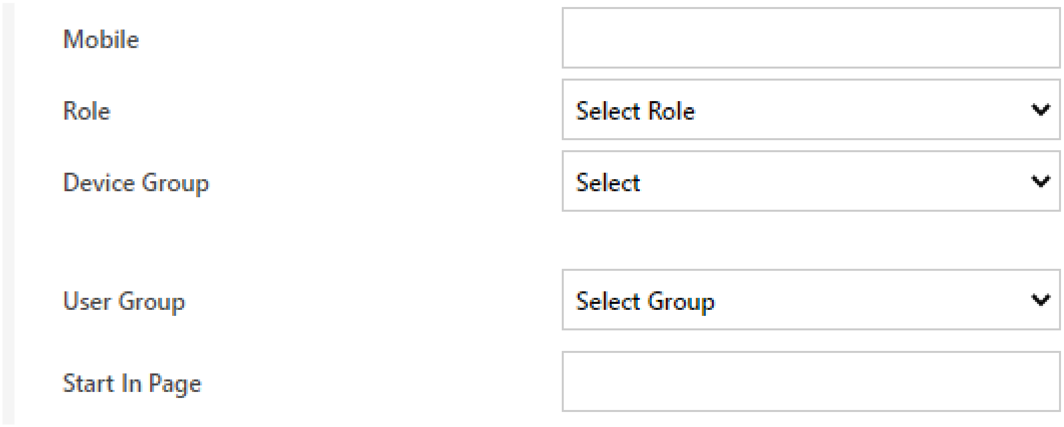
- Select the Account type using the dropdown menu. “Internal” user account created directly in Everest SecuRA system Select the Password policy applicable to this Account.
- Input the desired Username in the textbox.
- Input the Password in textbox.
- Confirm Password in textbox.
- Input Email ID* in textbox.



Add Account

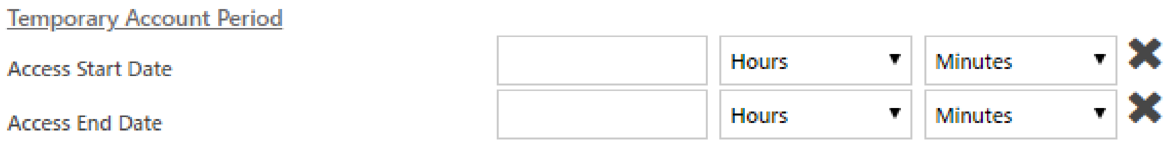
Account Type	Internal ▾
Password Policy	Default ▾
User Name*	
Password*	
Confirm Password*	
Email*	

- Input Mobile number in textbox.
- Select Role using the dropdown menu.
- Select Device Group using the dropdown menu.
- Select User Group using the dropdown menu.
- Select the Starting Page or the landing page, for the account.



Mobile	
Role	Select Role ⌄
Device Group	Select ⌄
User Group	Select Group ⌄
Start In Page	

It is possible to mark the account as a temporary one by selecting the Access Start and End date *(applicable for Pro Edition of **SecuRA** only).*



Temporary Account Period

Access Start Date		Hours ▾	Minutes ▾	✖
Access End Date		Hours ▾	Minutes ▾	✖

- Select the access Start date using the calendar option
- Select Start Time (Hours and Minutes)
- Select the access End date using the calendar option
- Select Start Time (Hours and Minutes)

Click Ok to add the Account or click Cancel to abort the operation.

Note: *The user account will be in disabled state until the account type is associated to a role and a Group.*

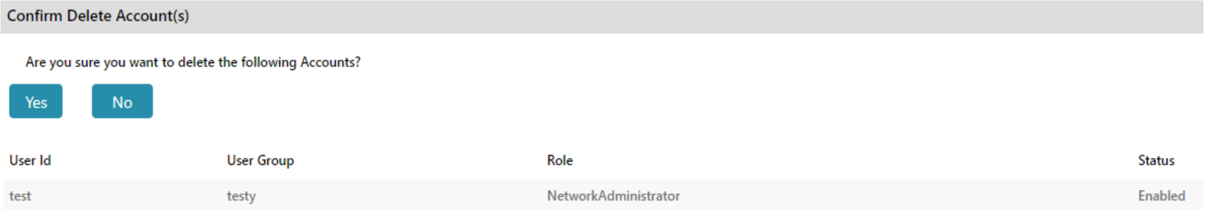
22.3.4. Edit Account

Click − to redirect to Edit account window. Make changes as necessary and click Ok to save the changes.

Note: *Username cannot be edited.*

22.3.5. Delete Account

Select the Account(s) and click ✖ to redirect to delete confirmation window.



Confirm Delete Account(s)

Are you sure you want to delete the following Accounts?

User Id	User Group	Role	Status
test	testy	NetworkAdministrator	Enabled

Click Yes to delete the account or click No to cancel the delete operation.

22.3.6. Enable Account

Select an Account(s) and click □ to activate the User to access SecuRA.

22.3.7. Disable Account

Select Account(s) and click ■ to disable the User from accessing SecuRA.

22.4. User Groups

SecuRA allows the user to deliver event notifications and escalations to a logical cluster of associated personnel, rather than individually assigning the notifications to different addressees one by one. This is achieved by assigning users into specific groups. This way, when an alarm is raised, the relevant notification is automatically sent by email/SMS to each user belonging to a designated group.

Three types of User Groups can be created on SecuRA.

- User Group – Where a group of ‘Users’ are added in a Group.
- User Group Groups – Where Multiple User groups can be added as a Group.

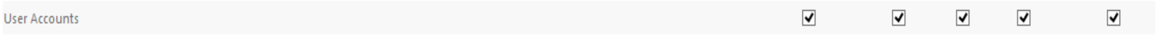
For example, let’s take a Bank, where multiple branches are mapped under a Circle, Multiple Circle Offices are mapped under a Zone and multiple zones are controlled directly by the administrators from the DC or the DRC Center.

In this scenario:

- Individual teams can be created for individual Branch Offices.
- Multiple Teams (Branches) can be added as a group (Circles).
- Multiple Groups (Circles) can be added as a group (Zones).

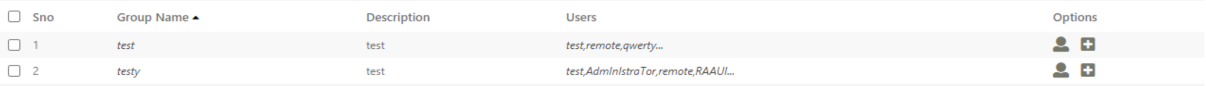
This is a Privilege based feature: The user will be able to access, view, add, edit, delete, execute & export, only if privileges have been given by the administrator. This will be defined under roles and privileges.

This menu is accessible only if the below privilege has been checked.



User Accounts	☑	☑	☑	☑	☑

From the left panel, click 👤 and select ‘User Groups’. The below page is displayed.

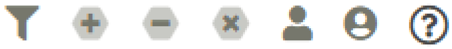


☐ Sno	Group Name ▲	Description	Users	Options
☐ 1	test	test	test,remote,qwerty...	👤 ⊞
☐ 2	testy	test	test,AdmInIstraTor,remote,RAAUI...	👤 ⊞

User Group details like Group Name, Description and Users.

22.4.1. Quick Action Icons

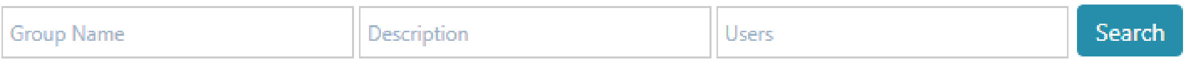
The below quick action icons are placed at the top right corner of the page.



Icons	Label	Actions
▼	Filter	Click to use filter options to search
⊕	Add	Click to add a 'User Group'

⊖	Edit	Click to edit a User Group
⊗	Delete	Click to delete a User Group
👤	Accounts	Click to navigate to the Accounts Page
👤	Roles	Click to navigate to the Roles & Privileges Page

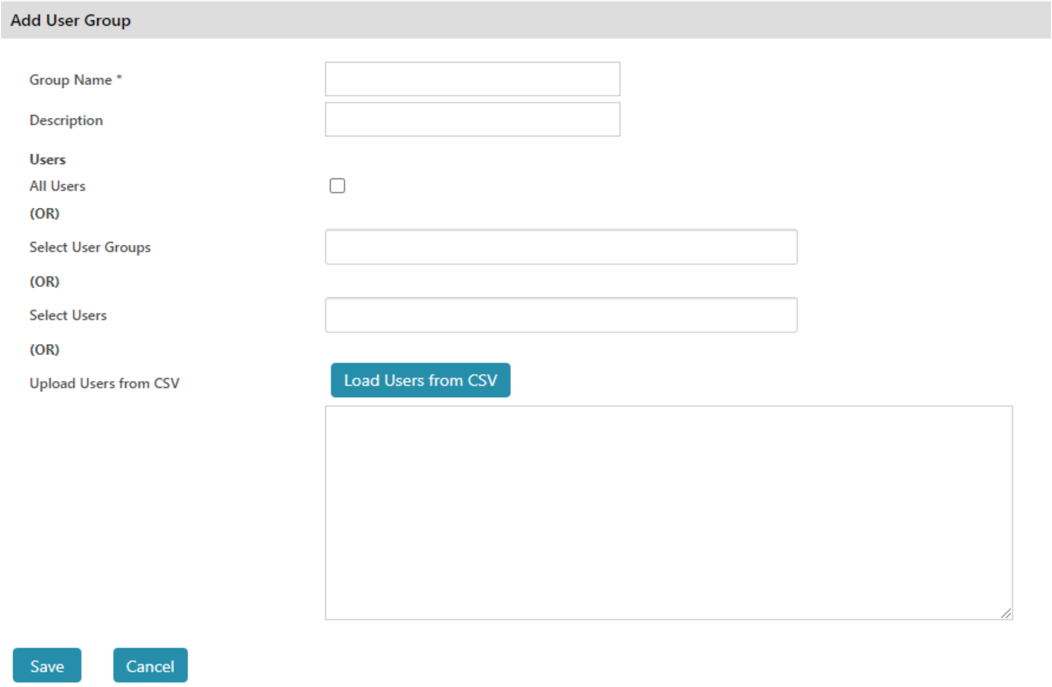
22.4.2. User Group Search



- Input Group Name in the textbox.
- Input Description in the textbox.
- Input User name in the given textbox.
- Click Search to perform the search based on the applied filter.

22.4.3. Add Group

Click ⊕ to redirect to the Add Group window.



- Input Group Name* in the textbox.

- Input Description in the textbox.

Users

- Use the Check Box □ to add ‘All Users’ to the group (or)
- Select the ‘User Groups’, to add to the Group(s) (or)
- Select ‘User(s)’ using the dropdown menu (or)
- Click Load Users from CSV to upload users from a CSV
- Click Choose File to browse and upload files.

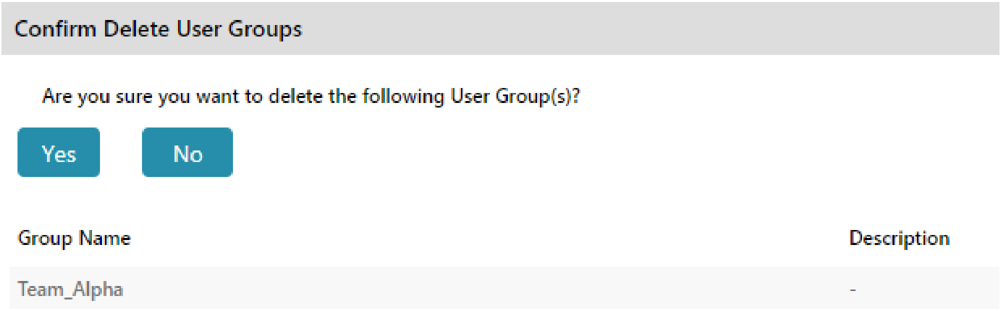
Click Load to upload or click Save to add the Group. Click Cancel to abort the operation.

22.4.4. Edit Group

Select the group and click ⊖ to edit the group. Make changes as necessary and click Ok to save the changes.

22.4.5. Delete Group

Select the Group(s) and click ✖ to redirect to the delete confirmation window.



Confirm Delete User Groups

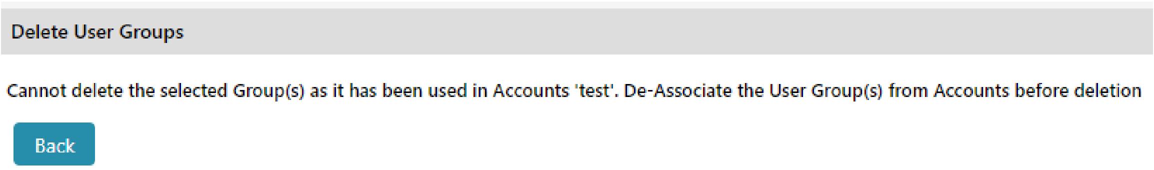
Are you sure you want to delete the following User Group(s)?

Yes No

Group Name	Description
Team_Alpha	-

Click Yes to delete the group and click No to abort the delete operation.

Note: *If the selected User Group is used in any accounts, the below message will be displayed. The Account must be de-associated before deleting the User Group.*



Delete User Groups

Cannot delete the selected Group(s) as it has been used in Accounts 'test'. De-Associate the User Group(s) from Accounts before deletion

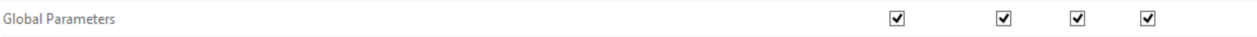
23. Global Parameters

Global Parameters are variables that can be added and used throughout the tool, as required.

The set of all global variables is known as the global environment or global state. In compiled languages, global variables are generally static variables, whose extent (lifetime) is the entire runtime of the program. In interpreted languages (including command-line interpreters), global variables are generally dynamically allocated at the time of declaration, since they are not known beforehand.

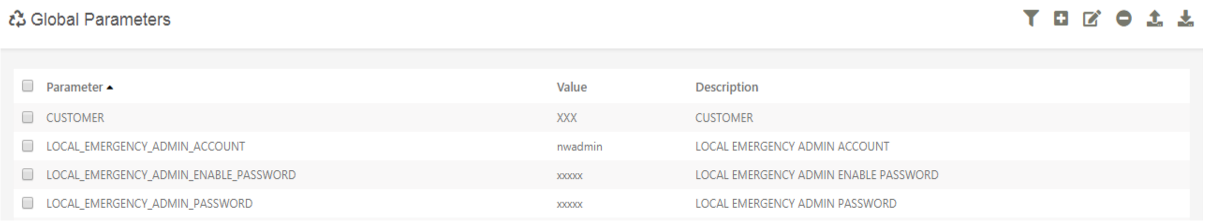
This is a Privilege based feature: The user will be able to access, view, add, edit, delete, execute & export, only if privileges have been given by the administrator. This will be defined under roles and privileges.

This menu is accessible only if the below privilege has been checked.



Global Parameters ☑ ☑ ☑ ☑

From the left panel, click ♻ and select ‘Global Parameters’.



□	Parameter ▲	Value	Description
□	CUSTOMER	XXX	CUSTOMER
□	LOCAL_EMERGENCY_ADMIN_ACCOUNT	nwadmin	LOCAL EMERGENCY ADMIN ACCOUNT
□	LOCAL_EMERGENCY_ADMIN_ENABLE_PASSWORD	xxxxx	LOCAL EMERGENCY ADMIN ENABLE PASSWORD
□	LOCAL_EMERGENCY_ADMIN_PASSWORD	xxxxx	LOCAL EMERGENCY ADMIN PASSWORD

23.1. Quick Action Icons

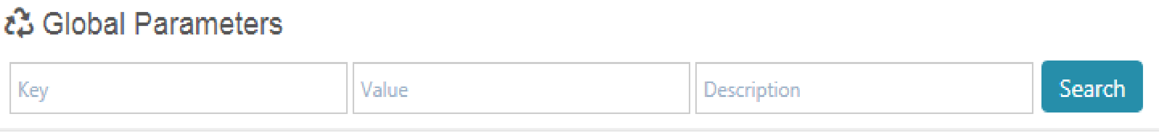
The below quick action icons are placed at the top right corner of the page.

Icons	Label	Actions
▼	Filter	Click to use filter options to search
⊕	Add	Click to add 'Global Parameter'
⊖	Edit	Click to edit a Global Parameter

✖	Delete	Click to delete a Global Parameter
⬆	Export	Click to export Global Parameters
⬇	Import	Click to import Global Parameters

23.2. Search

Click ▼ icon to open the search options.



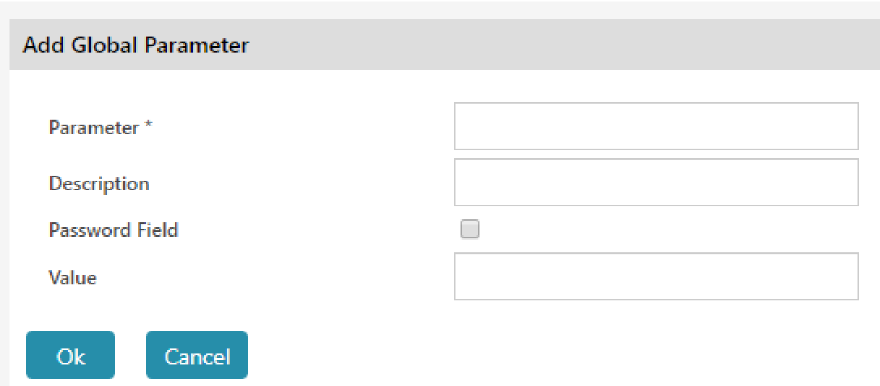
Global Parameters

Key | Value | Description | Search

- Input the Key in the textbox.
- Input the Value in the textbox.
- Input the Description in the textbox.
- Click Search to search based on the applied filter.

23.3. Add Global Parameter

Click ✚ to redirect to the Add Global Parameter window.



Add Global Parameter

Parameter *

Description

Password Field □

Value

Ok | Cancel

- Input Parameter Name in the textbox.
- Input the Description in the textbox.
- Check/Uncheck the Password field checkbox (When the Checkbox is ticked, password will be kept hidden).
- Input value in the textbox.

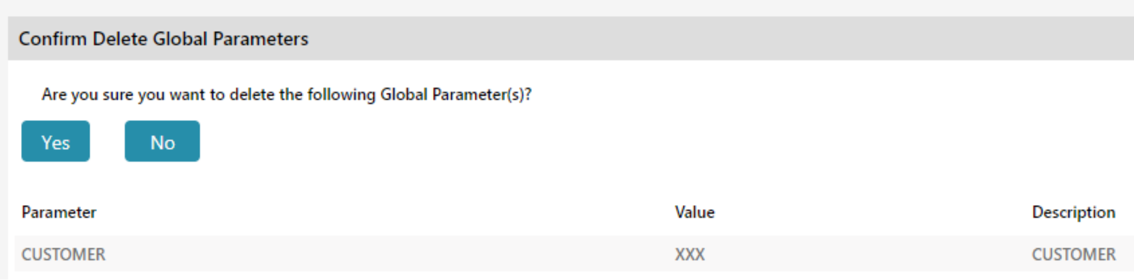
Click Ok to configure the Parameter or click Cancel to abort the operation.

23.4. Edit Parameter

Select a parameter and click ⊖ to redirect to the ‘Edit Parameter’ window. Make necessary changes and click Ok to save the changes.

23.5. Delete Parameter

Select the Parameter and click ✖ to redirect to the Delete confirmation window.



Confirm Delete Global Parameters

Are you sure you want to delete the following Global Parameter(s)?

Yes No

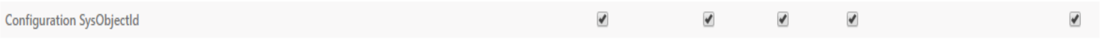
Parameter	Value	Description
CUSTOMER	XXX	CUSTOMER

Click Yes to delete the Parameter or No to cancel the delete operation.

24. System Object ID

This is a Privilege based feature: The user will be able to access, view, add, edit, delete, execute & export, only if privileges have been given by the administrator. This will be defined under roles and privileges.

This menu is accessible only if the below privilege has been checked.

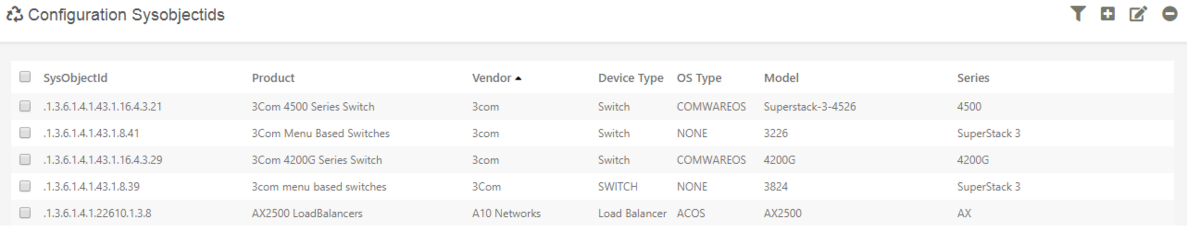


Configuration SysObjectId	☑	☑	☑	☑	☑

Each object in the MIB has an object identifier (OID), which the management station uses to request the object's value from the agent. An OID is a sequence of integers that uniquely identifies a managed object by defining a path to that object through a tree-like structure called the OID tree or registration tree.

To add new vendor onto SecuRA, it is necessary to register it in the system object ID.

From the left panel, click ♻ and select ‘SysObjectID’.



Configuration Sysobjectids

□	SysObjectId	Product	Vendor ▲	Device Type	OS Type	Model	Series
□	.1.3.6.1.4.1.43.1.16.4.3.21	3Com 4500 Series Switch	3com	Switch	COMWAREOS	Superstack-3-4526	4500
□	.1.3.6.1.4.1.43.1.8.41	3Com Menu Based Switches	3com	Switch	NONE	3226	SuperStack 3
□	.1.3.6.1.4.1.43.1.16.4.3.29	3Com 4200G Series Switch	3com	Switch	COMWAREOS	4200G	4200G
□	.1.3.6.1.4.1.43.1.8.39	3com menu based switches	3Com	SWITCH	NONE	3824	SuperStack 3
□	.1.3.6.1.4.1.22610.1.3.8	AX2500 LoadBalancers	A10 Networks	Load Balancer	ACOS	AX2500	AX

24.1. Quick Action Icons

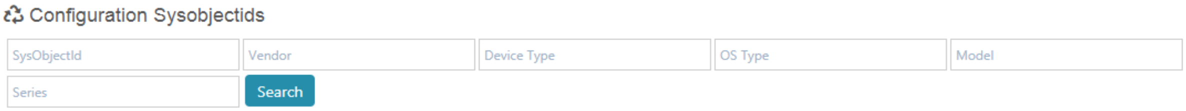
The below quick action icons are placed at the top right corner of the page.

▼ ⊕ ⊖ ⊗ ?

Icons	Label	Actions
▼	Filter	Click to use filter options to search
⊕	Add	Click to add 'Sysobjectid'
⊖	Edit	Click to edit a Sysobjectid
⊗	Delete	Click to delete a Sysobjectid

24.2. Search

Click ▼ will open the search options.



Configuration Sysobjectids

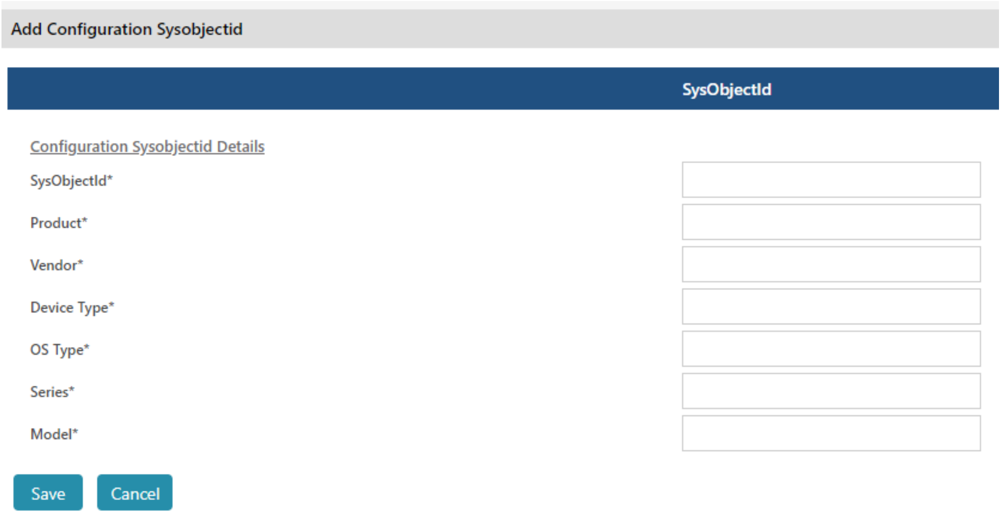
SysObjectId | Vendor | Device Type | OS Type | Model

Series | Search

- Input the systemobjectid in the textbox.
- Input the Vendor in the textbox.
- Input the Device type in the textbox.
- Input the OS type in the textbox.
- Input the Model in the textbox.
- Input the Series in the textbox.
- Click Search to search based on the applied filter.

24.3. Add SystemobjectiD

Click + to redirect to the Add Sysobjectid window.



Add Configuration Sysobjectid

SysObjectId

Configuration Sysobjectid Details

SysObjectId*	
Product*	
Vendor*	
Device Type*	
OS Type*	
Series*	
Model*	

- Input the SystemObject ID in the textbox.
- Input the Product in the textbox.
- Input the Vendor in the textbox.
- Input the Device type in the textbox.
- Input the OS type in the textbox.
- Input the Series in the textbox.
- Input the Model in the textbox.

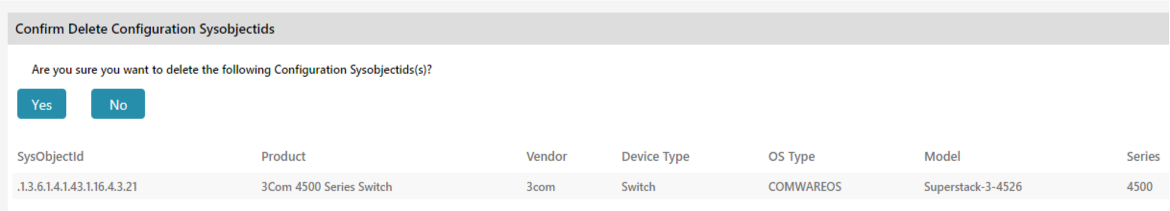
Click Save to save the systemObjectID or click Cancel to abort the Operation.

24.4. Edit SystemObject ID

Select a SystemObjectID and click − to redirects to an edit SystemObjectID window. Make the necessary changes and click Save to save the changes.

24.5. Delete SystemObjectID

Select the SystemObjectID(s) and click ✖ to redirect to the Delete confirmation window.



Confirm Delete Configuration Sysobjectids

Are you sure you want to delete the following Configuration Sysobjectids(s)?

SysObjectId	Product	Vendor	Device Type	OS Type	Model	Series
.1.3.6.1.4.1.43.1.16.4.3.21	3Com 4500 Series Switch	3com	Switch	COMWAREOS	Superstack-3-4526	4500

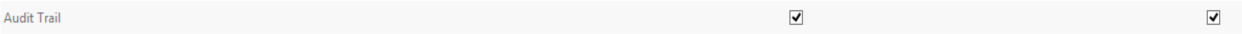
Click Yes to delete the SystemObjectID or click No to cancel the delete operation.

Note: If a new device must be adopted into SecuRA, SystemObjectID must be configured on this page.

25. Audit Trail

This is a Privilege based feature: The user will be able to access, view, add, edit, delete, execute & export, only if privileges have been given by the administrator. This will be defined under roles and privileges.

This menu is accessible only if the below privilege has been checked.



Audit Trail	☑	☑

From the left panel, click ☰ and select 'Audit Trail'.

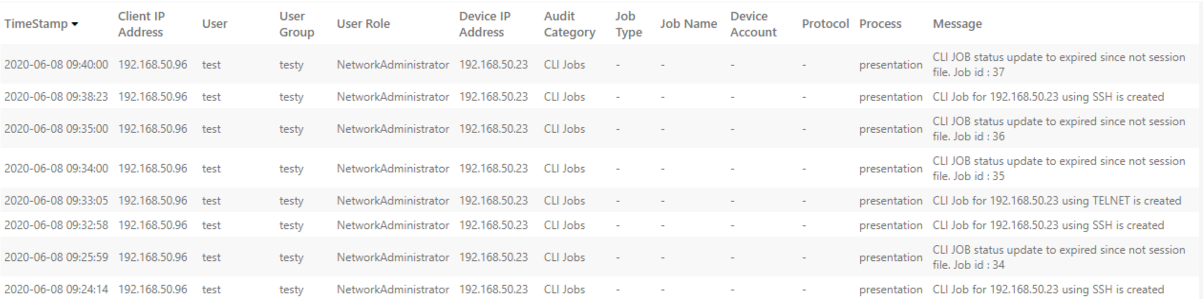
With multiple user tasks and access types in SecuRA, the vast array of actions involve numerous resources spans across hierarchies and privileges within the system.

As mandatory as it is to have a sophisticated security model, so is the need for an audit trail facility. SecuRA captures specifics of ever user's every activity across the system.

Infraon SecuRA implements the audit trail component of the system in order to perform the following audit checks:

- Automatically log all significant administrator or user actions.
- Allow the administrator to view the audit log file.

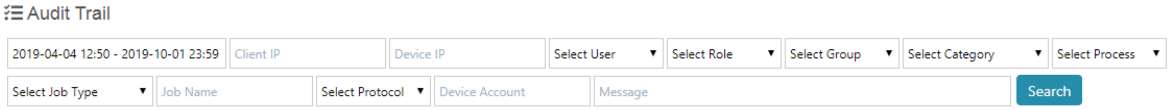
The user can view the Audit logs based on the filter criteria like Time Scale, User IP, User Name and Event Types etc.,



TimeStamp ▾	Client IP Address	User	User Group	User Role	Device IP Address	Audit Category	Job Type	Job Name	Device Account	Protocol	Process	Message
2020-06-08 09:40:00	192.168.50.96	test	testy	NetworkAdministrator	192.168.50.23	CLI Jobs	-	-	-	-	presentation	CLI JOB status update to expired since not session file. Job id : 37
2020-06-08 09:38:23	192.168.50.96	test	testy	NetworkAdministrator	192.168.50.23	CLI Jobs	-	-	-	-	presentation	CLI Job for 192.168.50.23 using SSH is created
2020-06-08 09:35:00	192.168.50.96	test	testy	NetworkAdministrator	192.168.50.23	CLI Jobs	-	-	-	-	presentation	CLI JOB status update to expired since not session file. Job id : 36
2020-06-08 09:34:00	192.168.50.96	test	testy	NetworkAdministrator	192.168.50.23	CLI Jobs	-	-	-	-	presentation	CLI JOB status update to expired since not session file. Job id : 35
2020-06-08 09:33:05	192.168.50.96	test	testy	NetworkAdministrator	192.168.50.23	CLI Jobs	-	-	-	-	presentation	CLI Job for 192.168.50.23 using TELNET is created
2020-06-08 09:32:58	192.168.50.96	test	testy	NetworkAdministrator	192.168.50.23	CLI Jobs	-	-	-	-	presentation	CLI Job for 192.168.50.23 using SSH is created
2020-06-08 09:25:59	192.168.50.96	test	testy	NetworkAdministrator	192.168.50.23	CLI Jobs	-	-	-	-	presentation	CLI JOB status update to expired since not session file. Job id : 34
2020-06-08 09:24:14	192.168.50.96	test	testy	NetworkAdministrator	192.168.50.23	CLI Jobs	-	-	-	-	presentation	CLI Job for 192.168.50.23 using SSH is created

25.1. Search

Click ▼ to open search options.



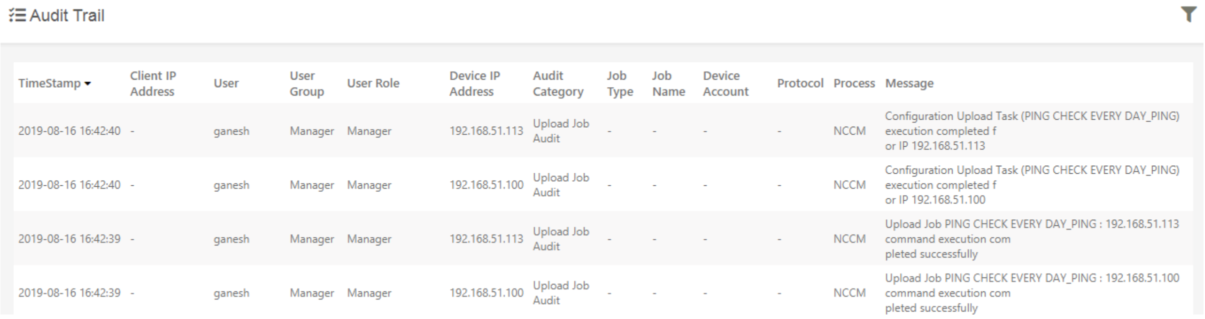
☰ Audit Trail

2019-04-04 12:50 - 2019-10-01 23:59

Input the desired data and click Search to search based on the applied filter.

26. Upload Audit

All upload audits are categorized further in this segment. From the left panel, click ☰ and select ‘Upload Audit’.



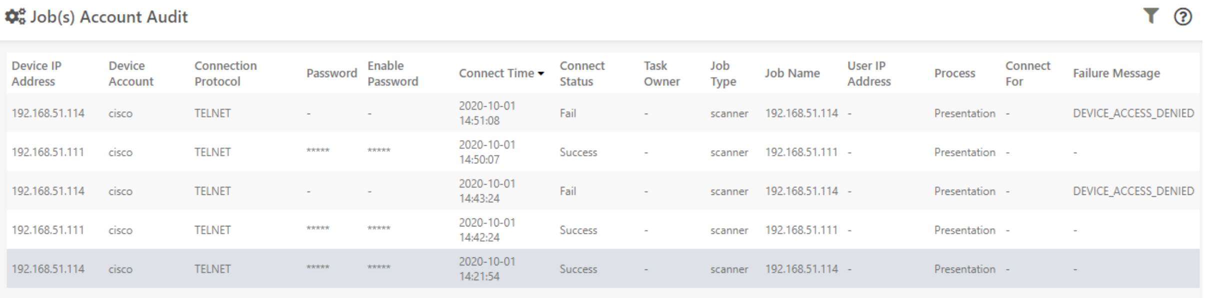
☰ Audit Trail

TimeStamp ▾	Client IP Address	User	User Group	User Role	Device IP Address	Audit Category	Job Type	Job Name	Device Account	Protocol	Process	Message
2019-08-16 16:42:40	-	ganesh	Manager	Manager	192.168.51.113	Upload Job Audit	-	-	-	-	NCCM	Configuration Upload Task (PING CHECK EVERY DAY_PING) execution completed f or IP 192.168.51.113
2019-08-16 16:42:40	-	ganesh	Manager	Manager	192.168.51.100	Upload Job Audit	-	-	-	-	NCCM	Configuration Upload Task (PING CHECK EVERY DAY_PING) execution completed f or IP 192.168.51.100
2019-08-16 16:42:39	-	ganesh	Manager	Manager	192.168.51.113	Upload Job Audit	-	-	-	-	NCCM	Upload Job PING CHECK EVERY DAY_PING : 192.168.51.113 command execution com pleted successfully
2019-08-16 16:42:39	-	ganesh	Manager	Manager	192.168.51.100	Upload Job Audit	-	-	-	-	NCCM	Upload Job PING CHECK EVERY DAY_PING : 192.168.51.100 command execution com pleted successfully

27. Job(s) Account Audit

Job(s) Account audit is basically User Account based audit information. From the left panel, click ☰ and select ‘Job(s) Account Audit’.

Audit information of actions performed through Download Jobs, Upload Jobs, Trigger & Network Diagnosis on the target device is captured and displayed on this page.



Job(s) Account Audit

Device IP Address	Device Account	Connection Protocol	Password	Enable Password	Connect Time	Connect Status	Task Owner	Job Type	Job Name	User IP Address	Process	Connect For	Failure Message
192.168.51.114	cisco	TELNET	-	-	2020-10-01 14:51:08	Fail	-	scanner	192.168.51.114	-	Presentation	-	DEVICE_ACCESS_DENIED
192.168.51.111	cisco	TELNET	*****	*****	2020-10-01 14:50:07	Success	-	scanner	192.168.51.111	-	Presentation	-	-
192.168.51.114	cisco	TELNET	-	-	2020-10-01 14:43:24	Fail	-	scanner	192.168.51.114	-	Presentation	-	DEVICE_ACCESS_DENIED
192.168.51.111	cisco	TELNET	*****	*****	2020-10-01 14:42:24	Success	-	scanner	192.168.51.111	-	Presentation	-	-
192.168.51.114	cisco	TELNET	*****	*****	2020-10-01 14:21:54	Success	-	scanner	192.168.51.114	-	Presentation	-	-

Job(s) account audit displays the below information.

- Device IP Address
- Device Account
- Connection Protocol
- Password
- Enable Password
- Connect Time
- Connect Status
- Task Owner
- Job Type
- Job Name
- User IP Address
- Process
- Connect for (reason given by the user)
- Failure Message

28. Notification Overview

Infraon SecuRA allows the user to subscribe for events, for which the user would receive notifications. When the defined type of event occurs, SecuRA notifies users through a notification method that the user has configured i.e., Email, SMS, SNMP trap, BatchNotifierAPI, XML notification etc.

There are multiple steps involved in configuring the notifiers, based on the type of notifier. Notifier method must be configured before adding notifier alerts.

Infraon SecuRA sends notifications on the occurrence of events within the network.

To enable notification alerts, the below configurations must be done.

An SMTP server.

A notification channel.

A business profile of the personnel who needs be notified.

Notification alerts are assigned to notification channels and business profiles. All business profiles linked to a notification alert receive notifications during specified time slots (as applicable).

Multiple notification channels can be used for the below type of events:

- Configuration upload fails.
- New devices are identified after a discovery is complete.
- Upload Job execution is unsuccessful.
- Latest Operating System has been released.
- Upload is created or modified.

Notification channels

The following notification channels are available for configuring notification alerts:

- SMS
- SNMP trap
- Email
- Syslog
- Batch File
- REST Approval API
- REST Incident API

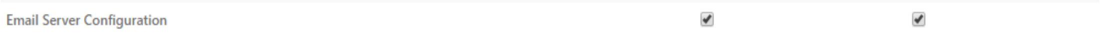
Rule to create Notifier

Notifier should be created using SecuRA configured Username for Upload job and CLI job requests, because approval and Requester notification will be sent by using this mechanism.
For example: If username is “NOCOperations”, a notifier with the same name must be created, which in this case is“NOCOperations”

29. Email Server Configuration

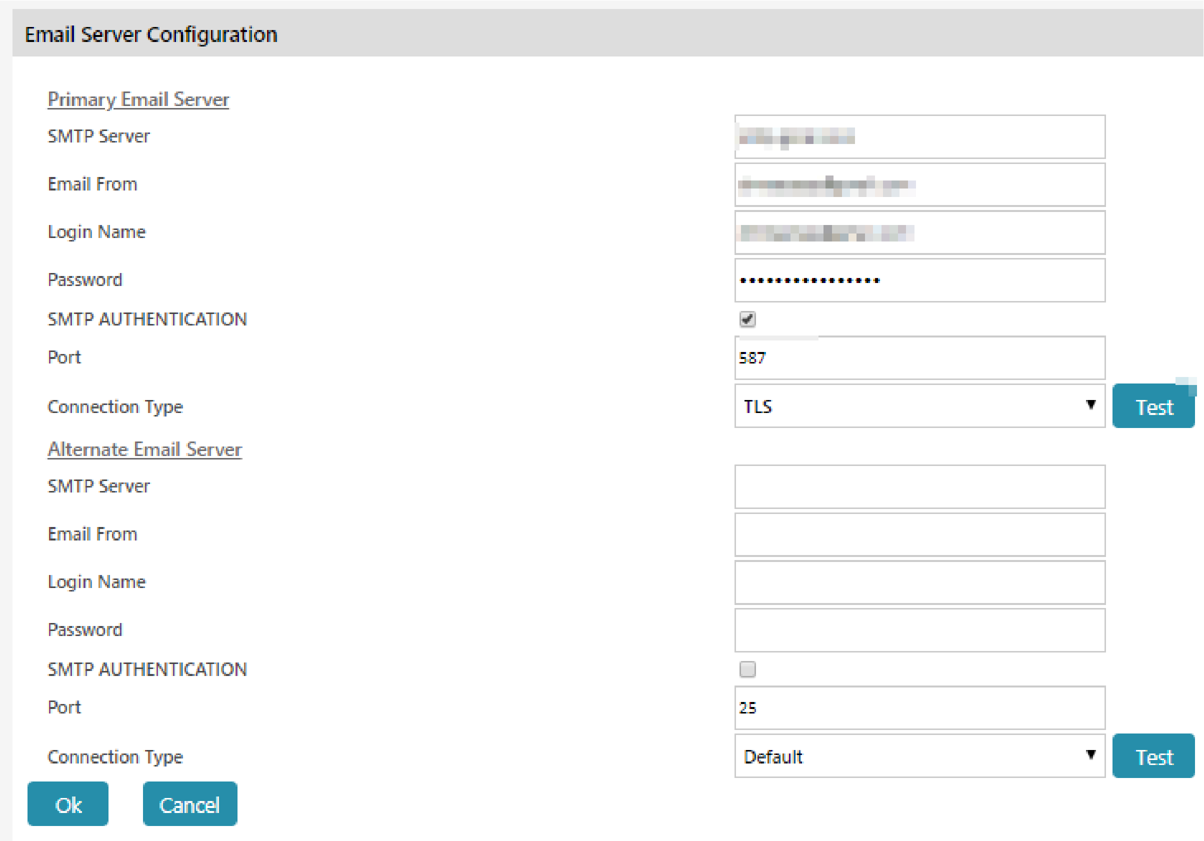
This is a Privilege based feature: The user will be able to access, view, add, edit, delete, execute & export, only if privileges have been given by the administrator. This will be defined under roles and privileges.

This menu is accessible only if the below privilege has been checked.



Email Server Configuration ☑ ☑

From the left panel, click ✉ and select 'Email Server Configuration'.



Email Server Configuration

Primary Email Server

SMTP Server	[redacted]
Email From	[redacted]
Login Name	[redacted]
Password	••••••••••••••••
SMTP AUTHENTICATION	☑
Port	587
Connection Type	TLS ▾ Test

Alternate Email Server

SMTP Server	
Email From	
Login Name	
Password	
SMTP AUTHENTICATION	☐
Port	25
Connection Type	Default ▾ Test

From the **Primary Email Server** section, in **SMTP Server**,

- Input the SMTP server name or the SMTP server IP address.
- Input the email address of the email notification sender.
- Input the User Name.
- Input the Password.
- For enhanced security, check the SMTP AUTHENTICATION from checkbox.
- In Port, Input the port number in textbox (default port is configured).

- Select the Connection type using the dropdown menu.

Click Test to check whether the configured Email server is working.

- Input relevant information in the Alternate Email Server section.

Click Ok to save the Email server configuration or click Cancel to abort the configuration.

30. Notifier Method

This is a Privilege based feature: The user will be able to access, view, add, edit, delete, execute & export, only if privileges have been given by the administrator. This will be defined under roles and privileges.

When a new 'User Account' is added in SecuRA, a Notifier is created automatically in the name of the corresponding user.

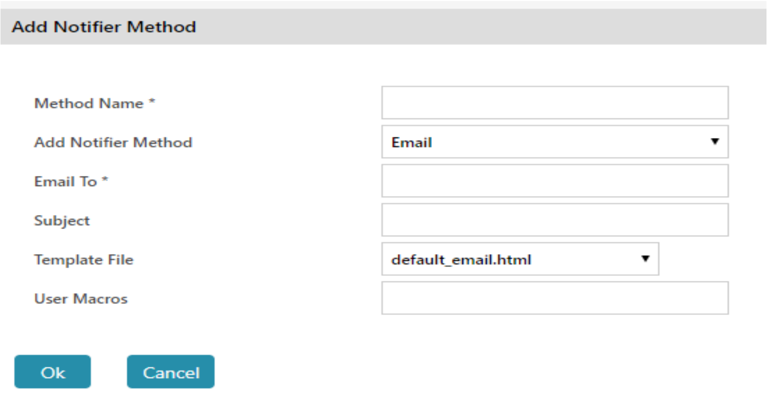
This menu is accessible only if the below privilege has been checked.

Notifier Methods	☑	☑	☑	☑

SecuRA allows the user to add, edit, or delete notifier methods. To view predefined notifier methods, from the left panel, click ✉ and select 'Methods'.

30.1. Add Email Notifier Method

Click + to redirect to the Add method window.



Add Notifier Method

Method Name *	
Add Notifier Method	Email ▾
Email To *	
Subject	
Template File	default_email.html ▾
User Macros	

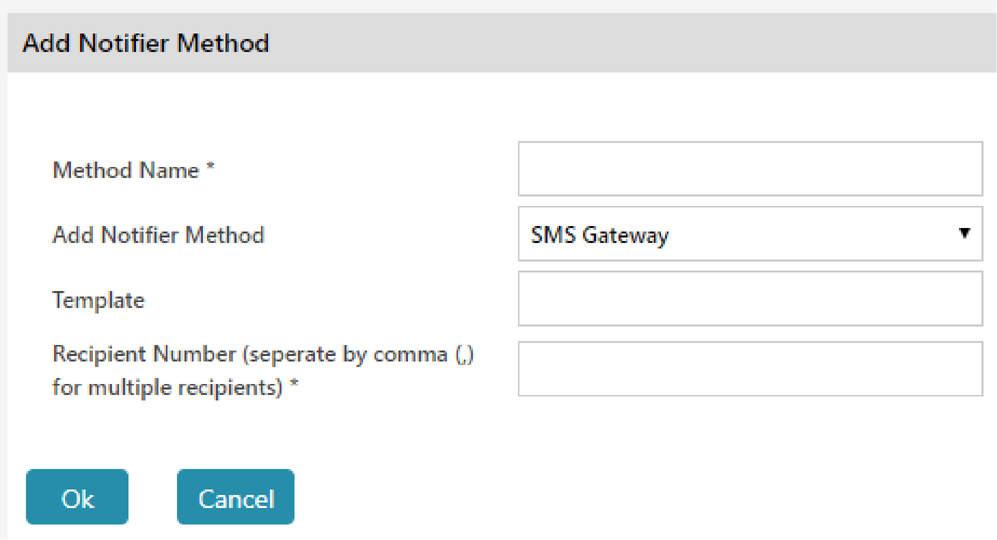
- Input the method name.

- Select method type using the dropdown menu.
- Input the Email To in the textbox.
- Input the subject in the textbox.
- Select the Template file using the dropdown menu.
- Input User Macros in the textbox.

Click Ok to save Email notifier method or click Cancel to abort the addition.

30.2. Add SMS Notifier Method

Click + to redirect to the Add method window.



Add Notifier Method

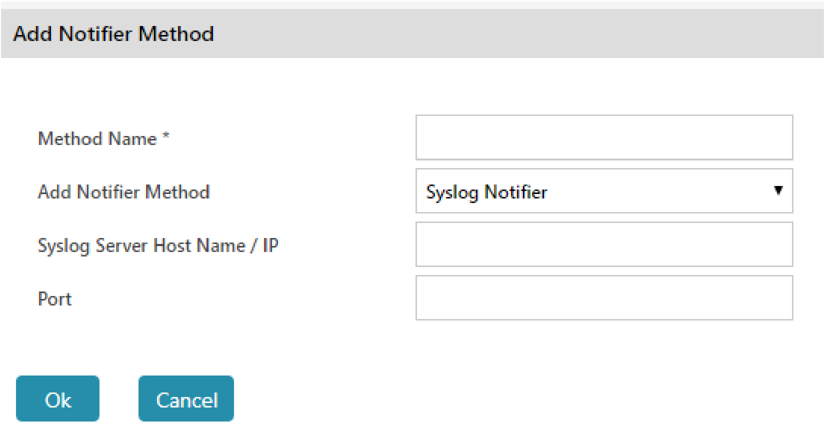
Method Name *	
Add Notifier Method	SMS Gateway ▾
Template	
Recipient Number (seperate by comma (,) for multiple recipients) *	

- Input method name.
- Select “SMS Gateway” using the dropdown menu.
- Input the Template file in the textbox.
- Input Recipient contact no. in the textbox (multiple numbers can be given using comma (,) as separator.

Click Ok to save SMS Notifier method or click Cancel to abort the addition.

30.3. Add Syslog Notifier Method

Click + to redirect to the Add method window.



Add Notifier Method

Method Name *

Add Notifier Method: Syslog Notifier ▾

Syslog Server Host Name / IP

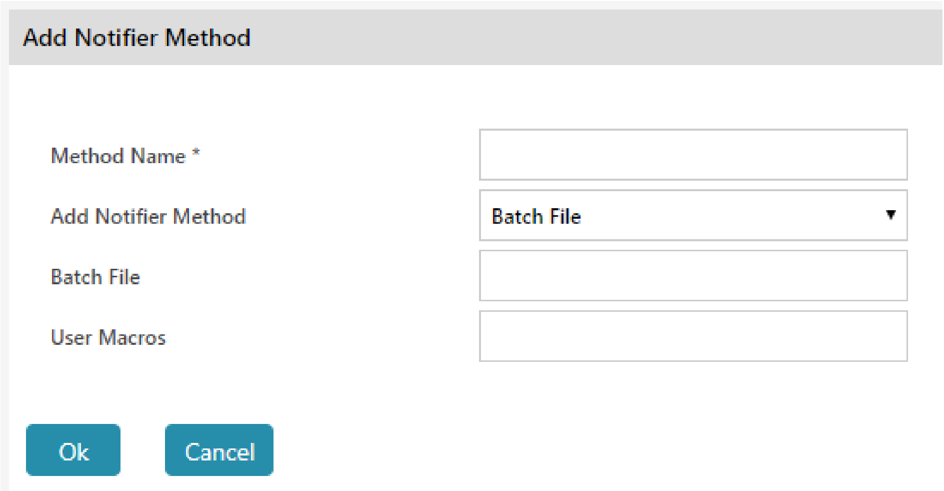
Port

- Input the method name.
- Select “Syslog Notifier” using the dropdown menu.
- Input the syslog server name in the textbox.
- Input the Port number in the textbox.

Click Ok to save the method or click Cancel to abort.

30.4. Add Batch File Method

Click + to redirect to the Add method window.



Add Notifier Method

Method Name *

Add Notifier Method: Batch File ▾

Batch File

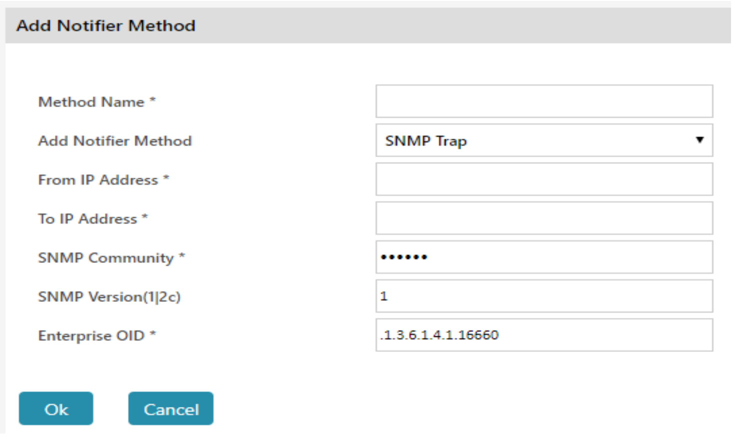
User Macros

- Input the method name.
- Select “Batch File” using the dropdown menu.
- Input the Batch File Location in the textbox.
- Input the User Macros in the textbox.

Click Ok to save the method or click Cancel to abort the addition.

30.5. Add SNMP Trap Method

Click + to redirect to the Add method window.


Add Notifier Method

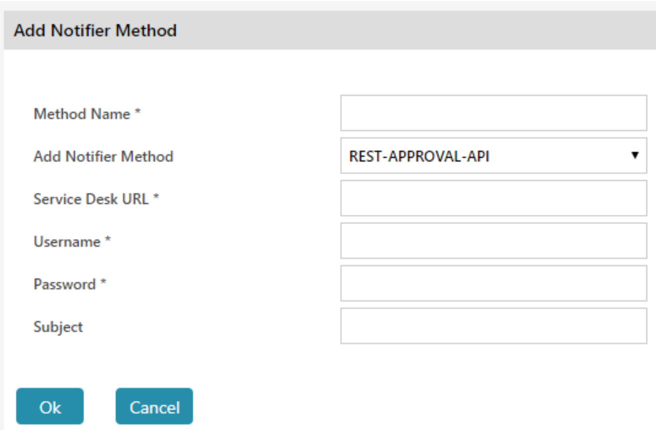
Method Name *	
Add Notifier Method	SNMP Trap ▾
From IP Address *	
To IP Address *	
SNMP Community *	••••••
SNMP Version(1|2c)	1
Enterprise OID *	.1.3.6.1.4.1.16660

- Input the method name
- Select “SNMP Trap” using the dropdown menu.
- Input ‘From IP address’ in the textbox (where the trap is received).
- Input ‘To IP address’ in the textbox (where the trap is sent).
- Input the SNMP Community in the textbox.
- Input the SNMP Version in the textbox.
- Input the Enterprise OID in the textbox.

Click Ok to save the method or click Cancel to abort.

30.6. Add REST Approval API Method

Click + to redirect to the Add method window.


Add Notifier Method

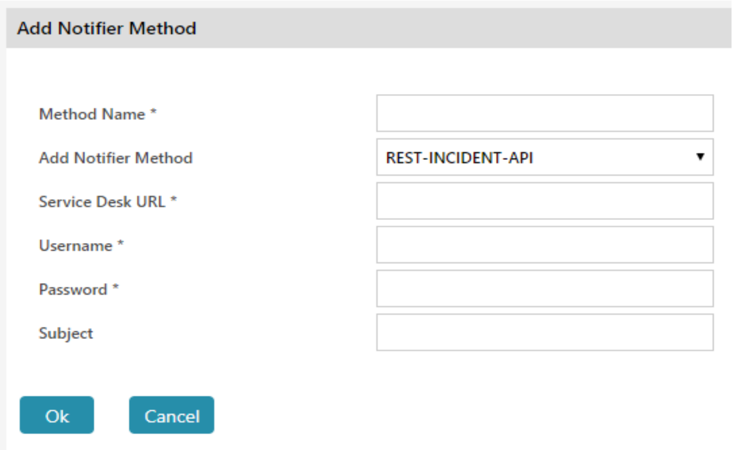
Method Name *	
Add Notifier Method	REST-APPROVAL-API ▾
Service Desk URL *	
Username *	
Password *	
Subject	

- Input the method name.
- Select “REST-APPROVAL-API” using the dropdown menu.
- Input the Service Desk URL in the textbox.
- Input the User Name in the textbox.
- Input the Password in the textbox.
- Input the Subject in the textbox.

Click Ok to save the method or click Cancel to abort.

30.7. Add REST Incident API Method

Click ⊕ to redirect to the Add method window.



Add Notifier Method

Method Name *

Add Notifier Method: REST-INCIDENT-API

Service Desk URL *

Username *

Password *

Subject

- Input the method name.
- Select “REST-INCIDENT-API” using the dropdown menu.
- Input the Service Desk URL in the textbox.
- Input the User Name in the textbox.
- Input the Password in the textbox.
- Input the Subject in the textbox.

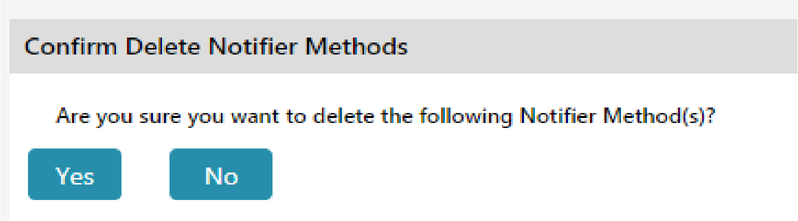
Click Ok to save the method or click Cancel to abort.

30.8. Edit Notifier Method

Select any of the existing method and click ⊖ to edit. Make necessary changes and save.

30.9. Delete Notifier Method

Select the Method and click ✖ to redirect to the Delete confirmation window.

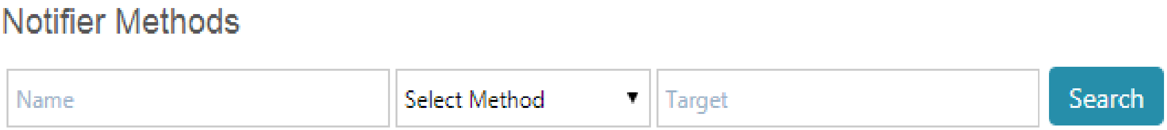


Confirm Delete Notifier Methods

Are you sure you want to delete the following Notifier Method(s)?

Click Yes to delete the Notifier Method or click No to abort.

30.10. Search



- Input the Name in textbox.
- Select method using the dropdown menu.
- Input the Target in the textbox.

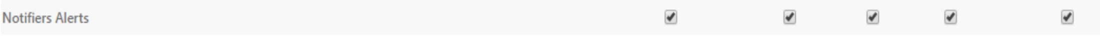
Click Search to perform the search based on the applied filter.

31. Notifier Alerts

SecuRA allows you to add new Notifier Alerts using this option. Alert can be generated for different severity levels such as Informational, Important Information, Warning, Serious Warning, Error, or Serious Error. When the user subscribes to event of a certain severity level, user gets notified of events that are equal to or above that severity level.

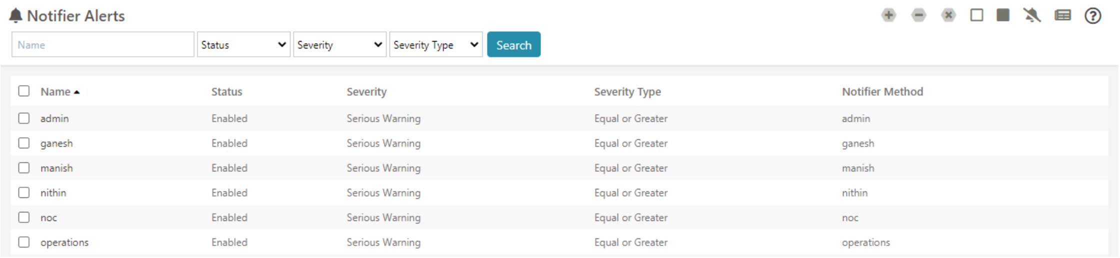
This is a Privilege based feature: The user will be able to access, view, add, edit, delete, execute & export, only if privileges have been given by the administrator. This will be defined under roles and privileges.

This menu is accessible only if the below privilege has been checked.



Notifiers Alerts	☑	☑	☑	☑	☑

From the left panel, click ✉ and select ‘Alerts’.



Notifier Alerts

Name | Status | Severity | Severity Type | Search

□	Name ▲	Status	Severity	Severity Type	Notifier Method
□	admin	Enabled	Serious Warning	Equal or Greater	admin
□	ganesh	Enabled	Serious Warning	Equal or Greater	ganesh
□	manish	Enabled	Serious Warning	Equal or Greater	manish
□	nithin	Enabled	Serious Warning	Equal or Greater	nithin
□	noc	Enabled	Serious Warning	Equal or Greater	noc
□	operations	Enabled	Serious Warning	Equal or Greater	operations

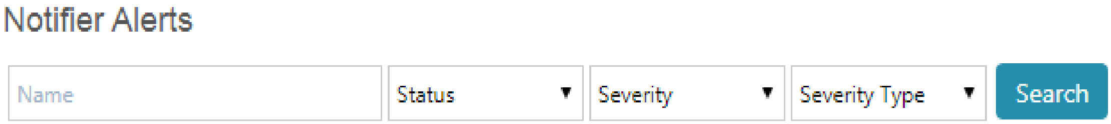
31.1. Quick Action Icons

The below quick action icons are placed at the top right corner of the page.

⊕ ⊖ ⊗ □ ■ 🔕 ▤ ?

Icons	Label	Actions
⊕	Add	Click to add a 'Notifier Alert'
⊖	Edit	Click to edit Notifier Alert
⊗	Delete	Click to delete Notifier Alert
□	Enable	Click to Enable Notifier Alert
■	Disable	Click to Disable Notifier Alert
🔕	NotifierMethods	Click to navigate to the Notifier Methods Page
▤	Monitor Messages	Click to navigate to Monitor Messages Page

31.2. Search



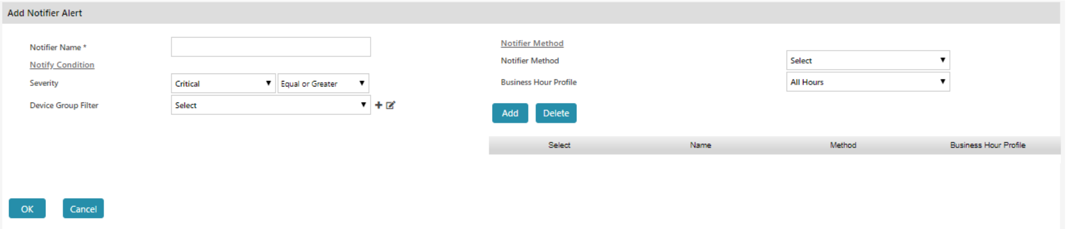
Notifier Alerts

- Input Name in textbox.
- Select status using the dropdown menu.
- Select the Severity using the dropdown menu.
- Select the Severity type using the dropdown menu.

Click Search to perform the search based on the applied filter.

31.3. Add Notifier Alert

Click ➕ to redirect to the Add Notifier Alert window.



Add Notifier Alert

Notifier Name *		
Notify Condition		
Severity	Critical ▼	Equal or Greater ▼
Device Group Filter	Select ▼	

Notifier Method

Notifier Method	Select ▼
Business Hour Profile	All Hours ▼

Add Delete

Select	Name	Method	Business Hour Profile

OK Cancel

- Input the Notifier name in textbox,
- In the Notifier Condition section, in Severity, select the severity level as Critical, Minor, or Major as applicable. For example, you can select the severity level as major and equal or Greater to indicate that the severity is major and critical.
- In Device Group Filter, select the specific group to apply the filter.
- In the Notifier Method section, in Notifier Method, associate the alert to the notifier method which was created.
- In Business Hour Profile, select the time slot for the notification to be sent.
- Click Add to associate the alert to the selected notification method.
- Click Delete to detach the method from the alert.

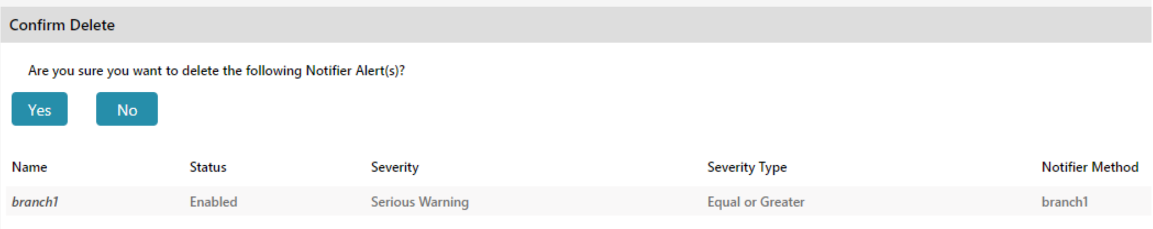
Click Ok to save the notifier alert or click Cancel to abort the changes.

31.4. Edit Notifier Alert

Select a Notifier Alert and click ➖. Make necessary changes and save the changes.

31.5. Delete Notifier Alert

Select the Alert and click ✖ to redirect to the Delete confirmation window.



Confirm Delete

Are you sure you want to delete the following Notifier Alert(s)?

Yes No

Name	Status	Severity	Severity Type	Notifier Method
branch1	Enabled	Serious Warning	Equal or Greater	branch1

Click Yes to delete the Alert or click No button to abort the operation.

31.6. Enable Notifier Alert

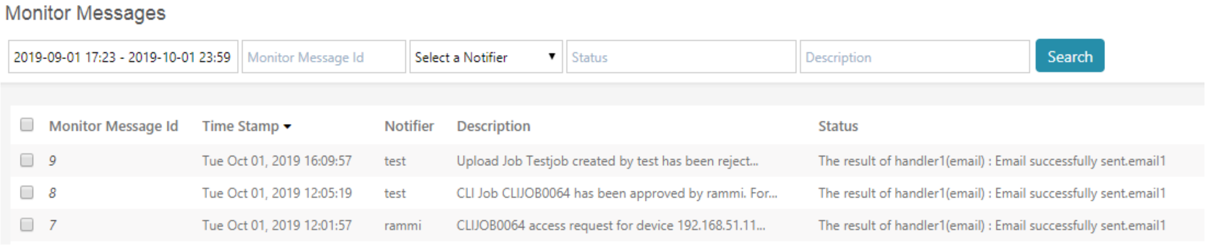
Select a profile and click □ to keep the notifier profile enabled, for further Notifications.

31.7. Disable Notifier Alert

Select profile and click ■ to disable the profile from further Notification.

32. Monitor Messages

Monitor Messages page displays all the notified messages. From the left panel, click ✉ and select ‘Monitor Messages’.



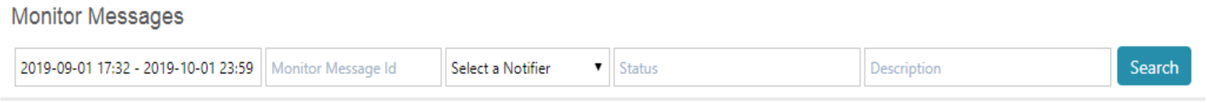
Monitor Messages

2019-09-01 17:23 - 2019-10-01 23:59 | Monitor Message Id | Select a Notifier ▾ | Status | Description | Search

□	Monitor Message Id	Time Stamp ▾	Notifier	Description	Status
□	9	Tue Oct 01, 2019 16:09:57	test	Upload Job Testjob created by test has been reject...	The result of handler1(email) : Email successfully sent.email1
□	8	Tue Oct 01, 2019 12:05:19	test	CLI Job CLIJOB0064 has been approved by rammi. For...	The result of handler1(email) : Email successfully sent.email1
□	7	Tue Oct 01, 2019 12:01:57	rammi	CLIJOB0064 access request for device 192.168.51.11...	The result of handler1(email) : Email successfully sent.email1

All Notifier alerts will be displayed here for tracking purpose.

32.1. Search



Monitor Messages

2019-09-01 17:32 - 2019-10-01 23:59 | Monitor Message Id | Select a Notifier ▾ | Status | Description | Search

- Select Time from the calendar options.
- Input Message ID in the textbox.
- Select notifier using the dropdown menu.
- Input Status using the dropdown menu.
- Input Description using the dropdown menu.

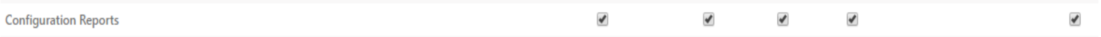
Click Search to perform the search based on the applied filter.

33. Reports

Report widgets are used to track and monitor the device audits and changes

This is a Privilege based feature: The user will be able to access, view, add, edit, delete, execute & export, only if privileges have been given by the administrator. This will be defined under roles and privileges.

This menu is accessible only if the below privilege has been checked.

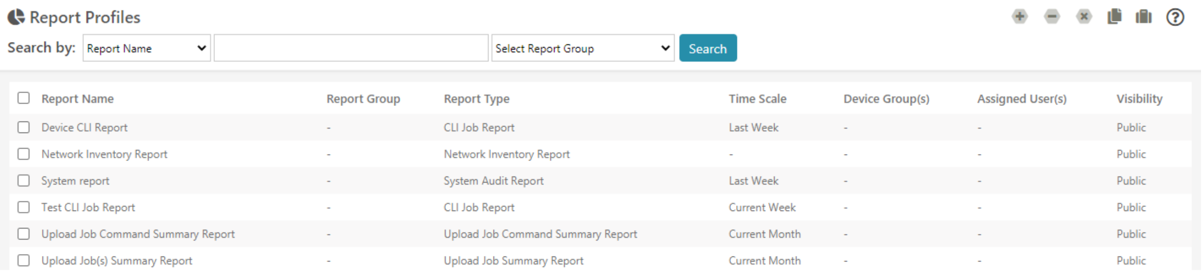


Configuration Reports ☑ ☑ ☑ ☑ ☑

The Report module allows the user to choose the kind of information the user needs and presents the complete details of the devices and its configuration in a user-friendly graph. With all relevant information plotted in a single graph, the user can easily access different statistics and isolate any potential bottlenecks in the infrastructure setup in the event of any performance situation.

A pre-defined list of 50+ report widgets is available to create reports containing crucial information about your network.

From the left panel, click and select 'Reports'.



Report Profiles

Search by: Report Name ▾ | | Select Report Group ▾ | Search

☐ Report Name	Report Group	Report Type	Time Scale	Device Group(s)	Assigned User(s)	Visibility
☐ Device CLI Report	-	CLI Job Report	Last Week	-	-	Public
☐ Network Inventory Report	-	Network Inventory Report	-	-	-	Public
☐ System report	-	System Audit Report	Last Week	-	-	Public
☐ Test CLI Job Report	-	CLI Job Report	Current Week	-	-	Public
☐ Upload Job Command Summary Report	-	Upload Job Command Summary Report	Current Month	-	-	Public
☐ Upload Job(s) Summary Report	-	Upload Job Summary Report	Current Month	-	-	Public

Access Control Restrictions

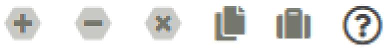
By defining access control restrictions on reports, you can control the users or user groups who have view access to the reports. All reports can be exported into a PDF format; however, data table reports are also available in Excel and CSV formats.

Filters

You can generate reports using the designated filters for each widget.

33.1. Quick Action Icons

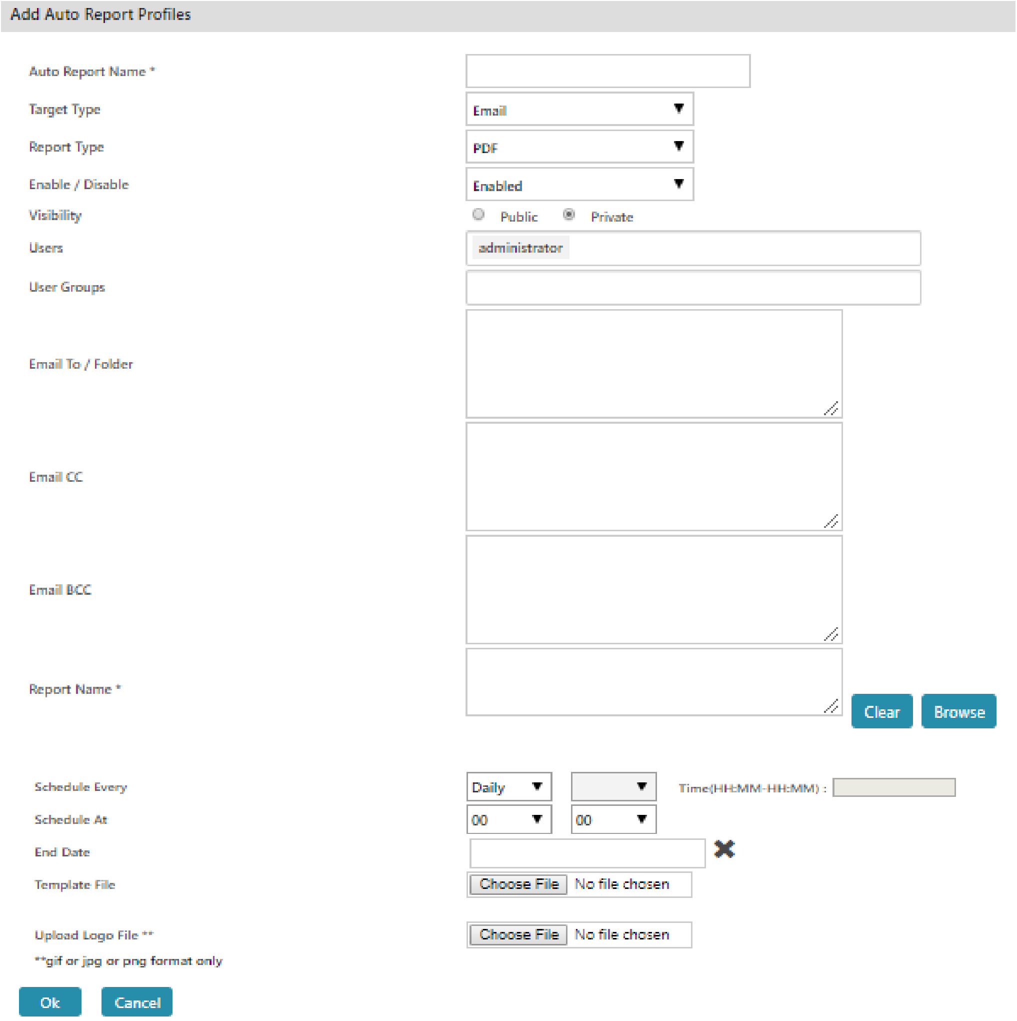
The below quick action icons are placed at the top right corner of the page.



Icons	Label	Actions
⊕	Add	Click to add 'Report Profile'
⊖	Edit	Click to edit a Report Profile
⊗	Delete	Click to delete a Report Profile
🗐	Copy	Click to copy a Report Profile
💼	Auto Report	Click to navigate to Auto Report Profile Page

33.2. Add Report Profile

To add a report, click ⊕ .



Add Auto Report Profiles

Auto Report Name *	
Target Type	Email ▼
Report Type	PDF ▼
Enable / Disable	Enabled ▼
Visibility	○ Public ● Private
Users	administrator
User Groups	
Email To / Folder	
Email CC	
Email BCC	
Report Name *	Clear Browse
Schedule Every	Daily ▼ ▼ Time(HH:MM-HH:MM) :
Schedule At	00 ▼ 00 ▼
End Date	✖
Template File	Choose File No file chosen
Upload Logo File **	Choose File No file chosen

**gif or jpg or png format only

Ok Cancel

- In **Report Type**, select the appropriate report widget.

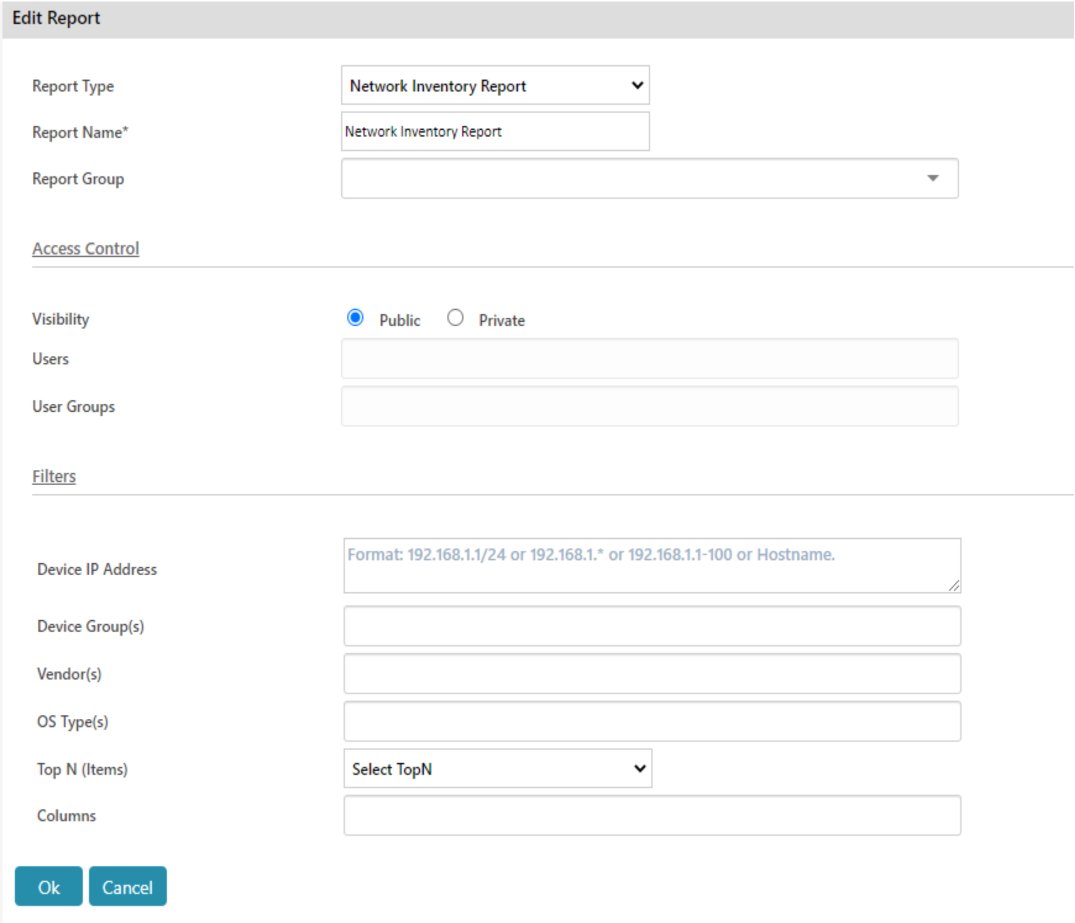
- Enter a **Report Name.**
- In the **Access Control** section, select **Public** to share the report with all users or select **Private** to share the report with specific users.

  Note: *If you select **Public**, skip to step 8.*
- Enter or select the user names with whom the reports are to be shared.
- Enter or select the user groups with whom the reports are to be shared.
- In the **Filters** section, enter or select the relevant filter parameters.

Click Ok

33.3. Edit Report Profile

To edit a report, select the report and click ⊖.



Edit Report

Report Type	Network Inventory Report
Report Name*	Network Inventory Report
Report Group	

Access Control

Visibility	● Public ○ Private
Users	
User Groups	

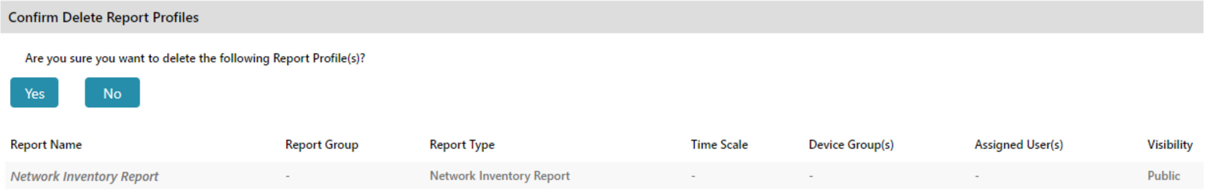
Filters

Device IP Address	Format: 192.168.1.1/24 or 192.168.1.* or 192.168.1.1-100 or Hostname.
Device Group(s)	
Vendor(s)	
OS Type(s)	
Top N (Items)	Select TopN
Columns	

Make changes as necessary and click Ok to save.

33.4. Delete Report Profile

To delete a report, select the report and click ✖. A confirmation box appears.



Confirm Delete Report Profiles

Are you sure you want to delete the following Report Profile(s)?

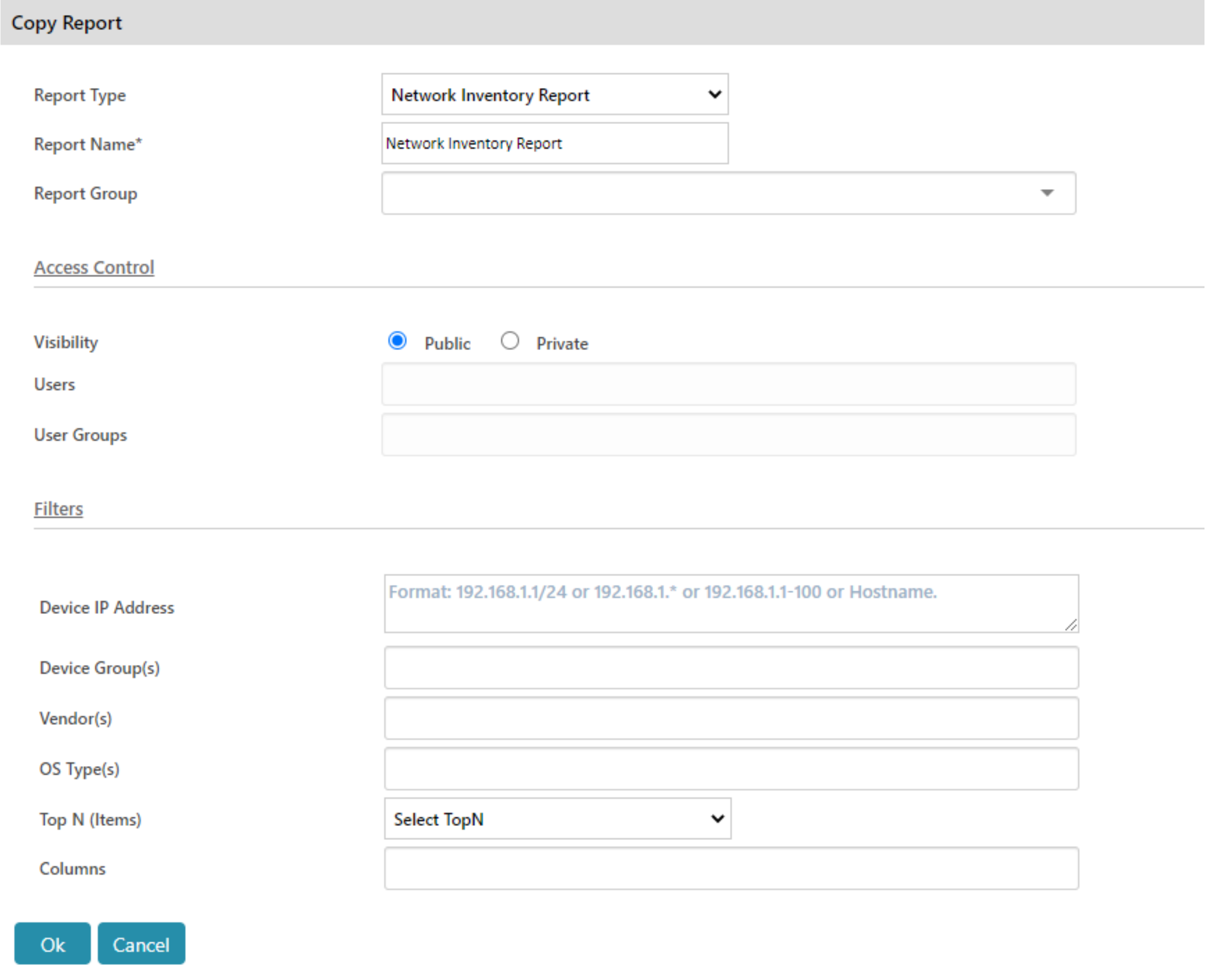
Yes No

Report Name	Report Group	Report Type	Time Scale	Device Group(s)	Assigned User(s)	Visibility
Network Inventory Report	-	Network Inventory Report	-	-	-	Public

Click Yes to delete the Report Profile or click No to abort.

33.5. Copy Report Profile

To copy a report, select the report and click 📋.



Copy Report

Report Type	Network Inventory Report
Report Name*	Network Inventory Report
Report Group	

Access Control

Visibility	● Public ○ Private
Users	
User Groups	

Filters

Device IP Address	Format: 192.168.1.1/24 or 192.168.1.* or 192.168.1.1-100 or Hostname.
Device Group(s)	
Vendor(s)	
OS Type(s)	
Top N (Items)	Select TopN
Columns	

Make changes as necessary and click Ok

33.6. Filter Report Data

Click on the report name to filter. The selected report opens.

To filter a report, click ▼. The filter fields are displayed below the report name.

- Enter the filter criterion. For example, to filter the **Detailed Inventory Report** data to view results for OS devices using IOS, enter or select IOS.
- Click Search. The search result appears.

33.7. Report Widgets

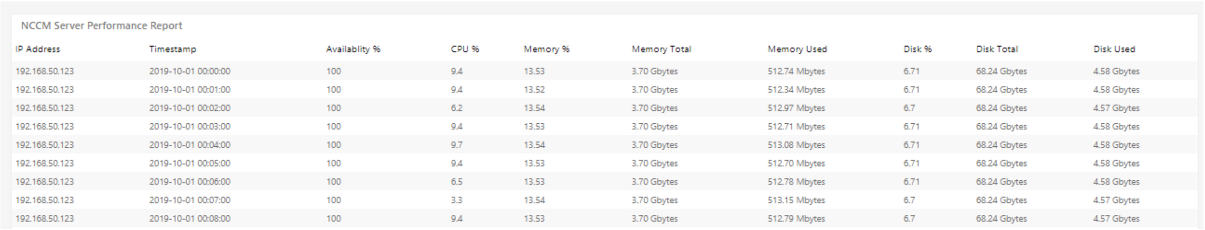
This section summarizes the list of report widgets and their corresponding parameters.

CLI Job Report

Detailed report of CLI requests with its status along with brief session details.

SecuRA Server Performance Report

Gives SecuRA installed server's status (self-monitoring) and performance.

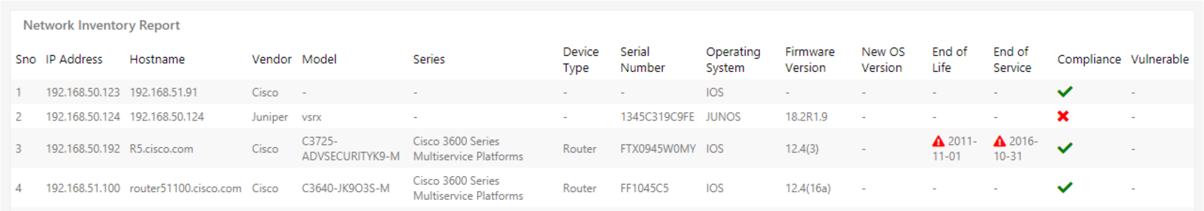


NCCM Server Performance Report

IP Address	Timestamp	Availablity %	CPU %	Memory %	Memory Total	Memory Used	Disk %	Disk Total	Disk Used
192.168.50.123	2019-10-01 00:00:00	100	9.4	13.53	3.70 Gbytes	512.74 Mbytes	6.71	68.24 Gbytes	4.58 Gbytes
192.168.50.123	2019-10-01 00:01:00	100	9.4	13.52	3.70 Gbytes	512.34 Mbytes	6.71	68.24 Gbytes	4.58 Gbytes
192.168.50.123	2019-10-01 00:02:00	100	6.2	13.54	3.70 Gbytes	512.97 Mbytes	6.7	68.24 Gbytes	4.57 Gbytes
192.168.50.123	2019-10-01 00:03:00	100	9.4	13.53	3.70 Gbytes	512.71 Mbytes	6.71	68.24 Gbytes	4.58 Gbytes
192.168.50.123	2019-10-01 00:04:00	100	9.7	13.54	3.70 Gbytes	513.08 Mbytes	6.71	68.24 Gbytes	4.58 Gbytes
192.168.50.123	2019-10-01 00:05:00	100	9.4	13.53	3.70 Gbytes	512.70 Mbytes	6.71	68.24 Gbytes	4.58 Gbytes
192.168.50.123	2019-10-01 00:06:00	100	6.5	13.53	3.70 Gbytes	512.78 Mbytes	6.71	68.24 Gbytes	4.58 Gbytes
192.168.50.123	2019-10-01 00:07:00	100	3.3	13.54	3.70 Gbytes	513.15 Mbytes	6.7	68.24 Gbytes	4.57 Gbytes
192.168.50.123	2019-10-01 00:08:00	100	9.4	13.53	3.70 Gbytes	512.79 Mbytes	6.7	68.24 Gbytes	4.57 Gbytes

Network Inventory Report

Summarizes EOS and EOL detail for every device.

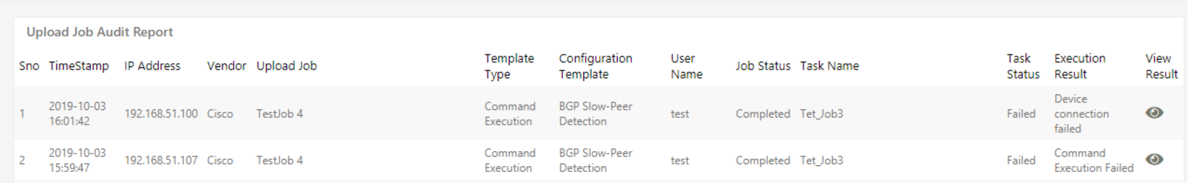


Network Inventory Report

Sno	IP Address	Hostname	Vendor	Model	Series	Device Type	Serial Number	Operating System	Firmware Version	New OS Version	End of Life	End of Service	Compliance	Vulnerable
1	192.168.50.123	192.168.51.91	Cisco	-	-	-	-	IOS	-	-	-	-	✓	-
2	192.168.50.124	192.168.50.124	Juniper	vsrx	-	-	1345C319C9FE	JUNOS	18.2R1.9	-	-	-	✗	-
3	192.168.50.192	R5.cisco.com	Cisco	C3725-ADVSECURITYK9-M	Cisco 3600 Series Multiservice Platforms	Router	FTX0945W0MY	IOS	12.4(3)	-	⚠ 2011-11-01	⚠ 2016-10-31	✓	-
4	192.168.51.100	router51100.cisco.com	Cisco	C3640-JK9O3S-M	Cisco 3600 Series Multiservice Platforms	Router	FF1045C5	IOS	12.4(16a)	-	-	-	✓	-

Upload Job Audit Report

Displays audit details of the upload jobs.

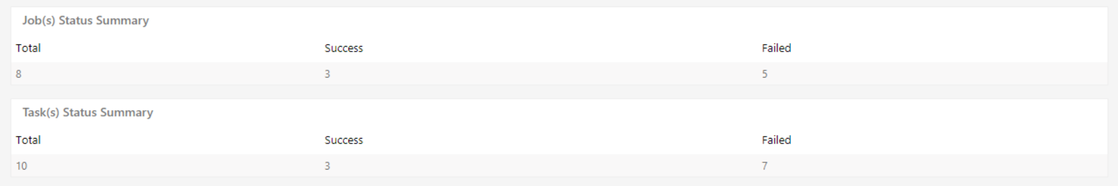


Upload Job Audit Report

Sno	TimeStamp	IP Address	Vendor	Upload Job	Template Type	Configuration Template	User Name	Job Status	Task Name	Task Status	Execution Result	View Result
1	2019-10-03 16:01:42	192.168.51.100	Cisco	TestJob 4	Command Execution	BGP Slow-Peer Detection	test	Completed	Tet_Job3	Failed	Device connection failed	👁
2	2019-10-03 15:59:47	192.168.51.107	Cisco	TestJob 4	Command Execution	BGP Slow-Peer Detection	test	Completed	Tet_Job3	Failed	Command Execution Failed	👁

Upload Job(s) Summary Report

Summarizes all aspects of upload jobs for a specific period.



Job(s) Status Summary

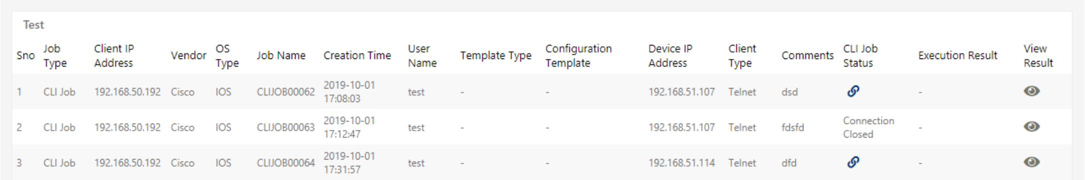
Total	Success	Failed
8	3	5

Task(s) Status Summary

Total	Success	Failed
10	3	7

User Activity Report

Summarizes activities of users for a specific period.



Test

Sno	Job Type	Client IP Address	Vendor	OS Type	Job Name	Creation Time	User Name	Template Type	Configuration Template	Device IP Address	Client Type	Comments	CLI Job Status	Execution Result	View Result
1	CLI Job	192.168.50.192	Cisco	IOS	CLIJOB00062	2019-10-01 17:08:03	test	-	-	192.168.51.107	Telnet	dsd	🔗	-	👁
2	CLI Job	192.168.50.192	Cisco	IOS	CLIJOB00063	2019-10-01 17:12:47	test	-	-	192.168.51.107	Telnet	fdsfd	Connection Closed	-	👁
3	CLI Job	192.168.50.192	Cisco	IOS	CLIJOB00064	2019-10-01 17:31:57	test	-	-	192.168.51.114	Telnet	dfd	🔗	-	👁

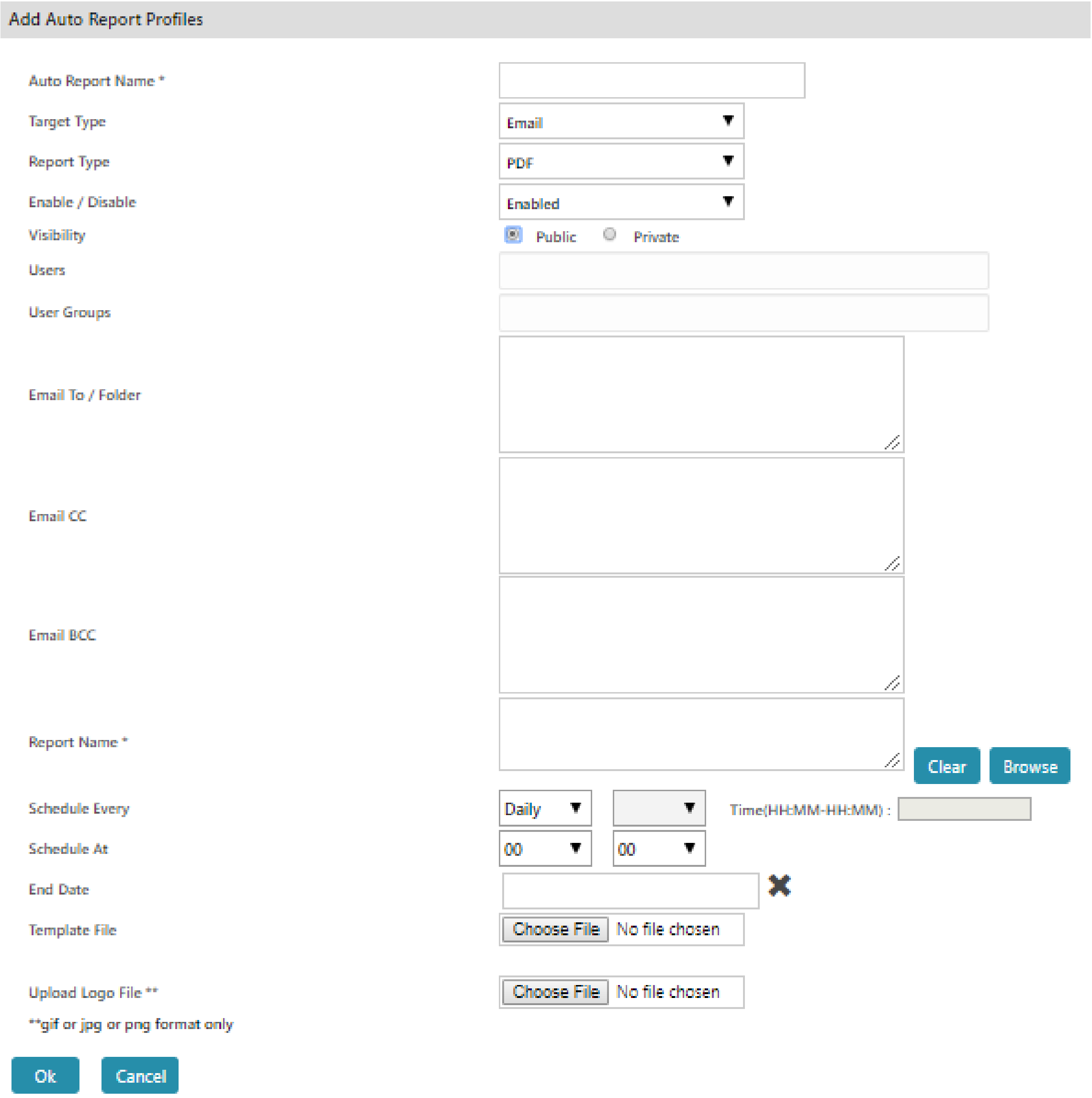
34. Schedule Report

The user can Schedule reports to run automatically on a daily, weekly, or monthly basis. Auto reports can be emailed to specific users or user groups or saved at a specified server location. Schedule Reports are also refererred to as Auto Reports

Note: *The Reporting feature is available based on your account privileges. Contact your administrator to enable/disable this feature.*

34.1. Add Auto Report Schedule

To add a report, click ⊕ . The **Add Auto Report Profiles** page appears.



Add Auto Report Profiles

Auto Report Name *	
Target Type	Email ▼
Report Type	PDF ▼
Enable / Disable	Enabled ▼
Visibility	● Public ○ Private
Users	
User Groups	
Email To / Folder	
Email CC	
Email BCC	
Report Name *	Clear Browse
Schedule Every	Daily ▼ ▼ Time(HH:MM-HH:MM) :
Schedule At	00 ▼ 00 ▼
End Date	✖
Template File	Choose File No file chosen
Upload Logo File **	Choose File No file chosen

**gif or jpg or png format only

- Provide a name for the Auto Report.
- Select Target Type using the dropdown menu.
- Select a Report Type using the dropdown menu.
- Select 'Enable' to enable the auto report.
- Select Visibility (Public/Private). If Private, select the user(s).

- Input the email ID, to mail the report. Or enter the folder location where the report must be saved.
- In 'Email CC' field, input the additional email ID's to send a copy.
- In 'Email BCC' field, input the email ID's to send blind copies of the email.
- Select the Report Name using Browse option.
- In 'Schedule Every' field, select the report delivery details.
- In Schedule At, select a start day.
- For the End Date, use the calendar view to select an end date.
- Select an email template and a Logo File (for personalization)

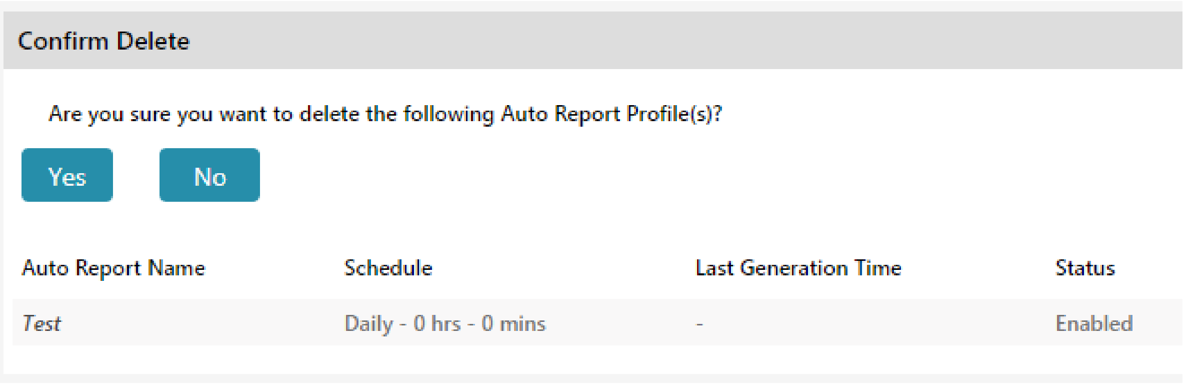
Click Save to schedule the offline report or click Cancel to abort the operation.

34.2. Edit Auto Report Schedule

Select an auto report and click ⊖ to redirect to the edit schedule Report window. Make changes as necessary and save the changes.

34.3. Delete Auto Report Schedule

Select a Report and click ⊗ to redirect to the Delete confirmation window.



Confirm Delete

Are you sure you want to delete the following Auto Report Profile(s)?

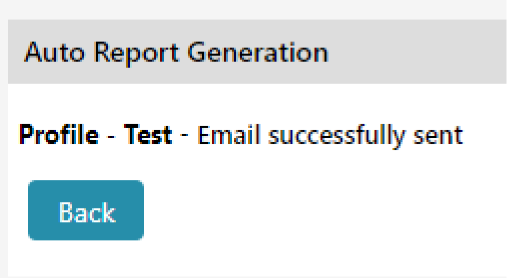
Yes No

Auto Report Name	Schedule	Last Generation Time	Status
Test	Daily - 0 hrs - 0 mins	-	Enabled

Click Yes to delete the schedule or click No to cancel the delete operation.

34.4. Send Immediately

Select Offline report(s) and click ➤ to send the scheduled report immediately.



Auto Report Generation

Profile - **Test** - Email successfully sent

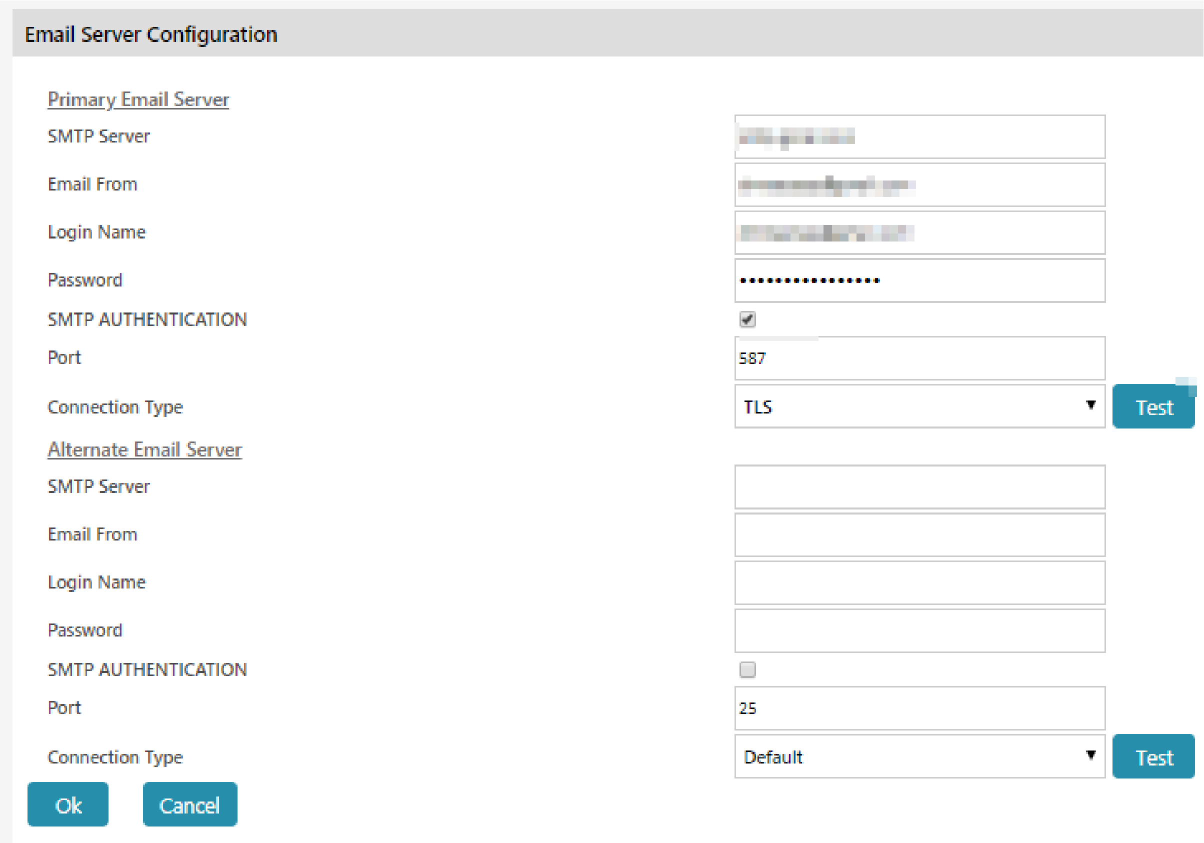
34.5. Email Server Configuration

This is a Privilege based feature: The user will be able to access, view, add, edit, delete, execute & export, only if privileges have been given by the administrator. This will be defined under roles and privileges.

This menu is accessible only if the below privilege has been checked.

Email Server Configuration	☑	☑

From the left panel, click and select ‘Email Server Configuration’.



Email Server Configuration

Primary Email Server

SMTP Server	[redacted]
Email From	[redacted]
Login Name	[redacted]
Password	••••••••••••••••
SMTP AUTHENTICATION	☑
Port	587
Connection Type	TLS ▾

Alternate Email Server

SMTP Server	
Email From	
Login Name	
Password	
SMTP AUTHENTICATION	□
Port	25
Connection Type	Default ▾

From the **Primary Email Server** section, in **SMTP Server**,

- Input the SMTP server name or the SMTP server IP address.

- Input the email address of the email notification sender.
- Input the User Name.
- Input the Password.
- For enhanced security, check the SMTP AUTHENTICATION from checkbox.
- In Port, Input the port number in textbox (default port is configured).
- Select the Connection type using the dropdown menu.

Click Test to check whether the configured Email server is working.

- Input relevant information in the Alternate Email Server section.

Click Ok to save the Email server configuration or click Cancel to abort the configuration.

35. Restart Application

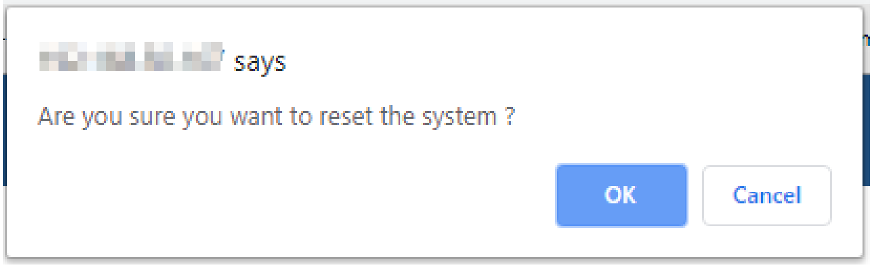
This is a Privilege based feature: The user will be able to access, view, add, edit, delete, execute & export, only if privileges have been given by the administrator. This will be defined under roles and privileges.

This menu is accessible only if the below privilege has been checked.

☑ System Administration

From the "Manage" menu (from the top panel) ⚙ , click "Restart Application"

Clicking on Restart application menu will directly restart the application with confirmation window.



[redacted] says

Are you sure you want to reset the system ?

Click OK to confirm the application restart.

- ○ Application will be restarted by using this option (but it is highly recommended to **NOT** USE this option)

Click Cancel to cancel the operation.

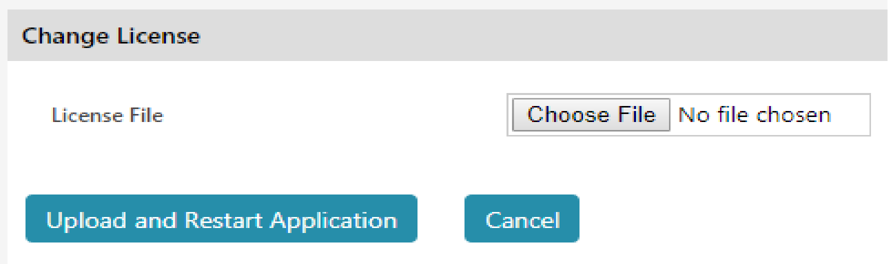
36. License Upgrade

This is a Privilege based feature: The user will be able to access, view, add, edit, delete, execute & export, only if privileges have been given by the administrator. This will be defined under roles and privileges.

This menu is accessible only if the below privilege has been checked.

☑ System Administration

From the "Manage" menu (from the top panel) ⚙ click "License Upgrade".



- Select the license file (*.txt or *.dat).
- Click Upload and Restart Application
- Infraon SecuRA application restarts when the license file is uploaded.
- Click Cancel to abort the operation.

37. Process Config

This is a Privilege based feature: The user will be able to access, view, add, edit, delete, execute & export, only if privileges have been given by the administrator. This will be defined under roles and privileges.

This menu is accessible only if the below privilege has been checked.

☑ System Administration

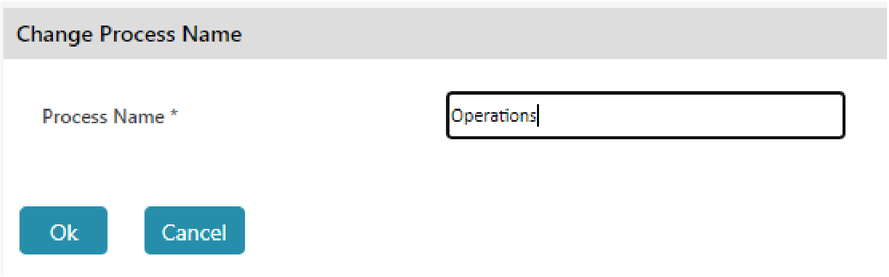
From the 'Manage' menu (from the top panel) ⚙ click "Process Config".

This menu lets the admin configure the process i.e. view and edit process related configurations.

37.1. Change Name

Click on Change Name to open the change process name window.

SecuRA allows user to change the name of the process, which is currently active on the system.



Change Process Name

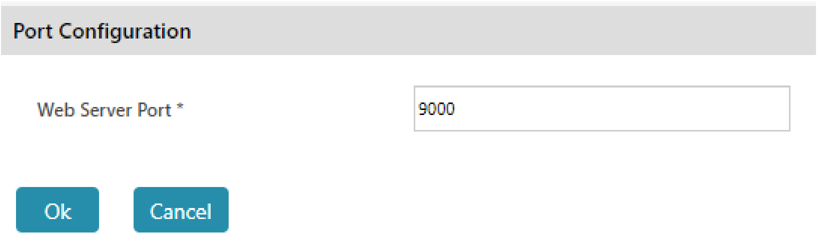
Process Name * Operations

- Input the new Process name in Process Name textbox.

Click Ok to save the new Process Name or click Cancel to abort the operation.

37.2. Port Configuration:

Click Port configuration to open the Port configuration window. The Port configuration details of SecuRA can be changed, using this option.



Port Configuration

Web Server Port * 9000

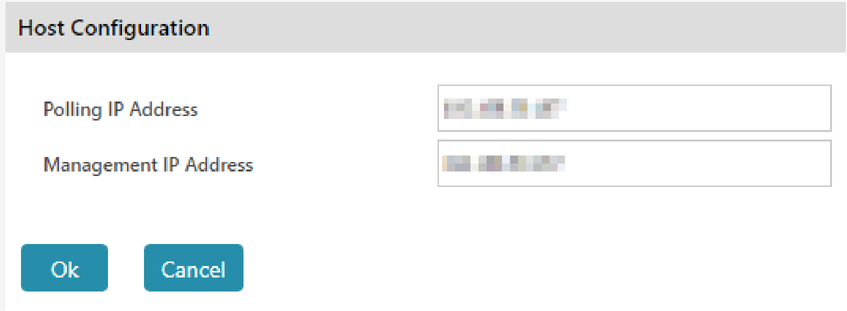
- Input the new Port in port configuration ‘Web Server Port’ textbox.

Click Ok to save the new port or click Cancel to abort the operation.

37.3. Host Configuration

Click on Port configuration will open the Port configuration window.

The Host Configuration details of SecuRA can be changed using this option.



Host Configuration

Polling IP Address	[redacted]
Management IP Address	[redacted]

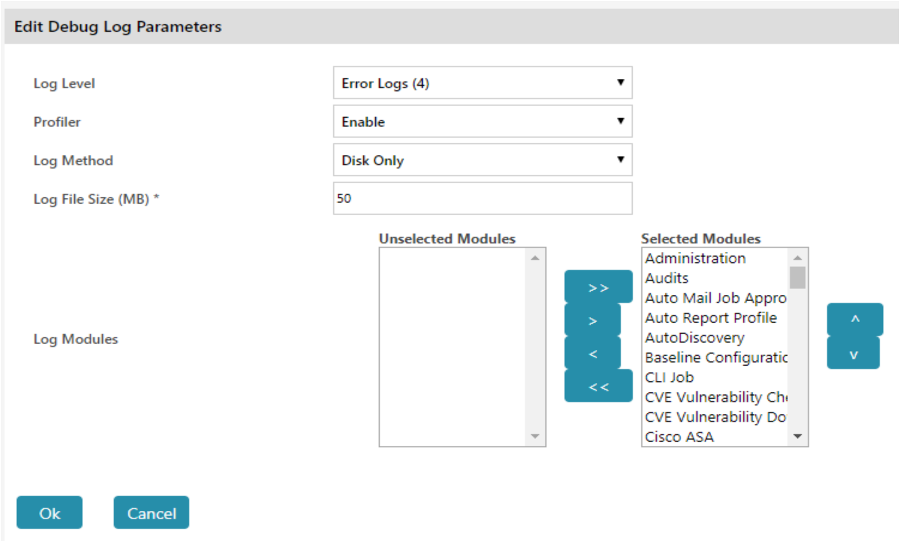
- Input the new polling address in the polling IP Address textbox
- Input the Management IP address in the Management IP Address textbox

Click Ok to save the new Host or click Cancel to abort the operation.

37.4. Debug Settings

This option is used to set the parameters for debugging the application, if encountered with any errors at run time.

Click on Debug settings to open the Debug settings window.



Edit Debug Log Parameters

Log Level	Error Logs (4)
Profiler	Enable
Log Method	Disk Only
Log File Size (MB) *	50

Log Modules

Unselected Modules

Selected Modules
Administration
Audits
Auto Mail Job Appro
Auto Report Profile
AutoDiscovery
Baseline Configuratic
CLI Job
CVE Vulnerability Ch
CVE Vulnerability Do
Cisco ASA

- Select the Log level using the dropdown menu.
- Select Profiler using the dropdown menu.
- Select Log method using the dropdown menu.
- Input the Log file size (MB) in the textbox.
- Move the Log Module(s) from “Unselected modules” list box to Selected Listbox.

Click Ok to save the changes made to debug settings or click Cancel to abort the operation.

Note: *If the system where SecuRA is deployed has more than one IP address, one IP address can be used for Polling and the other for Management. However, if only one IP address is available in the SecuRA, then the same can be used for Polling as well as Management.*

38. Database

This is a Privilege based feature: The user will be able to access, view, add, edit, delete, execute & export, only if privileges have been given by the administrator. This will be defined under roles and privileges.

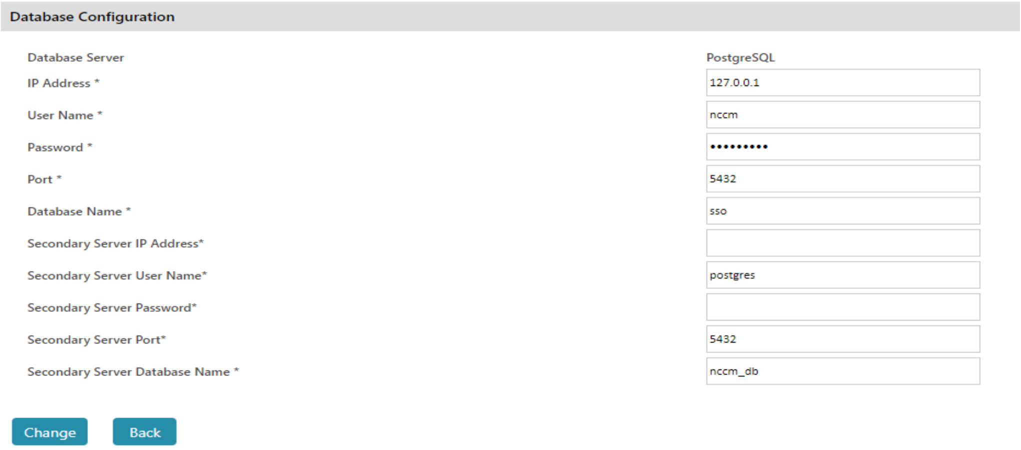
This menu is accessible only if the below privilege has been checked.

☑ System Administration

From ‘Manage’ menu (from the top panel) ⚙ click “Database”.

38.1. Database Configuration

Database configuration window will be displayed.



Database Configuration

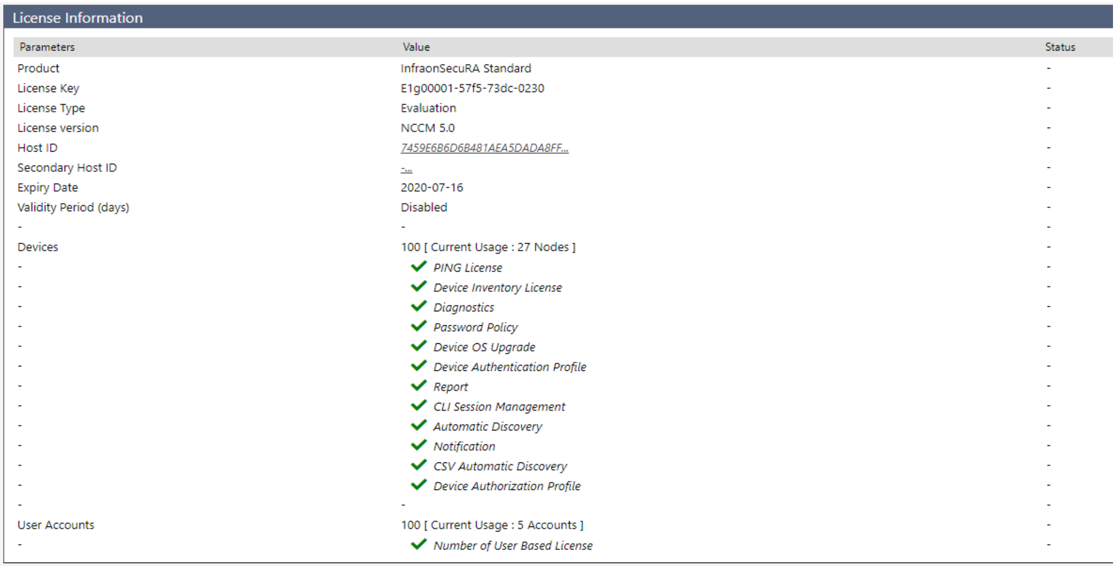
Database Server	PostgreSQL
IP Address *	127.0.0.1
User Name *	nccm
Password *	•••••••••
Port *	5432
Database Name *	sso
Secondary Server IP Address*	
Secondary Server User Name*	postgres
Secondary Server Password*	
Secondary Server Port*	5432
Secondary Server Database Name *	nccm_db

- Input IP Address in the textbox.
- Input Root username in the textbox.
- Input the Root password in the textbox.
- Input Port no. in the textbox.
- Input Database name in the textbox.

Click Change to save the Database configuration change or click Back to abort the changes.

39. Application Details

From 'Manage' menu (from the top panel) ⚙ click Application Details -> License Details to view License details, access the License Information.



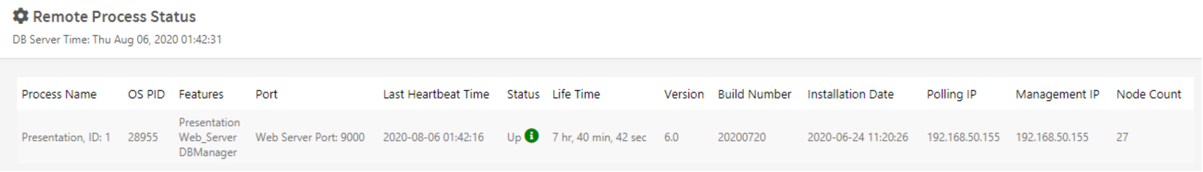
License Information

Parameters	Value	Status
Product	InfraonSecuRA Standard	-
License Key	E1g00001-57f5-73dc-0230	-
License Type	Evaluation	-
License version	NCCM 5.0	-
Host ID	7459E6B6D6B481AEA5DADA8FF...	-
Secondary Host ID	-...	-
Expiry Date	2020-07-16	-
Validity Period (days)	Disabled	-
-	-	-
Devices	100 [Current Usage : 27 Nodes]	-
-	✓ *PING License*	-
-	✓ *Device Inventory License*	-
-	✓ *Diagnostics*	-
-	✓ *Password Policy*	-
-	✓ *Device OS Upgrade*	-
-	✓ *Device Authentication Profile*	-
-	✓ *Report*	-
-	✓ *CLI Session Management*	-
-	✓ *Automatic Discovery*	-
-	✓ *Notification*	-
-	✓ *CSV Automatic Discovery*	-
-	✓ *Device Authorization Profile*	-
-	-	-
User Accounts	100 [Current Usage : 5 Accounts]	-
-	✓ *Number of User Based License*	-

The features available in SecuRA are dependent on the type of License purchased based on the requirements. An Interpretation of important parameters at the License Information page with examples is provided below for users to understand how Licensing works. This allows clear understanding of features that are enabled with License and the response to be taken in view of breach of one or more License Parameters in SecuRA.

40. Remote Process Status

From 'Manage' menu (from the top panel) ⚙ click Application Details -> Remote Process Status to view status of remote process within SecuRA.



Remote Process Status

DB Server Time: Thu Aug 06, 2020 01:42:31

Process Name	OS PID	Features	Port	Last Heartbeat Time	Status	Life Time	Version	Build Number	Installation Date	Polling IP	Management IP	Node Count
Presentation, ID: 1	28955	Presentation Web_Server DBManager	Web Server Port: 9000	2020-08-06 01:42:16	Up ⓘ	7 hr, 40 min, 42 sec	6.0	20200720	2020-06-24 11:20:26	192.168.50.155	192.168.50.155	27

Click ⓘ to view

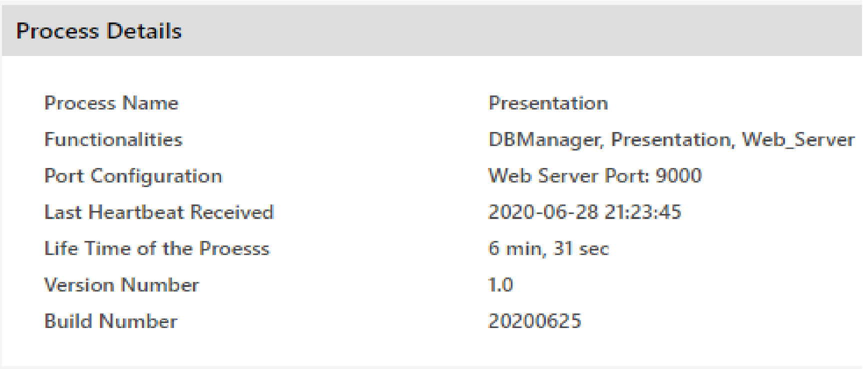
- Top commands executed on the device

- Memory of the Device
- Disk Information
- Network Information
- OS Information

These details are helpful at the time of Troubleshooting.

41. Process Details

This page displays information about the process i.e., Process Name, Functionalities etc. From the Manage menu, click Application Details -> Process Details.

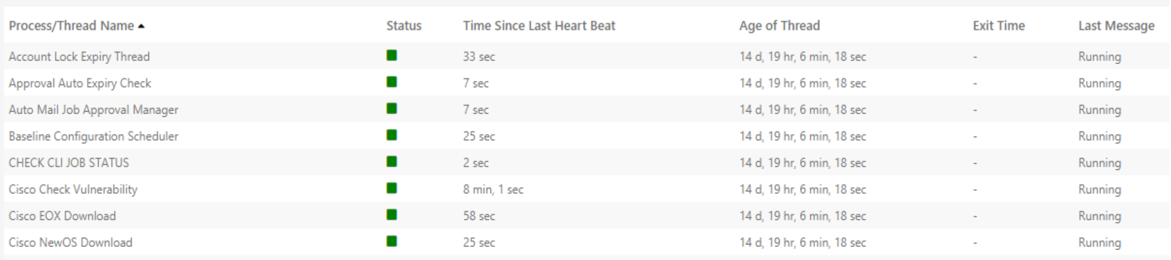


Process Details

Process Name	Presentation
Functionalities	DBManager, Presentation, Web_Server
Port Configuration	Web Server Port: 9000
Last Heartbeat Received	2020-06-28 21:23:45
Life Time of the Proesss	6 min, 31 sec
Version Number	1.0
Build Number	20200625

42. Thread Status

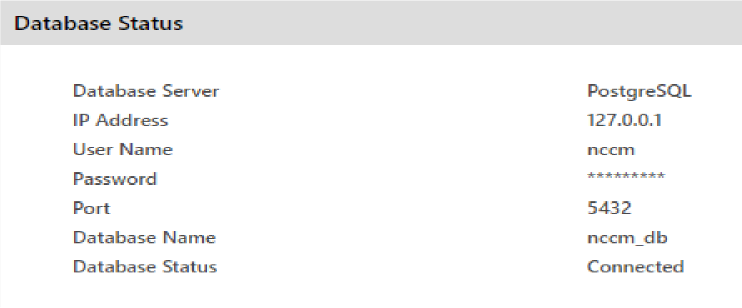
Threads are long-running background processes on SecuRA. From the Manage menu, click Application Details-> Thread Status to view the thread Status.



Process/Thread Name ▲	Status	Time Since Last Heart Beat	Age of Thread	Exit Time	Last Message
Account Lock Expiry Thread	🟩	33 sec	14 d, 19 hr, 6 min, 18 sec	-	Running
Approval Auto Expiry Check	🟩	7 sec	14 d, 19 hr, 6 min, 18 sec	-	Running
Auto Mail Job Approval Manager	🟩	7 sec	14 d, 19 hr, 6 min, 18 sec	-	Running
Baseline Configuration Scheduler	🟩	25 sec	14 d, 19 hr, 6 min, 18 sec	-	Running
CHECK CLI JOB STATUS	🟩	2 sec	14 d, 19 hr, 6 min, 18 sec	-	Running
Cisco Check Vulnerability	🟩	8 min, 1 sec	14 d, 19 hr, 6 min, 18 sec	-	Running
Cisco EOX Download	🟩	58 sec	14 d, 19 hr, 6 min, 18 sec	-	Running
Cisco NewOS Download	🟩	25 sec	14 d, 19 hr, 6 min, 18 sec	-	Running

43. Database Status

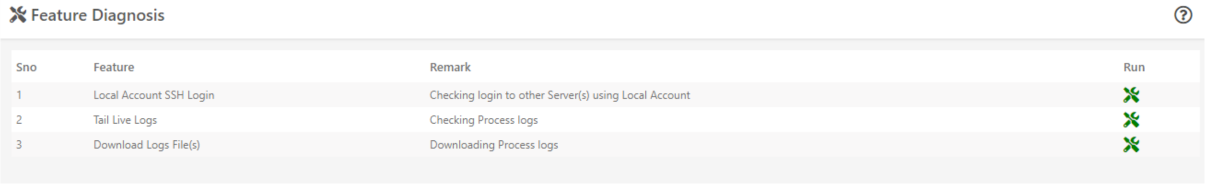
This page displays the details and the status of the configured database for the current process.



Database Status	
Database Server	PostgreSQL
IP Address	127.0.0.1
User Name	nccm
Password	*********
Port	5432
Database Name	nccm_db
Database Status	Connected

44. Feature Diagnosis

From the ‘Manage’ menu, select ‘Feature Diagnosis’ to view and download Application Logs. Click on 🛠 to run a check instantly. Feature Diagnosis is mainly used for troubleshooting purposes.

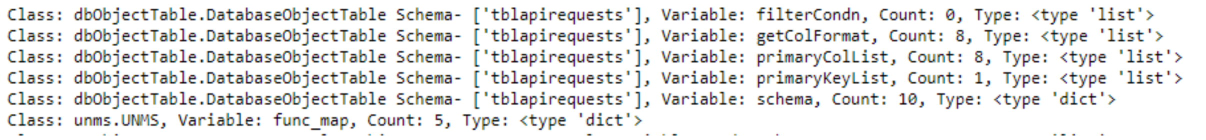


Feature Diagnosis

Sno	Feature	Remark	Run
1	Local Account SSH Login	Checking login to other Server(s) using Local Account	🛠
2	Tail Live Logs	Checking Process logs	🛠
3	Download Logs File(s)	Downloading Process logs	🛠

45. Memory Dump

From the ‘Manage’ menu, select Memory Dump to view the Memory details of the application.



```
Class: dbObjectTable.DatabaseObjectTable Schema- ['tblapirequests'], Variable: filterCondn, Count: 0, Type: <type 'list'>
Class: dbObjectTable.DatabaseObjectTable Schema- ['tblapirequests'], Variable: getColFormat, Count: 8, Type: <type 'list'>
Class: dbObjectTable.DatabaseObjectTable Schema- ['tblapirequests'], Variable: primaryColList, Count: 8, Type: <type 'list'>
Class: dbObjectTable.DatabaseObjectTable Schema- ['tblapirequests'], Variable: primaryKeyList, Count: 1, Type: <type 'list'>
Class: dbObjectTable.DatabaseObjectTable Schema- ['tblapirequests'], Variable: schema, Count: 10, Type: <type 'dict'>
Class: unms.UNMS, Variable: func_map, Count: 5, Type: <type 'dict'>
```