ICS SHIELD

R 510.2

Virtual Security Engine (VSE)

User Guide

CS-ICSW601en-510B

June 2020

Notices

Trademarks

Third-party licenses

About this Guide

This document provides detailed instructions for using the Virtual Security Engine (VSE). The VSE is an ICS Shield component that is installed at the remote site, monitors the devices at the site, and provides additional functionalities such as remote access.

Scope

This guide provides conceptual information and instructions on using the VSE with the operative privileges and menu options available to users. It describes how to use the VSE for collecting and monitoring devices at the site.

NOTE

In this guide, the term *user* refers to all non-administrator user roles:

- View Only
- Device Manager
- Operator
- Supervisor

For details, see chapter *VSE User Roles* in the *VSE Administrator Guide*.

Intended audience

As this guide instructs the configuration and operation of the VSE, the target audiences are:

- VSE administrators and users
- Security Center administrators

Prerequisite skills

This guide assumes basic knowledge of the ICS Shield modules relevant to the Security Center, the VSE, or both, depending on your specific role.

Related documents

The following list identifies publications that contain information relevant to the information in this document.

Document Name	Document Number
ICS Shield R510.2 - Security Center Getting Started Guide	CS-ICSW400en-510B

Revision history

Revision	Supported Release	Date	Description
B	R 510.2	June 28, 2020	This software is an upgrade-only release from Release 510.1
A	R 510.1	August 8, 2019	Updated release of ICS Shield documentation
A	R 500.1	February 27, 2019	First release of the ICS Shield documentation

Contents

1. SECURITY CONSIDERATIONS 9

1.1 Physical security 9

1.2 Secured zone 9

1.3 Limiting access 9

1.3.1 At the VSE level 9

1.3.2 At the directory or file level 10

1.3.3 Ports used by the application 10

1.4 Authorization measures 11

1.5 Encryption and validation 11

2. TERMS AND DEFINITIONS 12

3. OVERVIEW OF USER FUNCTIONS 14

3.1 Logging into the VSE 14

3.2 Editing your profile 15

3.3 Collecting Data 15

3.4 Managing reports 16

4. WORKING WITH DEVICES 17

4.1 Understanding protocol settings 17

4.2 Understanding device unique IDs 18

4.3 Adding a device 18

4.4 Editing a device 20

4.5 Deleting a device 21

4.6 Analysis rules 21

4.6.1 Configuring analysis rules at the product line level 21

4.6.2 Configuring analysis rules at the device level 22

4.6.3 Analysis rule violations 23

4.7 Managing invalid devices 23

5. COLLECTING DATA 25

5.1 Activating an execution profile 25

5.1.1 Automatically activating an execution profile 25

5.1.2 Manually activating an execution profile 26

5.1.3 Execution profile status 27

5.1.4 What happens when an execution profile runs? 28

5.2 Understanding execution results 29

5.2.1 Types of execution profiles 30

5.2.2 Protocols for collecting data 30

5.2.3 Execution profiles and system startup......31
5.2.4 What happens when an updated product line is received?......31
5.3 Deactivating an execution profile......32
5.4 Deactivating all active execution profiles......33
5.5 Activating all automatic execution profiles......33
5.6 Viewing execution profile status......34
5.7 Aborting an execution......35
6. MANAGING EXECUTION RESULTS......36
6.1 Searching for execution results......36
6.2 Viewing execution results......37
6.3 Deleting execution results......38
7. WORKING WITH PROBLEM REPORTS......39
7.1 Overview of problem reports......39
7.1.1 Automatic Reports......39
7.1.2 Periodic site reports......40
7.1.3 Manual reports......40
7.2 Creating a new problem report......41
7.3 Selecting specific execution results to attach......44
7.4 Managing problem reports......46
7.4.1 Finding a problem report in the database......46
7.4.2 Viewing a problem report......47
7.4.3 Sending a problem report......47
7.4.4 Exporting a problem report......49
7.4.5 Deleting problem reports......49
8. USING THE CONTROL PANEL......50
8.1 Retrieving toolkits manually......50
8.2 Switching between offline and online modes......50
8.3 Uploading script files......51
9. REMOTE ACTIVITIES......52
9.1.1 What are remote activities?......52
9.1.2 Remote Access......53
9.1.3 Using the Remote Activities screen......54
9.2 Remote Connections......62
10. REVERSE TUNNEL......64
11. OPERATIONAL LOG......65
A OPERATIONAL LOG EVENTS......67

List of Figures

FIGURE 3-1. EDITING A USER PROFILE........15

FIGURE 4-1. NEW DEVICE SCREEN........19

FIGURE 4-2. ANALYSIS RULES FOR PRODUCT LINE........22

FIGURE 4-3. LOCAL VALUE FOR ANALYSIS RULE........22

FIGURE 4-4. ANALYSIS RULE VIOLATIONS........23

FIGURE 5-1. CURRENT EXECUTION TAB........27

FIGURE 5-2. DEVICE CHECK BOX........33

FIGURE 5-3. CURRENT EXECUTION TAB........34

FIGURE 6-1. EXECUTION RESULT-VIEW FOR A SPECIFIC EXECUTION........38

FIGURE 7-1. REPORT SEARCH TAB........47

FIGURE 8-1. RETRIEVE TOOLKIT MESSAGE........50

FIGURE 9-1. FILTERING THE REMOTE ACTIVITIES LIST........56

FIGURE 9-2. REMOTE ACTIVITY DETAILS TAB........59

FIGURE 10-1. REMOTE ACCESS........64

List of Tables

TABLE 1-1. LIST OF PORTS 10

TABLE 4-1. DEVICE FIELDS 19

TABLE 5-1. STATUS OF ACTIVE EXECUTION PROFILES........ 27

TABLE 6-1. SEARCH CRITERIA FOR SELECTING EXECUTION RESULTS 36

TABLE 7-1. PARAMETERS FOR NEW PROBLEM REPORT........ 42

TABLE 7-2. PROBLEM DETAILS – SELECT EXECUTION RESULTS 44

TABLE 9-1. REMOTE ACTIVITY STATES 55

TABLE A-1. LOG EVENTS........ 67

1. Security Considerations

This chapter outlines the security measures for the VSE.

1.1 Physical security

⚠ CAUTION	**VSE is a mission-critical component.** **Take all necessary physical measures to prevent attacks or disasters.**

Ensure that the server where the product is installed is located in an approved physically secure location that is accessible only to authorized personnel.

1.2 Secured zone

VSE contains sensitive information, the loss of which could have severe consequences. Therefore, there is a need to protect the sensitive information and prevent attacks against the product. To do that, the VSE software, as well as its related extensions, must be installed in an internally secured zone such as the site's layer 3 network, with strict access control lists and appropriate firewall/routing rules.

Ensure that VSE is installed in a directory that is only accessible to authorized personnel responsible for the product.

⚠ CAUTION	**If VSE is installed on one or more servers that are exposed to untrusted networks such as the Internet, protection against denial-of-service (DoS) attacks must be implemented.**

1.3 Limiting access

It is highly recommended to follow regulatory, industry, and enterprise standards for limiting access to sensitive information as specified below.

1.3.1 At the VSE level

The user management at the host running the VSE must follow the principles of need to know and least privilege: Only users who absolutely must have access to the computer are granted access, and these users are assigned the minimal set of permissions allowing them to perform their job.

1.3.2 At the directory or file level

Access to directories and files should also be granted in accordance with the principles of need to know and least privilege: Only Users who absolutely must have access to the requested directory and file are granted access, and these Users are assigned the minimal set of permissions allowing them to perform their job.

Use the built-in file access audit logging of the OS to monitor unauthorized changes to sensitive files.

1.3.3 Ports used by the application

The ports used for the VSE are listed in the table below.

Table 1-1. List of Ports

Port Number	Port Type	Inbound/Outbound	Used for
8449	TCP	Inbound	Accessing the UI of the VSE (configurable value)
443	TCP	Outbound	Connecting to a communication server **Note** This value is configurable and depends on the communication server settings
444	TCP	Outbound	Connecting to a remote access bridge (RAB) **Note** This value is configurable and depends on the RAB settings
Note All ports listed below are not necessary for the VSE’s basic operation, and are provided as examples			
22	TCP	Outbound	Connecting to an SSH server on the same network
21	TCP	Outbound	Connecting to an FTP server on the same network

Port Number	Port Type	Inbound/Outbound	Used for
445	TCP	Outbound	Connecting through WMI to a device on the same network
162 (configurable)	UDP	Inbound	Used for SNMP traps
514 (configurable)	UDP	Inbound	Used for syslog events

1.4 Authorization measures

It is strongly recommended to implement the following security measures:

- Change the default administrative password and delete/disable the default service accounts as soon as new administrative accounts are created
- Disable any default Administrator/Root user on the computer
- Disable any default Guest user on the computer
- Disable any unauthenticated access to the computer via shared directories etc.
- Ensure that the OS is up to date with the latest security patches provided by the OS vendor
-

1.5 Encryption and validation

All cryptographic keys generated for the encrypted communication must follow the current industry standards, including key size, encryption suites, certificate swapping etc.

Operators and other personnel who have a low authorization level are advised to ensure that they only run software provided from the Headquarters as a code-signed execution file, such as Hyper Tunnel installer. A code-signed software displays *the signed* by notification when it starts to run.

It is recommended to use a valid certificate issued by a trusted Certificate Authority (CA), either the organization’s internal CA or an external CA.

2. Terms and definitions

NOTE	The terms and definitions are listed in alphabetical order

Term	Definition
add-on	An umbrella term for product lines and ESPs.
analysis rule	The user-defined range of values for a specific metric, such as CPU utilization or buffer cache hit ratio.
analysis rule violation	If the value collected meets the criteria defined by the analysis rule, this triggers an analysis rule violation.
asset	Any site component that is connected to the network and is accessible from the VSE
Communication Server (CS)	The Communication Server provides secure communication between the Security Center and the VSEs and, optionally, between the VSEs themselves.
corrective action	A collection profile that performs an action to correct a problem detected by other collection profiles; for example, if a monitoring profile detected a low disk space issue, a corrective action will delete obsolete and large temporary files
device	A representation of a physical or virtual server or machine in the VSE
diagnose routine (DR)	A collection profile that runs on demand and is intended to collect in-depth diagnostic data.
execution profile	A collection of scripts related to one logical area, such as machine security status, hardware information, event logs, or storage information; these scripts can either be run on demand (Diagnose Routine or Corrective Action) or based on a predefined schedule.
heartbeat	A periodic message sent between the VSE and the master Security Center, to verify that the connection is alive
Master Security	The only Security Center that handles heartbeat messages,

Term	Definition
Center	and from which the VSE receives remote activities. There can be only one Master per VSE.
monitoring profile (MP)	A collection profile configured to run at set time intervals, such as Every day at 18:00.
product line	A set of actions and scripts that together instruct the VSE to perform certain procedures on devices that are defined in the VSE.
Remote Access Bridge (RAB)	A Honeywell Forge Cybersecurity Software component installed externally to the SC which enables secure remote access between the SC and the VSE. On receiving communication requests from the VSE and the RAG, it creates a secure bridge between them, thereby enabling a secure communications tunnel from the SC to the VSE, and from there to the required asset.
reverse tunnel	A secured connection initiated by the VSE to the Security Center.
Security Center (SC)	**Error! Unknown document property name.** component that is installed at the corporate data center. The security center is composed of various software components, which enable to remotely collect, analyze, view, manage, and store data retrieved from the VSEs. This data refers to the monitored assets and network devices found at the VSE's sites.
severity level	A classification of information into one of the following levels: 1. Critical 2. Warning 3. Error 4. Info
site	A remote physical location, such as an industrial plant, which includes one or more network environments and has at least one VSE.
tunnel	A secure connection established from the Security Center to the VSE.

3. Overview of User Functions

This chapter describes the functions that VSE users can perform, from logging into the VSE through creating and managing devices and up to reporting issues encountered during data collection, as detailed in the following sections:

- 3.1, Logging into the VSE
- 3.2, Editing your profile
- 3.3, Collecting Data
- 3.4, Managing reports

3.1 Logging into the VSE

If this is the first time you are using VSE , ask the VSE administrators to register you in the system and supply you with a username and password. Once logged in, you can change your password at any time. For details, see section 3.2, Editing your profile.

To log into the VSE application:

1. Open a browser and type: **http://<host>:8449** in the address bar.

   The Login page appears.

2. Enter your username and password.
3. Click **Login**.

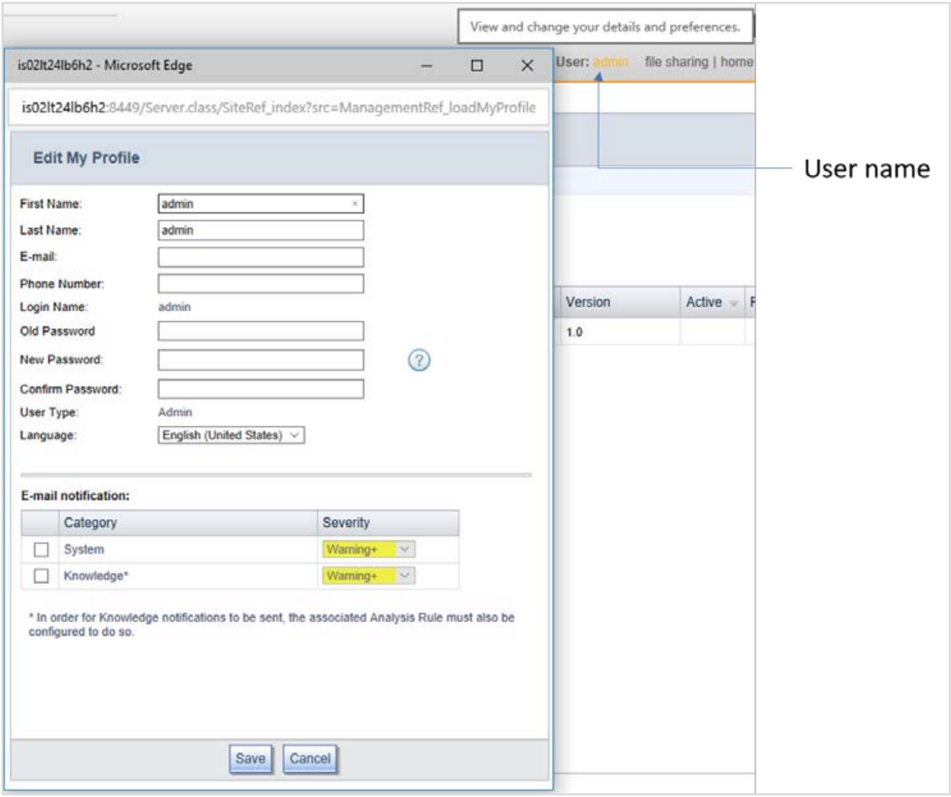
   The VSE main screen appears.

NOTE	The timeout for the VSE UI is 20 minutes (configurable).

3.2 Editing your profile

To edit your profile:

1. To display the **Edit My Profile** dialog, in the upper right corner of the screen click your username.


View and change your details and preferences.
is02lt24lb6h2 - Microsoft Edge
is02lt24lb6h2:8449/Server.class/SiteRef_index?src=ManagementRef_loadMyProfile
User: admin file sharing | home
User name
Version
Active
1.0
Save
Cancel

Edit My Profile

First Name:	admin
Last Name:	admin
E-mail:	
Phone Number:	
Login Name:	admin
Old Password	
New Password:	
Confirm Password:	
User Type:	Admin
Language:	English (United States)

E-mail notification:

	Category	Severity
□	System	Warning+
□	Knowledge*	Warning+

* In order for Knowledge notifications to be sent, the associated Analysis Rule must also be configured to do so.

Figure 3-1. Editing a user profile

2. Make the requested changes and click **Save.**

3.3 Collecting Data

Data is collected from a device by running execution profiles. Each execution profile contains instructions on how and when to collect data, and which data to collect. For details, see section 5.1, Activating an execution profile. It may also be necessary to deactivate execution profiles on devices and delete old execution results. See section 5.3, Deactivating an execution profile, and chapter 6, Managing Execution Results.

3.4 Managing reports

When an issue is encountered in one or more devices, you can send a report to the Security Center for analysis. See section 7.2, Creating a new problem report.

If there are problems in communication, or if requested by a Security Center representative, you may need to resend or re-export a report. See section 7.4.3, Sending a problem report and section 7.4.4, Exporting a problem report.

Some reports can take up a large amount of space in the limited size of the VSE database. Therefore, it is recommended to free up space in the database by deleting reports that are no longer necessary, otherwise the VSE will delete reports based on their date of creation, when the free space in the database falls below a predefined threshold. See section 7.4.5, Deleting problem reports.

4. Working with Devices

The elementary units in an ICS Shield installation are devices, which are created from a network element that has an IP address. Once a device is created in the VSE, it is assigned a product line - a set of actions and scripts that together instruct the VSE to perform certain procedures on the device.

Product lines are defined in the Security Center, and are delivered to the VSE through one of the following methods:

- During installation - As part of the VSE custom installation package.
- Distribution from the Security Center.
- Import from a file – for details, see the VSE Administrator Guide.

4.1 Understanding protocol settings

Protocol settings define how to communicate with the agent for each protocol running on the device. These settings also specify which ports to use for connecting to the device, and the required login parameters.

The values of the protocol settings can be defined at the following levels. Each specific level overrides more general levels:

Level	Interface	Applies To
SC	SC Policy Builder	All devices in all VSEs
VSE	Administration & Security > Product Line > Protocol Settings	All devices in the specific VSE
Device	Operations > Device Management > Edit	Only the specific device

NOTE

- Clicking **Restore Protocol Settings** at the device level resets all protocols to their default settings at the VSE level for that device. For details, see section 4.4, Editing a device.
- For information on the effects of changing Telnet/SSH or TL1 login values, see section *Changes to Telnet/SSH and TL1 login values* in the VSE Administrator Guide.

4.2 Understanding device unique IDs

When you define a new device, you need to provide a unique ID for the device. While this ID often corresponds to the device's serial number, your organization may identify devices by other means.

The unique ID can be provided either by entering the ID manually or by selecting the automatic unique ID retrieval, which is a customizable routine for generating the unique ID.

If a product line does not support automatic unique ID retrieval, the VSE calculates a unique ID for a new device using the following pattern:

<**Device address**>:<**VSE ID**>:<**random 3-digit number**>:<**Product Line ID**>

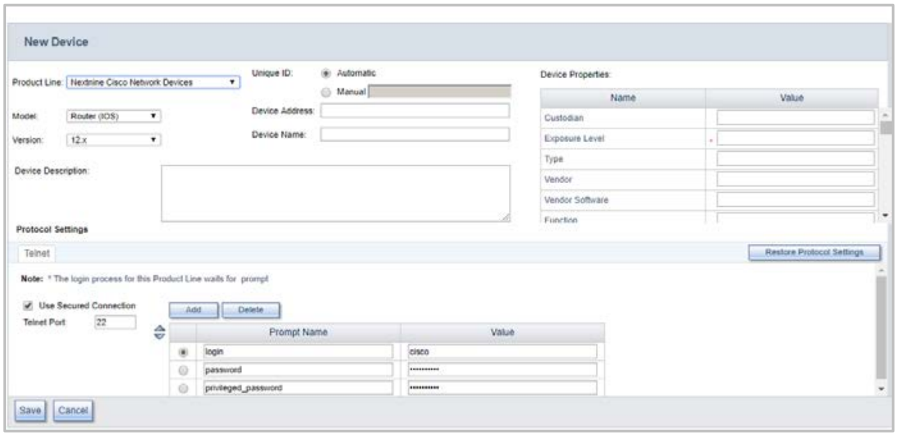
> NOTE
>
> Selecting the **Manual** option overrides all other values. The VSE uses the value you entered for **Unique ID** and sends a notification. If you enter a non-unique value, an error message will be displayed.
>
> If another device with the same name, associated with the same Product Line name, already exists.
>
> If another device by the same name, which is associated with another Product Line, already exists, the device will be created as usual.

4.3 Adding a device

The number of devices that can be defined in VSE is determined by your VSE license. If the current number of devices is the maximum number allowed in the VSE license, you cannot add a new device until you delete some old devices or upgrade your license.

To add a device:

1. Go to **Operations** > **Device Management** to display the **All Devices** screen.
2. Click **New** to display the **New Device** screen.



Product Line: Nextnine Cisco Network Devices ▾

Model: Router (IOS) ▾

Version: 12.x ▾

Unique ID: ● Automatic ○ Manual

Device Address:

Device Name:

Device Properties:

Name	Value
Custodian	
Exposure Level	*
Type	
Vendor	
Vendor Software	
Function	

Note: * The login process for this Product Line waits for prompt

☑ Use Secured Connection

Telnet Port 22

	Prompt Name	Value
●	login	cisco
○	password	•••••••••••
○	privileged_password	•••••••••••

Figure 4-1. New Device screen

3. Enter device information in the fields listed in the table below.

Table 4-1. Device fields

Field	Description
Product Line	Select the relevant product line from the list (mandatory).
Model and Version	Indicate the model and version of the device. This combination is highly customizable and can refer to hardware, software, or both. The values for the model and the version are both mandatory.
Unique ID – *Automatic*	If *Automatic* has been selected, this indicates that the VSE should automatically retrieve the device's unique ID. **Note:** If the product line does not support automatic unique ID retrieval, the VSE generates a unique ID for the device.
Unique ID – *Manual*	If *Manual* has been selected, this indicates that the unique ID should be entered manually.
Device Address	The IP address or hostname of the device (mandatory)
Device Name	A logical name for the device. Enter a name of your choice. Alternatively, you can leave this field empty, in which case the VSE

Field	Description
	generates a name automatically as described in step 4.
Device Description	A brief description of the device.
Device Properties	Customizable fields that provide additional information about the device. The values for the device properties can be mandatory.

4. To allow the VSE to generate a device name, leave the Device Name empty and enter the device IP address in the **Device Address** field. The VSE attempts to resolve the host name using the IP entered in the Device Address field. If successful, the host name is used as the device name. Otherwise, the device address is used as the device name.

5. Use the fields provided in the **Protocol Settings** area to enter the settings relevant to the selected product line.

   Any login parameter for Telnet/SSH, TL1 and Custom can be marked at the Security Center as a masked field for security purposes. When you edit the protocol settings, the values in masked fields appear as password-masking characters.

NOTE	To indicate changes made to the default protocol settings, any changed value is marked in red. You can restore the default settings for the product line at any time by clicking Restore Defaults. For information on the effects of changing Telnet/SSH or TL1 login values, see the section *Changes to Telnet/SSH and TL1 login values* in the VSE Administrator Guide.

6. Click **Save**.

   The VSE adds the device and indicates that the activity was completed successfully.

4.4 Editing a device

If you would like to make any modification to a device, select the requested device in the **Operations > Device Management > All Devices** screen and click **Edit.**

If any of the protocol settings for the device have changed and there are execution profiles running, the VSE warns you that the execution profiles currently running will be updated.

NOTE	If you changed the model or version of the device, the VSE stops all execution profiles on the device and restarts them with the proper model and version combination. If any of the previously running execution profiles on the device are incompatible with the new model and version combination, they are not restarted.

4.5 Deleting a device

If you would like to remove a device, select the requested device in the **Operations > Device Management > All Devices** screen and click **Delete.**

When a device is deleted, the following things happen:

- All active execution profiles are stopped.
- The device and all of its execution results are removed from the database.
- The VSE stops listening for Syslog events for this device (if relevant).
- The VSE stops listening for SNMP Traps for this device (if relevant).

4.6 Analysis rules

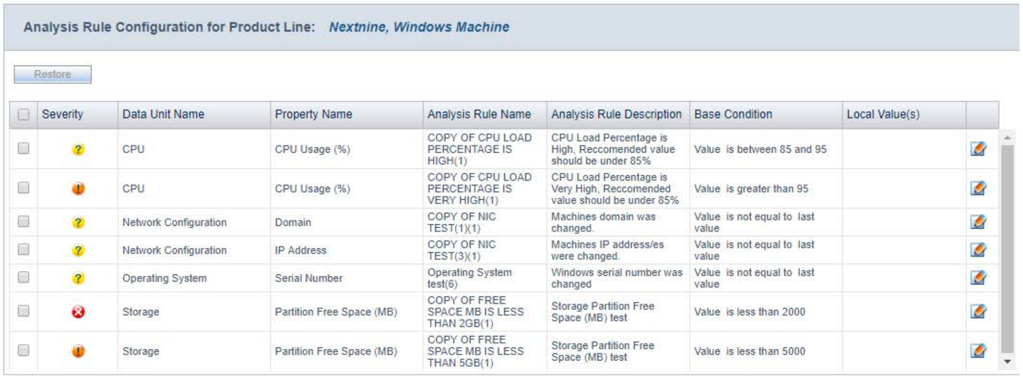
Analysis rules are configured in the Security Center's Policy Builder and define the parameters for raising alarms when their values exceed or fall below predefined thresholds. You can override the Security Center's configuration for specific VSEs and devices by setting local values on the VSE or device levels.

NOTE	The analysis rules defined at the device level override the analysis rules defined at the VSE level. Similarly, analysis rules defined at the VSE override the rules defined at the Security Center level.

4.6.1 Configuring analysis rules at the product line level

To configure analysis rule local values per VSE, go to **Administration & Security** > **Product Lines** > **Analysis Rule Configuration** tab.

The **Analysis Rule Configuration** window appears, displaying all of the analysis rules that are configured for the product line.



Analysis Rule Configuration for Product Line: *Nextnine, Windows Machine*

□	Severity	Data Unit Name	Property Name	Analysis Rule Name	Analysis Rule Description	Base Condition	Local Value(s)	
□	?	CPU	CPU Usage (%)	COPY OF CPU LOAD PERCENTAGE IS HIGH(1)	CPU Load Percentage is High, Reccomended value should be under 85%	Value is between 85 and 95		✎
□	!	CPU	CPU Usage (%)	COPY OF CPU LOAD PERCENTAGE IS VERY HIGH(1)	CPU Load Percentage is Very High, Reccomended value should be under 85%	Value is greater than 95		✎
□	?	Network Configuration	Domain	COPY OF NIC TEST(1)(1)	Machines domain was changed.	Value is not equal to last value		✎
□	?	Network Configuration	IP Address	COPY OF NIC TEST(3)(1)	Machines IP address/es were changed.	Value is not equal to last value		✎
□	?	Operating System	Serial Number	Operating System test(6)	Windows serial number was changed	Value is not equal to last value		✎
□	✖	Storage	Partition Free Space (MB)	COPY OF FREE SPACE MB IS LESS THAN 2GB(1)	Storage Partition Free Space (MB) test	Value is less than 2000		✎
□	!	Storage	Partition Free Space (MB)	COPY OF FREE SPACE MB IS LESS THAN 5GB(1)	Storage Partition Free Space (MB) test	Value is less than 5000		✎

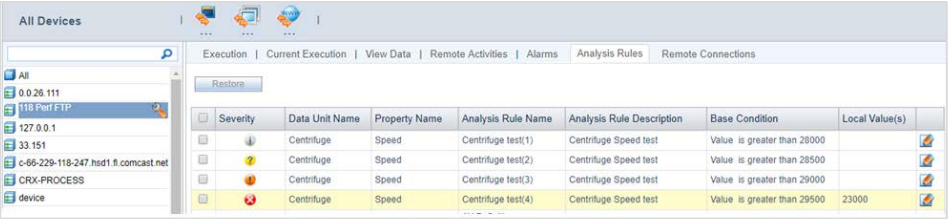
Figure 4-2. Analysis rules for product line

For each rule, you can press on the ✎ icon and set a local value that overwrites the value (base condition) applied at the product line level at the VSE.

4.6.2 Configuring analysis rules at the device level

To configure analysis rules local values at the device level:

1. Go to **Operations >Devices**.
2. From the **Devices** menu, select one of the devices.
3. Click the **Analysis Rules** tab display the analysis rules applied on the selected device.
4. For each rule, you can press on the ✎ icon and set a local value that overwrites the value applied at the product line level at the VSE. For example, in Figure 4-3 below, the threshold originally defined for this product line was 29500. Because the Base Condition was edited for this device, the number 23000 appears in the column **Local Value(s)** and the entire row is highlighted in yellow.



All Devices
All
0.0.26.111
118 Perf FTP
127.0.0.1
33.151
c-66-229-118-247.hsd1.fl.comcast.net
CRX-PROCESS
device
Execution | Current Execution | View Data | Remote Activities | Alarms | Analysis Rules | Remote Connections
Restore

□	Severity	Data Unit Name	Property Name	Analysis Rule Name	Analysis Rule Description	Base Condition	Local Value(s)	
□	i	Centrifuge	Speed	Centrifuge test(1)	Centrifuge Speed test	Value is greater than 28000		✎
□	?	Centrifuge	Speed	Centrifuge test(2)	Centrifuge Speed test	Value is greater than 28500		✎
□	!	Centrifuge	Speed	Centrifuge test(3)	Centrifuge Speed test	Value is greater than 29000		✎
□	✖	Centrifuge	Speed	Centrifuge test(4)	Centrifuge Speed test	Value is greater than 29500	23000	✎

Figure 4-3. Local Value for Analysis Rule

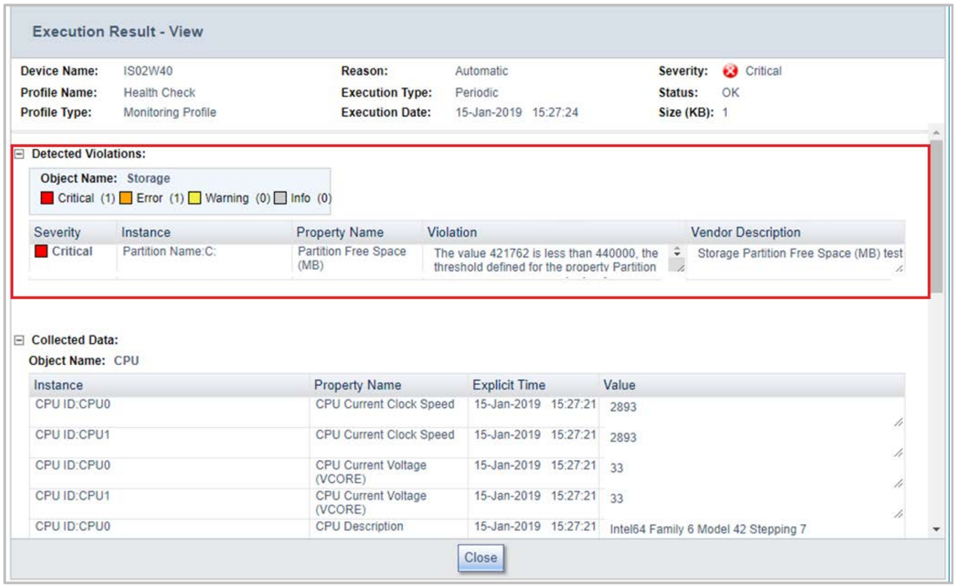
NOTE	Analysis rules configured relative to **Last Collected Value** cannot be modified.

4.6.3 Analysis rule violations

If the value collected meets the criteria defined by the analysis rule, this triggers an analysis rule violation.

To see analysis rule violations:

1. Go to **Operations > Devices**.
2. Select a device or **All** in the left pane.
3. In the **View Data** tab, click the link (**OK**, **Partial**, or **Error)** to display the screen **Execution Result – View** that contains the Detected Violations section.



Execution Result - View

Device Name:	IS02W40	Reason:	Automatic	Severity:	Critical
Profile Name:	Health Check	Execution Type:	Periodic	Status:	OK
Profile Type:	Monitoring Profile	Execution Date:	15-Jan-2019 15:27:24	Size (KB):	1

⊟ Detected Violations:

Object Name: Storage

🟥 Critical (1) 🟧 Error (1) 🟨 Warning (0) □ Info (0)

Severity	Instance	Property Name	Violation	Vendor Description
🟥 Critical	Partition Name:C:	Partition Free Space (MB)	The value 421762 is less than 440000, the threshold defined for the property Partition	Storage Partition Free Space (MB) test

⊟ Collected Data:

Object Name: CPU

Instance	Property Name	Explicit Time	Value
CPU ID:CPU0	CPU Current Clock Speed	15-Jan-2019 15:27:21	2893
CPU ID:CPU1	CPU Current Clock Speed	15-Jan-2019 15:27:21	2893
CPU ID:CPU0	CPU Current Voltage (VCORE)	15-Jan-2019 15:27:21	33
CPU ID:CPU1	CPU Current Voltage (VCORE)	15-Jan-2019 15:27:21	33
CPU ID:CPU0	CPU Description	15-Jan-2019 15:27:21	Intel64 Family 6 Model 42 Stepping 7

Figure 4-4. Analysis rule violations

4.7 Managing invalid devices

A device becomes invalid if an update to a product line no longer supports the model-version combination of that device. Invalid devices are marked in red in the list of devices. Even when a device is invalid, you can still create a report that contains previous execution results for the device.

When a device becomes invalid, you can:

- Re-activate the device in the VSE by editing the device definition to work with one of the supported model/version combinations; see section 4.4, Editing a device.
- Re-activate the device by updating the model and/or version on the device itself, and then editing the device definition in the VSE accordingly; see section 4.4, Editing a device.
- Remove (delete) the device from the VSE, so it will no longer be supported by the ICS Shield system; see section 4.5, Deleting a device.

5. Collecting Data

The VSE collects data from the devices by using execution profiles defined in the Security Center's Policy Builder. This chapter explains how to work with execution profiles.

Data is collected for the following purposes:

- To establish a history of how a device works under normal circumstances
- To analyze device data in order to detect issues and raise alarms

5.1 Activating an execution profile

To enable the VSE to collect data requested by an execution profile, the execution profile must be active.

Execution profiles can be activated in the following ways:

- **Automatic** – see section 5.1.1**,** Automatically activating an execution profile.
- **Manual** - see section 5.1.2, Manually activating an execution profile.

5.1.1 Automatically activating an execution profile

There are two ways to automatically activate execution profiles:

- Regular automatic activation
- One-time automatic activation

5.1.1.1 Regular automatic activation

As part of configuring a product line in the Policy Builder, you can mark execution profiles for automatic activation. These execution profiles are automatically activated on a device when the product lines containing them are imported and when a new device is created.

NOTE	The administrator can disable this option for all execution profiles. For details, see section *Configuring the System Settings* in the VSE Administrator Guide.

5.1.1.2 One-time automatic activation

Automatic one-time activation is triggered by an analysis rule violation.

You can configure an analysis rule violation to trigger an execution profile that collects data that might be relevant to the problem detected. Each analysis rule violation can trigger one execution profile.

When an execution profile is triggered by an analysis rule violation, it is executed on an immediate, one-time basis, regardless of its scheduling parameters.

5.1.2 Manually activating an execution profile

There are two types of manual activation:

- Regular manual activation
- One-time manual activation

In addition, you can globally activate all currently inactive execution profiles marked for automatic activation. For details, see section 5.5, Activating all automatic execution profiles.

5.1.2.1 Regular manual activation

When you manually activate an execution profile, it runs either a specific number of times, or on a specific schedule, depending on its definition.

To manually activate one or more execution profiles on a device:

1. Go to **Operations** > **Devices** to display the **All Devices** screen.
2. Select a device and click the **Execution** tab, which serves to manage execution profiles.

   A list of execution profiles for the device appears.
3. Select the requested execution profile(s) and click **Activate**.

   > **NOTE**
   > Only those execution profiles that match the device model-version combination appear in the **Execution Profile Management** list.

   The VSE activates the selected execution profile(s) for the device and informs you that the operation was completed successfully.
4. Click **OK**.

   A check mark appears in the **Active** column next to the selected execution profile(s).

5.1.2.2 Manually activate once

When you manually activate an execution profile by using the **Execute Once Now** option, the execution profile runs on an immediate, one-time basis, regardless of its scheduling parameters. For further information, see section 0,

Types of execution profiles.

The following example illustrates how this feature can be useful:

An execution profile is configured to run every 12 hours on a specific device. Due to a problem with this device, it is necessary to immediately collect data from it. Use the **Execute Once Now** option for this one-time execution.

To manually activate one or more execution profiles on a device once:

1. Go to **Operations > Devices** to display the **All Devices** screen.
2. Select a device and click the **Execution** tab. A list of execution profiles for the device appears.
3. Select the requested execution profile(s) and click **Execute Once Now**.

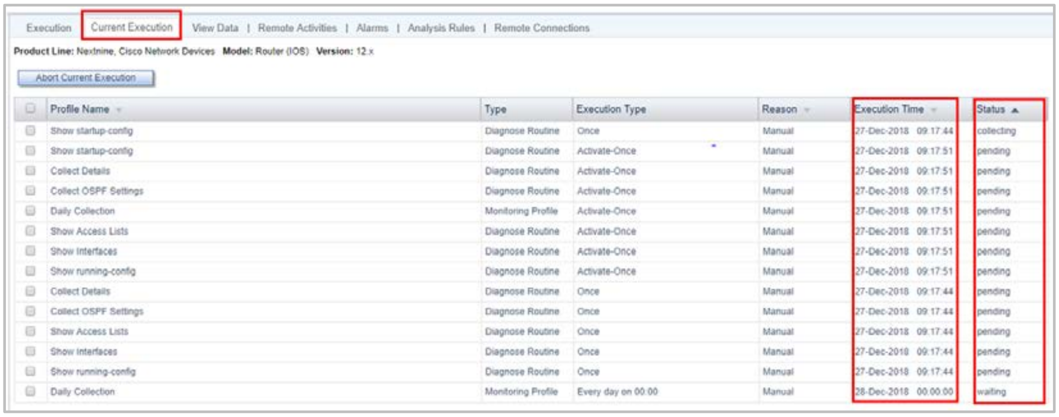
NOTE	Only those execution profiles that match the device model-version combination appear in the **Execution Profile Management** list.

   The VSE executes the selected execution profile(s) for the device once. A notification indicates that the operation was completed successfully.

4. To close the notification, click OK.

5.1.3 Execution profile status

You can monitor the current status of the execution profiles on a device using the **Current Execution** tab. To access the **Current Execution** tab, click on a device name in the device list under **Operations > Devices**. Table 5-1 details the meaning of the statuses and their execution times.


Execution
Current Execution
View Data | Remote Activities | Alarms | Analysis Rules | Remote Connections
Abort Current Execution

Product Line: Nextnine, Cisco Network Devices **Model:** Router (IOS) **Version:** 12.x

□	Profile Name	Type	Execution Type	Reason	Execution Time	Status ▲
□	Show startup-config	Diagnose Routine	Once	Manual	27-Dec-2018 09:17:44	collecting
□	Show startup-config	Diagnose Routine	Activate-Once	Manual	27-Dec-2018 09:17:51	pending
□	Collect Details	Diagnose Routine	Activate-Once	Manual	27-Dec-2018 09:17:51	pending
□	Collect OSPF Settings	Diagnose Routine	Activate-Once	Manual	27-Dec-2018 09:17:51	pending
□	Daily Collection	Monitoring Profile	Activate-Once	Manual	27-Dec-2018 09:17:51	pending
□	Show Access Lists	Diagnose Routine	Activate-Once	Manual	27-Dec-2018 09:17:51	pending
□	Show Interfaces	Diagnose Routine	Activate-Once	Manual	27-Dec-2018 09:17:51	pending
□	Show running-config	Diagnose Routine	Activate-Once	Manual	27-Dec-2018 09:17:51	pending
□	Collect Details	Diagnose Routine	Once	Manual	27-Dec-2018 09:17:44	pending
□	Collect OSPF Settings	Diagnose Routine	Once	Manual	27-Dec-2018 09:17:44	pending
□	Show Access Lists	Diagnose Routine	Once	Manual	27-Dec-2018 09:17:44	pending
□	Show Interfaces	Diagnose Routine	Once	Manual	27-Dec-2018 09:17:44	pending
□	Show running-config	Diagnose Routine	Once	Manual	27-Dec-2018 09:17:44	pending
□	Daily Collection	Monitoring Profile	Every day on 00:00	Manual	28-Dec-2018 00:00:00	waiting

Figure 5-1. Current execution tab

Table 5-1. Status of active execution profiles

Status	Meaning	Meaning of Execution Time column
collecting	The execution profile is currently collecting data from the device.	The time when the current execution started.
pending	The execution profile is queued and executes after other execution profiles using the same protocol on the same device complete running.	The time when the status of the execution became **pending**.
waiting	The execution profile is waiting for its next scheduled or triggered execution.	The time of the next scheduled execution.

5.1.4 What happens when an execution profile runs?

When an execution profile runs on a device, the VSE does the following:

1. Collects the specified data from the device, using the specified protocol and in accordance with the scheduling parameters.
2. Parses the raw collected data into individual properties.
3. Analyzes the parsed data by running analysis rules.

   NOTE

   Analysis rules are not applicable to data (for example, files) collected via FTP.

   If the VSE determines any of the data to be out of the range of acceptable values, it triggers an analysis rule violation.
4. Stores the execution results in the database.
5. If any analysis rule violations occurred, performs one or more actions in accordance with the definitions in the analysis rules.

   These actions may include:

   - Raising an alarm, which may be accompanied by an e-mail notification to the VSE users; for details, see section 5.1.4.1, E-mail notification of analysis rule violations

  - Running an additional execution profile (specified in the analysis rule) on the device

6. Sends an automatic report to the relevant Security Centers, when necessary.

5.1.4.1 E-mail notification of analysis rule violations

The definition of an analysis rule for a product line indicates which actions the VSE should take if the data violates a rule. One of the possible actions is to send an e-mail notification to the VSE user.

After the analysis of an execution result is completed, the VSE sends the VSE user an e-mail message with information about all violations marked by the Security Center.

The message includes the following information:

- Highest severity of all the analysis rule violations that occurred during the execution
- Execution profile name
- Device name
- How the execution profile was activated
- The time when the execution profile was scheduled to run
- The name and ID of the VSE
- Information about each marked violation

  The violations are grouped by objects. There are separators between violations of a single object and between objects.

- The name of the object for which the violation occurred
- The instance of the object (by listing the index values)
- The severity of the violation
- The details of the violation, including the property name and the actual values that were outside the acceptable range
- A description of the violation that cites the relevant analysis rule

5.2 Understanding execution results

Execution profiles are defined in the Security Center's Policy Builder and are then distributed to the VSEs as part of a Product Line. An execution profile instructs the VSE what information to collect from a device, how often to collect it, and when to start and end the execution. To enable an execution profile to collect data, the profile must be activated on a device. For further information, see section 5.1, Activating an execution profile.

After each run of an execution profile, an execution result is created and saved in the VSE database.

5.2.1 Types of execution profiles

The following execution types can be defined in the Policy Builder:

- **Once**
  These execution profiles are executed once as soon as they are activated.
- **Periodic**
  These execution profiles are set to run a specified number of times at specific intervals.
- **Scheduled**
  These execution profiles are set to run on a particular schedule, such as every day or every Monday and Wednesday, within a user-defined period such as from 7 p.m. to 11:59 p.m. During the times scheduled, they are run as periodic execution profiles.

  Execution results for scheduled execution profiles do not start until the scheduled start time.
- **On Trap**
  An SNMP Trap is a signal sent by the SNMP agent in a device, to indicate that an event has occurred on the device. If the trap is set to trigger one or more execution profiles, these profiles are activated in the device and begin collecting data.

5.2.2 Protocols for collecting data

Data can be collected from a device by using any protocols that are supported by the product line. The execution profile instructs the VSE:

- Which data to collect from the device
- How to collect each piece of data, including which protocol to use

The protocols supported by ICS Shield are:

- SNMP
- Telnet/SSH
- TL1

- FTP
- Syslog
- SNMP Trap
- WMI
- DBI
- OPC
- Custom protocol

> **NOTE**
>
> Syslog and SNMP Trap are event-driven protocols. Data collected by these protocols is preprocessed by a Perl script, and then stored in a cyclic buffer, from where it is retrieved by the execution profiles as required.
>
> For details about configuring the ports to which the VSE listens for Syslog and SNMP Trap events, as well as the size of both buffers, see section *Configuring the System Settings* in the *VSE Administrator Guide*

5.2.3 Execution profiles and system startup

When the VSE is started or restarted after a shutdown (either planned or unexpected), execution profiles that were activated by using either manual or auto activation retain their Active mode. Any execution profiles that were running on a one-time basis, either by manual execution (clicking **Execute Once Now**) or due to an analysis rule violation, will not resume or restart.

When a periodic execution profile is restarted, the counter that indicates how many executions have been done restarts.

5.2.4 What happens when an updated product line is received?

When an updated product line, which contains changes to an existing execution profile, is imported to the VSE, the newly imported execution profile replaces the existing one. If the existing execution profile is not active on any devices, the replacement takes place immediately. Otherwise, the replacement takes place after the existing execution profile completes its run.

If the updated execution profile is configured with a different model/version combination than the existing profile, the newly imported profile may not be able to run on some devices on which the existing profile was previously activated.

In such a case, you can update the model and version combination on the device (see section 4.4, Editing a device) to match that of the execution profile.

NOTE	Even if the newly imported execution profile collects different information than the existing one, existing execution results are not deleted.

5.3 Deactivating an execution profile

You may want to deactivate an execution profile while it is running. You can deactivate multiple execution profiles for a single device or deactivate all execution profiles on all devices. For details see section 5.4, Deactivating all active execution profiles

NOTE	When you deactivate an execution profile, this action affects both the currently running execution profile, which is stopped on the selected devices, and future executions that are prevented from running on these devices. To stop a currently active execution without affecting future executions, see section 5.7, Aborting an execution.

An execution profile running on a device is deactivated automatically when:

- You delete the device.
- You receive an updated version of the product line with an update to the execution profile. After the old version is deactivated, the new version is activated.
- The device becomes invalid (for example, because an updated product line was sent, and the model-version combination for the device is no longer included).
- The execution profile reaches its End condition (for example, it completed running the scheduled number of times).

To deactivate one or more execution profiles for a device:

1. Go to **Operations** > **Devices** to display the **All Devices** screen.
2. Select the device, and click the **Execution** tab.
3. Select the execution profiles that you want to stop and click **Deactivate**.

   The VSE deactivates the selected execution profile(s) for the device and informs you that it completed the remote activity successfully.
4. Click **OK**.

   The check mark in the **Active** column next to the selected execution profile disappears.

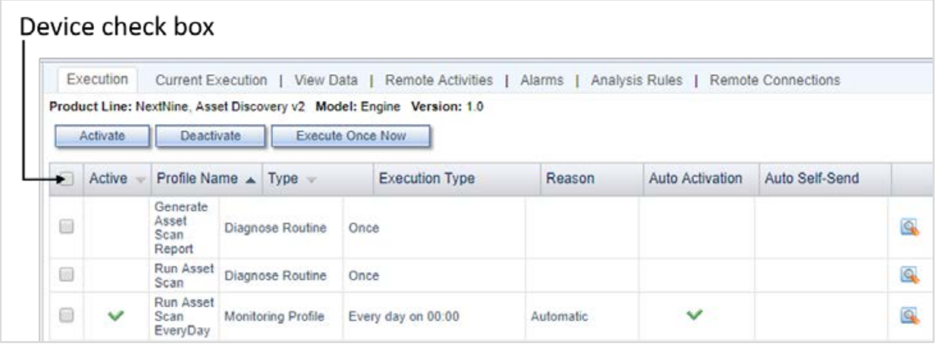
5.4 Deactivating all active execution profiles

The VSE allows you to abort or disable all active execution profiles. When you stop all active execution profiles, the VSE does the following:

- Aborts all execution profiles currently running on all devices for any reason, including:
  - Execution profiles triggered by analysis rule violations.
  - Execution profiles activated remotely from the Security Center.
- Deactivates all execution profiles that are active but are not currently running (such as scheduled or periodic executions).

To deactivate all active profiles:

1. Go to **Operations** > **Devices** to see a list of all monitored devices.
2. To deactivate all active profiles for a specific device, select the device checkbox under the **Execution** tab, and click **Deactivate**.


Device check box
Execution
Current Execution | View Data | Remote Activities | Alarms | Analysis Rules | Remote Connections
Activate
Deactivate
Execute Once Now

Product Line: NextNine, Asset Discovery v2 **Model:** Engine **Version:** 1.0

□	Active	Profile Name ▲	Type	Execution Type	Reason	Auto Activation	Auto Self-Send	
□		Generate Asset Scan Report	Diagnose Routine	Once				🔍
□		Run Asset Scan	Diagnose Routine	Once				🔍
□	✓	Run Asset Scan EveryDay	Monitoring Profile	Every day on 00:00	Automatic	✓		🔍

Figure 5-2. Device check box

A confirmation message appears.

3. Click **OK**.

5.5 Activating all automatic execution profiles

You can activate all automatic execution profiles by using the following methods:

- **Manually**

  You can activate one or more Execution Profiles manually, per product line or per device; for further details, see section 5.1, Activating an execution profile.

- **Automatically**

Any execution profile in a product line that was updated after the execution profile was stopped, and which was marked for automatic activation, is automatically activated.

NOTE	Automatic activation occurs only if this option is enabled in the VSE. For details, see section *Configuring the System Settings* in the *VSE Administration Guide*.

- **Globally**

  Clicking **Resume all Auto Profiles** activates all currently inactive execution profiles on the selected devices, which are marked for automatic activation, unless the auto-activation option of the VSE was disabled.

To activate all automatic profiles:

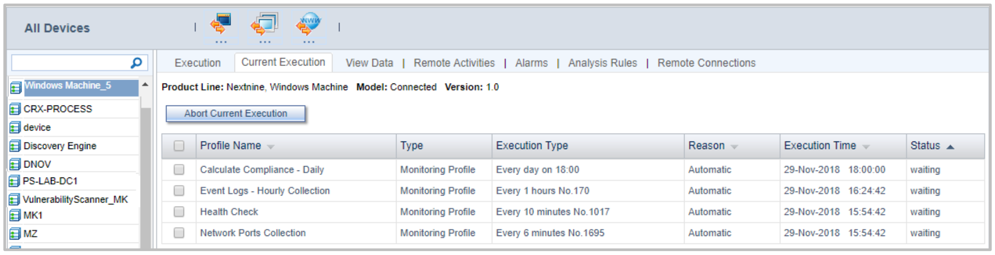
1. Go to **Operations** > **Devices** and select the **Execution** tab.
2. Ensure selecting the **All** option on the left.
3. Select one or more devices from the list.
4. Click **Resume All Auto Profiles**.
5. In the confirmation message that appears now, click **OK**.

   All currently inactive execution profiles, which were marked in the product line for automatic activation, are activated on the selected devices.

5.6 Viewing execution profile status

To view the status of all execution profiles for a device:

1. Go to **Operations** > **Devices**.
2. Select a device on the left and click the **Current Execution** tab to display a list of all current executions for the device.



Product Line: Nextnine, Windows Machine **Model:** Connected **Version:** 1.0

□	Profile Name	Type	Execution Type	Reason	Execution Time	Status
□	Calculate Compliance - Daily	Monitoring Profile	Every day on 18:00	Automatic	29-Nov-2018 18:00:00	waiting
□	Event Logs - Hourly Collection	Monitoring Profile	Every 1 hours No.170	Automatic	29-Nov-2018 16:24:42	waiting
□	Health Check	Monitoring Profile	Every 10 minutes No.1017	Automatic	29-Nov-2018 15:54:42	waiting
□	Network Ports Collection	Monitoring Profile	Every 6 minutes No.1695	Automatic	29-Nov-2018 15:54:42	waiting

Figure 5-3. Current execution tab

3. See the status of each of the execution profiles under the **Status** column.

For an explanation of the possible statuses, see section 5.1.3, Execution profile status.

5.7 Aborting an execution

When you abort an execution, it does not affect any executions scheduled to run in the future. For example, if there is a periodic execution profile that runs every two hours and is currently running, when you click **Abort Current Execution** under **the Current Execution tab**, you stop this current execution, but the execution profile will run again in two hours.

When you deactivate an execution profile, you abort the current execution (if there is one), and cancel any further scheduled executions (for information on deactivating execution profiles, see section 5.3, Deactivating an execution profile.

To abort an execution:

1. Go to **Operations** > **Devices** to display the **Device List** screen.
2. Select a device and click the **Current Execution** tab to display a list of all the currently active execution profiles for the device.
3. Select the execution you want to abort and click **Abort Current Execution**.
4. Click **OK** to confirm.

   The execution is aborted.

6. Managing Execution Results

After each run of an execution profile, an execution result is created and saved in the VSE database.

NOTE	For information about the VSE database, see section *The database quota* in the VSE Administrator Guide. For information on sending execution results to one or more Security Centers, see chapter *Managing Security Center* Information in the VSE Administrator Guide.

6.1 Searching for execution results

You can search for execution results by:

- Date and time the execution was performed
- Device Unique ID
- Product Line
- Activation reason
- Severity level

To search for execution results:

1. Go to **Operations** > **Devices** and click on the **View Data** tab.
2. On the device list on the left, click **All** to see results from all devices. Alternatively, click a specific device from the list to see results from that device.
3. To search for specific results, click **Filter** and define search criteria for finding the execution result(s) that you want to view, from the list on the table below.

Table 6-1. Search criteria for selecting execution results

Field	Description
During Last	Allows selecting execution results from the last X hours or days (in accordance with the time range selected from the drop-down list)
Between	Allows selecting start and end time for the search. Select the proper date by using the calendar and enter the appropriate hour.
Device	Allows selecting either all devices by leaving the default

Field	Description
	value **Any** or selecting the unique ID of a specific device.
Product Line	Allows selecting either all product lines, by leaving the default value **Any**, or selecting a specific product line.
Reason	The reason the execution was performed; you can select one or more reasons.
Severity	Allows selecting the minimum severity of the execution results you want to find (**Completed**, **All**, **Info+**, **Warning+**. **Error+** or **Critical**).
Maximum Rows	The maximum number of execution results to be displayed

4. Click **SEARCH**.

   The screen now displays a list of execution results that meet the search criteria.

6.2 Viewing execution results

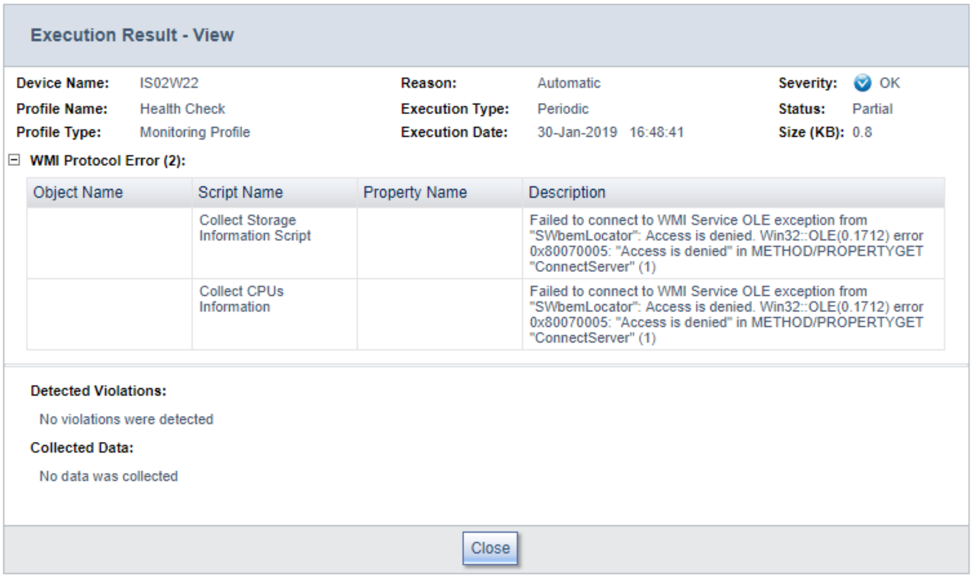
The list of results in the VSE includes a **Status** column, where the value can be one of the following:

- **Completed** The execution succeeded, and there were no errors.
- **Partial**: The execution succeeded, but there were some errors during execution.
  If the result value is **Partial**, you can click the link to view information about the execution and all the errors that occurred in the execution.
- **Failed**: The VSE could not connect to the device, and no data was collected.
  If the result value is **Error**, you can click the link to view the reason the VSE could not connect to the device.

To view execution results for a Partial or Error status:

1. Go to **Operations** > **Devices** > **View Data** tab.
2. Click the link in the **Status** column of the execution result whose details you wish to view, to display the **Execution Result-View** popup.

   This popup displays some general details about the execution, and a collapsible list of errors for each protocol used in the execution.



Execution Result - View

Device Name:	IS02W22	**Reason:**	Automatic	**Severity:**	✓ OK
Profile Name:	Health Check	**Execution Type:**	Periodic	**Status:**	Partial
Profile Type:	Monitoring Profile	**Execution Date:**	30-Jan-2019 16:48:41	**Size (KB):**	0.8

⊟ **WMI Protocol Error (2):**

Object Name	Script Name	Property Name	Description
	Collect Storage Information Script		Failed to connect to WMI Service OLE exception from "SWbemLocator": Access is denied. Win32::OLE(0.1712) error 0x80070005: "Access is denied" in METHOD/PROPERTYGET "ConnectServer" (1)
	Collect CPUs Information		Failed to connect to WMI Service OLE exception from "SWbemLocator": Access is denied. Win32::OLE(0.1712) error 0x80070005: "Access is denied" in METHOD/PROPERTYGET "ConnectServer" (1)

Detected Violations:

No violations were detected

Collected Data:

No data was collected

Figure 6-1. Execution Result-View for a specific execution

3. Expand any of the error lists to see a complete list of errors for that protocol, including the object name, script used, and property name.

4. When you are finished viewing the list of errors, click **Close**.

6.3 Deleting execution results

You may want to delete an execution result because you need the space on your hard disk, or because you no longer need the execution result.

NOTE	When the VSE DB Quota is reached, the VSE automatically deletes the oldest execution results and raises a system alarm, which can be accompanied by a notification sent to the VSE user. To change the size of the database quota, see section *The database quota* in the *VSE Administrator Guide*.

To delete execution results:

1. Go to **Operations** > **Devices** > **View Data** tab.
2. Select one or more execution results and click **Delete**.
3. Confirm the deletion operation.

   The VSE deletes the selected execution result(s) and informs you that the activity was performed successfully.

7. Working with Problem Reports

A problem report is a set of collections, to which the following information is added:

- Severity level
- The reason the report was sent
- A description of the problem (optional)

Problem reports are created in the VSE, either automatically or manually.

After a problem report is created, it is sent to the security center for analysis.

Problem reports describe problems occurring in one or more devices, and include data collected from these devices that may be related to the problem.

This chapter explains how to work with problem reports.

7.1 Overview of problem reports

There are several types of problem reports, as described in the following sections:

- 7.1.1, Automatic Reports
- 7.1.2, Periodic site reports
- 7.1.3, Manual reports

7.1.1 Automatic Reports

The VSE creates automatic reports and sends them immediately to master and subscriber Security Centers in the cases described below. This only occurs if the VSE is configured as follows:

- The method of communication with the Security Center is set to either **Communication Server** or **Direct**

NOTE	If the communication method is set to **Manual**, the report is created but you must send it manually.

- The option **Allow updated data to be sent to Security Center** is enabled

For details, see sections *Adding a new Security Center* and *Configuring application settings* in the Security Center Administrator Guide.

The VSE immediately creates and sends Automatic reports in the following cases:

- If a violation has been encountered during the execution of the execution profile.

- If the execution profile is marked **Auto Self-Send** (at the master Security Center) and the **Periodic Site Report** is not enabled (in the Configuration settings).

NOTE	If **Periodic Site Report** is enabled in the Configuration settings, the automatic report is not be sent immediately. It is added to the periodic report, which will then be sent at the next report interval.

7.1.2 Periodic site reports

Periodic site reports are accumulations of **Auto Self-Send** execution results that are created during the time interval (between 15 minutes and 24 hours) specified in the system settings.

If during the current time frame no results were generated, the VSE does not create a Periodic Site report for that time frame.

For details on how to enable the Periodic Site Report feature and set its time interval, see section *Configuring the System Settings* in the VSE Administrator Guide.

If the following conditions are met, the VSE creates a periodic site report once every specified time interval and sends it automatically to the master Security Center and subscribers:

- Both of the following check boxes are selected in the **Application** tab (**Administration & Security** > **Settings** > **Application**):
  - **Allow updated data to be sent to Security Center**
  - **Group Automatic Reports Into Periodic VSE Reports**
- The subscribed Security Centers use online communication.

7.1.3 Manual reports

If you detect a problem with one or more devices, you can manually create a new problem report and export or send it to the Security Center for analysis. For details, see section 7.2, Creating a new problem report.

When you create a new problem report, you can select to include the historical data with the report.

When using automatic communication methods, the new problem report is sent directly. If there are communication issues, or if the communication method is Manual, export the problem report to a file and then transport that file to the Security Center by whatever means you want, such as email or any storage media.

NOTE	If a device is invalid, it is marked in red in the list of devices. You can create new problem reports for invalid devices.

7.2 Creating a new problem report

To create a problem report:

1. Go to **Operations** > **New Problem Report** to display the **New Problem Report** screen.
2. Select the severity level in the drop-down list **Severity**, and fill in **Trouble Ticket**, and **Description**. See Table 7-1 for details.
3. Click **Select Devices** to display the **New Problem Report - Select Problematic Devices** dialog box.
4. From the list of devices, select any devices you want to include in the report and click **OK**.

   The devices you selected are added to the list of problematic devices. In addition, the execution results that will automatically be added to the new problem report are listed in the bottom left portion of the screen.

   By default, the new problem report:

   - Includes all execution results from the last 12 hours.
   - Includes details of the user who created the report, such as name and e-mail address
   - Is addressed to the master Security Center
5. If you want to change any of these defaults, click **Open Advanced**, and fill in the advanced information as shown in Table 7-1.

   If you chose to attach specific historical results, follow the instructions in the section 7.3, Selecting specific execution results to attach.

NOTE	If you edit the list of Problematic Devices via Select (Problematic Devices) after you select specific execution results, you must reselect the execution results based on the new list of devices.
6. To export the problem report as a file before sending it, proceed to step 8.

   To send the new problem report directly to the selected Security Center, click **Send**.

The following happens:

a. The new problem report is created. This may take a few minutes.

NOTE	If it takes the new problem report more than 40 seconds to be created, it will run in the background. To send this report later, you can search for it in the history and send it from there (see 7.4.3, Sending a problem report).

If the problem report takes more than 40 seconds to create, the creation continues in the background and you can keep working.

b. Selected execution results are attached to the new problem report.

c. The new problem report is sent to the Security Center.

d. The VSE notifies that the activity was performed successfully.

7. Click **OK.**

8. To export the new problem report to a file, click **Export**.

   The following happens:

   - The new problem report is created. This may take a few minutes.

NOTE	If it takes the New Problem Report more than 40 seconds to be created, it will run in the background. To export this report later, you can search for it in the history and export it from there (see section 7.4.4, Exporting a problem report).

   - Selected execution results are attached to the problem report.
   - After the problem report is ready to be exported, the **File Download** window appears.

9. Select **Save this file to disk** and use the **Save As** dialog box that appears to enter a name for the file; with the extension **.nnz** (internal format).

10. Navigate to the location where you want to save the file.

11. Click **Save** to save the new problem report to a new file with the name and location you indicated.

Table 7-1. Parameters for New Problem Report

Field	Comments
Problem Details	
Severity	Allows you to select a severity (Info, Warning, Error or Critical) for this new problem report. **Note** If the report contains an execution result with a higher severity than you choose, the system overrides your choice.
Trouble Ticket	The trouble ticket ID (optional), which the Security Center may assign to your problem for tracking it.
Description	A free-text description of the problem.
Execution Result Selection	**Note** Each new problem report must include at least one execution result.
Advanced information	
Attach historical data	
All results from last <> hours	Select this option to have the system attach all execution information from execution results made within the time frame you choose.
Select	Allows you to pick results information from specific execution results to attach to the Problem Report. See section 7.3, Selecting specific execution results to attach.
Customer Info	
First Name	The first name of the user who created the new problem report.
Last Name	
E-mail	
Phone	
Report Destination	
Send report to	The Security Center to which you want to send or export the new problem report.

Field	Comments
Problematic Devices	A read-only list of devices selected to include in the new report.

See also:

- Section 7.4.1, Finding a problem report in the database
- Section 7.4.2, Viewing a problem report
- Section 7.4.3, Sending a problem report
- Section 7.4.4, Exporting a problem report
- Section 7.4.5, Deleting problem reports

7.3 Selecting specific execution results to attach

The following instructions assume you are already in the process of creating a new problem report and are currently filling out the **Problem Report - Problem Details** form.

When you select results, the results show a list of execution results sorted by device. Each item in the list represents a single execution result from one device.

To select results to attach:

1. In the *Advanced* section of the **New Problem Report** form, under *Attach historical data*, select the button *Select Results*.
2. Click **Select Execution Result** to display the *New Problem Report - Search Execution Results* dialog box.
3. Fill in the search criteria.
4. Click **Search**.

   The **Problem Details – Select Execution Results** dialog box appears, with the list of results from the specified time range.

   For each execution result, you can see the information detailed in the table below.

   Table 7-2. Problem Details – Select Execution Results

Column heading	Description
Select	Checkbox for selecting execution results

Column heading	Description
Device Address	The name of the device on which the execution was done. If the device name is different than the IP address, then the IP address is shown in parenthesis next to the name.
Profile Name	The name of the execution profile used to collect the data **Note:** An internal execution profile called Violation Log is used to collect analysis rule violations for Periodic Site reports.
Type	The type of the execution profile (**Monitoring Profile**, **Corrective Action**, and **Diagnose Routine**).
Reason	The reason why the execution profile was run
Execution Type	The type of execution profile: Once, Periodic (Number X of Y), Scheduled, Trap, or Violation Log
Execution date	The date and time the execution profile was activated
Severity	The severity of the execution result, based on any analysis rule violations that occurred
Status	The status of the execution result (**OK**, **Partial,** or **Error**). If there were errors, you can click this link to open a list of execution result details, including all the errors that occurred.
Size (KB)	The size of the execution result. Next to the size is an icon you can click to see further information about the execution result.

5. Do one of the following:

   - Select the execution results you want to attach and click **OK**.

     The total size of all the execution results you chose to attach is listed next to the **Select** button in the **New Problem Report** form.

   - Click **Cancel** to close the form and return to the **New Problem Report - Problem Details** form.

   - If you did not find the execution results you wanted, click **Search Again** and redefine the search criteria.

6. To view the execution result, click 🔍.

7.4 Managing problem reports

When you create a problem report, the VSE database stores the report's metadata. If necessary, you can send or export the problem report again; the system uses the metadata to send the same execution results that were attached to the original problem report. You can also delete problem reports from the system when they are no longer necessary.

Managing Problem reports involves the actions described in the following sections:

- 7.4.1, Finding a problem report in the database
- 7.4.2, Viewing a problem report
- 7.4.3, Sending a problem report
- 7.4.4, Exporting a problem report
- 7.4.5, Deleting problem reports

7.4.1 Finding a problem report in the database

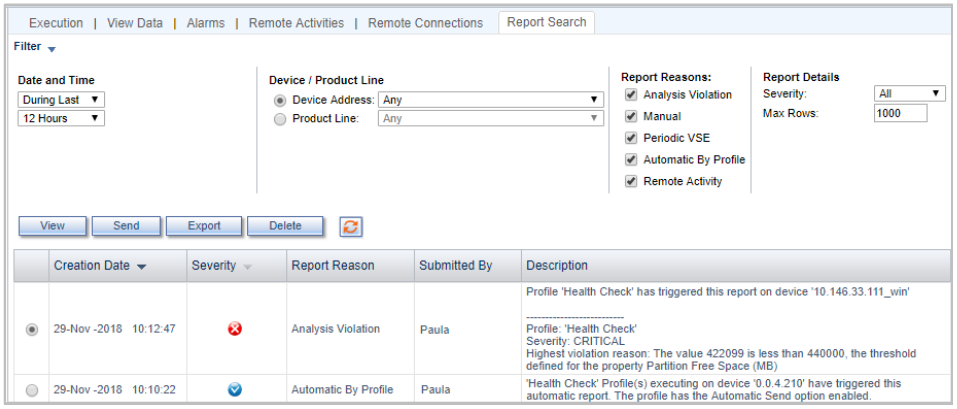
You can search for problem reports based on any combination of the following parameters:

- When the report was created
- Trouble ticket ID
- Severity
- Report reason
- Device Unique ID or Product Line

> **NOTE** The search results are limited to 1000 problem reports. If more problem reports matched the search criteria, they are not listed, and you are instructed to search again using more specific criteria to limit the number of search results.

To find a problem report in the database:

1. Go to **Operations** > **Devices**, and click the **Report Search** tab.


Execution | View Data | Alarms | Remote Activities | Remote Connections
Report Search
Filter
View
Send
Export
Delete

Date and Time

During Last ▼

12 Hours ▼

Device / Product Line

● Device Address: Any ▼

○ Product Line: Any ▼

Report Reasons:

☑ Analysis Violation

☑ Manual

☑ Periodic VSE

☑ Automatic By Profile

☑ Remote Activity

Report Details

Severity: All ▼

Max Rows: 1000

	Creation Date	Severity	Report Reason	Submitted By	Description
●	29-Nov -2018 10:12:47	☒	Analysis Violation	Paula	Profile 'Health Check' has triggered this report on device '10.146.33.111_win' ------------------------- Profile: 'Health Check' Severity: CRITICAL Highest violation reason: The value 422099 is less than 440000, the threshold defined for the property Partition Free Space (MB)
○	29-Nov -2018 10:10:22	✓	Automatic By Profile	Paula	'Health Check' Profile(s) executing on device '0.0.4.210' have triggered this automatic report. The profile has the Automatic Send option enabled.

Figure 7-1. Report Search tab

2. Optionally, search for specific problem reports by clicking **Filter** and defining the search criteria.

3. Click 🔄.

   The screen refreshes and shows a list of problem reports that meet all search criteria. The list is sorted by date.

7.4.2 Viewing a problem report

To view a problem report:

1. Go to **Operations** > **Devices**, and click the **Report Search** tab.

2. Optionally, define the search criteria under the **Filter** option.

   The **Search Results** screen appears, displaying a list of problem reports that meet all search criteria. The list is sorted by date.

3. Select the problem report you want to view.

4. Click **View** to display the **Problem Reports View**, which contains details of the selected problem report.

5. To display a list of execution results for a device in the problem report, click the Unique ID of the requested device in the **Device Unique ID** column.

   The list of execution results for the device appears at the bottom part of the screen.

7.4.3 Sending a problem report

You need to manually send/export newly created problem reports in any of these circumstances:

- You are using manual or off-line communication to communicate with one of the Security Centers to which the problem report must be sent
- You are using online communication to communicate with a Security Center, but encounter communication issues.
- You may want to resend or reexport an existing problem report, if the Security Center did not receive it.

When using automatic communication methods, you send the problem report directly. If there are communication problems, or if the communication method is manual, you export the problem report to a file and then transport that file to the Security Center manually.

When you send or export a report, the data sent is a snapshot of the current state of the report’s data in the database; therefore, when a report is resent or re-exported, any execution results and devices that were deleted since the report's creation will be missing. If all the execution results for a problem report were deleted, the problem report itself will be deleted from the database the first time you try to resend or re-export it.

NOTE	You cannot change the content of an existing problem report, that is, you cannot change the description or add execution results to it. If any execution results were deleted, they still appear in the list of attached execution results, but you cannot access them, nor can the Security Center to which you send the new problem report.

To send a problem report:

1. Go to **Operations** > **Devices**, and click the **Report Search** tab.
2. Optionally, define the search criteria under the **Filter** option.

   The **Search Results** screen appears, displaying a list of problem reports that meet all search criteria. The list is sorted by date.
3. Select the problem report you want to send and click **Send**.
4. Use the **Send Report** dialog box to select the Security Center to which you want to send the problem report.
5. Click **Send**.

   The problem report is sent to the Security Center and a message is displayed, stating that the activity was performed successfully.

6. Click **OK**.

7.4.4 Exporting a problem report

In certain configurations, the VSE and Security Center may not be constantly connected, in which case you need to manually export problem reports and then import them to the Security Center.

To export a problem report:

1. Go to **Operations** > **Devices**, and click the **Report Search** tab, as detailed in the previous sections.
2. Select the problem report you want to export and click **Export**.
3. Use the **Export Report** screen to select the Security Center to which you want to transfer the report export.
4. Click **Export**.
5. Use the **Save As** dialog box to navigate to the requested location. When done, click **Save** to save the file.
6. Click **Close** to close the screen.

NOTE	When you export a problem report, the Security Center ID is saved within the file. You cannot transfer this file to a different Security Center, because each Security Center only accepts files with its own ID number.

7.4.5 Deleting problem reports

You may want to delete problem reports that are no longer required. In most cases, you can also delete the following on a regular basis:

- Problem reports that have the *Auto by Profile* reason.
- Problem reports with the severity level of Info, and possibly also problem reports with the severity level of Warning

NOTE	When the maximum number of problem reports is reached, the system automatically deletes the oldest problem reports and raises a system alarm, which can be accompanied by a notification sent to the VSE user. For details, see section *The Database Quota* in the VSE Administrator Guide.

8. Using the Control Panel

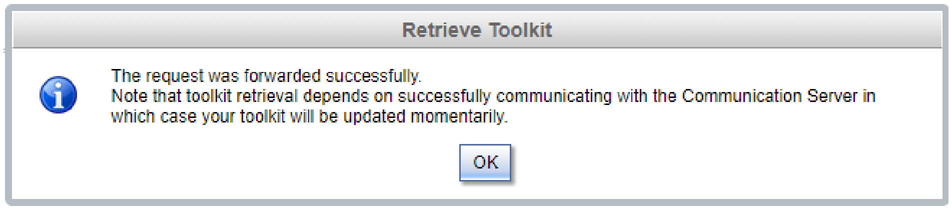
This chapter describes the operations accessible from the **Operations** > **Control Panel** tab.

8.1 Retrieving toolkits manually

To retrieve a toolkit manually (on demand):

1. Go to **Operations** > **Control Panel**.
2. Click the toolkit (🛠) icon.

   If the toolkit retrieval completed successfully, the message shown below appears.



Retrieve Toolkit

The request was forwarded successfully.
Note that toolkit retrieval depends on successfully communicating with the Communication Server in which case your toolkit will be updated momentarily.

Figure 8-1. Retrieve toolkit message

8.2 Switching between offline and online modes

The VSE can work in the following modes:

- **Online**

  Continuous in-out communication with Communications Server and Security Center. Reports are sent automatically.

- **Offline**

  A special mode for a VSE that is defined and presented in the Security Center but is deliberately restricted from sending any reports or data to the Security Center.

  For example, if a VSE is located in an organization (such as a nuclear facility) whose regulations forbid an ongoing connection to an external network, it can be set to work in Offline mode, which still allows monitoring the devices but gives the organization total control about which collected data is exported and when. The exported data can then be imported manually to the Security Center.

To switch the VSE to Offline Mode:

1. Go to **Operations** > **Control Panel**.

2. Click 🌐 next to **Change Online\Offline mode**.

   When prompted to confirm the action, click **OK**.

8.3 Uploading script files

The Script Files section of the Control Panel allows uploading files that supplement the data collection scripts, such as Perl libraries.

To upload script files:

1. Go to **Operations** > **Control Panel**.
2. Click 🌐 under the **Script Files** section.
3. Use the *Script Files* dialog box that opens now to upload files, by either dragging the files to the box or clicking Add Files.
4. Click Start Upload.
5. When the upload operation is complete, click **Done**.

9. Remote Activities

This chapter describes remote activities and connections in the VSE.

Specifically, the chapter deals with:

- Understanding and working with remote activities in the VSE.
- Understanding and working with remote connections from the VSE user interface.

  By default, the VSE is configured to automatically approve the execution of remote activities. This setting can be modified by a VSE administrator.

9.1.1 What are remote activities?

In the context of the ICS Shield system, a remote activity is a task sent by the master Security Center to one or more VSEs requesting that the VSE performs actions such as the following:

- Enabling remote access to a specific device
- Running an execution profile on or more devices
- Distributing a product line
- Distributing software
- Sending files to, and getting files from, the VSE

If you have a supervisor role, you can use the **Remote Activities** screen to view details of remote activities, to approve or reject remote activities, or to abort running remote activities.

9.1.1.1 Diagnose/Fix

The Security Center sends a Diagnose or Fix remote activity and requests the VSE to execute an existing execution profile. If the remote activity is approved, the VSE runs the specified execution profile.

Viewing execution profile information can help you decide whether to approve a Diagnose or Fix remote activity. For instructions, see section 9.1.3.7, Viewing execution profile information.

9.1.1.2 Distribute Product Line

The Security Center sends the remote activity *Distribute a Product Line* to the VSE, to install or update a product line on the VSE. If the remote activity is approved, the VSE imports the product line to the VSE database.

Viewing product line information can help you decide whether to approve a Distribute Product Line remote activity. For instructions, see section 9.1.3.6, Viewing product line information .

9.1.1.3 Distribute Software

The Security Center sends the remote activity *Distribute Software* to the VSE, to install a software module on the VSE. If the remote activity is approved, the VSE imports the software module and installs it on the appropriate device.

9.1.1.4 Send File

The Security Center sends a *Send File* remote activity to the VSE to store a file on a specific device. If the remote activity is approved, the VSE stores the file in the specified directory on the device.

9.1.2 Remote Access

The Security Center sends a *Remote Access* remote activity, to remotely access, configure, or troubleshoot either a VSE or a device.

The workflow for getting remote access is as follows:

1. The Security Center sends to the VSE a Remote Access remote activity, which appears in the list under the **Remote Activities** tab **(Operations** > **Devices** > **Remote Activities**).
2. In the left pane either select **All** to see remote activities for the VSE itself or select a specific device to see remote activities associated with this device.

   Unless the VSE is configured to automatically approve remote activities of type Remote Access, you need to manually approve or reject the remote activity.

   For information on automatically or manually approving or rejecting remote activities see 9.1.3.8, Approving or rejecting remote activities.
3. The Security Center receives a notification stating whether the remote activity was approved or rejected and by whom.
4. If you approved the remote activity (either automatically or manually), the Security Center user can remotely access the VSE or the requested device at any time, as long as the remote activity has not completed executing.

NOTE	The VSE and the Security Center exchange information via a secure connection (SSL over TCP).

The Remote Access remote activity ends when one of the following occurs:

- The remote activity times out.
- The remote activity is aborted by a VSE user; for details, see section 9.1.3.9, Aborting remote activities.
- An active connection for the remote activity is terminated by a VSE user.

You can track the state of the remote activity in the Remote Activities screen; for details, see section 9.1.3.2, Remote activity states.

9.1.3 Using the Remote Activities screen

The **Remote Activities** screen is used to view, approve, reject, or abort all types of remote activities. In addition, this screen is used for supervising VNC remote access sessions.

9.1.3.1 Opening the Remote Activities screen

Use the following procedure to open the **Remote Activities** screen. All subsequent procedures in this chapter start from the **Remote Activities** screen.

To open the Remote Activities screen:

- Go to **Operations** > **Devices** > **Remote Activities** tab**.**
  The list of **Remote Activities** appears on the right side of the screen, displaying a list of all remote activities (all remote activity types, all remote activity states, and remote activities for all devices) for the selected period (by default: past seven days).

The **Remote Activity** screen provides the following information for each remote activity:

- **State**; for details, see section 9.1.3.2, Remote activity states
- **Severity**; for details, see section 9.1.3.3, Remote activity severity
- **Type**
- **Device Name**
- **Brief**
- **Requested by**
- **Arrival Date** (the date the remote activity arrived at the VSE)

If you need more information about a specific remote activity, you can view details of that remote activity using the procedure described in section 9.1.3.5, Viewing remote activity details.

9.1.3.2 Remote activity states

Each remote activity has a state, which is displayed in the State column and indicates the remote activity's current life cycle stage. The remote activity state is represented by one of the icons displayed below.

Table 9-1. Remote activity states

State	Icon	Description
Waiting for Approval		Waiting for manual approval.
Scheduled		The activity was approved but has not yet been executed.
Executing		The activity is now being executed.
Finished		The remote activity ended due to any of the following reasons: • The activity completed its execution • The activity timed out before the execution was completed • The was rejected or aborted by the VSE user

9.1.3.3 Remote activity severity

Each remote activity is assigned a **Severity** level when it is finished.

The severity level may be one of the following:

- **Empty** (no severity description)
- **Info**
- **Warning**
- **Error**
- **Critical**

The severity is determined as follows:

- For remote activities of all types, if something prevents the remote activity from starting, the activity state is immediately changed to **Finished**, and the remote activity severity is immediately changed to **Error**.

  A remote activity can be prevented from starting due to any of the following reasons:

  - The VSE administrator rejected the remote activity
  - The VSE administrator terminated the remote connection
  - The VSE administrator aborted the remote activity

- For all remote activities other than Diagnose and Fix, if the remote activity was approved and ran successfully, the severity field remains empty.
- For Diagnose or Fix remote activities that completed executing, the severity of the remote activity is set to the highest severity of all of the executions results.

9.1.3.4 Filtering the list of remote activities

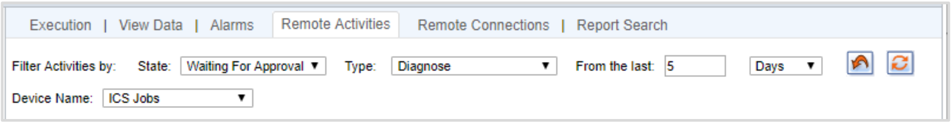
You can filter the list by any of the following:

- Remote activity state
- Remote activity type
- Time slot (from the last specified number of minutes, hours, or days)
- Device (from a list of devices defined in the VSE, including the VSE itself)

The filters are located at the top of the workspace.

To filter the remote activity list:

1. In the **State** field, select the state of the remote activities you want to display.
2. In the **Type** field, select the type of remote activities you want to display.
3. In the **From the last** field, select the time range for which you want to display remote activities.
4. Use the **Device Name** field to select the name or IP address of the requested device.


Execution | View Data | Alarms | Remote Activities | Remote Connections | Report Search

Filter Activities by: State: Waiting For Approval ▼ Type: Diagnose ▼ From the last: 5 Days ▼

Device Name: ICS Jobs ▼

Figure 9-1. Filtering the Remote Activities list

9.1.3.5 Viewing remote activity details

You can view the details of individual remote activities in the remote activity list.

To view the remote activity details:

1. Select the remote activity you want to view.
2. Click **View** or alternatively, click the activity icon in the **State** column to display the **Remote Activity Details** pop-up.

   The information provided depends on the remote activity you are viewing.
3. Use this screen to see the following information:
   - **Type**

     If you are viewing a Diagnose or Fix remote activity, this field contains a link to detailed execution profile information. For information on viewing execution profile details, see section 9.1.3.7, Viewing execution profile information.
   - **State**
   - **Severity**
   - **Result Message**: an error description, if an error occurred (only appears in Finished remote activities)
   - **Description**: description inserted by the Security Center user
   - **Last State Change**: date and time when the remote activity's state last changed
   - **Arrival Date**: date and time when the remote activity arrived at the VSE
   - **Submitted by**: name of the Security Center user who created the remote activity
   - **Approved (Rejected) by**: name of the VSE user who approved/rejected the remote activity, if the remote activity was handled manually
   - **Product Line**: name of Product Line (does not appear in Distribute a Software remote activities)
   - **Vendor**: name of vendor (does not appear in Distribute a Software remote activities)

- **Session Timeout (hours)**: The default timeout for a remote access activity is 6 hours.
- **Application**
- **Device Name**
- **Device Address**
- **Model**
- **Version**

If you are viewing the remote activity **Distribute a Product Line**, the Product Line Content area appears at the bottom of the screen. For information on viewing Product Line details, see section 9.1.3.6, Viewing product line information.

9.1.3.6 Viewing product line information

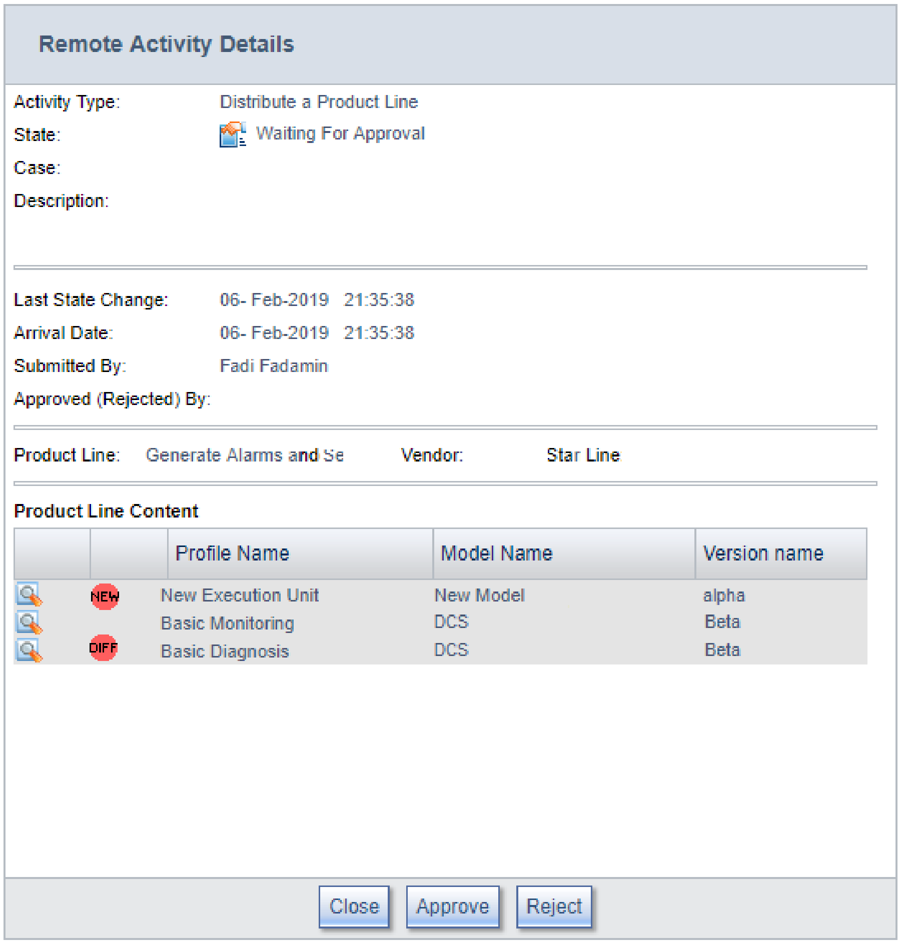
Viewing product line information for a Distribute a Product Line remote activity can help you decide whether to approve the remote activity. This information includes details of each execution profile variation and indicates whether it already exists in the VSE.

Viewing information for a remote activity of type **Distribute a Product Line** is only possible before the remote activity is approved. After approving the remote activity, the Remote Activities screen no longer displays this information; however, you can view product line information through the Product Line view or the device.

To view Distribute a Product Line information:

1. Select the Distribute a Product Line remote activity you want to view.
2. Click **View Details**.

   The **Remote Activities Details** web page for the selected activity opens. The display includes the **Product Line Content** area, which lists all execution profiles, including all variations.



Remote Activity Details

Activity Type: Distribute a Product Line
State: Waiting For Approval
Case:
Description:

Last State Change: 06- Feb-2019 21:35:38
Arrival Date: 06- Feb-2019 21:35:38
Submitted By: Fadi Fadamin
Approved (Rejected) By:

Product Line: Generate Alarms and Se Vendor: Star Line

Product Line Content

		Profile Name	Model Name	Version name
🔍	NEW	New Execution Unit	New Model	alpha
🔍		Basic Monitoring	DCS	Beta
🔍	DIFF	Basic Diagnosis	DCS	Beta

Figure 9-2. Remote Activity Details tab

NOTE	The Product Line Content area only appears if you have not yet approved the remote activity.

You can see the following information for each execution profile:

- Whether the execution profile already exists in the VSE.

  This is indicated by an icon:

  - NEW : This execution profile is new.
  - DIFF : A different version of this execution profile exists on the VSE.

If there is no icon, the execution profile is identical to an existing execution profile in the VSE.

3. For more detailed information on an execution profile, click the 🔍 icon.

The **Profile Content** web page dialog appears.

You can see the following details for the execution profile:

- **Profile Name**
- **Profile Type**: Diagnostic, Monitoring, or Corrective Action
- **Execution Type**: Once, Periodic, Scheduled, or On Trap
- **Product Line**
- **Vendor**
- **Auto Self-Send**: Whether the Security Center set the execution profile to automatically send the execution result to the master and subscribed Security Centers
- **Auto Activation**: Whether the Security Center set the execution profile to be automatically activated on any devices which have the appropriate model/version combination
- **Model Name** for which the execution profile is defined
- **Model Version** for which the execution profile is defined

All Scripts appear at the bottom of the web page dialog, in the order that they appear in the execution profile. You can see the following for each Script:

- Script name
- Protocol used (for example, Telnet/SSH or SNMP)
- Command type (PowerShell, Perl Script, VBScript, Command Line, get scalar, or get column)
- A box containing the Script itself

9.1.3.7 Viewing execution profile information

Viewing execution profile information for a Diagnose or Fix remote activity can help you decide whether to approve the remote activity.

To view execution profile information:

1. Select the Diagnose or Fix remote activity whose information you would like to view.
2. Click **View** to display the Remote Activities Details web page.

3. Proceed as detailed in step 2 and onwards of section 9.1.3.6.

9.1.3.8 Approving or rejecting remote activities

Each remote activity must be approved at the VSE level before it is executed.

There are two types of approval or rejection:

- Automatic approval/rejection
- Manual approval/rejection by a VSE administrator or supervisor

Unless the VSE is configured to automatically approve or reject a specific type of remote activity, each remote activity must be reviewed and manually approved or rejected it.

For information on enabling or disabling automatic remote activity approval, see section *Overview of policy management* in the VSE Administration Guide.

To manually approve or reject a remote activity:

1. Select the requested remote activity(s). The remote activity must have the state of *Waiting for Approval*.
2. Perform either of the requested operations:
   - Click **Approve**.

     The remote activity state changes to Scheduled, Executing or Finished. A success message appears.
   - Click **Reject**.

     The remote activity state changes to **Finished** and the remote activity severity changes to **Error**.
3. Click **OK**. The Security Center receives notification that the remote activity was approved or rejected.

9.1.3.9 Aborting remote activities

You can abort remote activities with the state **Scheduled** or **Executing**.

To abort a remote activity:

1. Select the requested remote activity(s). The remote activity must have the state of **Scheduled** or **Executing**.
2. Click **Abort**. A success message appears.

3. Click **OK**. The remote activity state changes to **Finished** and the remote activity severity changes to **Error**.

The Security Center receives notification that the remote activity was aborted.

9.2 Remote Connections

ICS Shield allows communication between the master Security Center, the VSE, and its connected devices via a secure communication tunnel.

The VSE allows:

- Administrator/operators to view all active remote connections and their details.
- Administrators to close any active or available connection directly from the VSE Remote Connections screen.
- Administrators/supervisors to supervise VNC connections to the VSE.

To perform the requested operation for a remote connection:

1. Go to **Operations** > **Devices**, and click the **Remote Connections** tab.

   The **Remote Connections** screen opens and displays a list of all active remote connections.

   You can see the following information:

   - **Device Name**
   - **Device Address**
   - **Protocol**
   - **Port**
   - **Requested by -** enter the Security Center user name
   - **Connection Time –** enter the time the connection started
   - **Ending Time** – the expected time when the connection times out

NOTE	The columns for Device Name and Device Address are only displayed when **All** is selected in the left pane, where the devices are listed.

2. Select the entry whose remote connection details you would like to view and process.
3. Click the relevant button:

- To see the details of the remote connection, click **View Details** to open the **Remote Activity Details** screen.
- To supervise the remote connection (administrators and supervisors only), click **Supervise** to open the **Remote Activities – Supervise** screen

NOTE	This is only relevant to the Virtual Network Computing (VNC) protocol. Any attempt to supervise a non-VNC connection will result in error message.

- To terminate the remote connection (Administrators only), click **Terminate** to open the **Remote Activities – Terminate screen**.

NOTE	When you terminate the active connection, the remote activity is aborted. As a result, the remote activity state will change to **Finished** and the severity will change to **Error**. Any Security Center user who wants to remotely reconnect to the device needs to create a new remote activity.

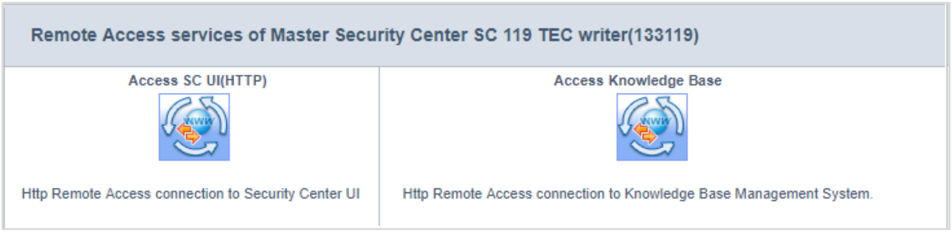
10. Reverse Tunnel

The reverse tunnel is a licensed feature, which enables a secured connection initiated by the VSE to the Security Center network.

NOTE	To connect to a remote service, users must have the required authentication credentials.

To use reverse tunneling:

1. Go to **Operations** > **Remote Access**.



Remote Access services of Master Security Center SC 119 TEC writer(133119)

Access SC UI(HTTP)	Access Knowledge Base
Http Remote Access connection to Security Center UI	Http Remote Access connection to Knowledge Base Management System.

Figure 10-1. Remote Access

2. Select the required protocol and launch the reverse tunnel

NOTE	In addition to the predefined remote access protocols shown above, you can configure proprietary protocols for establishing a reverse tunnel. Such protocols can be used, for example, to receive updates from sources such as anti-virus software and Windows Server Update Services (WSUS). To configure a custom protocol, contact Customer Support.

11. Operational Log

The operational log, accessible by going to **Operations** > **Operational Log,** stores a list of system events.

Activities in the log may include:

- Failure to establish communication with a Security Center
- Issues encountered while creating, removing, and updating devices and product lines
- Issues encountered while collecting data from devices
- Issues encountered while managing reports
- Failure to open the Syslog and SNMP Trap ports
- File distribution errors

For a full list of log events, see Appendix A, Operational Log Events.

You can determine the severity of activities that trigger notifications to the VSE administrator. For details, see the chapter *VSE Health Monitor* in the *VSE Administrator Guide*.

Appendices

This guide includes the following appendices:

- A, Operational Log Events

A Operational Log Events

The table below lists all entries that the operational log may contain, along with their severity.

Table A-1. Log events

Cause	Severity	Message
General Failure	Error	$site_name : General failure
Site Server set to Offline mode.	Warning	VSE $site_name set to Offline mode
Site Server set to Online mode.	Warning	VSE $site_name set to Online mode
No KeyStore detected	Warning	No Keystore detected
Security Center definition change	Warning	Security Center $Security_center definition has changed
Add Device (External / UI / internal)	Info	Device $Device_name:$Device_ip has been added
Edit Device (External / UI/ internal)	Warning	Device definition $Device_name:$Device_ip has been changed
Delete Device (External / UI/ internal)	Warning	Device $Device_name:$Device_ip has been deleted
Remote Access Request (except VNC)	Info	User $originator_User requests Remote Access using $protocol to $Device_name:$Device_ip
Remote Access Request (VNC only)	Info	User $originator_User requests Remote Access using $protocol to $Device_name:$Device_ip

Cause	Severity	Message
Diagnose	Info	User $originator_User want to run a diagnose routine on $Device_name:$Device_ip
Fix	Info	User $originator_User want to apply a fix on $Device_name:$Device_ip
Send file	Info	User $originator_User wants to put a file to $Device_name:$Device_ip
Get File	Info	User $originator_User wants to get a file from $Device_name:$Device_ip
SW distribution	Info	User $originator_User wants to install software on $Device_name:$Device_ip
Run Command Request	Info	User $originator_User wants to run a command on $Device_name:$Device_ip
Site Server is going down	Warning	Site Server $site_name shutting down
Site Server is starting	Info	Site Server $site_name staring. Operation System:$oper_sys Java Version:$java_version
License Limit for Devices	Error	Site Server $site_name has reached maximum allowed Devices. Please extend the license.
Protocol settings of Product Line has changed	Info	Product line definitions of $pl_name have been changed
Import Product Line	Info	Product line $pl_name has been updated
Delete Product Line	Warning	Product line $pl_name has been deleted
Change registration Info (operational, audit log only)	Warning	Site registration information has been changed

Cause	Severity	Message
Security Policy has changed	Warning	Security Policy has changed
Site Server configuration changed	Warning	Site Server configuration changed
Execute Profile (local) – [by User]	Info	Execution Profile(s) were executed on $Device_name:$Device_ip
Deactivate Script (by User)	Info	Execution Profile(s) were deactivated on $Device_name:$Device_ip
Abort Profile (by User)	Warning	Execution Profile(s) were aborted on $Device_name:$Device_ip
Send New Report	Info	New report has been sent
Send Report	Info	Report has been sent
Export New Report	Info	New report has been exported
Export Report	Info	Report has been exported
Delete Report	Info	Report has been deleted
Delete Data Collection	Info	Data collection(s) were deleted
Add User	Info	User $User_name has been added
Edit User	Warning	User definitions $User_name has been changed
Delete User	Warning	User definitions $User_name has been deleted
Import File	Info	A file has been imported
New certificate added to the Site Server	Info	A new SSL certificate has been registered

Cause	Severity	Message
Certificate has removed from the Site Server	Info	SSL certificate has been removed
Proxy Configuration has changed	Warning	Proxy Configuration has changed
Add Device with Hostname (External / UI / internal)	Warning	Device $Device_name:$Device_ip has been added. Note: In order for SNMP traps to be received from this device, its address must be set in IP format and not in host name format
Edit Device with Hostname (External / UI/ internal)	Warning	Device definition $Device_name:$Device_ip has been changed. Note: In order for SNMP traps to be received from this device, its address must be set in IP format and not in host name format
Remote VSE definition change	Warning	Remote VSE $remote_vse definition has changed
Invalid license or license not exist	Error	Invalid license or license not exist
Wrong Java version	Warning	Unexpected Java version $java_version detected
Security Center connection lost (UP or NR) - Set	Error	Security Center $Security_center not responding
Security Center connection lost (UP or NR) - Clear	Clear	Security Center $Security_center responding

Cause	Severity	Message
Failed to connect to Communication Server (NR or IF) - Set	Error	Connectivity to Security Center $Security_center has been lost
Failed to connect to Communication Server (NR or IF) - Clear	Clear	The connection to Security Center $Security_center has been established
Failed to send data (direct, failed to put to CS) - Set	Error	Failed to send data to Security Center $Security_center
Failed to send data (direct, failed to put to CS) - Clear	Clear	Successfully sent data to Security Center $Security_center
Failed Connect To Device (SNMP) - Set	Error	Failed to connect to $Device_name:$Device_ip using $protocol
Failed Connect To Device (SNMP) - Clear	Clear	Successfully established connection to $Device_name:$Device_ip using $protocol
Failed Connect To Device (Telnet) - Set	Error	Failed to connect to device using $protocol protocol to $Device_name:$Device_ip
Failed Connect To Device (Telnet) - Clear	Clear	Successfully established connection to device $Device_name:$Device_ip using $protocol protocol
Failed Connect To Device (FTP) - Set	Error	Failed to connect to device using $protocol protocol to $Device_name:$Device_ip

Cause	Severity	Message
Failed Connect To Device (FTP) - Clear	Clear	Successfully established connection to device $Device_name:$Device_ip using $protocol protocol
Failed Connect To Device (TL1) - Set	Error	Failed to connect to device using $protocol protocol to $Device_name:$Device_ip
Failed Connect To Device (TL1) - Clear	Clear	Successfully established connection to device $Device_name:$Device_ip using $protocol protocol
Remote connection is established	Info	Remote connection to device $Device_ip using $protocol protocol has been established
Remote connection is closed	Warning	Remote connection to device $Device_ip using $protocol protocol has been closed
Connectivity with the tunneling server has failed	Error	Remote Access: Failed to connect to Communication Server
Site Server in Debug Mode	Warning	Site Server working in debug mode
Recover file from backup	Error	The Site Server recovery the $file_name configuration file that represent the $file_type from the backup file
Recover file from default	Error	The Site Server recovery the $file_name configuration file that represent the $file_type and set the default values
Deleted corrupted file	Error	The Site Server delete the corrupted $file_name configuration file that represent the $file_type
SNMP storm	Error	The Site Server detects the SNMP trap storm at a rate of $snmp_traps_rate traps per 1 seconds for the duration of $duration_of seconds

Cause	Severity	Message
Failed to Login to Device (Telnet) - Set	Error	Failed to connect to device during authentication using $protocol protocol to $Device_name:$Device_ip
Failed to Login to Device (Telnet) - Clear	Clear	The connection to device using $protocol protocol to $Device_name:$Device_ip established
Failed to Open Connection to Device (Telnet) - Set	Error	Failed to open connection to the device using $protocol protocol to $Device_name:$Device_ip
Failed to Open Connection to Device (Telnet) - Clear	Clear	The connection to device using $protocol protocol to $Device_name:$Device_ip established
Failed to Login to Device (TL1) - Set	Error	Failed to connect to device during authentication using $protocol protocol to $Device_name:$Device_ip
Failed to Login to Device (TL1) - Clear	Clear	The connection to device using $protocol protocol to $Device_name:$Device_ip established
Failed to Open Connection to Device (TL1) - Set	Error	Failed to open connection to the device using $protocol protocol to $Device_name:$Device_ip
Failed to Open Connection to Device (TL1) - Clear	Clear	The connection to device using $protocol protocol to $Device_name:$Device_ip established
Failed to Login to Device (FTP) - Set	Error	Failed to connect to device during authentication using $protocol protocol to $Device_name:$Device_ip

Cause	Severity	Message
Failed to Login to Device (FTP) - Clear	Clear	The connection to device using $protocol protocol to $Device_name:$Device_ip established
Failed to Open Connection to Device (FTP) - Set	Error	Failed to open connection to the device using $protocol protocol to $Device_name:$Device_ip
Failed to Open Connection to Device (FTP) - Clear	Clear	The connection to device using $protocol protocol to $Device_name:$Device_ip established
Remote session recording failed	Error	VSE failed to record remote access session. Make sure recorded sessions folder has sufficient permission
Failed transfer file due to file size limitation	Warning	Failed to transfer file: '$file_name' to remote VSE(ID:$remote_site_id) because the file exceeded the maximum file size limit of $max_value kB
User clicks on Resume All Auto Profiles	Info	Auto Activation Execution Profile(s) resumed on device(s)
User clicks on Activate Profile	Info	Execution Profile(s) activated on $Device_name:$Device_ip
The report database size reached percent threshold.	Info	The report database size reached $percent_threshold%
The Data Collection database size reached percent threshold.	Info	The Data Collection database size reached $percent_threshold%

Cause	Severity	Message
Reverse Remote Access connection established - Set.	Warning	User $originator_User established Remote Access connection to Security: '$Security' of Security Center $Security_center
Reverse Remote Access connection established - Clear	Clear	Connection to Security: $Security of Security Center $Security_center has been closed for User $originator_User
Transfer file successful	Info	File '$file_name' was successfully transferred to VSE with ID: $remote_site_id
Transfer file communication problem	Error	Communication problem occurred while transferring file:$file_name to Remote VSE with ID: $remote_site_id
User try to perform forbidden action	Critical	User $User_name try to perform forbidden action:'$additional_msg'
Local User requests connection to Device	Info	Local User $User_name requests connection to device $Device using $protocol_name
Software Distribution Package Started Running	Info	The $software_dist_type Software Distribution package has started running on device $Device_name
Software Distribution Package failed	Error	The $software_dist_type Software Distribution package failed to complete successfully on device $Device_name

Cause	Severity	Message
Software Distribution Package finished running successfully	Info	The $software_dist_type Software Distribution package on device $Device_name finished successfully