



Monitoring Dell Force10 Ethernet Switches Using Dell SupportAssist

Dell Product Group Services
February 2014

THIS WHITE PAPER IS FOR INFORMATIONAL PURPOSES ONLY, AND MAY CONTAIN TYPOGRAPHICAL ERRORS AND TECHNICAL INACCURACIES. THE CONTENT IS PROVIDED AS IS, WITHOUT EXPRESS OR IMPLIED WARRANTIES OF ANY KIND.

© 2014 Dell Inc. All rights reserved. Reproduction of this material in any manner whatsoever without the express written permission of Dell Inc. is strictly forbidden. For more information, contact Dell.

Trademarks used in this text:

Dell™, the Dell logo, Dell Boomi™, Dell Precision™, OptiPlex™, Latitude™, PowerEdge™, PowerVault™, PowerConnect™, OpenManage™, EqualLogic™, Compellent™, KACE™, FlexAddress™, Force10™ and Vostro™ are trademarks of Dell Inc. Other Dell trademarks may be used in this document. Cisco Nexus®, Cisco MDS®, Cisco NX-OS®, and other Cisco Catalyst® are registered trademarks of Cisco System Inc. EMC VNX®, and EMC Unisphere® are registered trademarks of EMC Corporation. Intel®, Pentium®, Xeon®, Core® and Celeron® are registered trademarks of Intel Corporation in the U.S. and other countries. AMD® is a registered trademark and AMD Opteron™, AMD Phenom™ and AMD Sempron™ are trademarks of Advanced Micro Devices, Inc. Microsoft®, Windows®, Windows Server®, Internet Explorer®, MS-DOS®, Windows Vista® and Active Directory® are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries. Red Hat® and Red Hat® Enterprise Linux® are registered trademarks of Red Hat, Inc. in the United States and/or other countries. Novell® and SUSE® are registered trademarks of Novell Inc. in the United States and other countries. Oracle® is a registered trademark of Oracle Corporation and/or its affiliates. Citrix®, Xen®, XenServer® and XenMotion® are either registered trademarks or trademarks of Citrix Systems, Inc. in the United States and/or other countries. VMware®, Virtual SMP®, vMotion®, vCenter® and vSphere® are registered trademarks or trademarks of VMware, Inc. in the United States or other countries. IBM® is a registered trademark of International Business Machines Corporation. Broadcom® and NetXtreme® are registered trademarks of Broadcom Corporation. QLogic is a registered trademark of QLogic Corporation. Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and/or names or their products and are the property of their respective owners. Dell disclaims proprietary interest in the marks and names of others.



Table of contents

Introduction	4
1 Discovery and inventory	5
1.1 Prerequisites	5
1.2 Discovery range configuration	5
2 Discovering Force10 Ethernet switches	8
2.1 Setting up SNMP on the switch for successful discovery	10
2.2 Setting the trap destination on the Switch	10
3 Configuring SupportAssist	11
3.1 Default Credentials	11
3.2 Custom Credentials	12
4 Alerts in OpenManage Essentials	14
4.1 Alert threshold	14
5 Case creation and execution of the collection tool	17
6 Configuring periodic collection	18
7 Sending system logs manually (collection on demand)	19
7.1 Troubleshooting Send System Logs failure	19
Conclusion	20



Introduction

Dell SupportAssist is a remote support application providing proactive support capabilities that help identify and resolve issues faster and more accurately. It integrates with Dell OpenManage Essentials, and enables transparent visibility to your server, storage, and networking infrastructure, and proactively identifies hardware failures in your IT environment.

SupportAssist is designed with automated proactive features to help streamline support process steps, maintain your systems' health, and identify hardware failures faster and more accurately.

The key features of SupportAssist include:

- Remote monitoring for critical hardware alerts.
- Automatic collection of diagnostic logs and configuration information.
- Automatic case creation and alert notifications through email.
- Proactive support from a ProSupport Engineer, who has the information required to start resolving your case immediately.

SupportAssist gives you more oversight and control over your environment without the hassle of manual processes and more time. Equipping your OpenManage Essentials server with SupportAssist is voluntary, recommended for ProSupport and ProSupport Plus contracts and results in improved support, products, and services designed to meet your needs.

OpenManage Essentials interacts with supported devices that are to be monitored and receives SNMP traps. The SNMP traps are periodically retrieved as alerts by the SupportAssist application. The alerts are filtered using various policies to decide if the alerts qualify for creating a new support case or updating an existing support case.

All qualifying alerts are securely sent to the SupportAssist server hosted by Dell, for creating a new support case or updating an existing support case. After the support case is created or updated, the SupportAssist application runs the appropriate collection tools on the devices that generated the alerts, and uploads the log collection to Dell.

The information in the log collection is used by Dell technical support to troubleshoot the issue and provide an appropriate solution.

This technical white paper provides information about monitoring Dell Force10 Ethernet switches using Dell SupportAssist. The following are the high-level areas covered:

- Steps to perform discovery and inventory
- Configuring credentials in SupportAssist for Force10 Ethernet switches
- Alert processing
- Case creation in SupportAssist for an alert
- Sending system logs manually



1 Discovery and inventory

Discovery and inventory aids understanding of what hardware and software are installed across your organization and is the most basic step to effective systems management. Areas such as license compliance, health monitoring, security and upgrades, and migrations all require the networked hardware to be available to the System Administrator on a single console to help ease the process. OpenManage Essentials provides these capabilities to initialize the discovery and inventory process and perform required actions on these devices.

1.1 Prerequisites

The following are the prerequisites for performing discovery and inventory:

Credentials: The discovery process in OpenManage Essentials communicates with the Force10 Ethernet switches using SNMP protocol. You will be required to provide the SNMP community string during the discovery process.

Force10 device setup: There are a few settings to be performed on the managed nodes to make them discoverable over the network. For more information, see the *Making Your Environment Manageable with Dell OpenManage Essentials* technical whitepaper at delltechcenter.com/ome.

1.2 Discovery range configuration

This section provides information about providing a discovery range for discovering devices in OpenManage Essentials.

- i. In OpenManage Essentials, navigate to **Manage** → **Discovery and Inventory**. The **Discovery Range Summary** page is displayed.
- ii. Under **Discovery Ranges**, right-click **All Ranges**, and click **Add Discovery Range**.



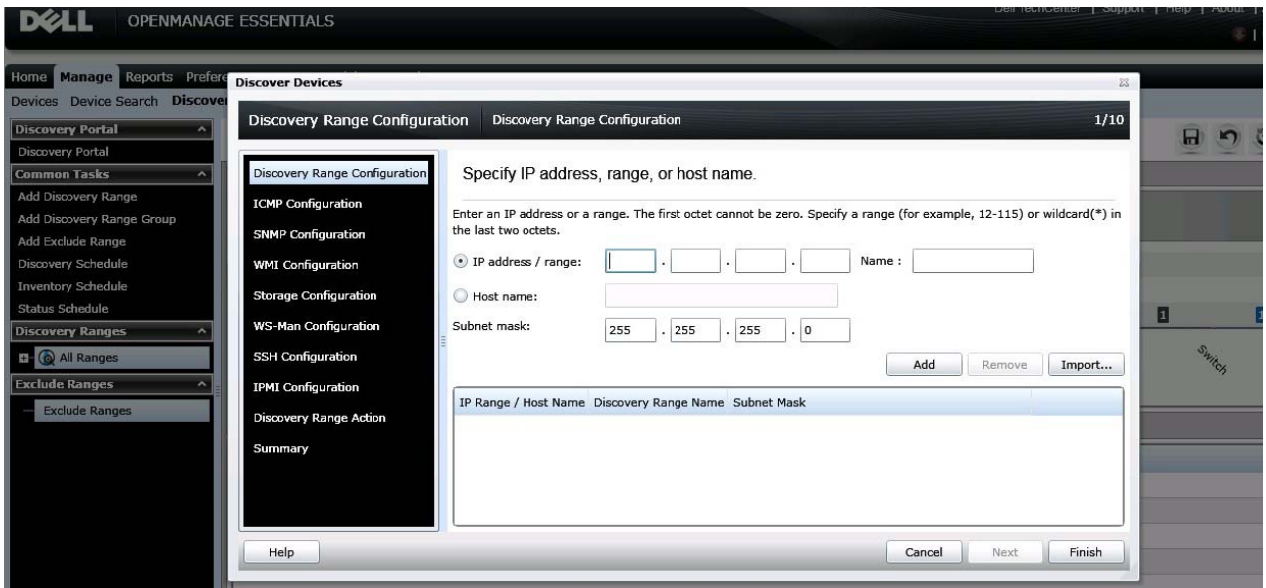


Figure 1 Discovery Range Wizard

- iii. Specify the IP ranges of devices in the environment. The following are examples of valid IP ranges that you can provide.

IP Range	193.109.112.*
	193.104.20-40.*
	192.168.*.*
	192.168.2-51.3-91
	193.109.112.45-99
Hostname	WIN-17L2JS8
Single IP	193.109.112.99

Figure 2 Sample IP ranges

Additionally, an Import functionality provided in OpenManage Essentials helps with importing a Discovery Range which is defined in a .csv file format, as shown in Figure 3. The maximum numbers of devices that can be imported using this method is 500.

Name	Type	Data
1750-win-r03-03	Host (A)	10.94.172.180
1750-win-r04-02	Host (A)	10.94.172.184
1850-win-r04-05	Host (A)	10.94.172.179
2650-win-r01-04	Host (A)	10.94.172.193
2800-W2K3	Host (A)	10.94.168.32
2850-win-r01-03	Host (A)	10.94.161.71
2900-win-r03-07	Host (A)	10.94.161.72
2970-esx	Host (A)	10.94.168.203
4600-WIN-R04-14	Host (A)	10.94.172.168

Figure 3 Sample .csv file



The following example demonstrates adding a discovery range using SNMP protocol with the Add Discovery Range Wizard.

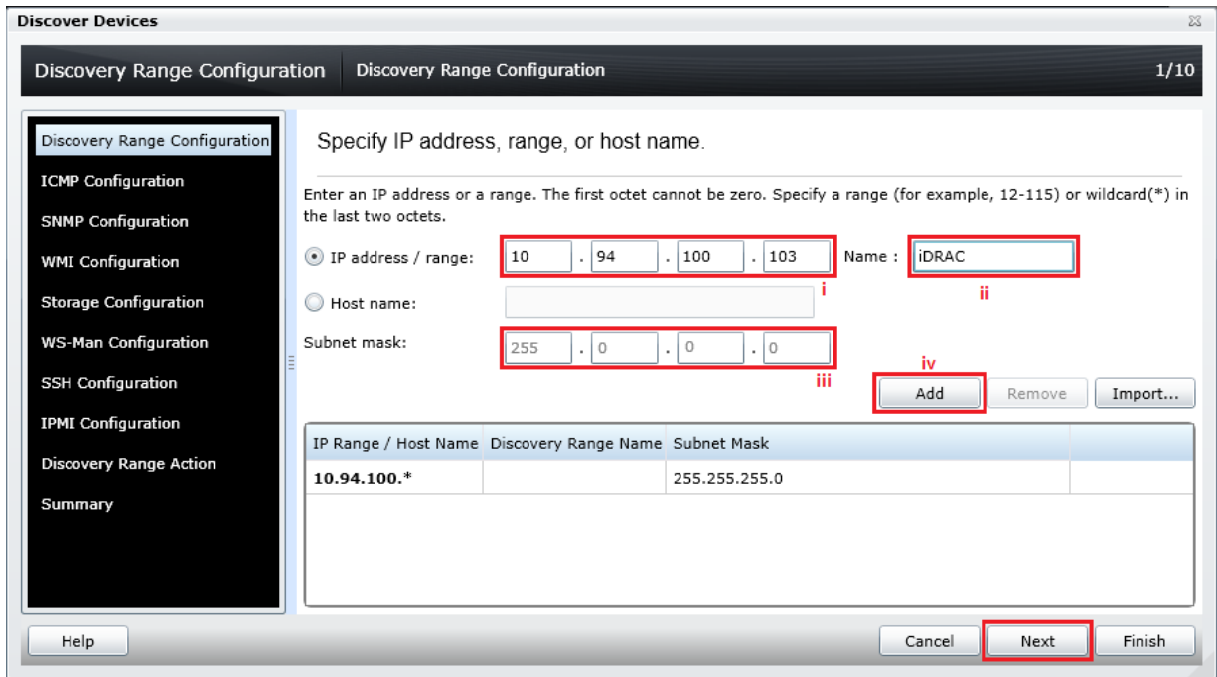


Figure 4 Specifying an IP range

- i. In the **IP address/range** field, type the IP address range.
- ii. In the **Name** field, provide a range name (optional).
- iii. In the **Subnet mask** field field, type the correct subnet mask.
- iv. Click **Add**.
- v. Repeat step i to step iii, to add more discovery ranges.
- vi. Click **Next** to proceed.



2 Discovering Force10 Ethernet switches

To discover Force10 Ethernet switches:

- i. In the **IP address/range** field, type the IP address range.
- ii. In the **Name** field, provide a range name (optional).
- iii. In the **Subnet mask** field, type the correct subnet mask.
- iv. Click **Add**.

NOTE: Repeat step i to step iii, to add more discovery ranges.

- v. Click **Next** to proceed.

Discover Devices

Discovery Range Configuration 1/10

Specify IP address, range, or host name.

Enter an IP address or a range. The first octet cannot be zero. Specify a range (for example, 12-115) or wildcard(*) in the last two octets.

IP address / range: 10 . 94 . 100 . 103 Name : iDRAC

Host name:

Subnet mask: 255 . 0 . 0 . 0

Add Remove Import...

IP Range / Host Name	Discovery Range Name	Subnet Mask
10.94.100.*		255.255.255.0

Help Cancel Next Finish

Figure 5 Specifying an IP range



- vi. In the **SNMP Configuration** screen, select the **Enable SNMP discovery** option.
- vii. Type the community name in the **Get community** field.

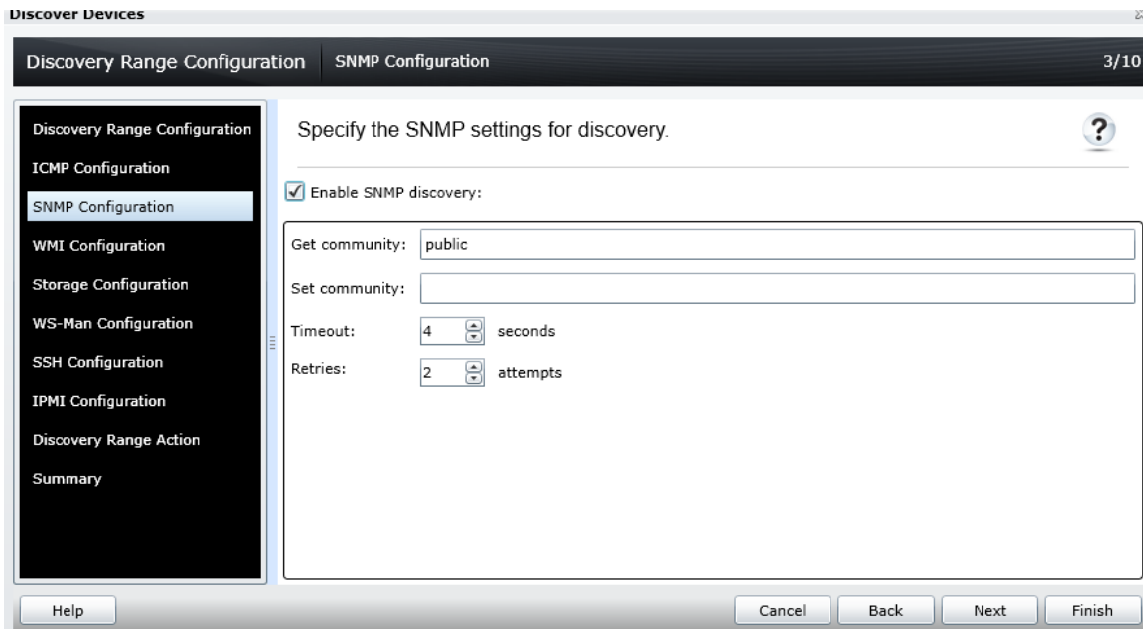


Figure 6 SNMP configuration screen

- viii. Click **Next** to proceed with the default settings until the **Discovery Range Action** screen.
- ix. In the **Discovery Range Action** screen, select one of the options, and click **Finish**.

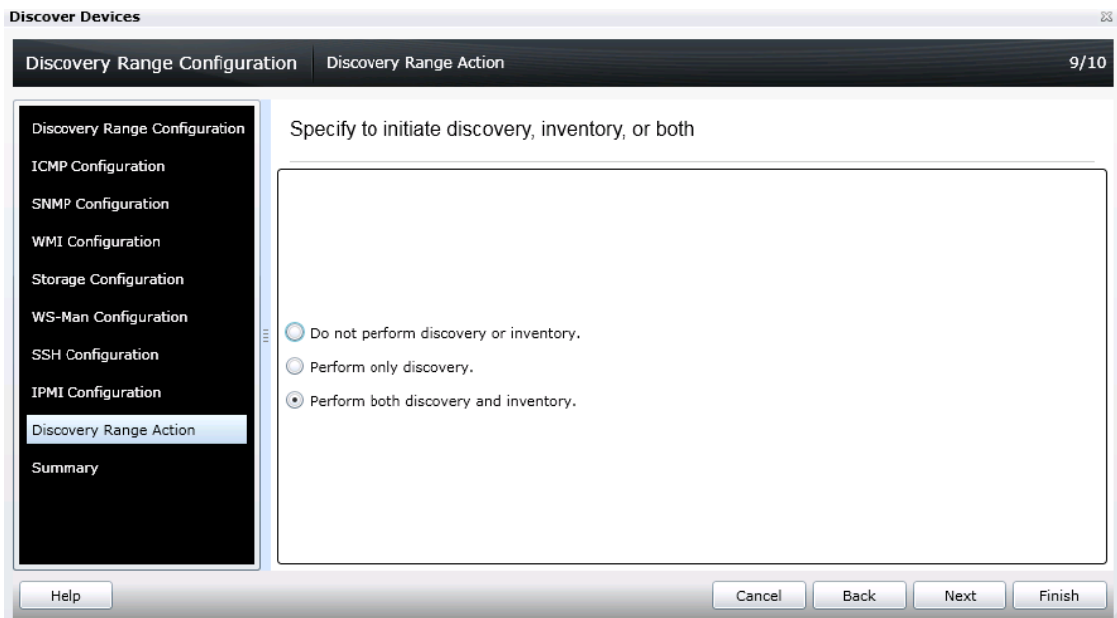


Figure 7 Discovery Range Action



2.1 Setting up SNMP on the switch for successful discovery

1. Log in to the Force10 switch.
2. Run the `en` command to enter exec mode.
3. Run the `config` command to enter configuration mode.
4. Run the following command to set the SNMP configuration:
`snmp-server community public rw`
5. Run the following command to enable the traps:
`snmp-server enable traps`
6. Run the `exit` command to exit the configuration mode.
7. Run the following command to copy the running configuration to the start-up configuration:
`copy running-config startup-config`

2.2 Setting the trap destination on the Switch

1. Log in to the Force10 switch.
2. Run the `en` command to enter exec mode.
3. Run the `config` command to enter configuration mode.
4. Run the following command to set the trap destination in the switch.
`snmp-server host <trap_Destination_IP> traps version <1|2c|3> public udp-port 162`
5. Run the `exit` command to exit the configuration mode.
6. Run the following command to copy the running configuration to the start-up configuration:
`copy running-config startup-config`

The Force10 Ethernet switch you discovered is displayed in the device tree in OpenManage Essentials.



3 Configuring SupportAssist

After successful discovery of the Force10 Ethernet switches in OpenManage Essentials, the **Devices** tab in SupportAssist displays the Force10 Ethernet switches.

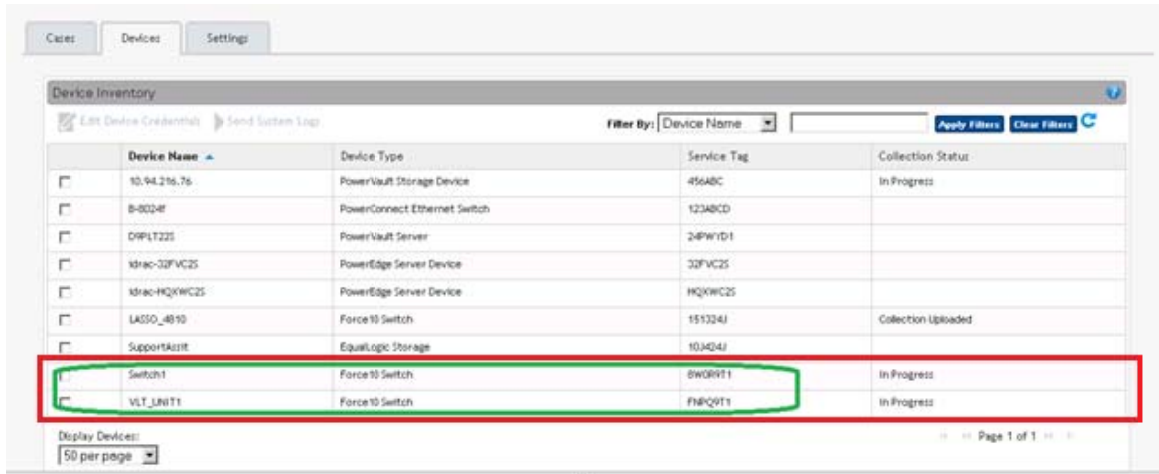


Figure 8 Devices tab

3.1 Default Credentials

SupportAssist runs the appropriate collection tools and gathers the system logs from OpenManage Essentials-managed Dell server, storage, and networking devices. To run the collection tools on your Force10 Ethernet switches, you must configure SupportAssist with the Administrator credentials of the Force10 Ethernet switch.

To provide the Administrator credentials:

NOTE: The **Settings** tab is accessible only if you are logged on as a member of the OpenManage Essentials Administrators or Power Users group.

- i. Navigate to the **Settings** tab. By default, the **System Logs** page is displayed.
- ii. In the **System Logs** page, under **Edit Device Credentials**, select the **Device Type** as **Switch**.
- iii. In the **Credential Type** list, select **Force10**.

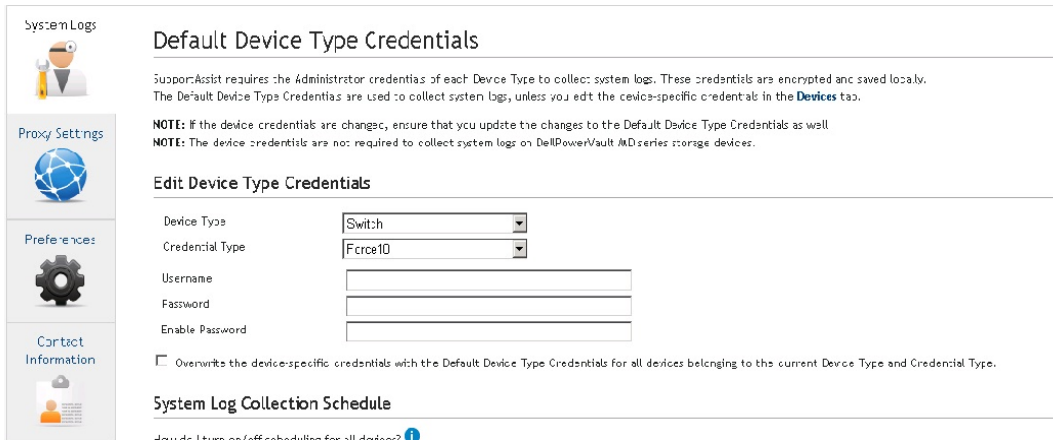


Figure 9 Providing the device credentials

NOTE: For Force10 Ethernet switches, the **Username**, **Password**, and **Enable Password** fields are optional. However, information must be provided for these fields if the Force10 Ethernet switch is configured with these details.

- iv. If applicable provide the username, password, and enable password in the appropriate fields.
- v. Click **Save**.

3.2 Custom Credentials

If you have more than one Force10 Ethernet switch, and the Administrator credentials of a particular Force10 Ethernet switch is different, you can configure the credentials for that Force10 Ethernet switch through the **Devices** tab.

To provide custom credentials:

- i. In the **Devices** tab, select the appropriate Force10 Ethernet switch.

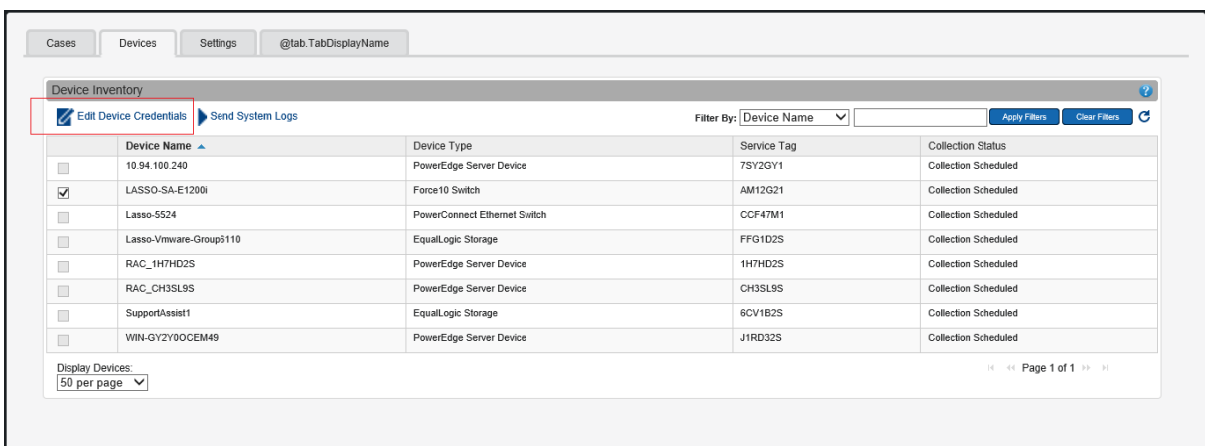
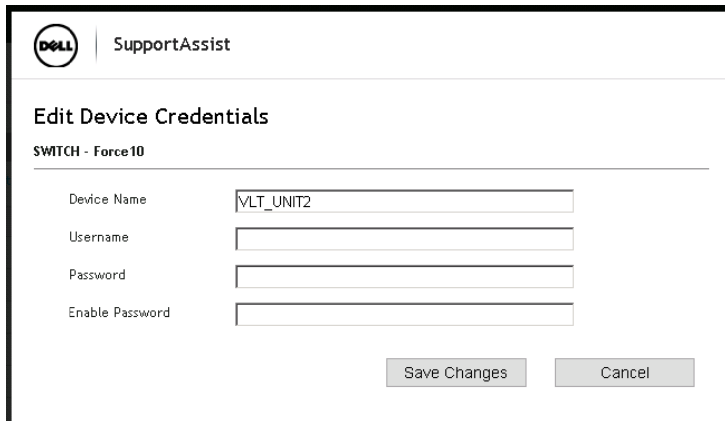


Figure 10 Devices tab



- ii. Click **Edit Device Credentials**.



The screenshot shows the Dell SupportAssist interface for editing device credentials. At the top left is the Dell logo and the text 'SupportAssist'. Below this is the title 'Edit Device Credentials' and the device identifier 'SWITCH - Force10'. The main area contains four input fields: 'Device Name' with the value 'VLT_UNIT2', 'Username', 'Password', and 'Enable Password'. At the bottom right are two buttons: 'Save Changes' and 'Cancel'.

Figure 11 Edit Device Credentials screen

- iii. In the **Edit Device Credentials** screen, provide the **Username**, **Password**, and **Enable Password** as appropriate.
- iv. Click **Save Changes**.
- v. At the confirmation prompt, click **Yes**.

4 Alerts in OpenManage Essentials

Dell OpenManage Essentials administrators can monitor the health of discovered assets through a centralized, easy-to-use dashboard and through automated, custom alerts. The dashboard provides an at-a-glance view and a scoreboard displaying the health and well-being of the infrastructure.

4.1 Alert threshold

The alert threshold specifies under what conditions the alert should cause a support case to be created (or appended). The syntax resembles a programming method and optionally may take additional arguments to refine its behavior.

Currently there are two possible values:

- FirstMatch () – The case should be created/appended each time this alert is detected.
- Occurs (count,duration) – The case should be created/appended only when the alert has occurred so many times within a specified duration.

The duration argument of the Occurs threshold defines a relative time in days, hours, minutes, and seconds and is formatted as dd-hh:mm:ss. The following are some examples of the Occurs threshold and their descriptions

Table 1 Examples of Occurs threshold

Example	Description
Occurs (5,1-00:00:00)	Create/append a case if the alert occurs 5 or more times within the previous 1 day
Occurs (3,0-05:00:00)	Create/append case if the alert occurs 3 or more times within the previous 5 hours
Occurs (8,1-12:00:00)	Create/append case if the alert occurs 8 or more times within the previous day and a half

Valid duration values – Days: 0 to 365, Hours: 0 to 23, Minutes: 0 to 59, Seconds: 0 to 59

Policies which specify the Occurs () threshold instruct the SupportAssist server to retain the timestamps of each alert. With each new alert occurrence, the SupportAssist server evaluates if the number of alerts within the duration exceeds the count, and if so, creates/appends the case. The timestamps are discarded to ensure the Occurs () threshold will not append the case until an entirely new set of alerts are received which fulfills the criteria.



Table 2 Examples of Policy file details

Policy Property	Description	Example
clientType	The type of client reporting the alert	"OME"
eventSourceType	The source of the alert	".1.3.6.1.4.1.6027.3.1.1.4"
trapId	The trap identifier	"32"
eventId	The event identifier	(null)
severity	Severity of the alert	"MAJOR"
description	Description of the alert	"The agents generate this trap when a power supply major alarm is issued."
autoCase	Indicates if the alert should be processed	True
alertThreshold	Policy filter when the case is created	"FIRST MATCH()"
deltaSeverity	Severity code passed to delta	"3"

Alerts with the following Enterprise OIDs for clientType OME are processed as alerts from Force10 Ethernet switches:

- .1.3.6.1.4.1.6027.3.1.1.4
- .1.3.6.1.4.1.6027.3.22.4
- .1.3.6.1.4.1.6027.3.2.2.1
- .1.3.6.1.4.1.6027.3.20.2
- .1.3.6.1.4.1.6027.3.19.1.4

SupportAssist processes all the alerts with Force10 OIDs, but only some specified alerts are considered to create a case (Service Requests or SR) provided they have Auto Case as "Yes" as shown in the following policy table.

Table 3 Policy table with threshold

Name	Description	TrapId	Eventid	Severity	Autocase	Alert threshold	Resolution type
.1.3.6.1.4.1.6027.3.1.1.4	Force10	32	(null)	Major	1	First Match()	FA
.1.3.6.1.4.1.6027.3.1.1.4	Force10	36	(null)	Minor	1	First Match()	FA
.1.3.6.1.4.1.6027.3.1.1.4	Force10	37	(null)	Warning	1	Occurs(10,0-05:00:00)	FA
.1.3.6.1.4.1.6027.3.1.1.4	Force10	39	(null)	Warning	1	Occurs(10,0-05:00:00)	FA
.1.3.6.1.4.1.6027.3.1.1.4	Force10	43	(null)	Major	1	Occurs(5,00-01:00:00)	FA
.1.3.6.1.4.1.6027.3.1.1.4	Force10	44	(null)	Info	1	Occurs(5,00-01:00:00)	FA



.1.3.6.1.4.1.6027.3.1.1.4	Force10	45	(null)	Critical	1	First Match()	FA
.1.3.6.1.4.1.6027.3.1.1.4	Force10	56	(null)	Warning	1	FirstMatch()	FA
.1.3.6.1.4.1.6027.3.22.4	Force10	7	(null)	Normal	1	Occurs(5,0-01:00:00)	FA
.1.3.6.1.4.1.6027.3.2.2.1	Force10	1	(null)	Warning	1	Occurs(10,0-00:30:00)	FA
.1.3.6.1.4.1.6027.3.20.2	Force10	1	(null)	(null)	1	Occurs(10,0-00:05:00)	FA
.1.3.6.1.4.1.6027.3.20.2	Force10	2	(null)	Critical	1	Occurs(10,0-00:05:00)	FA
.1.3.6.1.4.1.6027.3.19.1.4	Force10	5	(null)	Warning	1	FirstMatch()	FA
.1.3.6.1.4.1.6027.3.19.1.4	Force10	8	(null)	Normal	1	FirstMatch()	FA
.1.3.6.1.4.1.6027.3.19.1.4	Force10	3	(null)	Warning	1	Occurs(5,0-01:00:00)	FA
.1.3.6.1.4.1.6027.3.19.1.4	Force10	1	(null)	Critical	1	FirstMatch()	FA
.1.3.6.1.4.1.6027.3.19.1.4	Force10	7	(null)	Critical	1	Occurs(5,0-01:00:00)	FA

Currently SupportAssist OpenManage Essentials (OME) 1.3 (release), supports the following Force10 Ethernet switches: MXL, S4820T, S50, Z9000, S5000, and S6000.

Limitation in S-series and M-Series devices

Due to a known limitation in the Force10 S-series and M-series devices, certain alerts from Force10 S-series and M-series devices have been mapped in SupportAssist as generic alerts. When a support case is created because of these alerts, the alert description in the SupportAssist dashboard and the email notification may contain generic information which may not be indicative of the exact problem with the device.

The generic alert mapping is also applicable to Force10 E-series and C-series devices.

The following table provides a summary of the changes made to the policy table to handle these alerts. The changes have been made for OID .1.3.6.1.4.1.6027.3.1.1.4 and TrapIDs 1, 2, 3, 4, and 5.

Name	Description	Trapid	Eventid	Severity	Autocase	Alert threshold	Resolution type
.1.3.6.1.4.1.6027.3.1.1.4	Force10	1	(null)	Critical	1	First Match()	FA
.1.3.6.1.4.1.6027.3.1.1.4	Force10	2	(null)	Normal	0	First Match()	FA
.1.3.6.1.4.1.6027.3.1.1.4	Force10	3	(null)	Warning	1	Occurs(5,0-01:00:00)	FA
.1.3.6.1.4.1.6027.3.1.1.4	Force10	4	(null)	Warning	0	Occurs(10,0-05:00:00)	FA
.1.3.6.1.4.1.6027.3.1.1.4	Force10	5	(null)	Critical	1	First Match()	FA



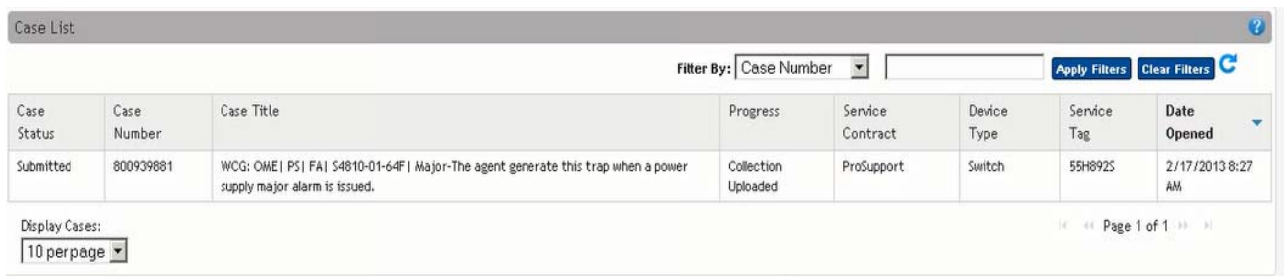
5 Case creation and execution of the collection tool

SupportAssist processes all alerts from OpenManage Essentials, but a support case is created only if:

- The policies qualify the alert for a support case creation.
- SupportAssist is configured to automatically generate support cases.

Once the support case is created for a Force10 Ethernet switch, the corresponding collection tool (Dell Lasso) is invoked, and the system log collection is generated and uploaded to Dell.

NOTE: For devices covered under Basic Support service contract type, the support case is not created, but the collection tools are invoked.



The screenshot shows a web interface titled "Case List" with a search filter set to "Case Number". Below the filter is a table with one row of data. The table has columns for Case Status, Case Number, Case Title, Progress, Service Contract, Device Type, Service Tag, and Date Opened. The row shows a "Submitted" case with number "800939881" and a title describing a power supply major alarm. The progress is "Collection Uploaded", the service contract is "ProSupport", the device type is "Switch", the service tag is "55H8925", and the date opened is "2/17/2013 8:27 AM". At the bottom, there is a "Display Cases:" section with a dropdown set to "10 per page" and a pagination indicator showing "Page 1 of 1".

Case Status	Case Number	Case Title	Progress	Service Contract	Device Type	Service Tag	Date Opened
Submitted	800939881	WCG: OME PS FA S4810-01-64F Major-The agent generate this trap when a power supply major alarm is issued.	Collection Uploaded	ProSupport	Switch	55H8925	2/17/2013 8:27 AM

Figure 12 Support case created for a Force10 Ethernet switch

6 Configuring periodic collection

By default, SupportAssist generates the system log collection from Force10 Ethernet switches every week, and uploads the system log collection to Dell. You can modify the frequency at which the system log collection is generated as required.

To configure the periodic collection:

- i. Click the **Settings** tab.
- ii. Under **Edit Device Type Credentials**, select **Device Type** as **Switch** and **Credential Type** as **Force10**.
- iii. Under **System Log Collection Schedule**, select the frequency, date, and time as required.
- iv. Click **Save Changes**.

The screenshot shows a web interface for configuring periodic collection. It is divided into two main sections: 'Edit Device Type Credentials' and 'System Log Collection Schedule'.

Edit Device Type Credentials

- Device Type: Switch (dropdown)
- Credential Type: Force10 (dropdown)
- Username: [text input]
- Password: [text input]
- Enable Password: [text input]
- Overwrite the device-specific credentials with the Default Device Type Credentials for all devices belonging to the current Device Type and Credential Type.

System Log Collection Schedule

How do I turn on/off scheduling for all devices? ⓘ

Frequency: Weekly (dropdown)

Specify day and time: Recur every 1 (dropdown) week(s) on Mon (dropdown) at 12:00 (dropdown) AM (dropdown)

Buttons: Save Changes (blue), Cancel (grey)

Figure 13 Configuring periodic collection

7 Sending system logs manually (collection on demand)

When a support case is opened or updated, the SupportAssist application, runs the collection tools on the devices that generated the alerts, and then uploads the system logs to Dell. In certain conditions, if required by Dell technical support, you may be required to manually collect the system logs and send it to Dell.

To send the system logs manually:

- i. Click the **Devices** tab.
- ii. Select a Force10 Ethernet switch in the **Device Inventory** table.
- iii. Click **Send System logs**.

The collection tool (Dell Lasso) is invoked and the generated system log collection is uploaded to Dell.

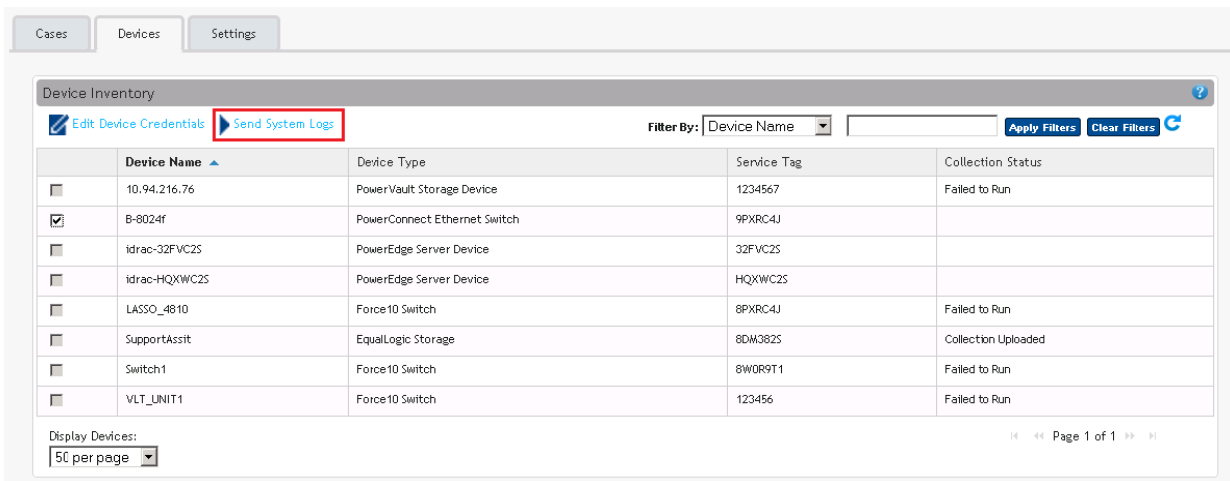


Figure 14 Sending system logs manually

7.1 Troubleshooting Send System Logs failure

The generation and upload of system logs to Dell may fail due to:

- Authentication failure (incorrect credentials): Verify the credentials provided for the switch in SupportAssist. If required, update the credentials using the Edit Device Credentials option.
- DNS failure: Add a host entry in the host file (/etc/host entry).

You can also check the log file in the installation folder for more details on the failure.

The screenshot shows the Dell SupportAssist interface for editing device credentials. At the top left is the Dell logo and the text 'SupportAssist'. Below this is the title 'Edit Device Credentials' and the device identifier 'SWITCH - Force10'. The form contains four input fields: 'Device Name' with the value 'VLT_UNIT2', 'Username', 'Password', and 'Enable Password'. At the bottom right of the form are two buttons: 'Save Changes' and 'Cancel'.

Figure 15 Edit Device Credentials screen

Conclusion

Dell SupportAssist identifies hardware failures on supported devices quickly and more accurately. It automates and streamlines the support process steps without much interaction from your side. With SupportAssist, integrated with OpenManage Essentials 1.3 (release), you have a single systems management console to remotely monitor and manage your environment, giving you instant insight into how your systems are performing at all times.