FUJITSU Software ServerView

PRIMEQUEST Enclosure Integration Pack V9.0 for MS SCOM

February 2017 Edition

Contents

1 Introduction

The PRIMERGY ServerView Suite from Fujitsu offers numerous ServerView integration modules which enable PRIMERGY and PRIMEQUEST servers to be integrated easily into other enterprise management systems.

This manual describes the ServerView PRIMEQUEST Enclosure Integration Pack V9.0, which enables Fujitsu PRIMEQUEST Enclosures to be integrated into System Center Operations Manager (SCOM). All SCOM editions from SCOM 2012 R2 up to SCOM 2016 are supported.

This integration of ServerView permits PRIMEQUEST Enclosures from Fujitsu to be monitored via SCOM. Monitoring of PRIMEQUEST Enclosures is implemented using the Simple Network Management Protocol (SNMP) to communicate with the enclosures. The Health State of monitored components is displayed by means of icons.

The PRIMEQUEST Enclosure Integration Pack provides monitors and rules that run on SCOM Management Servers and check the health state of PRIMEQUEST hardware components. If a problem occurs during monitoring this is indicated by the changed health state of the faulty component. Furthermore, rules can be applied which trigger an adequate action when a fault is detected, e.g. a mail describing the fault might be sent to hardware support.

For detailed analysis the PRIMEQUEST Web User Interface can be started directly from the SCOM Console.

The current PRIMEQUEST Enclosure Integration Pack for SCOM is provided on the latest PRIMERGY ServerView Suite DVD from Fujitsu or under:

http://download.ts.fujitsu.com/prim_supportcd/SVSSoftware/

1.1 Purpose and target groups

This manual is intended for system administrators, network administrators and service technicians who have a thorough knowledge of hardware and software. Likewise, a sound basic knowledge of the Microsoft System Center Operations Manager is required.

1.2 Changes since the last edition

The Fujitsu PRIMEQUEST Enclosure Integration Pack V9.0 includes the following new features:

● Full discovery of PRIMEQUEST Enclosures and their components.

● Health State monitoring of PRIMEQUEST Enclosures and their components.

● The PRIMEQUEST Enclosure Integration Pack now consists of a single MSI installer package, as the former PRIMEQUEST Monitor Service is no longer required to be able to receive SNMP traps. The management pack uses SCOM's ability to receive traps.

● New views were introduced to improve enclosure and component health overview.

1.3 ServerView Suite link collection

Via the link collection, Fujitsu provides their customers with numerous downloads and further information on the ServerView Suite and PRIMERGY servers

In "ServerView Suite" on the left side, links are offered on the following topics:

● Forum

● Service Desk

● Manuals

● Product information

● Security information

● Software downloads

● Training

The downloads include the following:

— Current software versions for the ServerView Suite and additional Readme files.

— Information files and update sets for system software components (BIOS, firmware, drivers, ServerView Agents and ServerView Update Agents) for updating the PRIMERGY servers via ServerView Update Manager or for locally updating individual servers via ServerView Update Manager Express.

— The current version of all documentation on the ServerView Suite.

All downloads from the Fujitsu web server are free of charge.

● For PRIMERGY servers, links are offered on the following topics:

● Service Desk

● Manuals

● Product information

● Spare parts catalogue

Access to the ServerView link collection

You can reach the link collection of the ServerView Suite in various ways:

1. Via ServerView Operations Manager.

    ▶ Select Help – Links on the start page or on the menu bar.
      This opens the start page of the ServerView link collection.

2. Via the start page of the online documentation for the ServerView Suite on the Fujitsumanual server.

    | i | The start page of the online documentation can be reached via the following link: http://manuals.ts.fujitsu.com |

    ▶ In the selection list on the left, select x86 servers.

    ▶ Click the menu item PRIMERGY ServerView Links.
      This opens the start page of the ServerView link collection.

3. Via the ServerView Suite DVD2

    ▶ In the start window of the ServerView Suite DVD2, select the option Select ServerView Software Products.

    ▶ Click Start to open the page with the software products of the ServerView Suite.

    ▶ On the menu bar select Links to open the start page of the ServerView link collection.

1.4 Documentation for ServerView Suite

The documentation can be downloaded free of charge from the Internet. You will find the online documentation at http://manuals.ts.fujitsu.com under the link *x86 servers*.

For an overview of the documentation to be found under ServerView Suite as well as the filing structure, see the ServerView Suite sitemap (*ServerView Suite -Site Overview*).

1.5 Notational Conventions

The following notational conventions are used in this manual:

⚠	**Warning** This symbol is used to draw attention to risks which may represent a health hazard or which may lead to data loss or damage to the hardware
i	**Information** This symbol highlights important information and tips.
▶	This symbol refers to a step that you must carry out in order to continue with the procedure.
italics	Commands, menu items, names of buttons, options, file names and path names are shown in italics in descriptive text.
<variable>	Angle brackets are used to enclose variables which are replaced by values.

Screen Output

Please note that the screen output shown in this manual may not correspond to the output from your system in every detail. System-related differences between the menu items available can also arise.

2 Integration requirements

The requirements specified below must be satisfied for integration.

Management station

- Windows Server 2008 R2 / 2012 / 2012 R2 / 2016.
  See the requirements for the relevant SCOM version

- SQL Server 2008 / 2012 / 2014 / 2016.
  See the requirements for the relevant SCOM version

- Microsoft System Center Operations Manager 2012 R2 / 2016

- Following management packs imported into System Center Operations Manager:

    o Windows Core Library 7.5.8501.0

    o Network Management Library 7.0.8560.0

    o SNMP Library 7.0.8427.0

- Windows PowerShell >= 4.0

- Microsoft .NET Framework >= 4.5.1

- SNMP Trap Service Disabled (optional, see chapter 2.1 SNMP Trap Listener Service)

Managed PRIMEQUEST Enclosures

- PRIMEQUEST 1400

- PRIMEQUEST 1800

- PRIMEQUEST 2800

2.1 SNMP Trap Listener Service

The following requirement must be met when the PRIMEQUEST Enclosure Integration Pack is supposed to display alerts derived from SNMP traps sent by PRIMEQUEST Enclosures.

The service "SNMP Trap" must be disabled on Management Servers which are monitoring PRIMEQUEST Enclosures. Moreover, any other service that listens for SNMP traps must be disabled. The only application which is allowed to listen for SNMP traps is the SCOM Monitoring Agent.

3 Installation and uninstallation

3.1 Installing ServerView Integration Pack

The installation program SVISCOM-PQ.exe is located on the ServerView Suite DVD at
<DVDroot>\SVSSoftware\Software\Integration_Solutions\SCOM

or as a download on the website at
http://download.ts.fujitsu.com/prim_supportcd/SVSSoftware/

The installation program first runs some basic checks then start the Installation Wizard. Follow the instructions displayed during the installation process.

3.1.1 Installed files

The default installation path on the management station is:

— %ProgramFiles%\Fujitsu\ServerView Suite\SCOM Integration

The following files are copied into the installation directories:

Folder	Files
Management Packs sub folder	• *Fujitsu.ServerView.Library.mpb* • *Fujitsu.ServerView.Image.Library.mpb* • *Fujitsu.PRIMEQUEST.mpb* • *Fujitsu.PRIMEQUEST.SnmpTraps.mpb*
SVISCOM-PQ sub folder	• *Eula_en.pdf* • *Eula_jp.pdf* • *sv-intpack-scom-pq-en.pdf*
SVISCOM-PQ/Tools sub folder	• *Clear-SecureReferenceOverrideMP.ps1*

i After Installation start the SCOM console with the command
Microsoft.EnterpriseManagement.Monitoring.Console.exe /clearcache.

⚠ In case other Fujitsu Integration Packs are also installed on the SCOM, the folder *Management Packs* may contain both the old *ServerView Core Library* (*Fujitsu.ServerView.Library.mp*) and the new *ServerView Core Library* (*Fujitsu.ServerView.Library.mpb*) after installation.

Please note that to install the new *ServerView Core Library* (*Fujitsu.ServerView.Library.mpb*) it is imperative not to also select the old *ServerView Core Library* (*Fujitsu.ServerView.Library.mp*) for import into SCOM. If both Libraries are selected, SCOM will refuse to import any of them.

3.1.2 Importing Management Packs

Management packs installed by the ServerView PRIMEQUEST Enclosure Integration Pack are located in the folder 'Management Packs' within the installation folder. This folder holds all management packs from ServerView Integration Packs for System Center Operations Manager not only from the ServerView PRIMEQUEST Enclosure Integration Pack.

Management packs are imported in the usual way from the SCOM Console.

All Management Packs of the ServerView PRIMEQUEST Enclosure Integration Pack must be imported, except *Fujitsu.PRIMEQUEST.SnmpTraps.mpb* which is optional. They can be installed all at one time. See chapter 3.1.1 Installed files for details.

Close the SCOM Console once after importing management packs to avoid locked files.

3.2 Update to a new version

Update installation is not supported by the ServerView PRIMEQUEST Enclosure Integration Pack. The process is a full uninstallation of the old version followed by the installation of the new version.

Follow chapter 3.4 Uninstalling ServerView Integration Pack to uninstall the old ServerView PRIMEQUEST Enclosure Integration Pack.

Follow chapter 3.1 Installing ServerView Integration Pack to install the new ServerView PRIMEQUEST Enclosure Integration Pack.

3.3   Updating the ServerView Library Management Packs

The ServerView Library Management Pack and the ServerView Image Library Management Pack are used and referenced by all Fujitsu ServerView Integration Packs for System Center Operations Manager.

> **i**   If a ServerView Integration Pack contains a newer version of one of the ServerView Library Management Packs this new version can usually be imported into SCOM without impact to any other Fujitsu ServerView Integration Management Packs.
>
> In the rare case that a new version of one of the ServerView Library Management Packs is not compatible with the old version, it is necessary to uninstall all Fujitsu Management Packs including their Override Management Packs and reinstall all Fujitsu Management Packs from the folder 'Management Packs' together with the updated ServerView Library and ServerView Image Library Management Packs.

3.4   Uninstalling ServerView Integration Pack

The ServerView PRIMEQUEST Enclosure Integration Pack is uninstalled via the following steps:

- Remove the corresponding override management packs if any from SCOM.
  To keep existing override settings, e.g. to re-use in a new version, the override management packs should be exported and saved.

- The Integration Pack provides one Run As profile (details in chapter 4.2.2 Run As profiles).
  If any SNMP accounts have been associated with these profiles then run the Clear-SecureReferenceOverrideMP.ps1 script from the Tools folder or manually perform these actions:

  - Remove all associated Run As Accounts from the Integration Pack's profiles.

  - Modify the Manifest section of the Microsoft.SystemCenter.SecureReferenceOverride by removing all references to management packs Fujitsu PRIMEQUEST Enclosure and Fujitsu PRIMEQUEST Enclosure (SNMP Traps).
    You need to export the Microsoft.SystemCenter.SecureReferenceOverride management pack, delete the references and re-import it again.

- Remove the Fujitsu PRIMEQUEST Enclosure management packs from SCOM.

| i | If other ServerView Integration Packs for System Center Operations Manager have been installed, the ServerView Library Management Packs cannot be uninstalled. |

● Uninstall the ServerView PRIMEQUEST Enclosure Integration Pack from the SCOM server.

| i | To remove the Management Packs you need SCOM administrator rights. The old ServerView Windows Server Integration Pack should be removed from all SCOM Remote Consoles. |

4 Properties of the ServerView PRIMEQUEST Enclosure Integration Pack

4.1 Management Packs

The *Fujitsu ServerView Core Library* Management Pack contains the basic definitions to manage Fujitsu systems in a consolidated manner in SCOM. This Management Pack is distributed with all Fujitsu SCOM Integration Packs. It is a sealed management pack.
The file name of this package is *Fujitsu.ServerView.Library.mpb.*

The *Fujitsu ServerView Image Library* Management Pack contains images common to all Fujitsu SCOM Management Packs. This Management Pack is distributed with all Fujitsu SCOM Integration Packs. It is a sealed management pack.
The file name of this package is *Fujitsu.ServerView.Image.Library.mpb.*

The *Fujitsu PRIMEQUEST Enclosure* Management Pack discovers and monitors PRIMEQUEST Enclosures and their components. It is a sealed management pack.
The file name of this package is *Fujitsu.PRIMEQUEST.mpb*.

The optional *Fujitsu PRIMEQUEST Enclosure (SNMP Traps)* Management Pack handles SNMP traps sent by PRIMEQUEST Enclosures. It is a sealed management pack.
The file name of this package is *Fujitsu.PRIMEQUEST.SnmpTraps.mpb*.

4.2 Communication methods

The Management Packs from the PRIMEQUEST Enclosure Integration Pack communicate with PRIMEQUEST Enclosures using SNMP. There are two communication methods:

1. Workflows from the management pack send SNMP requests to the PRIMEQUEST Enclosure, responses are sent back. This method is used by the Fujitsu PRIMEQUEST Enclosure management pack.

2. The PRIMEQUEST Enclosure is configured to send SNMP traps to the SCOM server and the management pack processes the received data. This method is used by the Fujitsu PRIMEQUEST Enclosure (SNMP Traps) management pack.

4.2.1   SNMP Support

SCOM can discover devices that use version 1, 2c or 3 of the Simple Network Management Protocol (SNMP). However, SCOM does not support receiving SNMP traps for SNMPv3. This has an impact on the Fujitsu ServerView PRIMEQUEST Integration Pack.

The following table shows the features of the Fujitsu ServerView PRIMEQUEST Integration Pack which are supported for specific versions of SNMP protocol:

Feature	SNMPv1	SNMPv2c	SNMPv3
Discovery and Health Monitoring	Yes	Yes	Yes
Receiving traps	Yes	Yes	No

More details on SNMP support in SCOM:
https://technet.microsoft.com/en-us/library/hh212935.aspx

4.2.2   Run As profiles

The ServerView PRIMEQUEST Enclosure Integration Pack uses Run As profiles provided by SCOM to get credentials for discovery and monitoring workflows. These profiles are:

● SNMP Monitoring Account

● SNMPv3 Monitoring Account

The Integration Pack provides its own Run As profile which is used to configure credentials for SNMP traps. This profile is defined in *Fujitsu PRIMEQUEST Enclosure (SNMP Traps)* management pack, its name is:

● Fujitsu PRIMEQUEST Trap

See chapter 4.4 Configuration for more details.

4.3 Representation of PRIMEQUEST components in SCOM

4.3.1 Basic information

A PRIMEQUEST Enclosure contains units like System Boards, Partitions, PCI Boxes and devices like temperature sensors or CPUs. The enclosure itself contains units. A unit may contain devices or no devices. Both units and devices have a health state that is monitored by PRIMEQUEST Enclosure Integration Pack.

The Fujitsu PRIMEQUEST Enclosure management pack represents PRIMEQUEST Enclosures and their components using objects of the following classes:

- Enclosure
- Unit collection
- Unit
- Device collection
- Device

The hosting relationships between the classes of this list are as follows:
Each class hosts the next class from list, e.g. Units host Device collections. The Enclosure class is hosted in the Node class (derived from Network Device class) which is a standard SCOM class.

The Enclosure object contains basic information about the PRIMEQUEST system, e.g. serial number or location. The Unit and Device classes represent units and devices respectively. Unit collection and Device collection classes group units and devices of the same type.

4.3.2 Unit types

The type of units is indicated by the attribute *Unit class* from the class Unit. The following table shows supported unit types.

Unit class attribute	Unit type description
du	Disk Unit
dvdb	DVD Board

fan unit	Fan module assigned to Fan Tray Unit or Power Supply Unit
fan-tray unit	Fan Tray Unit
gspb	Giga-LAN SAS and PCI-Box Interface Board
gspb-nodivided	Giga-LAN SAS and PCI-Box Interface Board
iou	I/O Unit
iou-nodivided	I/O Unit
lpci-box	Divided PCI Box
chassis-components	Components of the chassis
mmb	Management Board
op-panel	Operator panel
partition	Partition
pci-box	PCI Box
psu	Power Supply Unit
sas-unit	Serial Attached SCSI
sb	System Board

Units of the type *partition* have their own class derived from the Unit class. The other types do not have specific derived classes.

4.3.3 Device types

The PRIMEQUEST Enclosure has seven types of devices:

- Temperature Sensor
- Fan
- Power Supply
- Voltage
- CPU
- Memory Module

- Battery

Devices are represented by classes derived from the Device class

4.3.4 Device collection types

A PRIMEQUEST Enclosure contains a large number of components of the following types:

- Temperature Sensor
- Fan
- Voltage

The *Fujitsu PRIMEQUEST Enclosure* management pack does not model individual objects for these components because of performance reasons. These devices are represented only by generic Device collection objects.

Devices of the remaining types are represented both by Device collection and Device objects, i.e. every hardware component from an Enclosure has corresponding Device object in SCOM.

4.3.5 Example object tree
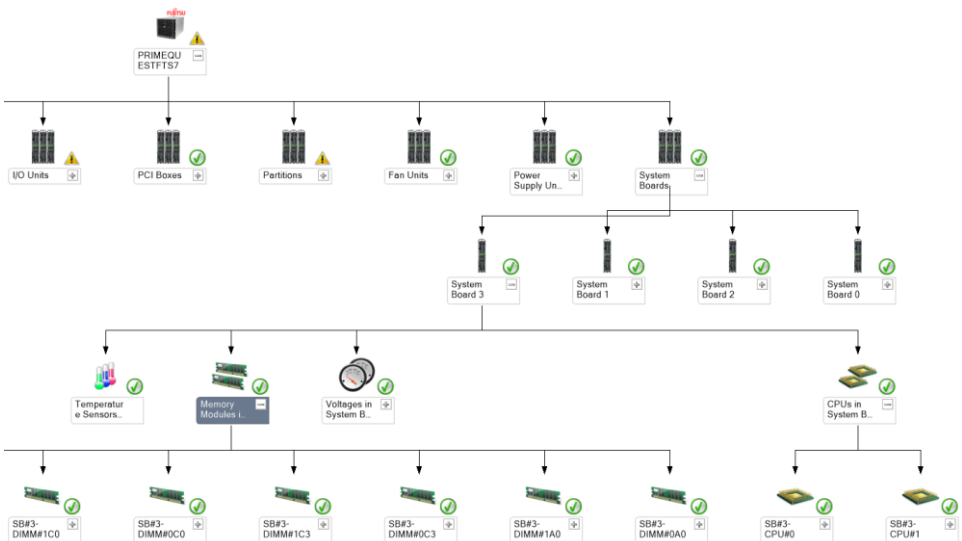
Example object tree

At the top of above diagram is an object of the Enclosure class which is the root element of the object tree. It is hosted by a network device (not shown in the diagram).

The Enclosure object hosts various Unit collection objects as seen in second row, e.g. *I/O Units* or *Partitions*.

The *System Boards* Unit collection hosts all units of type System Board (see third row).

The *System Board 3* object hosts four Device collections visible (see fourth row).

The collections *Memory Modules* and *CPUs* host devices where each Device object represents a specific hardware component (see last row).

The collections *Temperature Sensors* and *Voltages* do not host devices. For these device types hardware components are represented only by collection objects.

4.4   Configuration

4.4.1 Overview

PRIMEQUEST Enclosures have to be discovered by SCOM as Network Devices. The *Fujitsu PRIMEQUEST Enclosure* management pack uses the discovered Network Devices as starting point for discovery of PRIMEQUEST Enclosures and their components.

4.4.2 Network Device discovery

The first step is to discover PRIMEQUEST Enclosures as Network Devices using the functionality provided by SCOM.

In the SCOM Console create a new Network Discovery Rule or modify an existing one. Below are key elements of the discovery rule's properties.

▸   Select a management or gateway server – this server will perform the network discovery.

▸   Select a resource pool – the servers from the selected resource pool will perform the monitoring of discovered network devices. These servers will also be responsible for running the discovery and monitoring workflows from Fujitsu PRIMEQUEST Enclosure management pack and receiving SNMP traps sent by PRIMEQUEST Enclosures.

▸   Discovery method – select either explicit or recursive discovery.

▶ Specify devices – add an entry for each PRIMEQUEST Enclosure to be discovered. Provide the required SNMP credentials by selecting a Run As account. Select *Access mode*: *ICMP and SNMP* or *SNMP*.

You can run the Network Discovery Rule manually or wait until SCOM runs it.

4.4.3　SNMP Credentials

Valid credentials are required to communicate with the PRIMEQUEST Enclosure using SNMP.

Discovery and monitoring workflows, defined in *Fujitsu PRIMEQUEST Enclosure* management pack, use the same Run As accounts as selected during configuration of Network Device discovery. SCOM automatically stores this information in Run As profiles *SNMP Monitoring Account* and *SNMPv3 Monitoring Account*. These profiles are used by the management pack to get SNMP credentials. If network devices are successfully discovered then PRIMEQUEST discovery and monitoring will be executed and no additional credential configuration is needed.

To receive SNMP traps from PRIMEQUEST Enclosure, proper Run As Account must be added to Run As Profile *Fujitsu PRIMEQUEST Trap,* which is provided by *Fujitsu PRIMEQUEST Enclosure (SNMP Traps)* management pack. When adding an account to this profile the user has to choose a *Primequest Enclosure* object which is to be managed by this account.

SCOM only supports SNMPv1 and SNMPv2c traps. The PRIMEQUEST Enclosure must be configured accordingly.

Discovery and monitoring workflows use the SNMP community string "public" when no credentials are provided by SCOM.

Run As Accounts used for discovery and monitoring workflows are shown in column "RunAs Account" in SCOM view Administration -> Network Management -> Network Devices. This view does not show accounts used for SNMP trap receiving.

⚠ Column "RunAs Account" in Network Devices view may show invalid information if an account was added to *SNMP Monitoring Account* profile with target "All targeted objects". It is advised not to add such entry to this profile.

4.4.3.1　Changing account assignment

Following steps must be executed to change Run As Account used for discovery and monitoring workflows:

▶ Delete a network device. It will be automatically deleted from a discovery rule which was used to discover the device.

▶ Add the network device to a Network Discovery rule, choose new Run As Account.

▶ Run the discovery and wait for the device to be discovered.

To change account used for SNMP trap receiving, edit properties of *Fujitsu Primequest Trap* profile. No rediscovery of the device is needed.

4.4.3.2   SNMPv3 configuration

The configuration procedure has two steps.

In the first step, a SNMPv3 user is created in the PRIMEQUEST Enclosure via the WebUI. Go to *Network Configuration -> SNMP Configuration -> Community*. In the *Community* table enter the user configuration data in one of the rows. Click the *Apply* button after editing.

Description of the columns in the table:

- Community/User – SNMPv3 user name
- IP Address/MASK – host or network from which connections are allowed
- SNMP Version – SNMP version to use; select "3" from combo box to enable SNMPv3
- Access – read-only or read-write mode selection
- Auth – authentication and privacy protocols to use; possible values:
  - noauth – authentication and privacy protocols are enabled
  - auth – authentication protocol is enabled, privacy protocol is not enabled
  - priv – authentication and privacy protocols are enabled

Community table in PRIMEQUEST WebUI

Next, go to *SNMPv3 Configuration* in WebUI. Select the checkbox in one of the rows of the *User* table and edit the row. Click the *Apply* button after editing.

Description of the columns in the table:

- User Name – SNMPv3 user name, it must be the same as in the *Community* table
- Auth Type – MD5 or SHA authentication protocol; entry is ignored if authentication protocol is not enabled
- Auth passphrase – authentication key for the user; entry is ignored if authentication protocol is not enabled
- Priv passphrase –privacy key for the user; entry is ignored if privacy protocol is not enabled

> ℹ The PRIMEQUEST Enclosure supports only the DES privacy protocol.

User table in PRIMEQUEST WebUI

In the second step, a Run As Account is created in SCOM. In the SCOM Console go to the *Administration* pane and select the *Accounts* item. Create a Run As Account of type *SNMPv3 Account* or open the properties of an existing account of this type.

Credentials settings of a SCOM Run As Account

On the *Credentials* tab enter the same data as provided the first step in the PRIMEQUEST Enclosure WebUI. Enter the user name. Select the authentication protocol and key if authentication is used, otherwise select *None*. If a privacy protocol is used then select *DES* and enter the privacy key, otherwise select *None.* Leave the *Context* field empty.

When the Run As Account is configured it may be used in SCOM for network device discovery and PRIMEQUEST Enclosure monitoring.

4.4.4   Traps

To be able to receive SNMP traps from managed PRIMEQUEST Enclosures the *Fujitsu PRIMEQUEST Enclosure (SNMP Traps)* management pack must be imported to SCOM. SCOM only supports SNMPv1 and SNMPv2c traps. The PRIMEQUEST Enclosure must be configured accordingly.

All SNMP traps are handled by the resource pool that was selected in network device discovery configuration. SCOM arbitrarily chooses one Management Server from the pool to be the trap receiver. This server can be changed by SCOM at any time. For this reason PRIMEQUEST Enclosures have to be configured to send traps to all Management Servers from the resource pool.

Windows' *SNMP Trap* service must be disabled on all Management Servers from the resource pool. If the service is enabled SNMP traps are intercepted by this service and cannot be received

by SCOM. Any other service that listens for SNMP traps must also be disabled. The only application which is allowed to listen for SNMP traps is the SCOM Monitoring Agent.

The *Fujitsu PRIMEQUEST Trap* profile, installed by the *Fujitsu PRIMEQUEST Enclosure (SNMP Traps)* management pack, must be provided with Run As accounts with valid SNMP credentials for the PRIMEQUEST Enclosures which send the traps. When adding an account to the profile the PRIMEQUEST Enclosure object must be chosen. The same credentials must be set in PRIMEQUEST Enclosure through its WebUI.

To validate the configuration it is possible to send a test trap using an option in WebUI. If the configuration is correct an alert will appear in SCOM.

Each SNMP trap has its own rule in the *Fujitsu PRIMEQUEST Enclosure (SNMP Traps)* management pack.

SNMP traps with severity "INFORMATIONAL" are ignored (except the test trap). Rules for SNMP traps with severity "MINOR" are disabled by default. They can be enabled in Authoring pane in SCOM. Rules for SNMP traps with severity "MAJOR" and "CRITICAL" are enabled by default.

Example: SNMP trap with ID 777 is represented in the management pack as a rule with the name "Power unit sensor: major event occurred [PQ_MMBTRAP_777]".

4.4.5 Monitoring options

All components from one PRIMEQUEST Enclosure have the same monitoring period. It can be changed in Overrides section of PRIMEQUEST Enclosure discovery by adjusting the parameter *Monitoring Interval (seconds)*.

The new monitoring period will take effect after SCOM executes the discovery once. SCOM triggers a discovery shortly after its Overrides are changed.

4.4.6 Overrides

4.4.6.1 Discovery Overrides

The following discovery overrides are supported:

- Interval (seconds):
  Interval for the discovery scripts to run. The default is 14400 seconds (every 4 hours).

- Monitoring Interval (seconds):
  Monitoring interval applied to all objects hosted in a specific PRIMEQUEST Enclosure. This

override is available only in the PRIMEQUEST Enclosure discovery. The default is 360 seconds (every 6 minutes).

4.4.6.2 Monitor Overrides

Monitors do not have overrides other than the standard ones. The monitoring period is controlled by the *Monitoring Interval (seconds)* of the discovery.

4.4.6.3 Rule Overrides

Rules can be disabled or enabled with an override to the standard *Enabled* value.

4.4.7 Removing from monitoring

PRIMEQUEST Enclosure is removed from monitoring by deleting Network Device that represents this enclosure. The procedure is described below.

▸ Open the Administration pane in the SCOM Console and go to Network Devices.

▸ Select the Network Device that represents an enclosure.

▸ Click the *Delete* action.

▸ The action will delete the Network Device from SCOM together with the PRIMEQUEST Enclosure and its components.

4.5 Discovery

4.5.1 Discovery of PRIMEQUEST Enclosures and their components

The *Fujitsu PRIMEQUEST Enclosure* management pack checks the *System Object ID* attribute of each network device (represented by the *Node* class) in SCOM. If the ID is found to be the ID of a PRIMEQUEST Enclosure then the discovery workflow is executed for this Network Device.

The discovery process runs scripts that communicate with the PRIMEQUEST Enclosure using SNMP. Scripts create objects in SCOM that represent the discovered PRIMEQUEST Enclosure and its components.

The discovery process is composed of two workflows. The first workflow (PRIMEQUEST Enclosure discovery) is targeted to the Node class and creates an object that represents the discovered PRIMEQUEST Enclosure. The second workflow (PRIMEQUEST Unit discovery) is targeted to the PRIMEQUEST Enclosure class and creates objects which represent the enclosure's components.

Scripts are executed on the Management Servers of the resource pool which was selected in the network device discovery configuration.

The default discovery period is 4 hours. It can be changed via override. Each of the two discovery workflows has its own period setting.

4.5.2   PRIMEQUEST components

The hardware components of a PRIMEQUEST Enclosure which are listed below can be discovered and monitored.

4.5.2.1   Enclosure

This object hosts all components of a PRIMEQUEST Enclosure.

Icon	Information	
	Display Name:	<Enclosure name>
	Model:	<Model name>
	Serial Number:	<Serial number>
	Operating System:	<Operating system>
	IP address:	<IP address>
	Designation:	<Enclosure designation>
	Manufacturer:	<Manufacturer>
	Location:	<Location>
	Contact:	<Responsible person>
	Web Interface URL:	<URL of Web Interface>
	Monitoring interval (s):	<Monitoring interval in seconds>

4.5.2.2 Units

Available units are discovered and grouped in the collections. Their data is displayed, and their health state is monitored.

Collection Icon	Information	
	Display Name: Unit count: Collection ID:	<Name of the collection> <Number of hosted units> <ID of the collection>
Component Icon		
	Display Name: Unit ID: Unit class: Index: Designation: Model: Manufacturer: Serial Number:	<Unit name> <ID of the unit> <Unit type name> <Number indicating location inside the Enclosure> <Designation> <Model name> <Manufacturer> <Serial Number>

Units representing partitions have additional attributes:

- Management IP address
- Management IPv6 address

4.5.2.3 Temperature Sensors

Temperature sensors which physically exist are grouped in the collections. Their data is displayed and their health state is monitored. Specific components are not discovered.

Collection Icon	Information	
	Display Name: Device count: Collection ID:	Temperature Sensors in <hosting unit name> <Number of hosted devices> <ID of the collection>

4.5.2.4 Fans

Fan modules which physically exist are grouped in the collections. Their data is displayed and their health state is monitored. Specific components are not discovered.

Collection Icon	Information	
	Display Name: Device count: Collection ID:	Fans in <hosting unit name> <Number of hosted devices> <ID of the collection>

4.5.2.5 Voltages

Voltage sensors which physically exist are grouped in the collections. Their data is displayed and their health state is monitored. Specific components are not discovered.

Collection Icon	Information	
	Display Name: Device count: Collection ID:	Voltages in <hosting unit name> <Number of hosted devices> <ID of the collection>

4.5.2.6 Power Supplies

Power supply modules which physically exist are discovered and grouped in the collections. Their data is displayed and their health state is monitored.
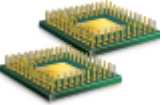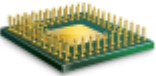
Collection Icon	Information	
	Display Name: Device count: Collection ID:	Power Supplies in <hosting unit name> <Number of hosted devices> <ID of the collection>

Component Icon		
	Display Name: Device ID: Designation:	\<Device name> \<Device ID> \<Designation>

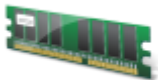## 4.5.2.7 CPUs

Processors which physically exist are discovered and grouped in the collections. Their data is displayed and their health state is monitored.

Collection Icon	Information	
	Display Name: Device count: Collection ID:	CPUs in \<hosting unit name> \<Number of hosted devices> \<ID of the collection>
Component Icon		
	Display Name: Device ID: Designation: Model: Number of cores:	\<Device name> \<Device ID> \<Designation> \<Model name> \<Number of cores>

4.5.2.8 Memory Modules

Memory modules which physically exist are discovered and grouped in the collections. Their data is displayed and their health state is monitored.

Collection Icon	Information	
	Display Name: Device count: Collection ID:	Memory Modules in \<hosting unit name> \<Number of hosted devices> \<ID of the collection>

Component Icon		
	Display Name: Device ID: Designation: Capacity:	<Device name> <Device ID> <Designation> <Capacity>

4.5.2.9 Batteries

Batteries which physically exist are discovered and grouped in the collections. Their data is displayed and their health state is monitored.

Collection Icon	Information	
	Display Name: Device count: Collection ID:	Batteries in <hosting unit name> <Number of hosted devices> <ID of the collection>
Component Icon		
	Display Name: Device ID: Designation:	<Device name> <Device ID> <Designation>

4.6 Monitoring

4.6.1 Monitor types

The *Fujitsu PRIMEQUEST Enclosure* management pack provides the following health monitors:

- Unit monitor
- Device monitor
- Device collection monitor

- Other components monitor

- Communication monitor

The *Fujitsu PRIMEQUEST Enclosure (SNMP Traps)* management pack provides the following monitors:

- SNMP Trap Service State monitor

The state of each discovered object is rolled up to its hosting object, up to the Enclosure object.

4.6.1.1 Unit monitor

A Unit Monitor monitors the health state of units. It has three possible values: Healthy, Warning and Critical. Each Unit object has its own monitor instance.

4.6.1.2 Device monitor

A Device Monitor monitors the health state of devices. It has three possible values: Healthy, Warning and Critical. Each Device object has its own monitor instance.

This monitor does not exist for devices of types:

- Temperature Sensor

- Fan

- Voltage

These devices are represented only by Device collections and do not have corresponding Device objects in SCOM.

4.6.1.3 Device collection monitor

A Device Collection Monitor shows the aggregated health state of all devices represented by a Device collection. Aggregation is done by evaluation the worst health state of all devices. This monitor has three possible values: Healthy, Warning and Critical. Each Device Collection object has its own monitor instance.

This monitor exists only for device types:

- Temperature Sensor

- Fan

- Voltage

Other Device Collection types do not have this monitor because their health state is monitored by dedicated Device monitors.

When the Device Collection monitor is in an unhealthy state this means that one or more of the collections devices are unhealthy. The list of unhealthy devices is shown in Health Explorer on the State Change Events tab in the Details section.

This section shows three entries: the aggregated health state, the designations of devices which are in Warning state and the designations of devices which are in Critical state.
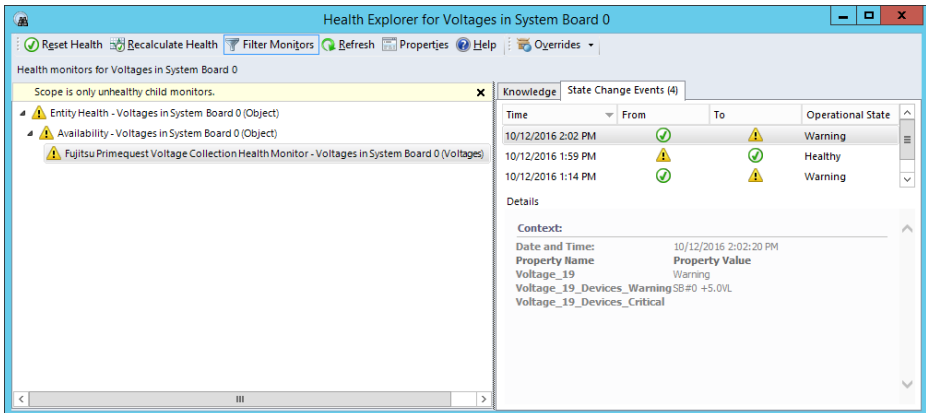
Example of an unhealthy state of the device collection monitor

4.6.1.4 Other components monitor

This monitor shows status of PRIMEQUEST components that are not represented in SCOM by dedicated object. It has three possible values: Healthy, Warning and Critical.
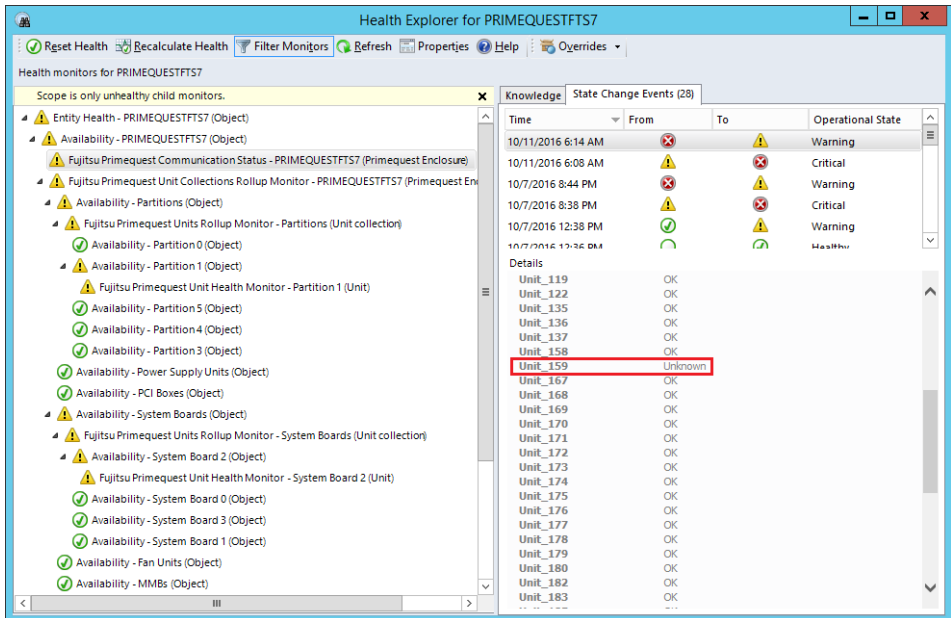
4.6.1.5 Communication monitor

This monitor checks the status of the communication between SCOM Management Server and a PRIMEQUEST Enclosure. It also verifies that the PRIMEQUEST Enclosure returned known values for all its components. There is one such monitor per PRIMEQUEST Enclosure.

It has three possible states:

- Healthy – communication is established and all components have a known state.

- Warning –communication is established, but at least one component (unit or device) has an unknown state.

- Critical – monitoring workflow cannot read data from PRIMEQUEST Enclosure.

A list of components which have an unknown state is shown in Health Explorer on the State Change Events tab in the Details section.

Example of an unhealthy state of the communication monitor

4.6.1.6   SNMP Trap Service State monitor

The Windows service *SNMP Trap* must be disabled on all Management Servers that listen for SNMP traps. If the service is enabled then SNMP traps will be intercepted by this service and will not be received by SCOM.

This monitor checks the *SNMP Trap* service state on all Management Servers in the SCOM Management Group. This monitor is disabled by default and must be enabled manually for all Management Servers which act as SNMP trap receivers.

This monitor shows warning if the SNMP Trap service is in "running" state. The following steps must be executed on the Management Server in this case:

▸   Disable the SNMP Trap service.

▸   Ensure that no other service listens for SNMP Traps (except SCOM Monitoring Agent).

▸   Restart the SCOM Monitoring Agent to ensure that all trap rules are loaded properly.

▸   Send a test trap using the PRIMEQUEST WebUI to verify that SCOM receives traps.

4.6.2 Alerts

The *Fujitsu PRIMEQUEST Enclosure* management pack generates an alert in SCOM when one of the health monitors becomes unhealthy. The alert is resolved automatically when the monitor goes back to the healthy state.

If the *Fujitsu PRIMEQUEST Enclosure (SNMP Traps)* management pack is installed and configured then alerts are created when a SNMP trap from a PRIMEQUEST Enclosure is received. The PRIMEQUEST Enclosure sends these traps when it detects a problem. Alerts from traps are not automatically resolved. Many identical SNMP traps are suppressed and shown in SCOM only in the increased repeat counter of the alert.

SNMP traps with severity *CRITICAL* and *MAJOR* are shown in SCOM as alerts with severity *Critical*. Traps with severity *MINOR* are shown as alerts with severity *Warning.* Rules for *MINOR* traps are disabled by default. Traps with severity *INFORMATIONAL* are ignored (except *Test Trap*). All alerts are generated with *Medium* priority.


4.7   Views

When integrating the *Fujitsu PRIMEQUEST Enclosure* management pack a new folder *PRIMEQUEST Enclosures* is created below the Fujitsu ServerView Systems folder in the Monitoring pane of the SCOM Console. The following views are displayed in this folder:

- Active Alerts

- Enclosure State

- Unit Health Monitoring

    - Disk Unit Health
    - I/O Unit Health
    - MMB Health
    - Other Unit Health
    - Partition Health
    - Power Supply Unit Health
    - SAS Unit Health
    - System Board Health

- Device Health Monitoring

    - Battery Health
    - CPU Health
    - Fan Health

- Memory Health
- Power Supply Health
- Temperature Health
- Voltage Health

*Fujitsu PRIMEQUEST Enclosure (SNMP Traps)* management pack does not provide additional views.
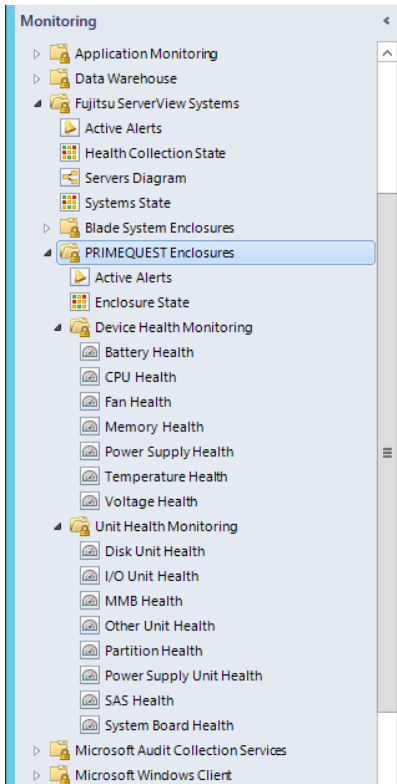
Folders and views of the *PRIMEQUEST Enclosure Integration Pack* with main folder selected.

4.7.1   Active Alerts

This view shows all alerts that apply to monitored PRIMEQUEST Enclosures and their components. Those alerts are generated by health monitors or by rules for SNMP traps.

4.7.2 Enclosure State

This view shows all monitored PRIMEQUEST Enclosures and their aggregated health states. The columns of the view display Enclosure properties and the aggregated health states of various unit types.
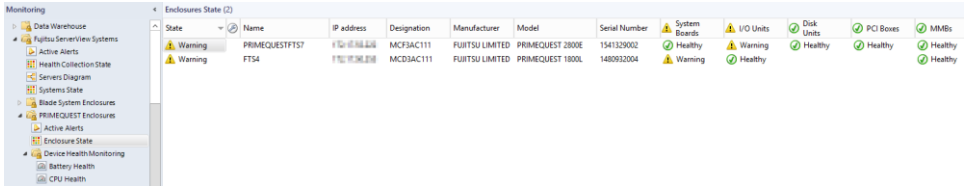
Enclosure State view

4.7.3 Unit Health Monitoring

The *Unit Health Monitoring* views display the health state and corresponding alerts of the specific units the view targets. The upper view lists units, their state and properties. The second view shows alerts that apply to the units from the upper view and to the devices that are hosted by those units.
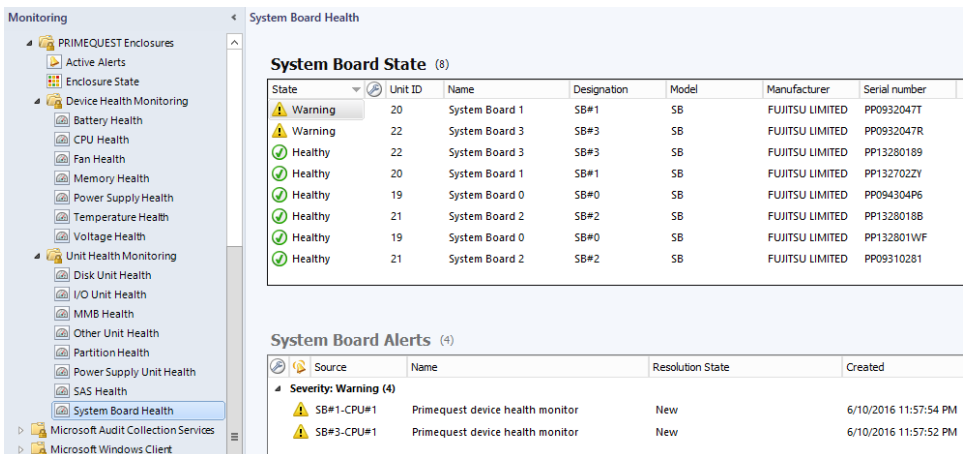
Unit Health view

4.7.4 Device Health Monitoring

The *Device Health Monitoring* views display the health state and corresponding alerts of the specific devices the view targets. The upper view lists devices or device collections, their state and properties. The second view shows alerts that apply to the devices or device collections from the upper view.

Device types which are represented only by device collections have views with a list of device collections. Remaining device types have views with a list of devices. For details, see chapter 4.3.4 Device collection.

Following views show devices:

- Battery Health

- CPU Health

- Memory Health

- Power Supply Health

Following views show device collections:

- Fan Health
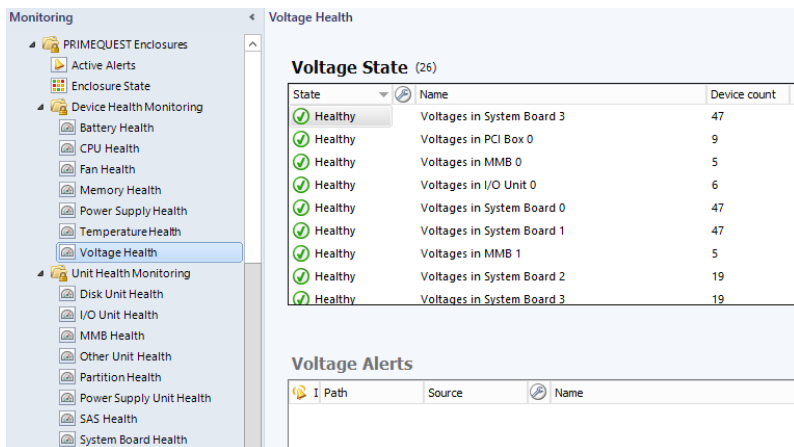
- Temperature Health

- Voltage Health

View with health status of devices

View with health status of device collections

4.8 Health Explorer

The Health Explorer can be started from various views. It shows the components and dependencies in a tree structure. When components are in the *Warning* or *Critical* state, the corresponding subdirectories are automatically expanded in the display.

Two different displays are possible in the right-hand window of the Health Explorer: *Knowledge* and *State Change Events*. Information on what the monitor displays and which actions (resolutions) are possible and recommended is provided under the *Knowledge* tab.

All state transitions (*OK* <-> *Degraded* <-> *Error*) of the component selected from the navigation window on the left are displayed under the *State Change Events* tab.

If the state is not *OK*, the component is placed in the *Degraded* or *Error* state. If two or more components show different health states, the instance with the severest error determines the overall status of the group.

4.9 Tasks

Tasks are actions which can be executed by user. They are displayed in the Tasks pane when a PRIMEQUEST Enclosure or its component is selected in a view.

The *Fujitsu PRIMEQUEST Enclosure* management pack provides following tasks:

● Open PRIMEQUEST Web UI – opens PRIMEQUEST WebUI in the default internet browser.

4.10 Knowledge Base

A Knowledge Base is provided for monitors and alerts. Various possible resolutions / actions are displayed after a problem is detected.

5 Appendix

5.1 Log files

Log files can be created for error analysis. The log files are stored in the subdirectory *SVISCOM\SVISCOM-PQ* of the directory entered in the system environment variable TEMP. Usually this is the *C:\Windows\TEMP* directory (where *C:* represents the system partition in this example).

Logging options are defined in the file *SVSISCOM-PQ-Log.xml* in this folder. If the file does not exist or was created by an older version of the Management Pack, a new file with the name *SVISCOM-PQ-Log.xm_* is generated in the *%TEMP%\SVSCOM\SVISCOM-PQ* folder.

*SVISCOM-PQ-Log.xm_* contains debug options for discovery and monitoring features of the management packs.

In the case of error analysis using log files proceed as follows.

▶   Rename SVISCOM-PQ-Log.xm_ to SVISCOM-PQ-Log.xml. If SVISCOM-PQ-Log.xml already exists, check that all options of SVISCOM-PQ-Log.xm_ also exist in SVISCOM-PQ-Log.xml.

▶   Set desired debug options in SVISCOM-PQ-Log.xml.

Description of debug options in the logging configuration file:

Parameter	Possible values	Default value	Description
DebugMode	yes, no	yes	Write log messages to files.
OverWrite	yes, no	no	Clear previous log file when script starts.
MaxLogSizeKB	>= 0	1024	Maximum size of log file before it is rotated. Parameter ignored when *OverWrite* set to yes. Setting it to 0 means continuous logging, no rotation is performed.

i	Each Management Server that handles PRIMEQUEST monitoring workflows has separate log files and separate logger configuration. For example, enabling logger on one Management Server does not enable it on other Management Servers.

▶ Up to 4 hours are necessary for all log files to be generated. This is equal to period of discovery workflow which has the longest period of all workflows.

▶ Log files created in %TEMP%\SVSCOM\SVISCOM-PQ folder must be sent to Fujitsu Support for further analysis.

If you wish to disable the creation of log files again, delete or rename *SVISCOM-PQ-Log.xml* or change the logging options within the file.

5.2   Troubleshooting

-

5.3   Hints and known issues

-