System System 800xA

PC, Network, and Software Monitoring Configuration

System Version 5.1

Power and productivity
for a better world™

ABB

System 800xA

PC, Network, and Software Monitoring Configuration

System Version 5.1

NOTICE

This document contains information about one or more ABB products and may include a description of or a reference to one or more standards that may be generally relevant to the ABB products. The presence of any such description of a standard or reference to a standard is not a representation that all of the ABB products referenced in this document support all of the features of the described or referenced standard. In order to determine the specific features supported by a particular ABB product, the reader should consult the product specifications for the particular ABB product.

ABB may have one or more patents or pending patent applications protecting the intellectual property in the ABB products described in this document.

The information in this document is subject to change without notice and should not be construed as a commitment by ABB. ABB assumes no responsibility for any errors that may appear in this document.

In no event shall ABB be liable for direct, indirect, special, incidental or consequential damages of any nature or kind arising from the use of this document, nor shall ABB be liable for incidental or consequential damages arising from use of any software or hardware described in this document.

This document and parts thereof must not be reproduced or copied without written permission from ABB, and the contents thereof must not be imparted to a third party nor used for any unauthorized purpose.

The software or hardware described in this document is furnished under a license and may be used, copied, or disclosed only in accordance with the terms of such license. This product meets the requirements specified in EMC Directive 2004/108/EC and in Low Voltage Directive 2006/95/EC.

TRADEMARKS

All rights to copyrights, registered trademarks, and trademarks reside with their respective owners.

Release: July 2015
Document number: 3BUA000447-510 B

Table of Contents

INDEX

About This Book

General

This instruction describes configuration activities for PC, Network and Software Monitoring, including Basic Computer Monitoring functionality. This product functionality consists of system extensions to the 800xA Base System.

Document Conventions

Microsoft Windows conventions are normally used for the standard presentation of material when entering text, key sequences, prompts, messages, menu items, screen elements, etc.

Warning, Caution, Information, and Tip Icons

This publication includes **Warning**, **Caution**, and **Information** where appropriate to point out safety related or other important information. It also includes **Tip** to point out useful hints to the reader. The corresponding symbols should be interpreted as follows:

Electrical warning icon indicates the presence of a hazard which could result in *electrical shock.*

Warning icon indicates the presence of a hazard which could result in *personal injury.*

Caution icon indicates important information or warning related to the concept discussed in the text. It might indicate the presence of a hazard which could result in *corruption of software or damage to equipment/property.*

Information icon alerts the reader to pertinent facts and conditions.

Tip icon indicates advice on, for example, how to design the project or how to use a certain function

Although **Warning** hazards are related to personal injury, and **Caution** hazards are associated with equipment or property damage, it should be understood that operation of damaged equipment could, under certain operational conditions, result in degraded process performance leading to personal injury or death. Therefore, **fully comply** with all **Warning** and **Caution** notices.

Terminology

A complete and comprehensive list of Terms is included in the System 800xA, Engineering Concepts instruction (3BDS100972*). The listing in Engineering Concepts include terms and definitions as they apply to the 800xA system where in the usage is different from generally accepted industry standard definitions and definitions in standard dictionaries such as ***Webster's Dictionary of Computer Terms***.

Related Documentation

A complete list of all documents applicable to the 800xA Extended Automation System is provided in Released User Documents, 3BUA000263*. This document lists applicable release notes and user instructions. It is provided in PDF format and is included on the Release Notes/Documentation media provided with the system. Released user documents are updated with each release and a new file is provided that contains all user documents applicable for that release with their applicable document number. Whenever a reference to a specific instruction is made, the instruction number is included in the reference.

Section 1 Introduction

Product Overview

Standard PC and network equipment is used extensively in automation systems. The correct behavior and status of this equipment has a significant impact on the performance, reliability, and functional availability of an automation system and thus the industrial process being controlled.

The PC, Network and Software Monitoring (PNSM) software can independently monitor the status of Information Technology (IT) Assets. By default, IT Asset status is viewable through the 800xA System Status Viewer, or through the standard faceplates provided with each of the predefined IT Assets. When used in conjunction with Asset Optimization Asset Monitoring alarms are generated based on error conditions. The IT Asset status is viewed through the Asset Viewer and Asset Reporter.

Asset Optimization functionality is not available unless Asset Optimization Asset Monitoring has been installed and a license has been purchased. Refer to *System, 800xA - Asset Optimization, Configuration (3BUA000118*)* and *System 800xA - Asset Optimization, Operation (3BUA000150*)* for detailed information pertaining to Asset Optimization Asset Monitoring.

Once PNSM is installed in the 800xA System, the data can be used to:

*   Generate alarms

*   Produce historical reports

*   Update live trends and graphics

*   Receive alert or trap messages from ESXi server

Basic Computer Monitoring (BCM) builds upon this framework to simplify the process of monitoring the workstation nodes in an 800xA System. Workstation nodes are monitored for key health indicators and alarms are generated if monitored values deviate from expected limits.

Product Scope

PC, Network and Software Monitoring comprises of the following components:

- An OPC Server (PC, Network and Software Monitoring Server) that supplies IT Asset data to the system.

- A set of IT Aspect types that access the IT status data inside the Operator Workplace making the IT status data available to any 800xA System client application.

- A set of predefined Object Types that allow a user to easily set up monitoring for many commonly used devices.

- An interface to Asset Optimization Asset Monitoring that generates alarms based on the state of the IT assets.

- SNMP Trap service to receive the trap messages from IT devices and generate alarm & event notifications in the system.

Data comes into the system through Windows Management Instrumentation (WMI) technology. WMI is a standard interface for IT instrumentation, and it supports a number of communication protocols, including the Simple Network Management Protocol (SNMP). The SNMP is the standard communication protocol used to monitor and manage network devices.

The PC, Network and Software Monitoring Server uses WMI to access live status information that is sent to the Operator Workplace through the standard OPC interface. The Operator Workplace makes the data available for use by any part of the system. It is accessible by properties on the asset objects configured in the Operator Workplace.

Asset Optimization Asset Monitoring uses these properties to access the data and determine if alarm conditions exist by processing configuration data provided by the user. If an alarm condition exists in any of the assets, Asset Optimization Asset Monitoring generates alarm messages and sends them to the Operator Workplace. The alarms are then integrated into the normal alarm stream and displayed using the standard alarm display tools.

In addition to the OPC access to IT device data, PC, Network and Software Monitoring Server receives the trap messages from IT devices. The trap messages are converted into the alarm and event messages.

The architecture drawing is shown in Figure 1.
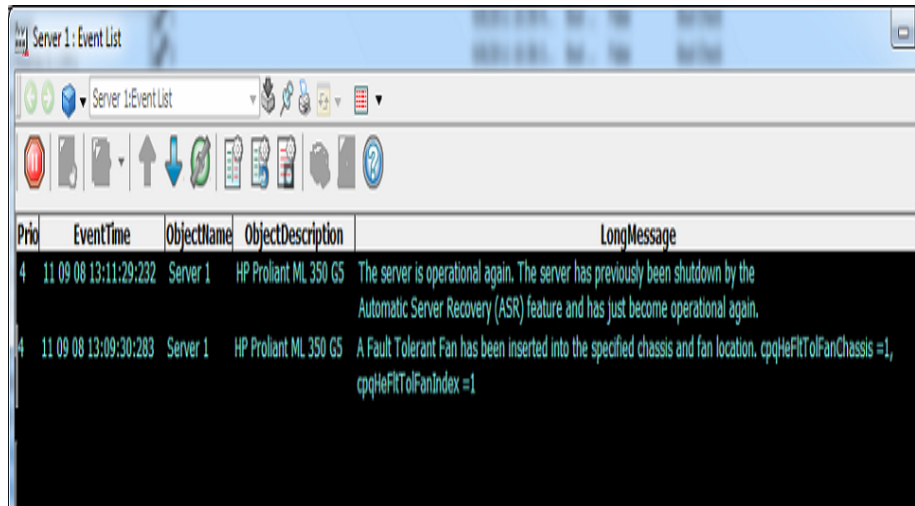
Figure 1. PC, Network and Software Monitoring Architecture

PC, Network and Software Monitoring uses the following terms to define its structure:

- IT Assets:
    - Assets such as computers, routers, switches, printers, etc.
    - Typically represented with an IP address.

- IT Devices:
    - Components of IT Assets. Parts of the IT Asset that have information which can be monitored.
    - A physical device (e.g. network card) or a software component (e.g. Operator Workplace).
    - IT Assets typically consist of multiple IT Devices.
    - The same IT Device may exist in different types of IT Assets (e.g. the same process may run on different computer configurations).

- Properties:
  - Individual monitoring of data elements on an IT Device (example error rate on a particular port on a particular switch).
  - Many properties may exist on a single IT Device.

Basic Computer Monitoring consists of a set of predefined 800xA System objects and a configuration tool that together provide the functionality required for configuration and monitoring.

Section 2 PC, Network and Software Monitoring Setup

Introduction

This section contains information for setting up PC, Network and Software Monitoring and Basic Computer Monitoring functionality.

PC, Network and Software Monitoring Server Configuration

The PC, Network and Software Monitoring server installation has the default IT OPC Server Network object provided with PNSM system extension and it should not be deleted.

The IT OPC Server Network object has the following functions:
- Integrate with AO to create IT Assets and provide the IT Assets with alarm generation capability.
- Provide IT Asset regeneration capabilities.

The following items are required in the PC, Network and Software Monitoring system:

- IT OPC Server Network Object.
- Configuring the OPC Data Source Definition.
- Asset Optimization Aspects.
- IT General Setup Aspect.
- Configuring IT SNMP Trap Service
- Configuring IT Device SNMP Configuration Aspect

IT OPC Server Network Object

> An IT OPC Network Object with the name "IT Server" is already defined in the default configuration and available under Root in Control Structure. It is recommended to retain this default name. Refer to Configuring the OPC Data Source Definition to configure an exiting IT OPC Network Object.

To create a new IT OPC Server Network:

1. Use the Structure Selector to open the Control Structure.

2. Right-click on `Root,Domain` and select **New Object...** from the context menu that appears.

3. The New Object dialog appears. Select `IT OPC Server Network` (under 3rd party OPC server support group) and click **Next**.

4. Click **Add** in the additional arguments dialog to select the PNSM connectivity server.

5. Select ABB.ShadowOPCServer under the OPC server, ProgID.

6. Click **Create**.

Configuring the OPC Data Source Definition

To edit the OPC data source definition:

> It is not recommended that multiple OPC data sources point to the same node.

1. Use the Structure Selector to open the Control Structure.

2. Use the Object Browser to navigate to and select `IT OPC Server Network` in the Aspect Object Area.

3. Right-click on `OPC Data Source Definition` in the Aspect List Area and select **Config View** from the context menu that appears.

4. Click **New** in the Preview Area.

5. Click **Add** and select the appropriate service provider from the list.

6. Click **OK** twice.

7. Click **Apply**.

Asset Optimization Aspects

When using PC, Network and Software Monitoring with Asset Optimization the software must communicate with two Asset Optimization aspects, the Asset Optimization Server and the AM Service Data Source Definition, in order to generate alarms.

ℹ The procedures for setting up the required Asset Optimization aspects are in the *Managing Data Source Connections* and *Loading Asset Monitor Configurations to an AO Server* topics in Section 2 of System *800xA - Asset Optimization, Configuration (3BUA000118*)*.

IT General Setup Aspect

The IT General Setup aspect is used to link the IT OPC Server Network object to the Asset Optimization monitoring Server and Asset Monitor Data Source.

The steps to create and configure an IT General Setup aspect is described below:

ℹ An IT General Setup aspect is already defined in the default IT Server configuration. To configure an existing aspect go to Step 6.

1. Use the Structure Selector to open the Control Structure.

2. Use the Object Browser to navigate `IT OPC Server Network`.

3. Right-click on `IT OPC Server Network` and select **New Aspect...** from the context menu.

4. The New Aspect dialog appears.

    a. Check the **Show all** check box and uncheck the **List presentation** check box.

    b. Navigate to and select `IT General Setup` from the list that appears.

5. Click **Create**.

6. Select IT General Setup in the Aspect List Area. Figure 2 shows a
    configured IT General Setup aspect.
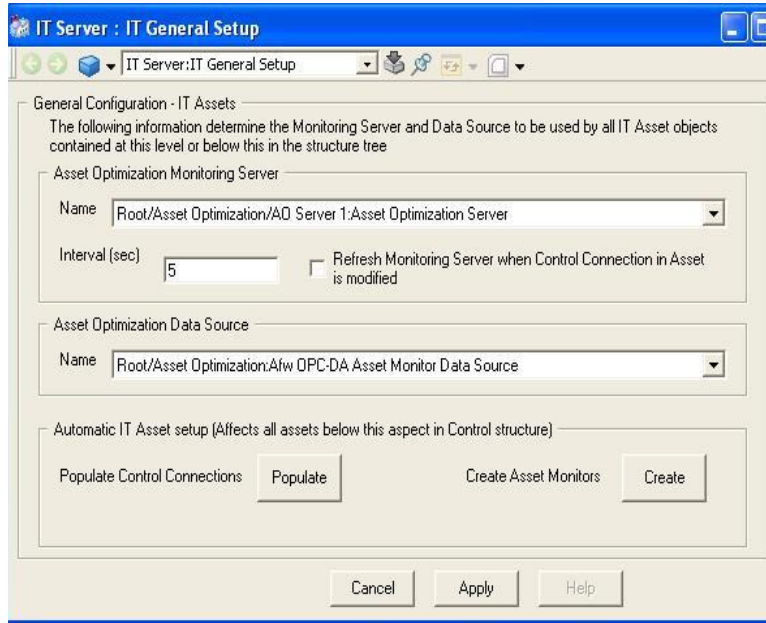
TC05108C

Figure 2. IT General Setup Aspect

The fields in the IT General Setup aspect are defined as follows:

–   **Name:** Two Name fields, one in the Asset Optimization Monitoring
    Server frame and the other in the Asset Optimization Data Source frame
    should be configured. Select the Asset Optimization Server to be
    monitored (suggested selection - Root/Asset Optimization/AO
    Server 1:Asset Optimization Server) and Asset Monitor Data
    Source (suggested selection - Root/Asset Optimization: Afw
    OPC-DA Asset Monitor Data Source) from the drop-down list
    boxes.

–   **Interval:** Value in seconds that defines how often the Asset Monitor is
    executed for each IT Asset.

– **Refresh Monitoring Server when Control Connection in Asset is modified:** If this check box is checked, populating the IT Control Connection from the IT Device Manager causes the same effect as clicking **Load all AMs** or **Load Selected Asset Monitors** from the Asset Monitors tab of the Asset Optimization Server aspect.

Refreshing the Monitoring Server frequently may cause a high CPU load.

– **Populate Control Connections:** Clicking on this button will populate the IT Control Connection for each of the IT Assets below this aspect.

– **Create Asset Monitors:** Clicking on this button will create IT Asset Monitor aspects for each of the IT Assets below this aspect.

An IT General Setup aspect can also be created inside an individual IT Asset object. The values used at this level will override the IT General Setup at the OPC Server network level, for this IT Asset only.

All custom values entered in the IT Asset Monitor aspect will be discarded when ITdevice manager regenerates the IT Asset Monitor. It is recommended to backup the custom values before regenerating the IT Asset Monitor.

Configuring IT SNMP Trap Service

IT SNMP Trap Service must be configured and running to monitor the ESXi server hardware, Tropos device and peripherals like SAN storage. The service is responsible to receive the trap messages from IT devices and present these messages as alarms & events in the system. Perform the following steps to configure IT SNMP Trap service.

In the Service Structure,

1. Open IT SNMP Trap Service, create new Service Group and then create the Service Provider.

2. Click on the **Service Provider** definition in the Aspect list area.

3. Click on the **Configuration Tab**. IT SNMP Trap Service should be enabled and Current state should be in **Service** and the node name should be the <Computer Name> as shown in the Figure 3.
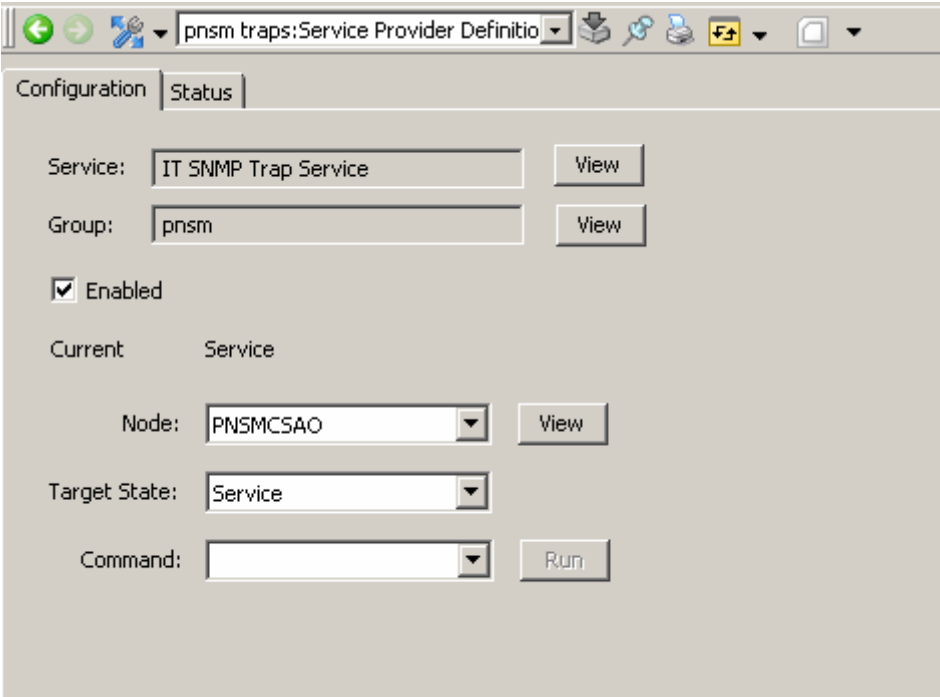
Figure 3. IT SNMP Trap Service in Service Structure

IT SNMP Trap Service is configured on PSNM Server.

There should be one IT SNMP Trap Service configured in the system.

Configuring IT Device SNMP Configuration Aspect

IT Device SNMP Configuration aspect is used to define the security aspect for monitoring SNMP Traps including V1, V2 and V3. For Tropos monitoring SNMP V3 is the only support available.

The device specific object types for Tropos Monitoring are included in the PNSM Library. Refer to the object type release notes for the configuration information.

Perform the following to configure IT Device SNMP.

1.   Select **IT Device SNMP Configuration** Aspect.

2.   In the IT Device SNMP Configuration window, provide the parameters configured in the device like User Name, Authentication Protocol, Authentication Password, Privacy Protocol and Privacy Password..

Figure 4. IT Device SNMP Configuration window

3.   Click **Apply**.

Configuring IT Device Traps Aspect

1. Select IT Device Traps.

2. Go to Configuration view of IT device Trap aspect.
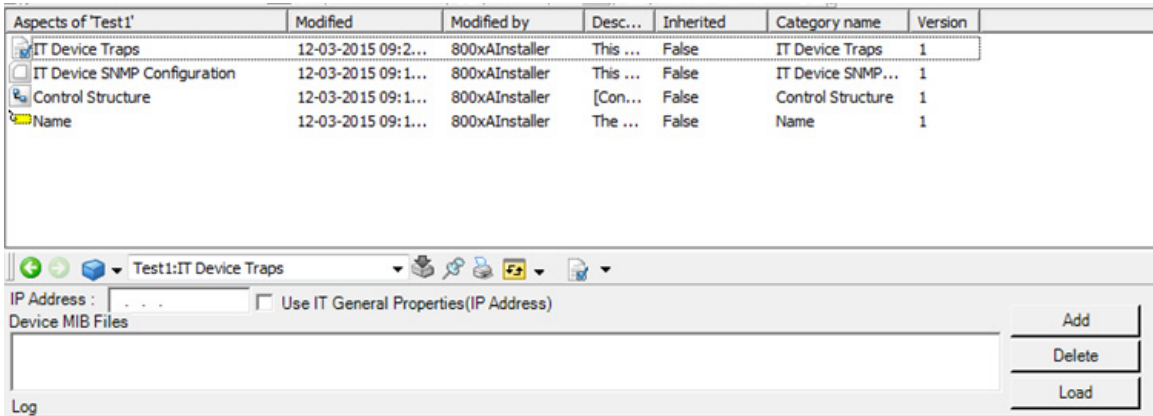
Figure 5. IT Device Traps selection

3. Click **Add** button and select the MIB files.
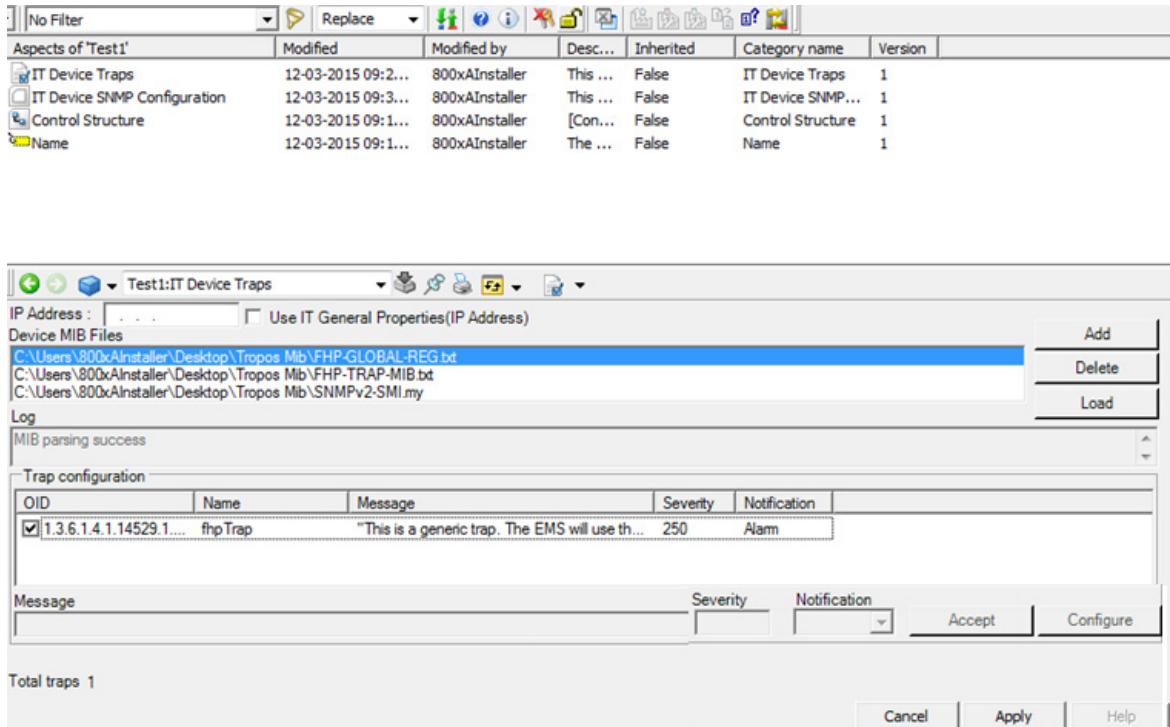
Figure 6. Selection of MIB Files

4.   Click **Load**.

Loaded trap gets displayed in the Trap configuration window. Refer Figure 6.

5.   Double click on Loaded Traps.

6.   Configure the Severity and Notification type and click **Accept**.

Severity needs to be defined as per the Notification Type.

If user needs to configure for sub-condition of Traps follow the steps from Step 7 to Step 10.

7.   Click **Configure**.

8.   In Configure Trap Objects window, select a valid **Trap Object** from the drop
      down.
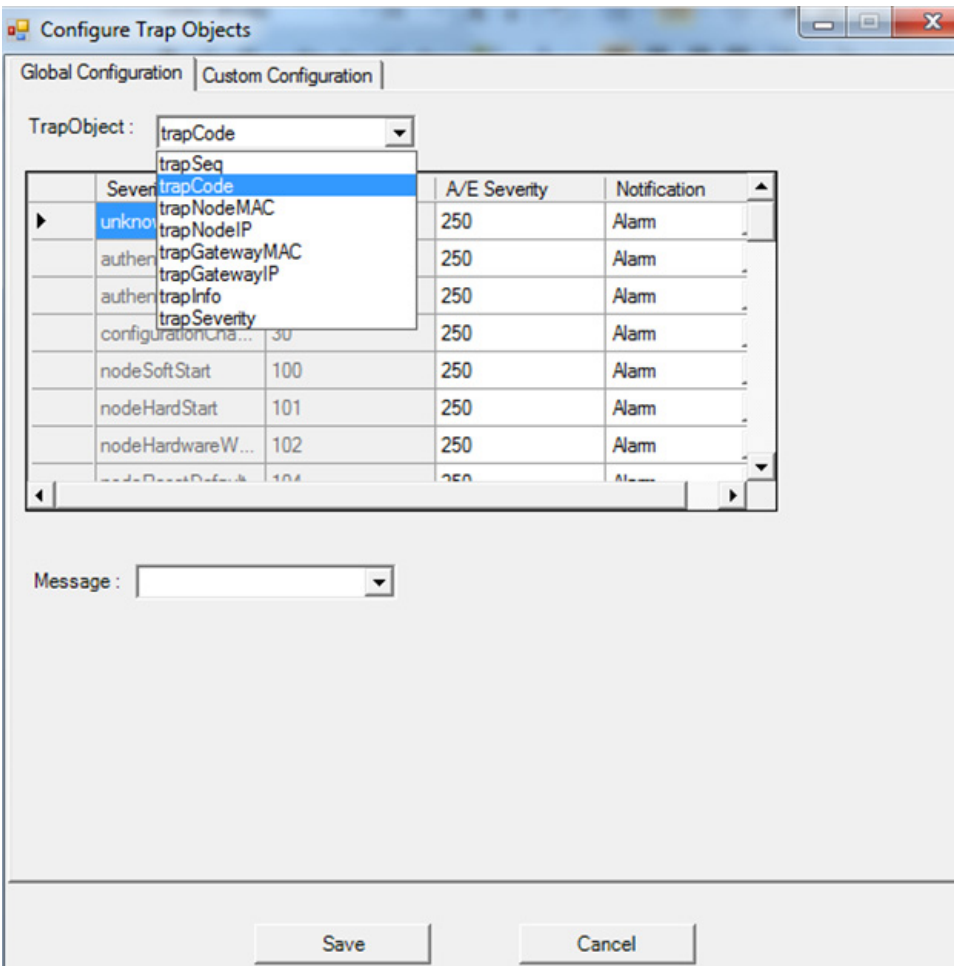
Figure 7. Selection of Trap Object

ℹ   Configure Traps sub condition as per the requirement of end user.

9. Select options from **Message** drop down to display the selected information in Alarm and Event list.
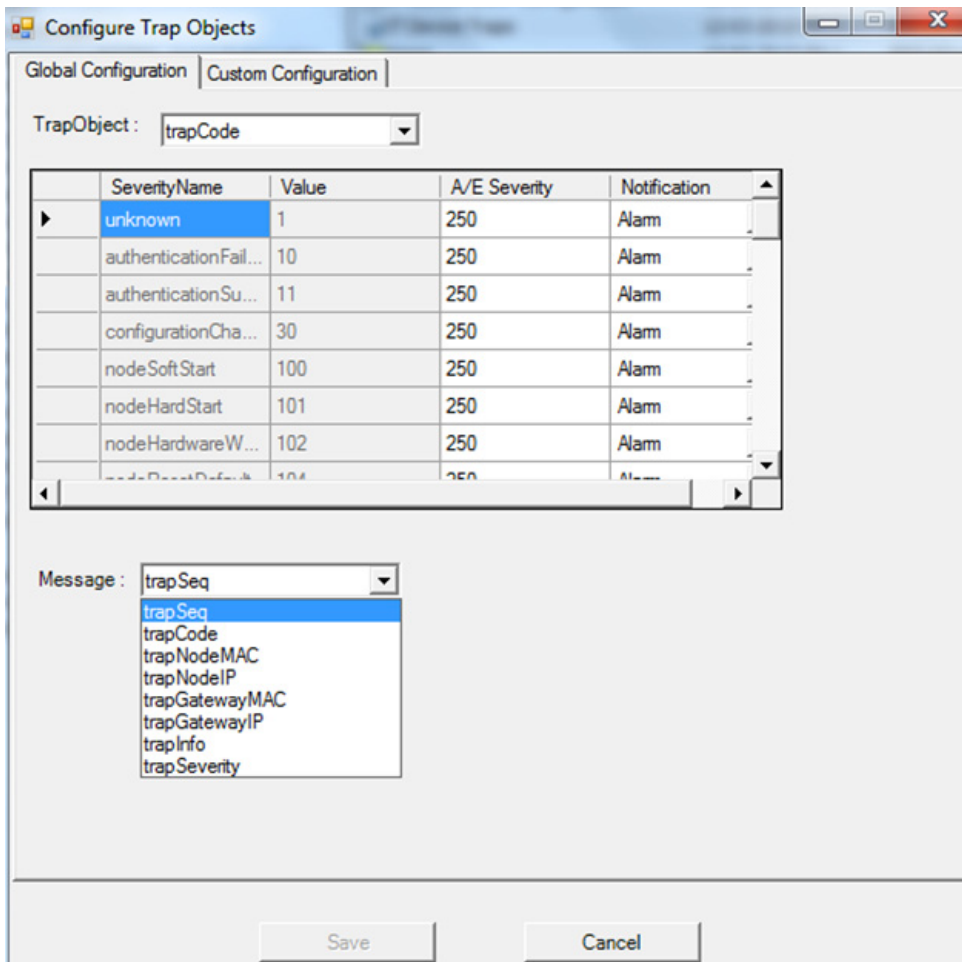
Figure 8. Selection of Objects from Message drop-down

10. Click **Save**.

If you want to override the Global Configuration for specific Traps, then follow Step 11 to Step 14:

11. Select the **Custom Configuration** tab and then select **trapCode** as Trap Object as shown in Figure 9.
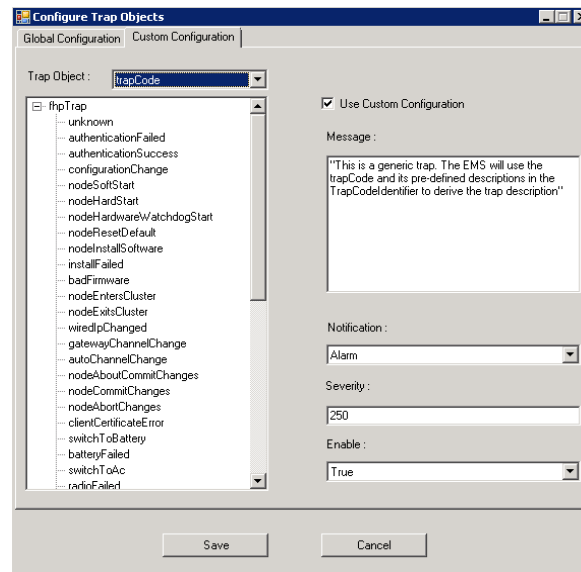
Figure 9. Trap Custom Configuration

12. Place a check mark next to **Use Custom Configuration** check box.

13. Set appropriate values under Message, Notification, Severity, and Enable.

14. Click **Save**.

15. Click **Apply** and then go to Main View of IT device SNMP configuration Aspect.

16. Provide **IP address** of Tropos device to be monitored or select General property to get IP address defined in Object type.

> If General property aspect is not available, IP address can be set from Object type faceplate or IT Device connection.

17. Click **Deploy**.

Configuring Alarm & Event List

Alarm and Event Lists are part of the base 800xA System and are added to objects when building the various structures. Building the various structures in the 800xA System is beyond the scope of this instruction. Refer to the appropriate System 800xA documentation for detailed information on the various 800xA System structures.

The Alarm and Event Lists are used to group alarm points together. They define the group of events being sent to the same group of people. For ease of use, take advantage of the defined structures to group the assets. All child objects in the structure can be defined as being included.

Operators can view Alarm and Event Lists according to the selected filter and presentation settings. These settings can be changed. For example, a list can be sorted by clicking on a column header, resizing columns, or moving them by using drag and drop.

Filtering and presentation functions allow alarms to be viewed in dedicated ways.

For example, a list can be configured to show all alarms or only those alarms relevant for the associated object and its descendents.

Traps are represented in 800xA as alarms and events.

Perform the following steps to configure Alarms in Alarm and Event List:

1. Use the **Object Browser** to navigate to an object with an Alarm and Event List to configure.

2. Select **Alarm and Event List** in the Aspect List Area.

3. Click the **View Configuration** button as shown in Figure 10.
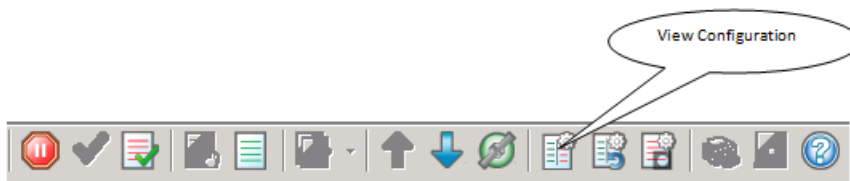
Figure 10. View Configuration button

The **Alarm and Event List Configuration** dialog appears as shown in Figure 11.
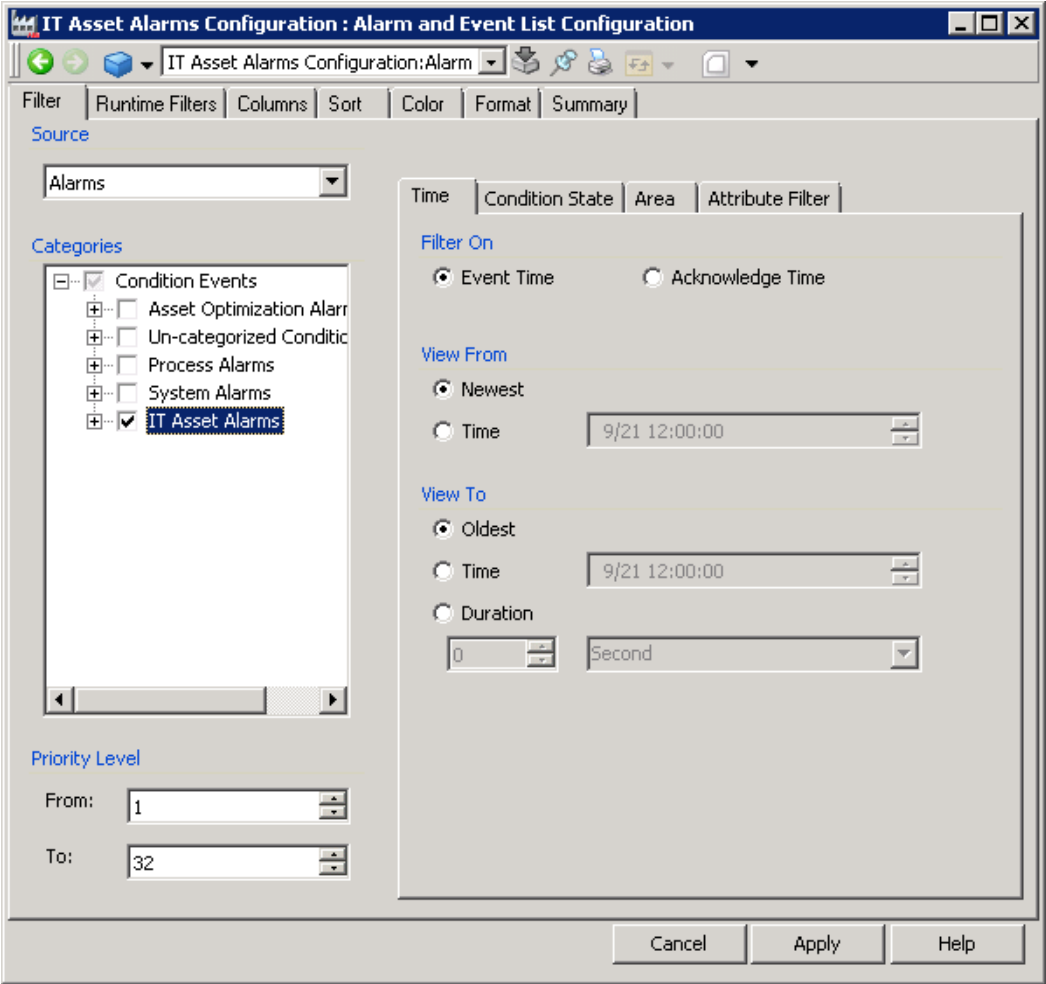
Figure 11. Alarm and Event List Configuration

4.   In the **Filter** tab on the Alarm and Event List, select the **IT Asset Alarms** checkbox to be filtered.

5.   Click **Apply** and then close the dialog.

Perform the following steps to configure Events in Alarm and Event List:

1.   Use the **Object Browser** to navigate to an object with Event List to configure.

2.   Select **Alarm and Event List** in the Aspect List Area.

3.   Click the **View Configuration** button as shown in Figure 12.
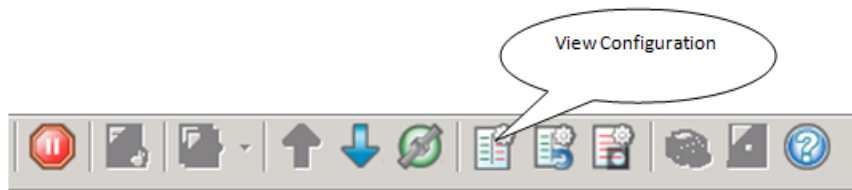
Figure 12. View Configuration button

The **Event List Configuration** dialog appears as shown in Figure 13.

4.   In the System events, select the **ITAssetTrapMessage** check box to filter out SNMP Traps.

5.   In the **Filter** tab on the Alarm and Event List, select these categories to be filtered.

6.   Click **Apply** and then close the dialog.
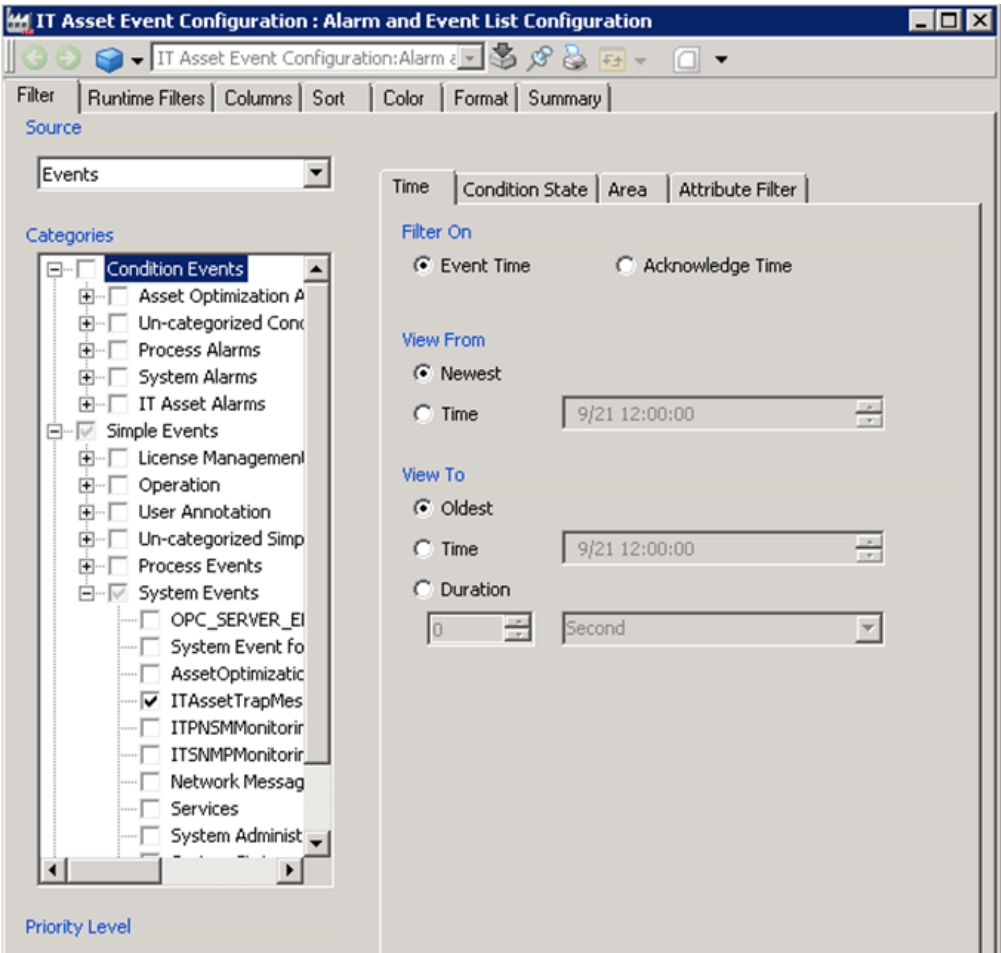
Figure 13. Alarm and Event List Configuration

Section 3 IT Assets in 800xA

Overview

The ABB PC, Network and Software Monitoring provides preconfigured IT Asset representation for integration of IT Assets, including Assets from third party vendors, into the System 800xA environment. The interoperability is proven by online tests of the IT Asset in the form of a single IT Asset type object.

The portfolio of IT Assets includes certified hardware (PCs, IT infrastructure, etc) and software (process, network utilization, etc).

The IT Asset type objects that monitor computer and process resources (handles, virtual memory, thread, and processor load) are delivered with the PNSM base product system extension. The entire IT infrastructure of System 800xA can be monitored by adding IT Asset type objects from PNSM Device Library.

The IT Assets certified by ABB for System 800xA are included in PNSM Device Library.

For a complete list of currently supported IT Assets and functionality, go to:

http://www.abb.com/controlsystems

Navigate to **Control Systems > 800xA -> System ->PC Network and Software Monitoring…**

Basic Computer Monitoring

Basic Computer Monitoring automatically monitors all 800xA System workstation nodes and alerts the operator of potential workstation resource problems through alarm messages.

Basic Computer Monitoring Configuration Tool

In order to create and configure the Basic Computer Monitoring functionality run the Basic Computer Monitoring Configuration Tool.

Run the Basic Computer Monitoring Configuration Tool on the node where PNSM server and Client software are installed. If new 800xA System workstation nodes are added or removed after the Basic Computer Monitoring Configuration Tool has been run, then the tool has to be re-run to ensure that the correct assets are included and monitored.

1. Select:

    Start > All Programs > ABB Industrial IT 800xA > Asset Optimization > PC, Network and Software Monitoring > Basic Computer Monitoring Configuration Tool

    to launch the Basic Computer Monitoring Configuration Tool.

2. Click **Start**. The wizard will close automatically when the configuration is complete.

During the creation of Basic Computer Asset object for each of the detected nodes, Alarm (*Category:System Alarm for SoftAlarms*) with the condition Node Status and the Computer Problem is reported. These Alarms will automatically be set to inactive in approximately 10 minutes from the creation time. During the initial operation time of the Asset, this alarm does not indicate any problem with the device.

Normally only minor configuration changes are required after the software is installed and the Basic Computer Monitoring Configuration Tool is run. The default alarm limits are expected to be suitable in most situations. In some cases it may be necessary to modify the hard drives that require monitoring.

The default IT server configuration is populated with the Basic Computer assets as long as the IT OPC Network Object is configured as recommended in the PNSM Configuration manual

Changing the alarm limits and the hard drives being monitored is done in the Basic Computer Device aspect as shown in Figure 14.

TC08134A
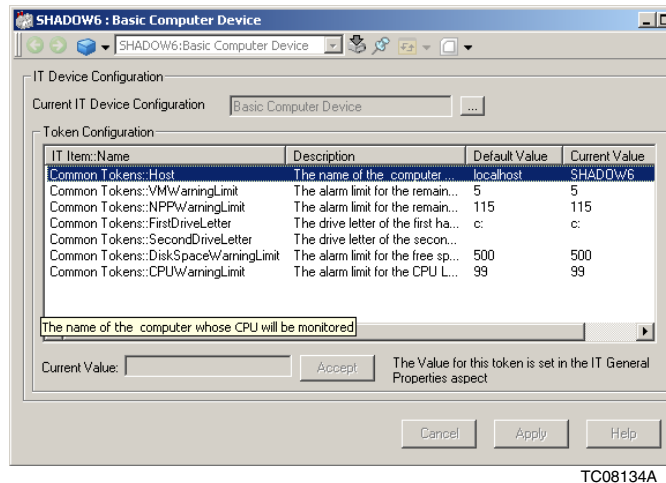
Figure 14. Basic Computer Device Aspect

Specifying the Workstation Node to Monitor

The workstation node to be monitored is automatically configured by the Basic Computer Monitoring Tool. This configuration should only be changed in exceptional cases, such as when workstation nodes are added manually. Refer to Manually Adding Workstation Nodes on page 39.

1. Go to the specific workstation node below the Control Structure\Root\ITServer\Basic Computer Monitoring object.

2. Select the IT General Property aspect.

3. Modify the Host token as required. The workstation name or IP address can be used. Click **Accept** and **Apply**.

4. Click **Populate** in the IT Device Manager aspect in the same object.

Specifying the Hard Drives to Monitor

Basic Computer Monitoring allows monitoring the free disk space of two hard drives. By default the first is set to **c:** and the second is not specified. The drives to be monitored are user configurable. The most important hard drives such as the drives hosting the operating system and the drive where either the 800xA System is installed or the drive being used to store 800xA System related data should be monitored.

1. Go to the specific workstation node with hard drives below the `Control Structure\Root\ITServer\Basic Computer Monitoring` object.

2. Select the `Basic Computer Device` aspect.

3. Modify the first (FirstDriveLetter) or second (SecondDriveLetter) drive token as required. Either token can be used to monitor a drive. Click **Accept** and **Apply**.

4. Click **Populate** in the IT Device Manager aspect in the same object.

Modifying Alarm Limits

The default level at which specific resources are considered to be in alarm is set to a level appropriate for most cases. These alarm limits are set at a level such that false alarms are minimized but the workstation node is still operational so that corrective steps can be taken.

In rare cases it may be necessary to override these default alarm limits to account for unusual behavior. It may be necessary to lower the alarm limit to increase the warning period to provide more time to correct the issue (For example increasing the hard drive disk space limit on workstation nodes with applications, such as Information Management that make extensive use of the hard drive).

Determining the appropriate value for an alarm limit is a complex undertaking. Setting an incorrect value may nullify the benefits of Basic Computer Monitoring. Modifying alarm limits should only be undertaken under the direction of the ABB Technical Support.

Alarm expression will be evaluated only after the IT Control connection is populated from IT device manager for Basic Computer Asset, IT Asset. The error message in Alarm and Event list will be as follows: "The alarm expression could not be activated. Changes on the OPC properties will not generate alarms"

Table 1 lists and describes the resource alarm limits, their token names, default values, and acceptable modification ranges.

Table 1. Resource Alarm Limits

Resource	Alarm Limit Description	Token Name	Default Value	Modification Range
Memory	Total free virtual memory as a percentage of the total available virtual memory. An actual value **less than or equal** to this limit will cause an alarm.	VMWarningLimit	10%	This value should not be increased as this will decrease the time to respond to the problem before the workstation fails; however, it can be increased up to about 25%. A higher limit may cause spurious alarms.
Non-Paged Pool	The total non-paged pool for a workstation in Megabytes. An actual value **greater than or equal** to this limit will cause an alarm.	NPPWarningLimit	500 MB	Can be lowered to 85 MB if a more conservative alarm limit is required. This limit should not be increased
Hard Drive Disk Space	The free hard drive space in Megabytes. An actual value **less than or equal** to this will cause an alarm.	DiskSpaceWarningLimit	500MB	This limit should not be set less than 200 MB. The upper limit is set by the available disk space, but too large a number may cause spurious alarms.
CPU Load	The sustained 2-minute average total CPU load as a percentage. An actual value **greater than or equal** to this limit will cause an alarm.	CPUWarningLimit	99%	It may be set between 90% and 100%. Lowering the limit may cause spurious alarms.

Modifying Alarm Limits for Individual Workstation Nodes

The alarm limits for an individual 800xA System node can be changed by modifying the appropriate limit in the Basic Computer Monitoring Device aspect for that node.

1. Select the Basic Computer Monitoring object for the workstation of interest.

2. Select the Basic Computer Device aspect.

3. Modify the appropriate limit, click **Select** and then **Apply**.

4. Click **Populate** in the IT Device Manager aspect in the same object.

Modifying Alarm Limits for all Workstation Nodes

The alarm limits for all workstation nodes can be modified by changing the Basic Computer Monitoring IT Device Configuration.

Modifying alarm limits for all workstation nodes is an advanced feature that should only be undertaken in consultation with ABB Technical Support.

1. Go to Basic Computer Monitoring IT Asset in the Object Type Structure.

2. Select the Basic Computer Device aspect.

3. Modify the appropriate limit, click **Select** and then **Apply**.

4. Delete the Basic Computer Monitoring object level under the Control Structure/IT Server object.

5. Select **Yes** if asked to confirm deletion of object and its children.

6. Run the Basic Computer Monitoring Configuration Tool (refer to Basic Computer Monitoring Configuration Tool on page 34).

Adding or Removing 800xA System Workstation Nodes

Workstation nodes can be added or removed from the 800xA System by the Configuration Wizard (e.g. to add 800xA Clients). When this has been done, synchronize Basic Computer Monitoring with the 800xA System to ensure that the correct workstation nodes are being monitored.

Run the Basic Computer Monitoring Configuration Tool (refer to Basic Computer Monitoring Configuration Tool on page 34) to modify what is being monitored:

•   New nodes will be monitored.

- Removed nodes will be removed from monitoring.

Manually Adding Workstation Nodes

Use the Basic Computer Monitoring Configuration Tool to identify and add 800xA System workstation nodes that are to be monitored by Basic Computer Monitoring. If 800xA System workstation nodes are added or removed, running the Basic Computer Monitoring Configuration Tool again will modify what is being monitored to match the new setup.

The Basic Computer Monitoring Configuration Tool identifies workstation nodes that are part of the 800xA System (those that were added or removed using the 800xA Configuration Wizard).

It may be required to monitor workstation nodes that are not part of an 800xA System. These workstation nodes must be added manually.

Do not add workstation nodes that are not part of the 800xA System under the Basic Computer Monitoring subdirectory. Manually added nodes will be removed from this subdirectory if the Basic Computer Monitoring Configuration Tool is run again.

There is a dialog during the PNSM installation that specifies the account that PNSM will run under. PNSM is typically configured to use the 800xA Service account. For PNSM to operate correctly, it must be able to access the remote workstation nodes using its account. This is not an issue with 800xA System workstation nodes. If the 800xA System is configured to use the domain Service account, it will be available to all workstation nodes on the domain. If the 800xA System is running as a Workgroup, the same identical Service account will be configured on all 800xA System nodes. However, if additional workstation nodes that are not part of the 800xA System are added, and they are part of a Workgroup, identical Service account (username and password) should be added.

1. Make sure the workstation node to be added is configured and operational.

2. Select the IT Server object in the Control Structure. Do not manually add nodes in the Basic Computer Monitoring subdirectory.

3. Add the Basic Computer Monitoring object from the list of available IT Asset types.

4. Configure the Host field in the IT General Property aspect with the workstation name or IP address.

5. Configure the hard drives to be monitored. There is no restriction as to what drives are monitored with which token.

6. Click **Accept** and then **Apply**.

7. Click **Populate** in the IT Device Manager aspect in the same object.

Basic Computer Asset

This section describes the Basic Computer Asset and the IT Device aspect it contains.

Description: The Basic Computer Asset (Table 2) monitors the five core indicators of the health of a Microsoft Windows workstation node. The health indicators that are monitored are virtual memory, non-paged pool, CPU load, and hard drive space on two drives.

Table 2. Basic Computer Asset

Device Name	IT Device	Description
Basic Computer Device	Basic Computer Device	This device provides the complete alarm and the alert functionality for the Basic Computer Device.

IT General Property Aspect

The item in Table 3 can be modified in the IT General Property aspect.

Table 3. IT General Property Aspect

Name	Default Value	Description
Host	localhost	Change this to the name or IP address of the computer to monitor

Basic Computer Device

The tokens listed in Table 4 can be modified in the Basic Computer Device aspect.

Table 4. Basic Computer Device Aspect

Modifiable Tokens	Default Value	Description
Common Tokens::VMWarningLimit	10%	The total computer free virtual memory as a percentage of the total available virtual memory. An actual value **less than or equal to** this limit will cause an alarm.
Common Tokens::NPPWarningLimit	500MB	The total non-paged pool for a computer in Megabytes. An actual value **greater than or equal to** this limit will cause an alarm.
Common Tokens::FirstDriveLetter	c:	The first hard drive to be monitored. A drive letter must be specified. **NOTE:** The colon (:) after the drive letter is required.
Common Tokens::SecondDriveLetter		The optional second hard drive to be monitored. A blank indicates no drive to be monitored. **NOTE:** The colon (:) after the drive letter is required.
Common Tokens::DiskSpaceWarning Limit	500MB	The free hard drive space in Megabytes. An actual value **less than or equal to** this will cause an alarm.
Common Tokens::CPUWarningLimit	99%	The sustained 2-minute average total CPU load as a percentage. An actual value **greater than or equal to** this limit will cause an alarm

Process Monitoring

Process monitoring is accomplished using the object type Light Generic Computer Process.

Description: The Device Name list represents the alarm detection of a software process.

Table 5 lists the IT Devices for Light Generic Computer Process

Table 5. IT Devices for Light Generic Computer Process

Device Name	IT Device	Description
Alarms:		
Process.exe Alarm	Light Computer Process Alarm	Generates an alarm when a problem is detected with the process.
Status:		
Process.exe Alert	Light Computer Process Alert	Provides summaries of the state of several key indicators within the process.
Process.exe Status	Light Computer Process Status	Provides the values of several indicators within the process.

IT General Property

Table 6 lists the IT General Properties for Light Generic Computer Process.

Table 6. IT General Properties for Light Generic Computer Process

Name	Default Value	Description
Host	localhost	Change this to the name or IP address of the computer to monitor.

Table 6. IT General Properties for Light Generic Computer Process (Continued)

Name	Default Value	Description
SettlingTime	30	The amount of time (30 minutes) to allow the system to settle before establishing a baseline for alarming. This is the recommended minimum value.
OSType	XP	The operating system of the process to be monitored. Leave this field at the default value for Windows 7 and Windows 2008 Server.

Process.exe Alarm

Table 7 lists the IT Device Token Configurations for Process monitoring that can be modified. Process level handle/memory leak limit settings can be further fine tuned using a set of parameters called sensitivity limits. Refer to Table 7 for default values and description of sensitivity limit.

The preset values in the IT device configuration for Process.exe Alarm and Process.exe Alert is set at optimum levels and can be modified as needed.

.

Table 7. Modifiable IT Device Token Configurations for Process monitoring

IT Device Name	Modifiable Tokens	Default Value	Description
Process.exe Alarm	CommonTokens::ProcessName		The Process name to be monitored.
	ProcessHealth::WarningIncrease	24	The number of continuous sample increases that will cause a warning for threads, handles or VM levels. Values are averaged over a 15 minute interval, so a value of 48 implies a 360 minute period of continually increasing resource usage before the warning occurs.
	ProcessHealth::ErrorIncrease	48	The number of continuous sample increases that will cause a warning for threads, handles or VM levels. Values are averaged over a 15 minute interval, so a value of 48 implies a 720 minute period of continually increasing resource usage before the warning occurs.

Table 7. Modifiable IT Device Token Configurations for Process monitoring (Continued)

IT Device Name	Modifiable Tokens	Default Value	Description
Process.exe Alarm ...continued	ProcessHealth::CPUWarningLimit	85%	The sustained CPU load that indicates a warning situation.
	ProcessHealth::CPUErrorLimit	95%	The sustained CPU load that indicates a serious problem.
	ProcessHealth::HandleSensitivityLimit	25	Number of Handles can be used by the process per hour.
	ProcessHealth::ThreadSensitivityLimit	5	Number of Threads can be used by the process per hour.
	ProcessHealth::VMSensitivityLimit	61440 bytes	Number of bytes can be used by the process per hour.

Process.exe Alert

.

Table 8. Modifiable IT Device Token Configurations for Process monitoring

IT Device Name	Modifiable Tokens	Default Value	Description
Process.exe Alert	CommonTokens::ProcessName		The process name to be monitored.
	CommonTokens::WarningIncrease	24	The number of continuous sample increases that will cause a warning for threads, handles or VM levels. Values are averaged over a 15 minute interval, so a value of 48 implies a 360 minute period of continually increasing resource usage before the warning occurs.
	CommonTokens::ErrorIncrease	48	The number of continuous sample increases that will cause a warning for threads, handles or VM levels. Values are averaged over a 15 minute interval, so a value of 48 implies a 720 minute period of continually increasing resource usage before the warning occurs.

Table 8. Modifiable IT Device Token Configurations for Process monitoring (Continued)

IT Device Name	Modifiable Tokens	Default Value	Description
Process.exe Alert ...continued.	CommonTokens::CPUWarningLimit	85%	The sustained CPU load that indicates a warning situation.
	CommonTokens::CPUErrorLimit	95%	The sustained CPU load that indicates a serious problem.
	CommonTokens::SampleAverages	6	The number of samples used to calculate the CPU moving average.
	CommonTokens::HandleSensitivityLimit	25	Number of Handles used by the process per hour.
	CommonTokens::ThreadSensitivityLimit	5	Number of Threads used by the process per hour.
	CommonTokens::VMSensitivityLimit	61440 bytes	Number of bytes used by the process per hour.

Process.exe Status

Table 9. Modifiable IT Device Token Configurations for Process monitoring

IT Device Name	Modifiable Tokens	Default Value	Description
Process.exe Status	CommonTokens::ProcessName		The process name to be monitored.

IT Device Configuration Library

Light Alarm Device - Light Computer Process Alarm (Compact)

Description: Generates a single alarm based on the combination of several checks done on a given software process. The device automatically detects trends in resource usage and generates alarms when it anticipates a problem.Table 10 lists the Light Computer Process Alarm (Compact) Conditions/Subconditions.

Table 10. Light Computer Process Alarm (Compact) Conditions/Subconditions

Conditions	Subconditions Generated	Description
ProcessHealth	Normal	Process is functioning normally.
	Bad	The device was not properly configured. No process name was given.
	ProcessNotRunning	The given process is not running.
	MemoryLeak	The system has observed a sustained upward trend in the amount of Virtual Memory used by the process.
	HandleLeak	The system has observed a sustained upward trend in the number of Handles used by the process.
	ThreadsLeak	The system has observed a sustained upward trend in the number of Threads used by the process.
	CPUOverLoad	The system has observed a sustained period of high CPU usage.

Light Status Device - Light Computer Process Alert

Description: This IT Device Library returns a set of strings indicating the health of several software process attributes.

Table 11 lists the Light Computer Process Alert properties.

Table 11. Light Computer Process Alert Properties

Property	Data Type	Description
Handles	String	The string indicating the state of the Handles resource on the given software process.
Memory		The string indicating the state of the Memory resource on the given software process.
Threads		The string indicating the state of the Threads resource on the given software process.
CPULoad		The string indicating the state of the CPU usage by the given software process.
Value-Handles	Numeric	The numeric representation of the current state of the Handles resource on the given software process.
Value-Memory		The numeric representation of the current state of the Memory resource on the given software process.
Value-Threads		The numeric representation of the current state of the Threads resource on the given software process.
Value-CPULoad		The numeric representation of the current state of the CPU usage on the given software process.

Light Status Device - Light Computer Process Status

Description: Returns several key status values for a given software process.

Table 12 lists the Light Computer Process Status properties.

Table 12. Light Computer Process Status Properties

Property	Data Type	Description
HandleCount	Numeric	The total number of Handles currently in use by this software process.
VM		The total amount of Virtual Memory currently in use by this software process.
ProcessID		The process ID of the given software process.
ThreadCount		The total number of Threads currently in use by this software process.
CPULoad		The percentage load this software process is putting on the CPU.
ProcessName	String	The name of the given process.

Light Generic Computer Process Configuration

This section describes configuration of the Light Generic Computer Process Object Type.

Figure 15 displays the Light Generic Computer Process Asset
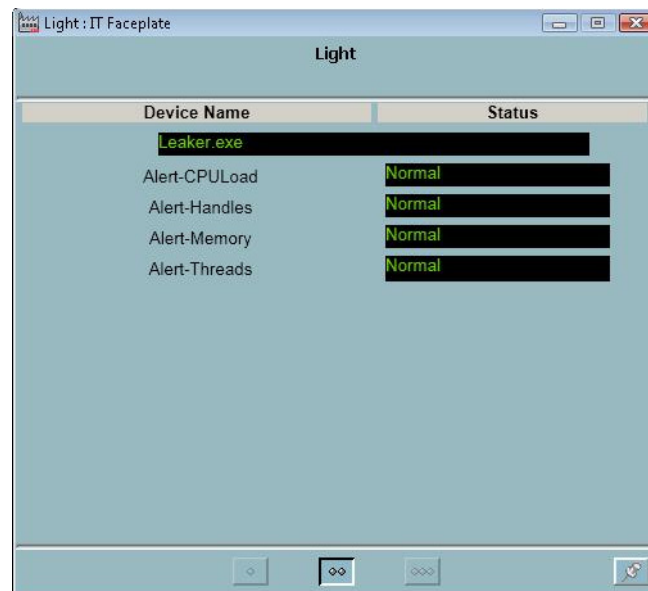
Figure 15. Light Generic Computer Process IT Faceplate

Configuring Light Generic Computer Process Asset

1. In control structure, Create New object.

2. Select Light IT Assets > Light Computer Nodes > Light General Computer Nodes > Light Generic ComputerProcess Lib 1.0-0 > Light Generic Computer Process.

3. Provide a name to the Computer process, preferably the name of the process that will be monitored.

4.   Select the object aspect Process.exe Alarm and then click on Common tokens::Process Name

5.   Enter process name to be monitored in the Current value field. For example: "Leaker.exe". Click **Apply**

6.   Select the object aspect Process.exe Status and then click on Common tokens::Process Name and enter the same process name as entered in step 5. Click **Apply**.

7.   Select the object aspect Process.exe Alert and then click on Common tokens::Process Name and enter the same process name as entered in step 5. Click **Apply**.

ℹ️   It is important to enter the correct process name as displayed in the Windows Task Manager, otherwise the faceplate will not display the correct status of the monitored process.

8.   Go to IT device Manager and in IT Control Connection tab, Select **populate**.

9.   Go to Faceplate and check if the monitored process is running.

When the process to be monitored is not configured, a status message "Process to be monitored is not configured" is displayed on the faceplate. Refer to Figure 16

Figure 16. Light Generic Computer Process IT Faceplate - not configured

All processes need not be monitored. Only processes suspected of memory/handle leak or consuming high CPU capacity are monitored. An alarm is generated when the monitored resource exceeds the preset value defined in the Process.alarm and Process.Alert aspect.

PNSM Device Library

PNSM Device Library is classified into following Object Types:

1. **Base Object Type** - Includes IT Device Configurations, Management Information Base (MIB) files, script files etc.

2. **Asset Object Type** - Includes IT Asset specific data i.e. import files, specific asset monitor.

In the Plant Explorer for every installed IT Asset type object, a preconfigured object type with the following set of aspects is provided:

• Asset Monitors, to detect fault condition

• Asset Reporter with System Status, to add IT Asset to system status

• Asset Viewer, to display asset quality status

• Faceplate, for easy configuration and operation

• Alarm and Event List, to display asset specific alarms

• Product Documentation, to access product information for maintenance activities

• Web Page, to access "Management" software

Prerequisites

• Asset Optimization is a prerequisite for PNSM Device Library.

• Set the Community setting for SNMP service. Refer to Installing and Configuring the SNMP Service on page 58.

PNSM Device Library Object Type Aspects

This section describes the PNSM Device Library Object Type Aspects that are used to configure device library objects.

IT Device

The IT Device allows connecting to any of the IT Device Configurations. The connection decides the device that is to be monitored by the Object Type.

It allows the user to include or exclude OPC items to or from IT Control Connection.

Figure 17 displays the Current IT Device Configuration.
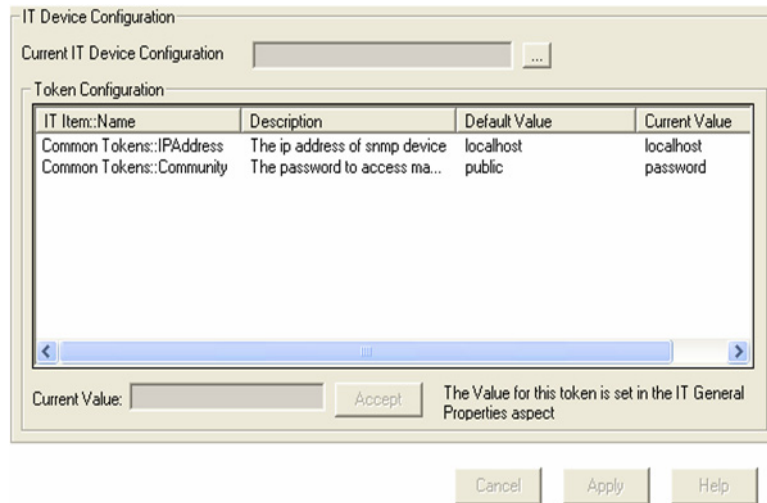
Figure 17. Current IT Device Configuration

IT Control Connection

The IT Control Connection is an OPC Client that provides OPC item namespace to asset monitor input records and subscription to WMI data through Shadow OPC Server.

Refer to Figure 18

Figure 18. IT Control Connection

IT General Property

The IT General Property contains the configuration parameters applicable to the whole object type. The configuration is referred by all IT Devices on the Object Type. Refer to Figure 19

Figure 19. IT General Property

IT Device Manager

The IT Device Manager creates an OPC item ID for all the items in the IT Control Connection. It creates or deletes the OPC Items from IT Control Connection depending upon the IT Device configuration.
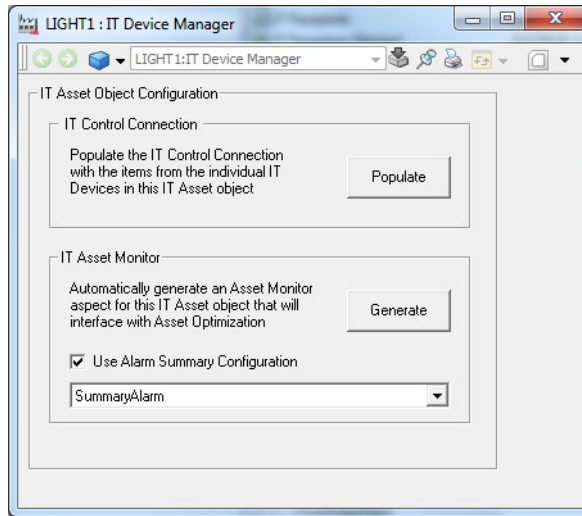
Figure 20. IT Device Manager

IT Device Configuration

The IT Device Configuration aspect configures the device parameters (WMI Class and properties) that are monitored. Figure 21 displays the IT Device Configuration.
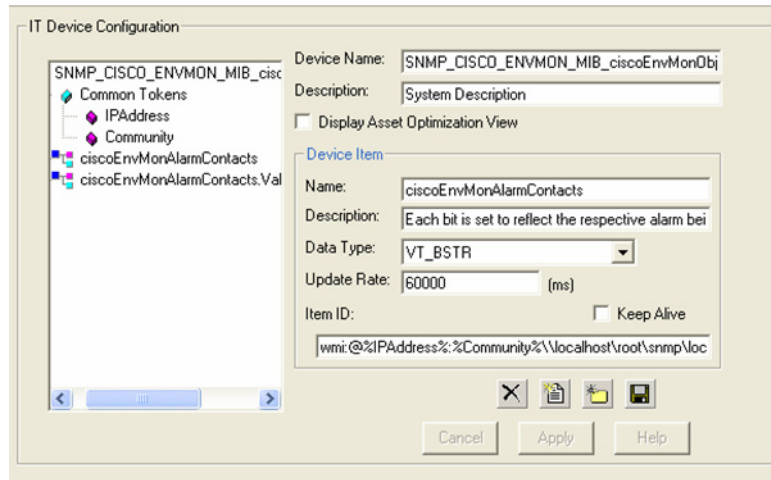
Figure 21. IT Device Configuration

Installing and Configuring the SNMP Service

To install the SNMP service on Windows Server 2008:

1. Click **Start**, click **Control Panel**, double-click **Programs and Features**.

2. Click **Turn Windows features on or off** on the left navigation pane.

3. Server Manager window appears, Click **Features** on the left navigation pane.

4. Click **Add Features.**

5. Select the **SNMP Services** check box, and click **Next**.

6. Information message window appears with the list of components to be installed. Click **Install**.

To install the SNMP service on Windows 7:

1.   Click **Start**, click **Control Panel**, double-click **Programs and Features**.

2.   Click **Turn Windows features on or off** on the left navigation pane.

3.   Windows Features dialog appears, click to select **Simple Network Management Protocol (SNMP)** check box**.**

4.   Click **OK**.

To configure the SNMP service (Windows Server 2008 and Windows 7), do the following:

1.   Click **Start**, click **Control Panel**, double-click **Administrative Tools**, and then double-click **Computer Management**.

2.   In the console tree, open **Services And Applications**, and then click **Services**.

3.   In the details pane, right-click **SNMP Service**, and then click **Properties**.

SNMP service can be configured through the **Security** tab. Follow the steps mentioned below:

a.   Under Accepted community names, click **Add**.

b.   In the Community Name field, type the case sensitive community name and then click **Add**.

c.   Select **Accept SNMP packets from any host** radio button.

d.   Click **Apply** and then click **OK**.

Installation

The combination of batch file procedures and 800xA Import/Export wizard allow easy installation and update of IT Asset type objects in PNSM Device Library.

In Plant Explorer, each IT Asset is represented in Object Type Structure by an IT Asset type object. The IT Asset type objects are located under Object Type Group, PNSM. Refer to Figure 22.
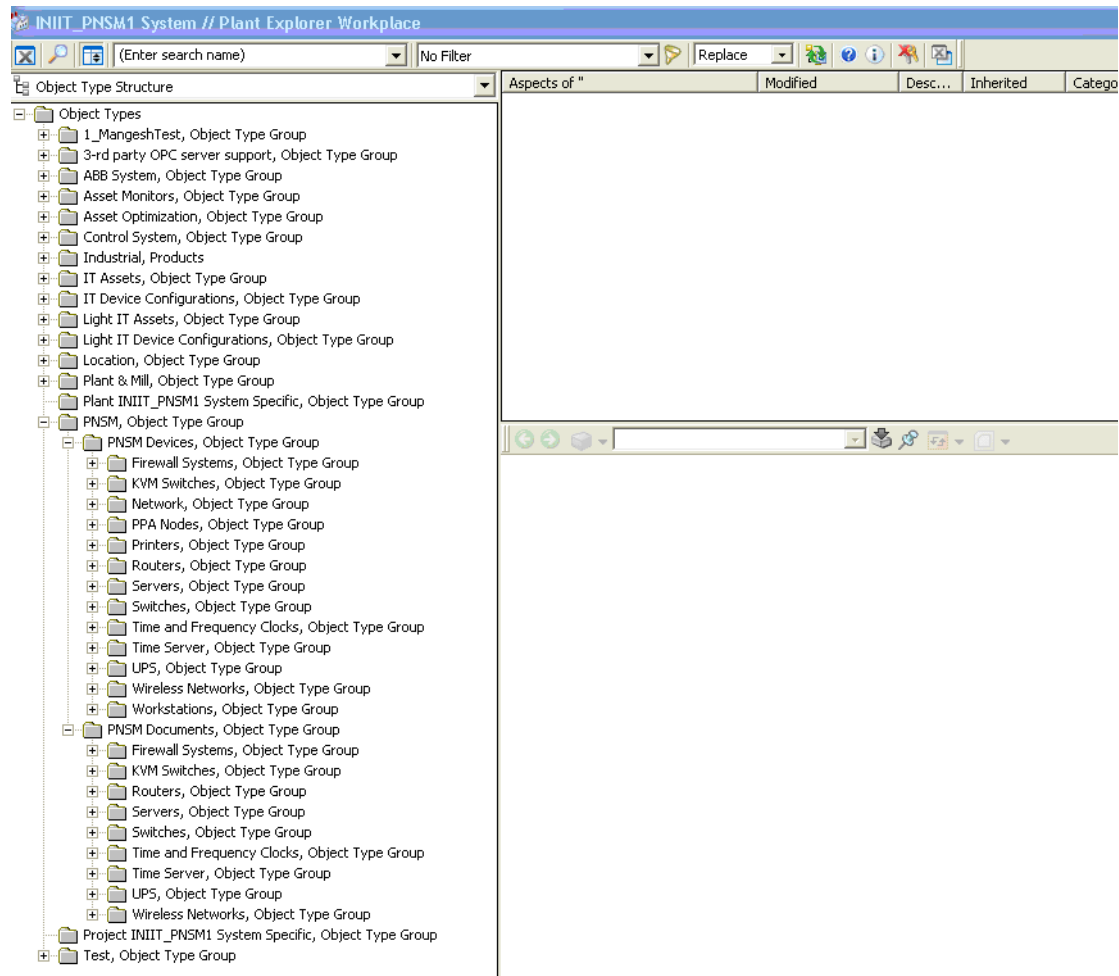
Figure 22. PNSM Object Type Group

.

Installation of Base object type is prerequisite for installation of IT Asset specific object type

1.   Double Click and extract the contents of the object type file.

2. Import **10_Object Type Name.afw** using the Import/Export Wizard.

3. Depending on user preferences select the appropriate option.

    a. Import **11_Object Type Name_VB6.afw** to obtain the VG graphics.

    b. Import **12_Object Type Name_PG2.afw** to obtain the PG2 graphics.

4. Select **Import All** from the Actions Menu.

Refer to the object type specific release notes located in ABB SolutionsBank for more information.

Object Type Configuration
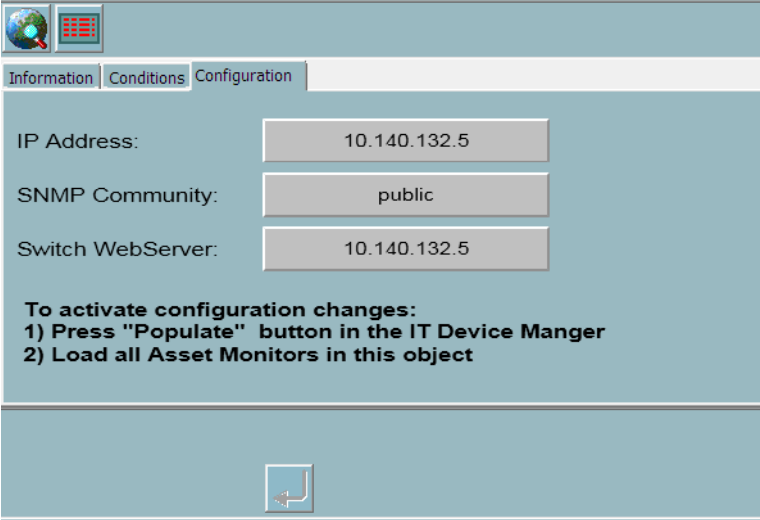
1. Create an instance of the object type in the Control Structure for each IT Asset to be monitored.

2. In the IT Faceplate, select the Configuration Tab and provide the Configuration Information (IP Address and SNMP Password).

3. Click Populate Button on the IT Device Manager Aspect.

4. Load Asset Monitor Aspects present in the instance of the Object Type.

For more information on prerequisites, installation/post installation procedures refer to 2PAAxxxxxx Release Notes for each device object type located in ABB SolutionsBank.

IT Faceplate Configuration

Figure 23 displays the configuration view of the IT Faceplate. The object configurations such as IP address, SNMP password are managed from the configuration tab of the Faceplate.

Figure 23. Configuration View IT Faceplate

WebPage Aspect

This provides configuration of device diagnosis web page URL. If there is no URL available for particular device, then web page aspect will not be provided for that object type.

Figure 24 displays the log in for configuration of device diagnosis web page URL. This is a typical login window of a Dell computer device

WebPage aspect opens the web server of the device. This may contain detailed diagnostics and configuration information. To login to the web server of the device, username and password are required.

Figure 24. Device Diagnosis configuration log in

Browse the web server page for detailed device status, device configuration changes, and more. Figure 25 shows a web server page.
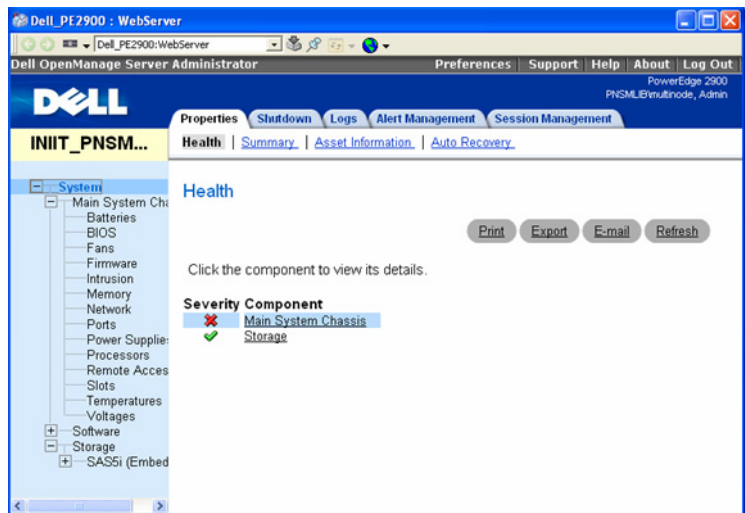
Figure 25. Web Page aspect with detailed diagnostics

IT Assets Supported by PNSM Device Library

The table is updated during the release of Rev B. *Refer to System 800xA PNSM Integrated Device List for latest object types present in ABB Solutions Bank.*

Table 13 lists the Object Types supported by the PSNM Device library and their corresponding Release Notes.

Table 13. Object Types

Category	Vendor	Device Type	Release Notes ID
Base		Base	2PAA102558
Computer	All	Work Station	2PAA103024
	Dell	Dell Power Edge 29xx	2PAA102937
		Dell Power Edge R710	2PAA105768
		Dell PowerEdge R710 ESXi	2PAA208732
	HP	HP Proliant BL460 C	2PAA105776
		HP Proliant DL380 G5	2PAA102746
		HP Proliant DL380 G6	2PAA105565
		HP Proliant ML350 G5	2PAA103028
		HP BladeCenter	2PAA105549
		HP Proliant DL380 G6 ESXi	2PAA208722
	IBM	IBM BladeCenter S	2PAA104385
		IBM x3650	2PAA105130
		IBM x3650 M2 ESXi	2PAA208726
Firewall System	Hirschmann	Hirschmann EAGLE 20	2PAA105142

Table 13. Object Types (Continued)

Category	Vendor	Device Type	Release Notes ID
Switch	Hirschmann	Hirschmann MACH 100	2PAA105118
		Hirschmann MACH 1000	2PAA104275
		Hirschmann MACH 4000	2PAA103159
		Hirschmann MS20_MS30	2PAA102563
		Hirschmann MS4128	2PAA103163
		Hirschmann RS2	2PAA105986
		Hirschmann RS20_RS30	2PAA102769
		Hirschmann RS40	2PAA103436
		Hirschmann RSR20_RSR30	2PAA104271
	CISCO	Cisco CATALYST 2960	2PAA104267
		Cisco IE 3000	2PAA104648
		Cisco 12_24_48 Port Switch	2PAA105978
	MOXA	MOXA EDS-405A	2PAA103420

Table 13. Object Types (Continued)

Category	Vendor	Device Type	Release Notes ID
		MOXA EDS-408A	2PAA103424
		MOXA EDS-505A	2PAA103760
		MOXA EDS-508	2PAA102945
		MOXA EDS-508A	2PAA103678
		MOXA EDS-510A	2PAA103428
		MOXA EDS-516A	2PAA103440
		MOXA EDS-518A	2PAA103432
		MOXA EDS-726	2PAA102941
		MOXA EDS-728	2PAA104574
		MOXA EDS-828	2PAA104576
		MOXA EDS-P510	2PAA105122
	N-Tron	N-Tron 708	2PAA104578
	Phoenix	Phoenix MMS MCS	2PAA102773
	Weidmuller	Weidmuller IE-SW6-2ST-M	2PAA103768
		Weidmuller IE-SW16-M	2PAA103764
	Westermo	Westermo OnTime Lynx	2PAA103300
		Westermo OnTime R200	2PAA103155
		Westermo OnTime T200	2PAA103032
	GarrettCom	GarrettCom Magnum 6K32T	2PAA104667
	Sixnet	Sixnet SLX8MG	2PAA105990
Wireless Networks	Hirschmann	Hirschmann BAT54	2PAA105126

Table 13. Object Types (Continued)

Category	Vendor	Device Type	Release Notes ID
Network	All	Generic Network Interface	2PAA104580
		Network Utilization	2PAA105550
		Node to Node Utilization	2PAA105557
		Single Node Utilization	2PAA105561
PPA Nodes	All	Generic Computer Node	2PAA104292
Printer	All	Printer	2PAA103784
UPS	All	UPS	2PAA103444

ESXi Server Monitoring

Virtualization for 800xA has been supported for a basic physical server configuration running the full VMware ESXi. ESXi is embedded directly into the firmware of the server allowing the server to boot directly into ESXi. ESXi does not support the service console (and does not support any management software) that was available in ESX. Hence monitoring of ESXi server hardware using OPC server is not possible.

Apart from this SAN devices, which are connected in the ESXi network, have the capability to generate SNMP traps. In order to monitor the ESXi server hardware and SAN devices in System 800xA, SNMP trap support is added to PC, Network and Software Monitoring.

SNMP Trap is an unsolicited message that is initiated by an IT asset (agent) and sent to the network management system (manager). If an event has occurred, the agent communicates it to the manager using the Trap. Traps are sent asynchronously and not in response to the queries from the manager. The manager is responsible for performing an action, based on the Trap it receives from the agent. SNMP trap messages are presented as Alarms or Events in System 800xA. It is possible to configure the severity and notification type (alarm or event) for every trap message.

Configure error or warning trap messages as alarms and information trap messages as events.

i The device specific object types for ESXi Server Monitoring are included in the PNSM Library. Refer to the object type release notes for the configuration information.

Deprecated IT Asset Object Types

A set of IT Asset object types are deprecated since the release of 800xA 5.1. New enhancements (Process Graphics 2 and Native Language Support) are not applied to deprecated IT Asset type objects. Replacements for deprecated IT Asset type objects are available in PNSM Device Library.

It is recommended to migrate deprecated IT Asset type objects to PNSM Device Library. Refer to Appendix - Mapping of Deprecated IT Asset Object Types in *System 800xA Upgrade instruction (3BSE036342*).*

> The deprecated IT Asset type objects are delivered with ABB PNSM VB Graphics Extension.

Deprecated IT Asset Object Types describe the deprecated IT Assets and lists the IT Devices that comprise them. Additionally, the user defined parameters in the IT Devices and the IT General Properties indicating the parameters that need to be modified during configuration of IT Assets are also described.

The IT Assets described in this section are:
- Asset – Generic Computer Node on page 72.
- Light Asset - Light Generic Computer Node on page 79.
- Light Computer Assets Process Alarm List on page 79.
- Computer Assets on page 79.
    - Asset - Batch Client on page 79.
    - Light Asset - Batch Client on page 80.
    - Asset - Batch Primary Server with Client on page 80.
    - Light Asset - Batch Primary Server with Client on page 82.
    - Asset - Batch Secondary Server with Client on page 83.
    - Light Asset - Batch Secondary Server with Client on page 84.
    - Asset - Inform IT Calculations on page 85.
    - Light Asset - Inform IT Calculations on page 85.
    - Asset - Inform IT Complete on page 86.
    - Light Asset - Inform IT Complete on page 87.
    - Asset - Inform IT Display on page 88.
    - Light Asset - Inform IT Display on page 88.
    - Asset - Inform IT History on page 89.
    - Light Asset - Inform IT History on page 90.

Asset – Generic Computer Node

Description: Represents a typical personal computer running Microsoft Windows. Includes basic status and alarm detection for the computer processor and hard drive performance, as well as memory and resource consumption.

Assets can be customized by adding additional Disk Devices.

Table 14 lists the Generic Computer Node Asset Devices.

Table 14. Generic Computer Node Asset Device List

Device Name	IT Device	Description
Alarms		
CPU Alarm	Computer CPU Alarm	Generates an alarm when the CPU utilization becomes too high.

Table 14. Generic Computer Node Asset Device List (Continued)

Device Name	IT Device	Description
Disk C Alarm	Disk Volume Alarm	Generates an alarm when the C disk drive partition becomes too full.
Disk Drive 0 Alarm	Disk Drive Alarm	Generates an alarm when the system detects any kind of problem with the physical hard drive. Only disk drive 0 is monitored.
General Computer Alarm	Computer General Alarm (Auto)	Generates one or more alarms based on several factors. This device will automatically detect trends in resource usage and generate alarms when it anticipates a problem.
Status		
CPU Status	Computer CPU Status	Provides the current CPU loading percentage.
CPU Alert	Computer CPU Alert	Generates an alert when the CPU utilization becomes too high.
Disk C Status	Disk Volume Status	Provides the C disk partition usage as a percentage of the total.
Status (continued)		
Disk C Alert	Disk Volume Alert	Generates an alert when the C disk drive partition becomes too full.
Disk Drive 0 Status	Disk Drive Status	Provides model and status data for a hard drive.
Disk Drive 0 Alert	Disk Drive Alert	Generates an alert when the system detects any kind of problem with the physical hard drive. Only disk drive 0 is monitored.
General Computer Status	Computer General Status	Provides general status data for a computer, such as virtual memory usages, etc.
General Computer Alert	Computer General Alert	Generates one or more alerts based on several factors. This device will automatically detect trends in resource usage and generate alerts when it anticipates a problem.

Table 15 lists the IT General Properties for the Generic Computer Node Asset.

Table 15. IT General Properties for Generic Computer Node Asset

Name	Default Value	Description
Host	localhost	Change this to the name or IP address of the computer to monitor.
NumberCPUs	1	Change this to match the number of CPUs on the computer being monitored. This can be determined by checking the hardware configuration.

IT Device Tokens are properties used by the PC, Network and Software Monitoring system to pass configuration information to the OPC server. VM, threads and handles usage limit settings can further be fine tuned using **sensitivity limits** parameters. (Refer to Table 16 for more details.)

Table 16 lists the Modifiable IT Device Token Configuration for the Generic Computer Node Asset.

Table 16. Modifiable IT Device Token Configuration for Generic Computer Node Asset

IT Device Name	Modifiable Tokens	Default Value	Description
CPU Alarm	CPUOverload::LowLimit	80%	The CPU load limit at which an alarm is generated. The value at which the system is still functional, but is being stressed beyond its normal means.
	CPUOverload::MediumLimit	90%	The CPU load limit at which a medium alarm is generated. The value at which the system is probably starting to experience significant performance problems.
	CPUOverload::HighLimit	100%	The CPU load limit which a high alarm is generated. The value at which a serious problem is occurring. This limit will only be reached if the CPU usage is at 100% for 10 seconds or more.
CPU Alert	Common Tokens::LowLimit	80%	The CPU load limit at which an event is generated. The value at which the system is still functional, but is being stressed beyond its normal means.
	Common Tokens::MediumLimit	90%	The CPU load limit at which a medium event is generated. The value at which the system is probably starting to experience significant performance problems.
	Common Tokens::HighLimit	100%	The CPU load limit at which a high event is generated. The value at which a serious problem is occurring. This limit will only be reached if the CPU usage is at 100% for 10 seconds or more.

Table 16. Modifiable IT Device Token Configuration for Generic Computer Node Asset (Continued)

IT Device Name	Modifiable Tokens	Default Value	Description
Disk C Alarm	Common Tokens::Drive	c:	The drive letter that is being monitored.
	FreeSpace::WarningLimit	5%	The percentage of hard disk free disk space required before a Free Space warning alarm occurs.
	FreeSpace::SeriousLimit	3%	The percentage of hard disk free disk space required before a Free Space serious alarm occurs.
	FreeSpace::CriticalLimit	1%	The percentage of hard disk free disk space required before a Free Space critical alarm occurs.
Disk C Alert	Common Tokens::Drive	c:	The drive letter that is being monitored.
	Common Tokens::WarningLimit	5%	The percentage of hard disk free disk space required before a Free Space warning alert occurs.
	Common Tokens::SeriousLimit	3%	The percentage of hard disk free disk space required before a Free Space serious alert occurs.
	Common Tokens::CriticalLimit	1%	The percentage of hard disk free disk space required before a Free Space critical alert occurs.
Disk C Status	Common Tokens::Drive	c:	The drive letter that is being monitored.
General Computer Alarm	VM-Absolute::WarningLimit	5%	The value at which the system is still functional, but is being stressed beyond its normal means, issuing an alarm.
	VM-Absolute::ErrorLimit	2%	The value at which the system is probably starting to experience significant performance problems issuing an alarm.

Table 16. Modifiable IT Device Token Configuration for Generic Computer Node Asset (Continued)

IT Device Name	Modifiable Tokens	Default Value	Description
	CommonTokens:: WarningIncrease	48	The number of continuous sample increases that will cause a warning for threads, handles or VM levels. Values are averaged over a 15 minute interval, so a value of 48 implies a 720 minute period of continually increasing resource usage before the warning occurs.
	CommonTokens ::ErrorIncrease	96	The number of continuous sample increases that will cause an error for threads, handles or VM levels. Values are averaged over a 15 minute interval, so a value of 96 implies a 1440 minute period of continually increasing resource usage before the error occurs.
	CommonTokens ::VMSensitivityLimit	256000	Number of Bytes can be used by the process per hour.
	CommonTokens:: ThreadSensitivityLimit	10	Number of Threads can be used by the process per hour.
	CommonTokens:: HandleSensitivityLimit	40	Number of Handles can be used by the process per hour.

Table 16. Modifiable IT Device Token Configuration for Generic Computer Node Asset (Continued)

IT Device Name	Modifiable Tokens	Default Value	Description
General Computer Alert	Common Tokens::WarningLimit	5%	The value at which the system is still functional, but is being stressed beyond its normal means, issuing an alert.
	Common Tokens::ErrorLimit	2%	The value at which the system is probably starting to experience significant performance problems, issuing an alert.
	CommonTokens:: WarningIncrease	48	The number of continuous sample increases that will cause a warning for threads, handles or VM levels. Values are averaged over a 15 minute interval, so a value of 48 implies a 720 minute period of continually increasing resource usage before the warning occurs.
	CommonTokens:: ErrorIncrease	96	The number of continuous sample increases that will cause an error for threads, handles or VM levels. Values are averaged over a 15 minute interval, so a value of 96 implies a 1440 minute period of continually increasing resource usage before the error occurs.
	CommonTokens:: VMSensitivityLimit	256000	Number of Bytes can be used by the process per hour.
	CommonTokens:: ThreadSensitivityLimit	10	Number of Threads can be used by the process per hour.
	CommonTokens:: HandleSensitivityLimit	40	Number of Handles can be used by the process per hour.

Light Asset - Light Generic Computer Node

A Light Generic Computer Node Asset is available providing basic alarm detection for the Generic Computer Node Asset. Status information is not returned. The data is subscribed at a slower rate (60 seconds) when using Light Assets. Follow the configuration procedures for the Asset – Generic Computer Node on page 72 to set up the Light Generic Computer Node Asset. Refer to Table 16 to complete the Light Generic Computer Node Asset configuration.

Light Computer Assets Process Alarm List

A Light Computer Assets Process Alarm list is available providing basic alarm detection of a key software process associated with a specific node type. Status information is not returned. The data is subscribed at a slower rate (60 seconds). This set of devices is repeatedly used for each of the processes in all of the Light Computer Assets.

Computer Assets

Description: A superset of the Generic Computer, the Computer Assets monitor all of the status and alarm detection properties of the Generic Computer Asset, plus key software processes associated with each type of node. They can be customized in the same way as the Generic Computer Asset and have additional software processes added as required.

Asset - Batch Client

The Batch Client Asset contains the Generic Computer subset plus the processes listed in the Batch Client Software Process Name List.

Batch Client Software Process Name List.

- AbbClientLicenseProvider
- AfwFsdNode
- AfwSMClient
- Batch_netRouter.exe
- Batch_nwkser.exe

Table 17 lists the IT General Properties for the Batch Client Asset.

Table 17. IT General Properties for Batch Client Asset

Name	Default Value	Description
Host	localhost	Change this to the name or IP address of the computer to monitor.
SettlingTime	30	The required time (30 minutes) to allow the system to settle before establishing a baseline for alarming. This is the recommended minimum value.
NumberCPUs	1	Change this to match the number of CPUs on the computer being monitored. This can be determined by checking the hardware configuration.
OSType	XP	The operating system of the process to be monitored. Leave this field at the default value for Windows 7 and Windows 2008 Server.

Refer to Table 16 and Table 17 to complete the Batch Client Asset configuration.

Light Asset - Batch Client

A Light Batch Client Asset is available providing basic alarm detection for the Computer Asset and the Batch Client Asset. Status information is not returned. The data is subscribed at a slower rate (60 seconds) when using Light Assets. Follow the configuration procedures for Asset - Batch Client on page 79 to set up the Light Batch Client Asset.

Asset - Batch Primary Server with Client

Description: The Batch Primary Server with Client Asset contains the Generic Computer subset plus the processes listed in the Batch Primary Server with Client Software Process Name List.

Batch Primary Server with Client Software Process Name List.

- AbbClientLicenseProvider
- AfwFsdNode
- AfwSMClient
- Batch_batch.exe
- Batch_bmscache.exe
- Batch_netRouter.exe
- Batch_nwkser.exe
- Batch_phased.exe
- Batch_recipem.exe
- Batch_Service.exe
- Batch_tab.exe
- Batch_tabi.exe
- Batch_unitm.exe
- BatchOPCAeServer.exe

PC, Network and Monitoring Software currently does not have the capability to detect the failover of the redundant batch server's from Primary to secondary server.

In case of a failover, Batch Primary Server can be monitored by switching the two Batch servers, i.e. switch the IP addresses (computer names) in IT General Property for the two Batch Servers IP assets, then go the IT Device Manager and press the Populate button. The above manual step will be required to perform as the processes monitored by Batch primary and Secondary Server are not the same.

Table 18 lists the IT General Properties for Batch Primary Server with Client Asset.

Table 18. IT General Properties for Batch Primary Server with Client Asset

Name	Default Value	Description
Host	localhost	Change this to the name or IP address of the computer to monitor.
SettlingTime	30	The amount of time (30 minutes) to allow the system to settle before establishing a baseline for alarming. This is the recommended minimum value.
NumberCPUs	1	Change this to match the number of CPUs on the computer being monitored. This can be determined by checking the hardware configuration.
OSType	XP	The operating system of the process to be monitored. Leave this field at the default value for Windows 7 and Windows 2008 Server.

Refer to Table 16 and Table 18 to complete the Batch Primary Server with Client Asset configuration.

Light Asset - Batch Primary Server with Client

A Light Batch Primary Server with Client Asset is available providing basic alarm detection for the Computer Asset and the Batch Primary Server with Client Asset. Status information is not returned. The data is subscribed at a slower rate (60 seconds) when using Light Assets. Follow the configuration procedures for Asset - Batch Primary Server with Client on page 80 to set up the Light Batch Primary Server with Client Asset.

Asset - Batch Secondary Server with Client

Description: The Batch Secondary Server with Client Asset contains the Generic Computer subset plus the processes listed in the Batch Secondary Server with Client Process Name List.

Batch Secondary Server with Client Process Name List.

- AbbClientLicenseProvider
- AfwFsdNode
- AfwSMClient
- Batch_netRouter.exe
- Batch_nwkser.exe
- Batch_Service.exe
- BatchOPCAeServer.exe

Table 19 lists the IT General Properties for the Batch Secondary Server with Client Asset.

Table 19. IT General Properties for Batch Secondary Server with Client Asset

Name	Default Value	Description
Host	localhost	Change this to the name or IP address of the computer to monitor.
SettlingTime	30	The amount of time (30 minutes) to allow the system to settle before establishing a baseline for alarming. This is the recommended minimum value.
NumberCPUs	1	Change this to match the number of CPUs on the computer being monitored. This can be determined by checking the hardware configuration.
OSType	XP	The operating system of the process to be monitored. Leave this field at the default value for Windows 7 and Windows 2008 Server.

Refer to Table 16 and Table 19 to complete the Batch Secondary Server with Client Asset configuration.

Light Asset - Batch Secondary Server with Client

A Light Batch Secondary Server with Client Asset is available providing basic alarm detection for the Computer Asset and the Batch Secondary Server with Client Asset. Status information is not returned. The data is subscribed at a slower rate (60 seconds) when using Light Assets. Follow the configuration procedures for Asset - Batch Secondary Server with Client on page 83 to set up the Light Batch Secondary Server with Client Asset.

Asset - Inform IT Calculations

Description: The Inform IT Calculations Asset contains only the software processes listed in the Inform IT Calculations Software Process Name List (not the Generic Computer subset) and is to be used with the Asset - Inform IT History on page 89.

Inform IT Calculations Software Process Name List.

• CalculationService.exe

Table 20 lists the IT General Properties for the Inform IT Calculations Asset.

Table 20. IT General Properties for Inform IT Calculations Asset

Name	Default Value	Description
Host	localhost	Change this to the name or IP address of the computer to monitor.
SettlingTime	30	The required time (30 minutes) to allow the system to settle before establishing a baseline for alarming. This is the recommended minimum value.
OSType	XP	The operating system of the process to be monitored. Leave this field at the default value for Windows 7 and Windows 2008 Server.

Refer to Table 16 and Table 20 to complete the Inform IT Calculations configuration.

Light Asset - Inform IT Calculations

A Light Inform IT Calculations Asset is available providing basic alarm detection for the Inform IT Calculations Asset. Status information is not returned. The data is subscribed at a slower rate (60 seconds) when using Light Assets. Follow the configuration procedures for the Asset - Inform IT Calculations on page 85 to set up the Light Inform IT Calculations Asset.

Asset - Inform IT Complete

Description: The Inform IT Complete Asset contains the Generic Computer subset plus the processes listed in the Inform IT Complete Software Process Name List.

Inform IT Complete Software Process Name List.

- AdsAbsDeployMgr.exe
- AdsCsCommSrv.exe
- AdsScadaSrv.exe
- AfwScheduler.exe
- CalculationService.exe
- EHOPCAEServer.exe
- hsAdmin.exe
- hsArchiveService.exe
- hsCollection.exe
- hsEventLogCollector.exe
- hsHDAServer.exe
- hsHistoryService.exe
- hsLogman.exe
- hsMsgServer.exe
- hsPDLStorage.exe
- hsProfileServer.exe
- hsRetrieval.exe
- hsServer.exe
- hsStorage.exe
- hsSuperIPC.exe
- odaServer.exe
- odaService.exe
- omfCleanup.exe
- omfNameProc.exe
- omfPM.exe
- omfService.exe
- omfTimer.exe
- omoNameBroker.exe
- omoNodeBroker.exe
- omoService.exe
- omoStorageDomain.exe

- omoTypeDirectory.exe
- PAS_Service.exe
- PdlApiSrv.exe
- SesServer.exe

Table 21 lists the IT General Properties for the Inform IT Complete Asset.

Table 21. IT General Properties for Inform IT Complete Asset

Name	Default Value	Description
Host	localhost	Change this to the name or IP address of the computer to monitor.
SettlingTime	30	The required time (30 minutes) to allow the system to settle before establishing a baseline for alarming. This is the recommended minimum value.
OSType	XP	The operating system of the process to be monitored. Leave this field at the default value for Windows 7 and Windows 2008 Server.
NumberCPUs	1	Change this to match the number of CPUs on the computer being monitored. This can be determined by checking the hardware configuration.

Refer to Table 16 and Table 21 to complete the Inform IT Complete Asset configuration.

Light Asset - Inform IT Complete

A Light Inform IT Complete Asset is available providing basic alarm detection for the Computer Asset and the Inform IT Complete Asset. Status information is not returned. The data is subscribed at a slower rate (60 seconds) when using Light Assets. Follow the configuration procedures for the Asset - Inform IT Complete on page 86 to set up the Light Inform IT Complete Asset.

Asset - Inform IT Display

Description: The Inform IT Display Asset contains only the software processes listed in the Inform IT Display Software Process Name List (not the Generic

Computer subset) and is to be used with the Asset - Inform IT History on page 89.

Inform IT Display Software Process Name List.

- ADSdpADO.exe
- ADSdpDCS.exe
- ADSdpDDR.exe
- ADSdpLOG.exe
- ADSdpOPC.exe
- ADSdpOPCHDA.exe
- ADSS.exe
- ADSspCOM.exe

Table 22 lists the IT General Properties for the Inform IT Display Asset.

Table 22. IT General Properties for Inform IT Display Asset

Name	Default Value	Description
Host	localhost	Change this to the name or IP address of the computer to monitor.
SettlingTime	30	The amount of time (30 minutes) to allow the system to settle before establishing a baseline for alarming. This is the recommended minimum value.
OSType	XP	The operating system of the process to be monitored. Leave this field at the default value for Windows 7 and Windows 2008 Server.

Refer to Table 16 and Table 22 to complete the Inform IT Display configuration.

Light Asset - Inform IT Display

A Light Inform IT Display Asset is available providing basic alarm detection for the Inform IT Display Asset. Status information is not returned. The data is subscribed at a slower rate (60 seconds) when using Light Assets. Follow the configuration procedures for the Asset - Inform IT Display on page 88 to set up the Light Inform IT Display Asset.

Asset - Inform IT History

Description: The Inform IT History Asset contains the Generic Computer subset plus the processes listed in the Inform IT History Software Process Name List.

Inform IT History Software Process Name List.

- EHOPCAEServer.exe
- hsAdmin.exe
- hsArchiveService.exe
- hsCollection.exe
- hsEventLogCollector.exe
- hsHDAServer.exe
- hsHistoryService.exe
- hsLogman.exe
- hsMsgServer.exe
- hsPDLStorage.exe
- hsProfileServer.exe
- hsRetrieval.exe
- hsServer.exe
- hsStorage.exe
- hsSuperIPC.exe
- omfCleanup.exe
- omfNameProc.exe
- omfPM.exe
- omfService.exe
- omfTimer.exe
- omoNameBroker.exe
- omoNodeBroker.exe
- omoService.exe
- omoStorageDomain.exe
- omoTypeDirectory.exe
- PAS_Service.exe
- PdlApiSrv.exe
- SesServer.exe

Table 23 lists the IT General Properties for the Inform IT History Asset.

Table 23. IT General Properties for the Inform IT History Asset

Name	Default Value	Description
Host	localhost	Change this to the name or IP address of the computer to monitor.
SettlingTime	30	The required time (30 minutes) to allow the system to settle before establishing a baseline for alarming. This is the recommended minimum value.
OSType	XP	The operating system of the process to be monitored. Leave this field at the default value for Windows 7 and Windows 2008 Server.
NumberCPUs	1	Change this to match the number of CPUs on the computer being monitored. This can be determined by checking the hardware configuration.

Refer to Table 16 and Table 23 to complete the Inform IT History configuration.

Light Asset - Inform IT History

A Light Inform IT History Asset is available providing basic alarm detection for the Computer Asset and the Inform IT History Asset. Status information is not returned. The data is subscribed at a slower rate (60 seconds) when using Light Assets. Follow the configuration procedures for the Asset - Inform IT History on page 89 to set up the Light Inform IT History Asset.

Asset - Inform IT ODA

Description: This Asset contains only the software processes listed in the Inform IT ODA Software Process Name List (not the Generic Computer subset) and is to be used with the Asset - Inform IT History on page 89.

Inform IT ODA Software Process Name List.

•   odaServer.exe
•   odaService.exe

Table 24 lists the IT General Properties for the Inform IT ODA Asset.

Table 24. IT General Properties for Inform IT ODA Asset

Name	Default Value	Description
Host	localhost	Change this to the name or IP address of the computer to monitor.
SettlingTime	30	The amount of time (30 minutes) to allow the system to settle before establishing a baseline for alarming. This is the recommended minimum value.
OSType	XP	The operating system of the process to be monitored. Leave this field at the default value for Windows 7 and Windows 2008 Server.

Refer to Table 16 and Table 24 to complete Inform IT ODA Asset configuration.

Light Asset - Inform IT ODA

A Light Inform IT ODA Asset is available providing basic alarm detection for the Inform IT ODA Asset. Status information is not returned. The data is subscribed at a slower rate (60 seconds) when using Light Assets. Follow the configuration procedures for the Asset - Inform IT ODA to set up the Light Inform IT ODA Asset.

Asset - Inform IT Scheduler

Description: The Inform IT Scheduler Asset contains only the software processes listed in the Inform IT Scheduler Software Process Name List (not the Generic

Computer subset) and is to be used with the Asset - Inform IT History on page 89.

Inform IT Scheduler Software Process Name List.

•   Afwscheduler.exe

Table 25 lists the IT General Properties for the Inform IT Scheduler Asset.

Table 25. IT General Properties for Inform IT Scheduler Asset

Name	Default Value	Description
Host	localhost	Change this to the name or IP address of the computer to monitor.
SettlingTime	30	The amount of time (30 minutes) to allow the system to settle before establishing a baseline for alarming. This is the recommended minimum value.
OSType	XP	The operating system of the process to be monitored. Leave this field at the default value for Windows 7 and Windows 2008 Server.

Refer to Table 16 and Table 25 to complete the Inform IT Scheduler Asset configuration.

Light Asset - Inform IT Scheduler

A Light Inform IT Scheduler Asset is available providing basic alarm detection for the Inform IT Scheduler Asset. Status information is not returned. The data is subscribed at a slower rate (60 seconds) when using Light Assets. Follow the configuration procedures for the Asset - Inform IT Scheduler to set up the Light Inform IT Scheduler Asset.

Asset - Inform IT SoftPoint Server

Description: This Asset contains only the software processes listed in the Inform IT SoftPoint Server Software Process Name List (not the Generic Computer subset) and is to be used with the Asset - Inform IT History on page 89.

Inform IT SoftPoint Server Software Process Name List.

- AdsAbsDeployMgr.exe
- AdsCsCommSrv.exe
- AdsScadaSrv.exe

- Table 26 lists the IT General Properties for the Inform IT SoftPoint Server Asset.

Table 26. IT General Properties for Inform IT Softpoint Server Asset

Name	Default Value	Description
Host	localhost	Change this to the name or IP address of the computer to monitor.
SettlingTime	30	The amount of time (30 minutes) to allow the system to settle before establishing a baseline for alarming. This is the recommended minimum value.
OSType	XP	The operating system of the process to be monitored. Leave this field at the default value for Windows 7 and Windows 2008 Server.

Refer to Table 16 to complete the Inform IT SoftPoint Server Asset configuration.

Light Asset - Inform IT SoftPoint Server

A Light Inform IT SoftPoint Server Asset is available providing basic alarm detection for the Inform IT SoftPoint Server Asset. Status information is not returned. The data is subscribed at a slower rate (60 seconds) when using Light Assets. Follow the configuration procedures for the Asset - Inform IT SoftPoint Server to set up the Light Inform IT SoftPoint Server Asset.

Asset - 800xA AS (Tertiary)

Description: The 800xA AS (Tertiary) Asset contains the Generic Computer subset plus the processes listed in the 800xA AS (Tertiary) Software Process Name List.

800xA AS (Tertiary) Software Process Name List.

- AbbClientLicenseProvider.exe
- AdvAeAlarmManager.exe
- AdvAeEventCollector.exe
- AdvAeSoftAlarms.exe
- AfwADServer.exe
- AfwEAEngine.exe
- AfwBackupService.exe
- AfwFsdNode.exe
- AfwFsdSrv.exe
- AfwServiceManager.exe
- AfwSMClient.exe
- AfwSystemMessage.exe
- AfwTimeSrvHdlr.exe
- AfwXRefSrv.exe

Table 27 lists the IT General Properties for the 800xA AS (Tertiary) Asset.

Table 27. IT General Properties for 800xA AS (Tertiary) Asset

Name	Default Value	Description
Host	Localhost	Change this to the name or IP address of the computer to monitor.
SettlingTime	30	The amount of time (30 minutes) to allow the system to settle before establishing a baseline for alarming. This is the recommended minimum value.
NumberCPUs	1	Change this to match the number of CPUs on the computer being monitored. This can be determined by checking the hardware configuration.
OSType	XP	The operating system of the process to be monitored. Leave this field at the default value for Windows 7 and Windows 2008 Server.

Refer to Table 16 and Table 27 to complete the 800xA AS (Tertiary) Asset configuration.

Light Asset - 800xA AS (Tertiary)

A Light 800xA AS (Tertiary) Asset is available providing basic alarm detection for the Computer Asset and the 800xA AS (Tertiary) Asset. Status information is not returned. The data is subscribed at a slower rate (60 seconds) when using Light Assets. Follow the configuration procedures for the Asset - 800xA AS (Tertiary) on page 94 to set up the Light 800xA AS (Tertiary) Asset.

Asset - 800xA AS

Description: The 800xA AS Asset contains the Generic Computer subset plus the processes listed in the 800xA AS Software Process Name List.

800xA AS Software Process Name List.

- AbbClientLicenseProvider.exe
- AdvAeAlarmManager.exe
- AdvAeEventCollector.exe
- AdvAeEventStorage.exe
- AdvAeSoftAlarms.exe
- AdvEAEngine.exe
- AfwADServer.exe
- AfwBackupService.exe
- AfwFsdNode.exe
- AfwFsdSrv.exe
- AfwServiceManager.exe
- AfwSMClient.exe
- AfwSystemMessage.exe
- AfwTimeSrvHdlr.exe
- AfwXRefSrv.exe

Table 28 lists the IT General Properties for the 800xA AS Asset.

Table 28. IT General Properties for 800xA AS Asset

Name	Default Value	Description
Host	Localhost	Change this to the name or IP address of the computer to monitor.
SettlingTime	30	The amount of time (30 minutes) to allow the system to settle before establishing a baseline for alarming. This is the recommended minimum value.
NumberCPUs	1	Change this to match the number of CPUs on the computer being monitored. This can be determined by checking the hardware configuration.
OSType	XP	The operating system of the process to be monitored. Leave this field at the default value for Windows 7 and Windows 2008 Server.

Refer to Table 16 and Table 28 to complete the 800xA AS Asset configuration.

Light Asset - 800xA AS

A Light 800xA AS Asset is available providing basic alarm detection for the Computer Asset and the 800xA AS Asset. Status information is not returned. The data is subscribed at a slower rate (60 seconds) when using Light Assets. Follow the configuration procedures for the Asset - 800xA AS on page 96 to set up the Light 800xA AS Asset.

Asset - 800xA Client

Description: The 800xA Client Asset contains the Generic Computer subset plus the processes listed in the 800xA Client Software Process Name List.

800xA Client Software Process Name List.

- AbbClientLicenseProvider.exe
- AfwFsdNode.exe
- AfwSMClient.exe

Table 29 lists the IT General Properties for the 800xA Client Asset.

Table 29. IT General Properties for 800xA Client Asset

Name	Default Value	Description
Host	Localhost	Change this to the name or IP address of the computer to monitor.
SettlingTime	30	The amount of time (30 minutes) to allow the system to settle before establishing a baseline for alarming. This is the recommended minimum value.
NumberCPUs	1	Change this to match the number of CPUs on the computer being monitored. This can be determined by checking the hardware configuration.
OSType	XP	The operating system of the process to be monitored. Leave this field at the default value for Windows 7 and Windows 2008 Server.

Refer to Table 16 and Table 29 to complete the 800xA Client Asset configuration.

Light Asset - 800xA Client

A Light 800xA Client Asset is available providing basic alarm detection for the Computer Asset and the 800xA Client Asset. Status information is not returned. The data is subscribed at a slower rate (60 seconds) when using Light Assets. Follow the configuration procedures for the Asset - 800xA Client to set up the Light 800xA Client Asset.

Asset - 800xA Combined AS-CS

Description: The 800xA Combined AS-CS Asset contains the Generic Computer subset plus the processes listed in the 800xA Combined AS-CS Software Process Name List.

800xA Combined AS-CS Software Process Name List.

- AbbClientLicenseProvider.exe
- AdvAeAlarmManager.exe
- AdvAeEventCollector.exe #0
- AdvAeEventCollector.exe #1
- AdvAeEventStorage.exe
- AdvAeLogger.exe
- AdvAeSoftAlarms.exe
- AdvEAEngine.exe
- AdvHtHistorySrv.exe
- AfwADServer.exe
- AfwBackupService.exe
- AfwFsdNode.exe
- AfwFsdSrv.exe
- AfwServiceManager.exe
- AfwSMClient.exe
- AfwSystemMessage.exe
- AfwTimeSrvHdlr.exe
- AfwXRefSrv.exe

A process name with a #n after it, where n is the instance number, indicates an instance of the process. Example: process.exe would be treated the same as process.exe #0 but process.exe #1 would be a second instance of the same process.

Table 30 lists the IT General Properties for the 800xA Combined AS-CS Asset.

Table 30. IT General Properties for 800xA Combined AS-CS Asset

Name	Default Value	Description
Host	Localhost	Change this to the name or IP address of the computer to monitor.
SettlingTime	30	The amount of time (30 minutes) to allow the system to settle before establishing a baseline for alarming. This is the recommended minimum value.
NumberCPUs	1	Change this to match the number of CPUs on the computer being monitored. This can be determined by checking the hardware configuration.
OSType	XP	The operating system of the process to be monitored. Leave this field at the default value for Windows 7 and Windows 2008 Server.

Refer to Table 16 and Table 30 to complete the 800xA Combined AS-CS Asset configuration.

Light Asset - 800xA Combined AS-CS

A Light 800xA Combined AS-CS Asset is available providing basic alarm detection for the Computer Asset and the 800xA Combined AS-CS Asset. Status information is not returned. The data is subscribed at a slower rate (60 seconds) when using Light Assets. Follow the configuration procedures for the Asset - 800xA Combined AS-CS on page 99 to set up the Light 800xA Combined AS-CS Asset.

Asset - 800xA CS

Description: The 800xA CS Asset contains the Generic Computer subset plus the processes listed in the 800xA CS Software Process Name List.

800xA CS Software Process Name List.

- AbbClientLicenseProvider.exe
- AdvHtHistorySrv.exe
- AfwFsdNode.exe
- AfwServiceManager.exe
- AfwSMClient.exe

Table 31 lists the IT General Properties for the 800xA CS Asset.

Table 31. IT General Properties for 800xA CS Asset

Name	Default Value	Description
Host	Localhost	Change this to the name or IP address of the computer to monitor.
SettlingTime	30	The amount of time (30 minutes) to allow the system to settle before establishing a baseline for alarming. This is the recommended minimum value.
NumberCPUs	1	Change this to match the number of CPUs on the computer being monitored. This can be determined by checking the hardware configuration.
OSType	XP	The operating system of the process to be monitored. Leave this field at the default value for Windows 7 and Windows 2008 Server.

Refer to Table 16 and Table 31 to complete the 800xA CS Asset configuration.

Light Asset - 800xA CS

A Light 800xA CS Asset is available providing basic alarm detection for the Computer Asset and the 800xA CS Asset. Status information is not returned. The data is subscribed at a slower rate (60 seconds) when using Light Assets. Follow the configuration procedures for the Asset - 800xA CS on page 101 to set up the Light 800xA CS Asset.

Asset - PPB Client

Description: The PPB Client Asset contains the Generic Computer subset plus the processes listed in the PPB Client Software Process Name List.

PPB Client Software Process Name List.

- EBDataSyncService.exe
- EbEventconServer.exe #0
- EBServerBroker.exe

A process name with a #n after it, where n is the instance number, indicates an instance of the process. Example: process.exe would be treated the same as process.exe #0 but process.exe #1 would be a second instance of the same process.

Table 32 lists the IT General Properties for the PPB Client Asset.

Table 32. IT General Properties for PPB Client Asset

Name	Default Value	Description
Host	Localhost	Change this to the name or IP address of the computer to monitor.
SettlingTime	30	The amount of time (30 minutes) to allow the system to settle before establishing a baseline for alarming. This is the recommended minimum value.
NumberCPUs	1	Change this to match the number of CPUs on the computer being monitored. This can be determined by checking the hardware configuration.
OSType	XP	The operating system of the process to be monitored. Leave this field at the default value for Windows 7 and Windows 2008 Server.

Refer to Table 16 and Table 32 to complete the PPB Client Asset configuration.

Light Asset - PPB Client

A Light PPB Client Asset is available providing basic alarm detection for the Computer Asset and the PPB Client Asset. Status information is not returned. The data is subscribed at a slower rate (60 seconds) when using Light Assets. Follow the configuration procedures for the Asset - PPB Client on page 102 to set up the Light PPB Client Asset.

Asset - PPB Config Server

Description: The PPB config server asset contains the generic computer subset plus the processes listed in the PPB Config Server Software Process Name List.

PPB Config Server Software Process Name List.

• EBDataSyncService.exe
• EBServerBroker.exe

Table 33 lists the IT general properties for the 800xA AS Asset.

Table 33. IT General Properties for PPB Config Server Asset

Name	Default Value	Description
Host	Localhost	Change this to the name or IP address of the computer to monitor.
SettlingTime	30	The amount of time (30 minutes) to allow the system to settle before establishing a baseline for alarming. This is the recommended minimum value.
NumberCPUs	1	Change this to match the number of CPUs on the computer being monitored. This can be determined by checking the hardware configuration.
OSType	XP	The operating system of the process to be monitored. Leave this field at the default value for Windows 7 and Windows 2008 Server.

Refer to Table 16 and Table 33 to complete the PPB Config Server Asset configuration.

Light Asset - PPB Config Server

A Light PPB Config Server Asset is available providing basic alarm detection for the Computer Asset and the PPB Config Server Asset. Status information is not returned. The data is subscribed at a slower rate (60 seconds) when using Light Assets. Follow the configuration procedures for the Asset - PPB Config Server on page 103 to set up the Light PPB Config Server Asset.

Asset - PPB Harmony RTDS with Client

Description: The PPB Harmony RTDS with Client Asset contains the Generic Computer subset plus the processes listed in the PPB Harmony RTDS with Client Process Name List.

PPB Harmony RTDS with Client Process Name List.

- EBDataSyncService.exe
- EbEventconServer.exe #0
- EbEventconServer.exe #1
- EbI90Server.exe
- EBServerBroker.exe
- EbSystemServer.exe
- SOAPSymTagAtomSrv.exe

> A process name with a #n after it, where n is the instance number, indicates an instance of the process. Example: process.exe would be treated the same as process.exe #0 but process.exe #1 would be a second instance of the same process.

Table 34 lists the IT General Properties for the PPB Harmony RTDS with Client Asset.

Table 34. IT General Properties for PPB Harmony RTDS with Client Asset

Name	Default Value	Description
Host	Localhost	Change this to the name or IP address of the computer to monitor.
SettlingTime	30	The amount of time (30 minutes) to allow the system to settle before establishing a baseline for alarming. This is the recommended minimum value.
NumberCPUs	1	Change this to match the number of CPUs on the computer being monitored. This can be determined by checking the hardware configuration.
OSType	XP	The operating system of the process to be monitored. Leave this field at the default value for Windows 7 and Windows 2008 Server.

Refer to Table 16 and Table 34 to complete the PPB Harmony RTDS with Client Asset configuration.

Light Asset - PPB Harmony RTDS with Client

A Light PPB Harmony RTDS with Client Asset is available providing basic alarm detection for the Computer Asset and the PPB Harmony RTDS with Client Asset. Status information is not returned. The data is subscribed at a slower rate (60 seconds) when using Light Assets. Follow the configuration procedures for the Asset - PPB Harmony RTDS with Client on page 104 to set up the Light PPB Harmony RTDS with Client Asset.

Asset - PPB Historian

Description: The PPB Historian Asset contains the Generic Computer subset plus the processes listed in the PPB Historian Software Process Name List.

PPB Historian Software Process Name List.

• EBDataSyncService.exe
• EBHistorianServer.exe
• EBServerBroker.exe

Table 35 lists the IT General Properties for the PPB Historian Asset.

Table 35. IT General Properties for PPB Historian Asset

Name	Default Value	Description
Host	Localhost	Change this to the name or IP address of the computer to monitor.
SettlingTime	30	The amount of time (30 minutes) to allow the system to settle before establishing a baseline for alarming. This is the recommended minimum value.
NumberCPUs	1	Change this to match the number of CPUs on the computer being monitored. This can be determined by checking the hardware configuration.
OSType	XP	The operating system of the process to be monitored. Leave this field at the default value for Windows 7 and Windows 2008 Server.

Refer to Table 16 and Table 35 to complete the PPB Historian Asset configuration.

Light Asset - PPB Historian

A Light PPB Historian Asset is available providing basic alarm detection for the Computer Asset and the PPB Historian Asset. Status information is not returned. The data is subscribed at a slower rate (60 seconds) when using Light Assets. Follow the configuration procedures for the Asset - PPB Historian to set up the Light PPB Historian Asset.

Asset - PPB Melody RTDS with Client

Description: The PPB Melody RTDS with Client Asset contains the Generic Computer subset plus the processes listed in the PPB Melody RTDS with Client Software Process Name List.

PPB Melody RTDS with Client Software Process Name List.

- EBDataSyncService.exe
- EbEventconServer.exe #0
- EbEventconServer.exe #1
- EbMelodyServer.exe
- EBServerBroker.exe
- EbSystemServer.exe
- SOAPSymTagAtomSrv.exe

A process name with a #n after it, where n is the instance number, indicates an instance of the process. Example: process.exe would be treated the same as process.exe #0 but process.exe #1 would be a second instance of the same process.

Table 36 lists the IT General Properties for the PPB Melody RTDS with Client Asset.

Table 36. IT General Properties for PPB Melody RTDS with Client Asset

Name	Default Value	Description
Host	Localhost	Change this to the name or IP address of the computer to monitor.
SettlingTime	30	The amount of time (30 minutes) to allow the system to settle before establishing a baseline for alarming. This is the recommended minimum value.
NumberCPUs	1	Change this to match the number of CPUs on the computer being monitored. This can be determined by checking the hardware configuration.
OSType	XP	The operating system of the process to be monitored. Leave this field at the default value for Windows 7 and Windows 2008 Server.

Refer to Table 16 and Table 36 to complete the PPB Melody RTDS with Client Asset configuration.

Light Asset - PPB Melody RTDS with Client

A Light PPB Melody RTDS with Client Asset is available providing basic alarm detection for the Computer Asset and the PPB Melody RTDS with Client Asset. Status information is not returned. The data is subscribed at a slower rate (60 seconds) when using Light Assets. Follow the configuration procedures for the Asset - PPB Melody RTDS with Client on page 108 to set up the Light PPB Melody RTDS with Client Asset.

Asset - PPB OPC RTDS with Client

Description: The PPB OPC RTDS with Client contains the Generic Computer subset plus the processes listed in the PPB OPC RTDS with Client Software Process Name List.

PPB OPC RTDS with Client Software Process Name List.

- EBDataSyncService.exe
- EbEventconServer.exe #0
- EbEventconServer.exe #1
- EbOPCServer.exe
- EBServerBroker.exe
- EbSystemServer.exe
- SOAPSymTagAtomSrv.exe

A process name with a #n after it, where n is the instance number, indicates an instance of the process. Example: process.exe would be treated the same as process.exe #0 but process.exe #1 would be a second instance of the same process.

Table 37 lists the IT General Properties for the PPB OPC RTDS with Client Asset.

Table 37. IT General Properties for PPB OPC RTDS with Client Asset

Name	Default Value	Description
Host	Localhost	Change this to the name or IP address of the computer to monitor.
SettlingTime	30	The amount of time (30 minutes) to allow the system to settle before establishing a baseline for alarming. This is the recommended minimum value.
NumberCPUs	1	Change this to match the number of CPUs on the computer being monitored. This can be determined by checking the hardware configuration.
OSType	XP	The operating system of the process to be monitored. Leave this field at the default value for Windows 7 and Windows 2008 Server.

Refer to Table 16 and Table 37 to complete the PPB OPC RTDS with Client Asset configuration.

Light Asset - PPB OPC RTDS with Client

A Light PPB OPC RTDS with Client Asset is available providing basic alarm detection for the Computer Asset and the PPB OPC RTDS with Client Asset. Status information is not returned. The data is subscribed at a slower rate (60 seconds) when using Light Assets. Follow the configuration procedures for the Asset - PPB OPC RTDS with Client on page 109 to set up the Light PPB OPC RTDS with Client Asset.

Asset - Symmetricom XLi Clock Alarm

Description: Represents the Symmetricom XLi Satellite Clock device. It generates alarms when one of the fault conditions of the clock enters the fault state. It indicates clock related data such as clock status and clock source.

Table 38 lists IT Devices for the Symmetricom XLi Clock Asset.

Table 38. Symmetricom XLi Clock Asset IT Device List

Device Name	IT Device	Description
Alarms		
Symmetricom XLi Clock Alarm	Symmetricom XLi Clock Alarm	Generates an alarm if one of the clock fault conditions enters the fault state.
Status		
Symmetricom XLi Clock Status	Symmetricom XLi Clock Status	Returns the basic status attributes.

Table 39 lists the IT General Properties for the Symmetricom XLi Clock Asset.

Table 39. IT General Properties for Symmetricom XLi Clock Asset

Name	Default Value[1]	Description
Host	localhost	Change this to the name or IP address of the computer making the status requests to the clock. This is typically the same computer running the monitoring software. This is not the IP address of the clock.
Community		Change the SNMP community name for the device being monitored. This name is equivalent to a password allowing communication. Check with network personnel responsible for configuring this device to determine the name.
IP Address		Enter the IP address of the clock being monitored.

NOTE:
1. Blank cells in the **Default Value** column indicate that a **value must be entered**.

Table 40 lists the Modifiable IT Device Token Configurations for the Symmetricom XLi Clock Asset.

Table 40. Modifiable IT Device Token Configurations for a Symmetricom XLi Clock Asset

IT Device Name	Modifiable Token	Default Value	Description
Symmetricom XLi Clock Alarm	statusPrimaryRefClk::Enable	True	Enables or disables the alarm for this item.
	statusSecondaryRefClk::Enable		
	statusIrig::Enable		
	statusAuxRef::Enable		
	statusPrimaryPower::Enable		
	statusSecondaryPower::Enable		
	statusRbOsc::Enable		
	statusDac::Enable		
	statusTimeError::Enable		
	statusTimeout::Enable		

Inform IT Performance Assets

The basic categories of Inform IT Performance Assets are:

- IM API Counters
- IM Archive Counters
- IM Storage Counters
- IM Collection Counters

Each Inform IT Performance Asset listed in this section indicates the category to which it belongs.

Asset - hsMsgServer Messages In per Minute

Description: This asset provides status information and alarming for the rate of speed of messages received by the History Message Server.

Table 41 lists IT devices for the hsMsgServer messages in per minute performance counter.

Table 41. hsMsgServer Messages In per Minute Performance Counter IT Device List

Device Name	IT Device	Description
Alarms		
Message per Minute	Performance Counter Alarm	Generates an alarm when the performance counter has reached or exceeded its acceptable limits.
Status		
Message per Minute	Performance Counter Alert	Generates an alert when the performance counter has reached or exceeded its acceptable limits.
Message per Minute	Performance Counter Status	Provides the current value of the performance counter.

Table 42 lists the IT general properties for the hsMsgServer Messages In per Minute Performance Counter.

Table 42. IT General Properties for hsMsgServer Messages In per Minute Performance Counter

Name	Default Value[1]	Description
Host	Localhost	Change this to the name or IP address of the computer to monitor.
Category	**IM API Counters**	**For System Use – Do not modify.** The Windows performance monitor category that this counter can be found in.
Counter	**Msg / Minute In**	**For System Use – Do not modify.** The number of messages per minute received by the History Message Server. The typical maximum value is 30 messages per second.
Instance	**hsMsgServer Msgs per minute**	**For System Use – Do not modify.** Windows performance name that this counter belongs to.
LowLevel	3600	Default low alarm limit, value at which the system is still functional but is being stressed beyond its normal capabilities. This is the recommended minimum value.
MediumLevel	3650	Default medium alarm limit, value at which the system is starting to experience significant performance problems. This is the recommended minimum value.
HighLevel	3700	Default high alarm limit, value at which a serious problem is occurring. This is the recommended minimum value.
Condition	**IM hsMsgServer Messages In / Minute are High**	**For System Use – Do not modify.** An alarm would mean that the messages in per minute are higher than design limits.

NOTE:

1. All **bold** entries in the **Default Value** column are for system use only. **DO NOT modify** the values in the **Default Value** column.

Asset - hsMsgServer Messages in Queue

Description: This Asset provides status information and alarming for the number of unprocessed messages in the History Message Server queue.

Table 43 lists IT Devices for the hsMsgServer Messages In Queue Performance Counter.

Table 43. hsMsgServer Messages in Queue Performance Counter IT Device List

Device Name	IT Device	Description
Alarms		
Message per Minute	Performance Counter Alarm	Generates an alarm when the performance counter has reached or exceeded its acceptable limits.
Status		
Message per Minute	Performance Counter Alert	Generates an alert when the performance counter has reached or exceeded its acceptable limits.
Message per Minute	Performance Counter Status	Provides the current value of the performance counter.

Table 44 lists the IT general properties for the hsMsgServer Messages In Queue Performance Counter.

Table 44. IT General Properties for hsMsgServer Messages In Queue Performance Counter

Name	Default Value[1]	Description
Host	localhost	Change this to the name or IP address of the computer to monitor.
Category	**IM API Counters**	**For System Use – Do not modify.** The Windows performance monitor category that this counter can be found in.
Counter	**Msgs in Queue**	**For System Use – Do not modify.** The number of messages in the queue.

Table 44. IT General Properties for hsMsgServer Messages In Queue Performance Counter (Continued)

Name	Default Value[1]	Description
Instance	**hsMsgServer Msgs per minute**	**For System Use – Do not modify.** Windows performance name that this counter belongs to.
LowLevel	3600	Default low alarm limit, value at which the system is still functional but is being stressed beyond its normal capabilities. This is the recommended minimum value.
MediumLevel	3650	Default medium alarm limit, value at which the system is starting to experience significant performance problems. This is the recommended minimum value.
HighLevel	3700	Default high alarm limit, value at which a serious problem is occurring. This is the recommended minimum value.
Condition	**IM hsMsgServer Messages in Queue are High**	**For System Use – Do not modify.** An alarm indicates that the messages in the queue are higher than design limits and the queue is filling up and may overflow.

NOTE:

1. All **bold** entries in the **Default Value** column are for system use only. **DO NOT modify** the values in the **Default Value** column.

Asset - hsMsgServer Messages Out per Minute

Description: This Asset provides status information and alarming for the rate of speed of messages sent by the History Message Server.

Table 45 lists IT devices for the hsMsgServer Messages Out per Minute Performance Counter.

Table 45. hsMsgServer Messages Out per Minute Performance Counter IT Device List

Device Name	IT Device	Description
Alarms		
Message per Minute	Performance Counter Alarm	Generates an alarm when the performance counter has reached or exceeded its acceptable limits.
Status		
Message per Minute	Performance Counter Alert	Generates an alert when the performance counter has reached or exceeded its acceptable limits.
Message per Minute	Performance Counter Status	Provides the current value of the performance counter.

Table 46 lists the IT General Properties for the hsMsgServer Messages Out per Minute Performance Counter.

Table 46. IT General Properties for hsMsgServer Messages Out per Minute Performance Counter

Name	Default Value[1]	Description
Host	localhost	Change this to the name or IP address of the computer to monitor.
Category	**IM API Counters**	**For System Use – Do not modify.** The Windows performance monitor category that this counter can be found in.
Counter	**Msgs/Minute Out**	**For System Use – Do not modify.** The number of messages processed per minute.

Table 46. IT General Properties for hsMsgServer Messages Out per Minute Performance Counter (Continued)

Name	Default Value[1]	Description
Instance	**hsMsgServer Msgs per minute**	**For System Use – Do not modify.** Windows performance name that this counter belongs to
LowLevel	3600	Default low alarm limit, value at which the system is still functional but is being stressed beyond its normal capabilities. This is the recommended minimum value.
MediumLevel	3650	Default medium alarm limit, value at which the system is starting to experience significant performance problems. This is the recommended minimum value.
HighLevel	3700	Default high alarm limit, value at which a serious problem is occurring. This is the recommended minimum value.
Condition	**IM hsMsgServer Msgs Messages Out/ Minutes are high**	**For System Use – Do not modify.** An alarm indicates that the messages per minute out are higher than design limits.

NOTE:

1. All **bold** entries in the **Default Value** column are for system use only. **DO NOT modify** the values in the **Default Value** column.

Asset - PDL Messages In per Minute

Description: This Asset provides status information and alarming for the rate of speed of messages received by the Production Data Logger.

Table 47 lists IT Devices for the PDL Messages In per Minute Performance Counter.

Table 47. PDL Messages In per Minute Performance Counter IT Device List

Device Name	IT Device	Description
Alarms		
Message per Minute	Performance Counter Alarm	Generates an alarm when the performance counter has reached or exceeded its acceptable limits.
Status		
Message per Minute	Performance Counter Alert	Generates an alert when the performance counter has reached or exceeded its acceptable limits.
Message per Minute	Performance Counter Status	Provides the current value of the performance counter.

Table 48 lists the IT General Properties for the PDL Messages In per Minute Performance Counter.

Table 48. IT General Properties for PDL Messages In per Minute Performance Counter

Name	Default Value[1]	Description
Host	localhost	Change this to the name or IP address of the computer to monitor.
Category	**IM API Counters**	**For System Use – Do not modify.** The Windows performance monitor category that this counter can be found in.
Counter	**Msgs/Minute In**	**For System Use – Do not modify.** The number of messages received per minute. The typical maximum value is 30 messages per second.
Instance	**PDL Msgs per minute**	**For System Use – Do not modify.** Windows performance name that this counter belongs to
LowLevel	3600	Default low alarm limit, value at which the system is still functional but is being stressed beyond its normal capabilities. This is the recommended minimum value.
MediumLevel	3650	Default medium alarm limit, value at which the system is starting to experience significant performance problems. This is the recommended minimum value.
HighLevel	3700	Default high alarm limit, value at which a serious problem is occurring. This is the recommended minimum value.
Condition	**IM PDL Messages in / Minutes are High**	**For System Use – Do not modify.** An alarm indicates that the messages per minutes in are higher than design limits.

NOTE:

1. All **bold** entries in the **Default Value** column are for system use only. **DO NOT modify** the values in the **Default Value** column.

Asset - PDL Messages in Queue

Description: This Asset provides status information and alarming for the number of unprocessed messages in the Production Data Logger queue.

Table 49 lists IT Devices for the PDL Messages In Queue Performance Counter.

Table 49. PDL Messages In Queue Performance Counter IT Device List

Device Name	IT Device	Description
Alarms		
Message per Minute	Performance Counter Alarm	Generates an alarm when the performance counter has reached or exceeded its acceptable limits.
Status		
Message per Minute	Performance Counter Alert	Generates an alert when the performance counter has reached or exceeded its acceptable limits.
Message per Minute	Performance Counter Status	Provides the current value of the performance counter.

Table 50 lists the IT General Properties for the PDL Messages in Queue Performance Counter.

Table 50. IT General Properties for PDL Messages in Queue Performance Counter

Name	Default Value	Description
Host	localhost	Change this to the name or IP address of the computer to monitor.
Category	**IM API Counters**	**For System Use – Do not modify.** The Windows performance monitor category that this counter can be found in.
Counter	**Msgs in Queue**	**For System Use – Do not modify.** The number of messages remaining to be processed.
Instance	**PDL Msgs per minute**	**For System Use – Do not modify.** Windows performance name that this counter belongs to.
LowLevel	3600	Default low alarm limit, value at which the system is still functional but is being stressed beyond its normal capabilities. This is the recommended minimum value.
MediumLevel	3650	Default medium alarm limit, value at which the system is starting to experience significant performance problems. This is the recommended minimum value.
HighLevel	3700	Default high alarm limit, value at which a serious problem is occurring. This is the recommended minimum value.
Condition	**IM PDL Messages in Queue are High**	**For System Use – Do not modify.** An alarm indicates that the messages in the queue are higher than design limits and the queue is filling up and may overflow.

NOTE:
1. All **bold** entries in the **Default Value** column are for system use only. **DO NOT modify** the values in the Default **Value** column.

Asset - PDL Messages Out per Minute

Description: This Asset provides status information and alarming for the rate of speed of messages sent by the Production Data Logger.

Table 51 lists IT Devices for the PDL Messages Out per Minute Performance Counter.

Table 51. PDL Messages Out per Minute Performance Counter IT Device List

Device Name	IT Device	Description
Alarms		
Message per Minute	Performance Counter Alarm	Generates an alarm when the performance counter has reached or exceeded its acceptable limits.
Status		
Message per Minute	Performance Counter Alert	Generates an alert when the performance counter has reached or exceeded its acceptable limits.
Message per Minute	Performance Counter Status	Provides the current value of the performance counter.

Table 52 lists the IT General Properties for the PDL Messages Out per Minute Performance Counter.

Table 52. IT General Properties for PDL Messages Out per Minute Performance Counter

Name	Default Value	Description
Host	localhost	Change this to the name or IP address of the computer to monitor.
Category	**IM API Counters**	**For System Use – Do not modify.** The Windows performance monitor category that this counter can be found in.
Counter	**Msgs /Minute Out**	**For System Use – Do not modify.** The number of messages processed per minute.
Instance	**PDL Msgs per minute**	**For System Use – Do not modify.** Windows performance name that this counter belongs to
LowLevel	3600	Default low alarm limit, value at which the system is still functional but is being stressed beyond its normal capabilities. This is the recommended minimum value.
MediumLevel	3650	Default medium alarm limit, value at which the system is starting to experience significant performance problems. This is the recommended minimum value.
HighLevel	3700	Default high alarm limit, value at which a serious problem is occurring. This is the recommended minimum value.
Condition	**IM PDL Messages Out/ Minutes are High**	**For System Use – Do not modify.** An alarm indicates that the messages per minute out are higher than design limits.

NOTE:
1.   All **bold** entries in the **Default Value** column are for system use only. **DO NOT modify** the values in the Default **Value** column.

Asset - Disk Free

Description: This Asset displays the amount of space that is left on either the hard disk or removable media that is being used for archiving historical data.

Table 53 lists IT Devices for the Disk Free Asset.

Table 53. Disk Free Asset IT Device List

Device Name	IT Device	Description
Alarms		
Free Disk Space	Performance Counter Alarm (Reversed)	Generates an alarm when the performance counter has reached or exceeded its acceptable limits.
Status		
Free Disk Space	Performance Counter Alert (Reversed)	Generates an alert when the performance counter has reached or exceeded its acceptable limits.
Free Disk Space	Performance Counter Status	Provides the current value of the performance counter.

Table 54 lists the IT General Properties for the Disk Free Asset.

Table 54. IT General Properties for Disk Free Asset

Name	Default Value[1]	Description
Host	localhost	Change this to the name or IP address of the computer to monitor.
Category	**IM Archive Counters**	**For System Use – Do not modify**. The category that this counter can be found in.
Counter	**Disk Free**	**For System Use – Do not modify.** Percentage disk free space left on either the hard drive or removable media.
Instance	**IM Archive**	**For System Use – Do not modify**. Used for archiving historical data.
WarningLevel	15	Default warning alarm limit. The percentage of hard disk space required before a Free Space Warning alarm occurs.
SeriousLevel	10	Default serious alarm limit. The percentage of hard disk space required before a Free Space Serious alarm occurs.
CriticalLevel	5	Default critical alarm limit. The percentage of hard disk space required before a Free Space Critical alarm occurs.
Condition	**IM Archive Disk Free Space Low**	**For System Use – Do not modify.** An alarm indicates that the percent free space is lower than the set limits.

NOTE:

1. All **bold** entries in the **Default Value** column are for system use only. **DO NOT modify** the values in the **Default Value** column.

Asset - Failures

Description: This Asset provides status information and alarming for the number of Archive Failures since the last reboot on the computer in which Archiving is being executed.

Table 55 lists IT Devices for the Failures Asset.

Table 55. Failures Asset IT Device List

Device Name	IT Device	Description
Alarms		
Archive Failure Alarm	Performance Counter Alarm	Generates an alarm when the performance counter has reached or exceeded its acceptable limits.
Status		
Archive Failure Alert	Performance Counter Alert	Generates an alert when the performance counter has reached or exceeded its acceptable limits.
Failures Since Last Reboot	Performance Counter Status	Provides the current value of the performance counter.

Table 56 lists the IT General Properties for the Failures Asset.

Table 56. IT General Properties for Failures Asset

Name	Default Value[1]	Description
Host	Localhost	Change this to the name or IP address of the computer to monitor.
Category	**IM Archive Counters**	**For System Use – Do not modify.** The category that this counter can be found in.
Counter	**Failures**	**For System Use – Do not modify.** Failures since last reboot.
Instance	**IM Archive**	**For System Use – Do not modify.** Used for archiving data.
LowLevel	10	Default low alarm limit. The number of archive failures before a low alarm occurs.
MediumLevel	20	Default medium alarm limit. The number of archive failures before a medium alarm occurs.
HighLevel	30	Default high alarm limit. The number of archive failures before a high alarm occurs.
Condition	**IM Archive Failures are High**	**For System Use – Do not modify.** An alarm indicates that more failures have occurred then expected.

NOTE:

1.   All **bold** entries in the **Default Value** column are for system use only. **DO NOT modify** the values in the **Default Value** column.

Asset - Storages

Description: This Asset provides status information and alarming for the rate of speed of numeric data points being stored for historical purposes.

Table 57 lists IT Devices for the Storages Asset.

Table 57. Storages Asset IT Device List

Device Name	IT Device	Description
Alarms		
Storages Alarm	Performance Counter Alarm	Generates an alarm when the performance counter has reached or exceeded its acceptable limits.
Status		
Storages Alert	Performance Counter Alert	Generates an alert when the performance counter has reached or exceeded its acceptable limits.
Messages per Minute	Performance Counter Status	Provides the current value of the performance counter.

Table 58 lists the IT General Properties for the Storages Asset.

Table 58. IT General Properties for Storages Asset

Name	Default Value[1]	Description
Host	Localhost	Change this to the name or IP address of the computer to monitor.
Category	**IM Storage Counters**	**For System Use – Do not modify.** The category that this counter can be found in.
Counter	**Pts/minute**	**For System Use – Do not modify.** The number of numeric data points being stored to history per minute.
Instance	**IM Storage**	**For System Use – Do not modify.** Windows performance name that this counter belongs to.
LowLevel	60000	Default low alarm limit. If the number of numeric data being stored to history goes above the default limit a low alarm occurs.
MediumLevel	65000	Default medium alarm limit. If the number of numeric data being stored to history goes above the default limit a medium alarm occurs.
HighLevel	70000	Default high alarm limit. If the number of numeric data being stored to history goes above the default limit a high alarm occurs.
Condition	**IM Storages are High**	**For System Use – Do not modify.** An alarm indicates that more failures have occurred then expected.

NOTE:

1.   All **bold** entries in the **Default Value** column are for system use only. **DO NOT modify** the values in the **Default Value** column.

Asset - DA Collection

Description: This Asset provides status information and alarming for the rate of speed of data collection by the DA Server.

Table 59 lists IT Devices for the DA Collection Asset.

Table 59. DA Collection Asset IT Device List

Device Name	IT Device	Description
Alarms		
DA Collection Alarm	Performance Counter Alarm	Generates an alarm when the performance counter has reached or exceeded its acceptable limits.
Status		
DA Collection Alert	Performance Counter Alert	Generates an alert when the performance counter has reached or exceeded its acceptable limits.
Points Collected per Minute	Performance Counter Status	Provides the current value of the performance counter.

Table 60 lists the IT General Properties for the DA Collection Asset.

Table 60. IT General Properties for DA Collection Asset

Name	Default Value	Description
Host	Localhost	Change this to the name or IP address of the computer to monitor.
Category	**IM Collection Counters**	**For System Use – Do not modify.** The category that this counter can be found in.
Counter	**Pts/Minute**	**For System Use – Do not modify.** The number of points per minute being collected from the 800xA DA server.
Instance	**IM DA_Collection**	**For System Use – Do not modify.** Windows performance name the counter belongs to.
LowLevel	60000	Default low alarm limit. The number of DA points collected before a low alarm occurs.
MediumLevel	65000	Default medium alarm limit. The number of DA points collected before a medium alarm occurs.
HighLevel	70000	Default high alarm limit. The number of DA points collected before a high alarm occurs.
Condition	**IM DA Collection is High**	**For System Use – Do not modify.** An alarm indicates that the DA points per minute are higher than the default limits.

NOTE:

1. All **bold** entries in the **Default Value** column are for system use only. **DO NOT modify** the values in the **Default Value** column.

Asset - HDA Collection

Description: This Asset provides status information and alarms for the rate of speed of data collection by the HDA Server.

Table 61 lists IT Devices for the HDA Collection Asset.

Table 61. HDA Collection Asset IT Device List

Device Name	IT Device	Description
Alarms		
HDA Collection Alarm	Performance Counter Alarm	Generates an alarm when the performance counter has reached or exceeded its acceptable limits.
Status		
HDA Collection Alert	Performance Counter Alert	Generates an alert when the performance counter has reached or exceeded its acceptable limits.
Points Collected per Minute	Performance Counter Status	Provides the current value of the performance counter.

Table 62 lists the IT General Properties for the HDA Collection Asset.

Table 62. IT General Properties for HDA Collection Asset

Name	Default Value	Description
Host	Localhost	Change this to the name or IP address of the computer to monitor.
Category	**IM Collection Counters**	**For System Use – Do not modify.** The category that this counter can be found in.
Counter	**Pts/Minute**	**For System Use – Do not modify.** The number of points per minute being collected from the 800xA HDA server.
Instance	**IM HDA_Collection**	**For System Use – Do not modify.** Windows performance name the counter belongs to.

Table 62. IT General Properties for HDA Collection Asset (Continued)

Name	Default Value	Description
LowLevel	60000	Default low alarm limit. The number of HDA points collected before a low alarm occurs.
MediumLevel	65000	Default medium alarm limit. The number of HDA points collected before a medium alarm occurs.
HighLevel	70000	Default high alarm limit. The number of HDA points collected before a high alarm occurs.
Condition	**IM HDA Collection is High**	**For System Use – Do not modify.** An alarm indicates that the HDA points per minute are higher than the default limits.

NOTE:

1.　All **bold** entries in the **Default Value** column are for system use only. **DO NOT modify** the values in the **Default Value** column.

Asset - Generic Network Interface

Description: This Asset provides status information and alarming for a network interface card in a computer.

Table 63 lists IT Devices for the Generic Network Interface Asset.

Table 63. Generic Network Interface Asset IT Device List

Device Name	IT Device	Description
Alarms		
Network Interface Alarm	Generic Interface Alarm	Generates an alarm when an abnormal condition occurs.
Status		
Network Interface Alert	Generic Interface Alert	Generates an alert when an abnormal condition occurs.
Network Interface Status	Generic Interface Status	Returns the status of key attributes of a network interface.

Table 64 lists the IT General Properties for the Disk Free Asset.

Table 64. IT General Properties for Generic Network Interface Asset

Name	Default Value	Description
Host	Localhost	Change this to the name or IP address of the computer where the network interface is installed and requires monitoring.

In order to complete the configuration requirements for the Generic Network Interface Asset, identify the Device ID number using the WMI Object Browser. A free download of the WMI Administrative Tools, including the WMI Object Browser is available at:

> http://www.microsoft.com/downloads/details.aspx?FamilyID=6430f853-1120-48db-8cc5-f2abdc3ed314&DisplayLang=en

1. The first step in finding the Device ID is determining the Device Name. Open the Network Connections dialog.

    The Local Area Connection lists the network cards that are installed in the workstation. The Device Name column contains the name, for example, Intel(R) PRO/1000 MT Network Connection. This is the name to search for in the WMI Object Browser.

2. Launch the WMI Object Browser. Select:

    Start > All Programs > WMI Tools > WMI Object Browser

3. Navigate to and select the following directory:

        root\CIMV2\Win32_SystemDevices\Win32_NetworkAdapter

    The right-hand pane displays information regarding the network cards.

4. Scroll through the columns on the right and locate the Name column.

5. Find the row with the Device Name that was determined in Step 1.

6. Scroll to the left, back to the DeviceID column (the first column) to find the corresponding Device ID number. This number is the WMI key entered in the IT Device Token Configuration, refer to Table 65.

Table 65. Modifiable IT Device Token Configurations for Generic Network Interface

IT Device Name	Modifiable Tokens	Default Value[1]	Description
Network Interface Alarm	CommonTokens::DeviceID		Enter the WMI key that identifies the network interface.
Network Interface Alert	CommonTokens::DeviceID		Enter the WMI key that identifies the network interface. This will be the same number as used in the Network Interface Alarm default value.
Network Interface Status	CommonTokens::DeviceID		Enter the WMI key that identifies the network interface. This will be the same number as used in the Network Interface Alarm default value.

NOTE:

1. Blank cells in the **Default Value** column indicate that a **value must be entered**.

Asset - Generic Printer

Description: This Asset represents a typical network printer. It includes basic status information, and alarm detection for items such as out of paper. The printer models tested and supported by this object type are HP Laserjet 5M and Xerox Document Center 470ST.

Table 66 lists the IT Devices for the Generic Printer Asset.

Table 66. Generic Printer IT Device List

Device Name	IT Device	Description
Alarms		
Printer Alarm	Printer Alarm	Generates alarms for low toner, paper jammed, etc.
Status		
Printer Alert	Printer Alert	Generates alerts for low toner, paper jammed, etc.
Printer Status	Printer Status	Provides key status information pertaining to the printer, such as name, location, printer status, etc.

Table 67 lists the IT General Properties for the Generic Printer Asset.

Table 67. IT General Properties for Generic Printer Asset

Name	Default Value[1]	Description
Host	Localhost	Leave this name as the default local host.
Community		Change the SNMP community name for the device being monitored. This name is equivalent to a password allowing communication. Check with network personnel responsible for configuring this device to determine the name.
IP Address		Enter the IP address of the printer being monitored.

NOTE:
1.   Blank cells in the **Default Value** column indicate that a **value must be entered**.

Network Monitoring

Asset - Network Utilization

Description: The Network Utilization Asset monitors network traffic on the network segment.

Table 68 lists IT Devices for the Network Utilization Asset.

Table 68. Network Utilization Asset IT Device List

Device Name	IT Device	Description
Alarms		
Network Alarm	Network Utilization Alarm	Alarms when the utilization exceeds the nominal bandwidth at three thresholds.
Status		
Network Alert	Network Utilization Alert	Alerts when the utilization exceeds the nominal bandwidth at three thresholds.
Network Utilization (Bytes per s) Status	Network Utilization (Bytes per s) Status	Utilization in bytes per second.
Network Utilization (Percent) Status	Network Utilization (Percent) Status	Utilization in percent of nominal bandwidth.

Table 69 lists the IT General Properties for the Network Utilization Asset.

Table 69. IT General Properties for Network Utilization Asset

Name	Default Value[1,2]	Description
Host		Enter the name or IP address of the host computer where the network monitor is running.
IP Address		Enter the IP address of the network adapter in the host computer that is connected to the target network.
Family	All	The IP protocol family. This is the recommended value.
Protocol		The IP protocol. This is the recommended value.
Application		The IP application. This is the recommended value.
Port		**This must be left blank.** The Port used by the network monitor.

NOTES:
1. Blank cells in the **Default Value** column indicate that a **value must be entered**.
2. Shaded cells in the **Default Value** column indicate that the **value must be left blank.**

Table 70 lists the modifiable IT Device Token Configurations for the Network Utilization Asset.

Table 70. Modifiable IT Device Token Configurations for Network Utilization Asset

IT Device Name	Modifiable Tokens	Default Value	Description
Network Alarm	CommonTokens::Family	All	The IP protocol family. This is the recommended value.
	CommonTokens::Protocol	All	The IP protocol. This is the recommended value.
	CommonTokens::Application	All	The IP application. This is the recommended value.
	CommonTokens::LowLevel	25%	The low level network utilization threshold, exceeding the default value causes an alarm.
	CommonTokens::MediumLevel	50%	The medium level network utilization threshold, exceeding the default value causes an alarm.
	CommonTokens::HighLevel	75%	The high level network utilization threshold, exceeding the default value causes an alarm.
	CommonTokens::SampleCount	15	The number of samples used to average the utilization calculation.
Network Alert	CommonTokens::Family	All	The IP protocol family. This is the recommended value.
	CommonTokens::Protocol	All	The IP protocol. This is the recommended value.
	CommonTokens::Application	All	The IP application. This is the recommended value.
	CommonTokens::LowLevel	25%	The low level network utilization threshold, exceeding the default value causes an alert.

Table 70. Modifiable IT Device Token Configurations for Network Utilization Asset (Continued)

IT Device Name	Modifiable Tokens	Default Value	Description
	CommonTokens::MediumLevel	50%	The medium level network utilization threshold, exceeding the default value causes an alert.
	CommonTokens::HighLevel	75%	The high level network utilization threshold, exceeding the default value causes an alert.
	CommonTokens::SampleCount	15	The number of samples used to average the utilization calculation.
Network Utilization (Bytes per s) Status	Network Utilization (Bytes per s) Status::Family	All	The IP protocol family. This is the recommended value.
	Network Utilization (Bytes per s) Status::Protocol	All	The IP protocol. This is the recommended value.
	Network Utilization (Bytes per s) Status::Application	All	The IP application. This is the recommended value.
	Network Utilization (Bytes per s) Status::SampleCount	15	The number of samples used to average the utilization calculation.
Network Utilization (Percent) Status	Network Utilization (Percent) Status::Family	All	The IP protocol family. This is the recommended value.
	Network Utilization (Percent) Status::Protocol	All	The IP protocol. This is the recommended value.
	Network Utilization (Percent) Status::Application	All	The IP application. This is the recommended value.
	Network Utilization (Percent) Status::SampleCount	15	The number of samples used to average the utilization calculation.

Asset - Node to Node Utilization

Description: The Node to Node Utilization Asset monitors traffic between two specific nodes.

Table 71 lists IT Devices for the Node to Node Utilization Asset.

Table 71. Node to Node Utilization Asset IT Device List

Device Name	IT Device	Description
Alarms		
Node to Node Alarm	Node to Node Utilization Alarm	Alarms when the utilization exceeds the nominal bandwidth at three thresholds.
Status		
Node to Node Alert	Node to Node Utilization Alert	Alerts when the utilization exceeds the nominal bandwidth at three thresholds.
Node to Node Utilization (Bytes per s)	Node to Node Utilization (Bytes per s) Status	Node to Node utilization in bytes per sec.
Node to Node Utilization (Percent)	Node to Node Utilization (Percent)	Node to Node utilization in percent of nominal bandwidth.

Table 72 lists the IT General Properties for the Node to Node Utilization Asset.

Table 72. IT General Properties for Node to Node Utilization Asset

Name	Default Value[1,2]	Description
Host		Enter the name or IP address of the host computer where the network monitor is running.
IP Address		Enter the IP address of the network adapter on the host computer that is connected to the target network.
Port		**This must be left blank.** The Port used by the network monitor.

NOTES:
1.   Blank cells in the **Default Value** column indicate that a **value must be entered**.
2.   Shaded cells in the **Default Value** column indicate that the **value must be left blank.**

Table 73 lists the modifiable IT Device Token Configurations for the Node to Node Utilization Asset.

Table 73. Modifiable IT Device Token Configurations for Node to Node Utilization Asset

IT Device Name	Modifiable Tokens	Default Value[1]	Description
Node to Node Alarm	CommonTokens::Node1		Enter the computer name or IP address of the first computer that is being monitored.
	CommonTokens::Node2		Enter the computer name or IP address of the second computer that is being monitored.
	CommonTokens::Family	All	The IP protocol family. This is the recommended value.
	CommonTokens::Protocol	All	The IP protocol. This is the recommended value.
	CommonTokens::Application	All	The IP application. This is the recommended value.
	CommonTokens::LowLevel	25%	The low level network utilization threshold, exceeding the default value causes an alarm.
	CommonTokens::MediumLevel	50%	The medium level network utilization threshold, exceeding the default value causes an alarm.
	CommonTokens::HighLevel	75%	The high level network utilization threshold, exceeding the default value causes an alarm.
	CommonTokens::SampleCount	15	The number of samples used to average the utilization calculation.

Table 73. Modifiable IT Device Token Configurations for Node to Node Utilization Asset (Continued)

IT Device Name	Modifiable Tokens	Default Value[1]	Description
Node to Node Alert	CommonTokens::Node1		Enter the computer name or IP address of the first computer that is being monitored.
	CommonTokens::Node2		Enter the computer name or IP address of the second computer that is being monitored.
	CommonTokens::Family	All	The IP protocol family. This is the recommended value.
	CommonTokens::Protocol	All	The IP protocol. This is the recommended value.
	CommonTokens::Application	All	The IP application. This is the recommended value.
	CommonTokens::LowLevel	25%	The low level network utilization threshold, exceeding the default value causes an alert.
	CommonTokens::MediumLevel	50%	The medium level network utilization threshold, exceeding the default value causes an alert.
	CommonTokens::HighLevel	75%	The high level network utilization threshold, exceeding the default value causes an alert.
	CommonTokens::SampleCount	15	The number of samples used to average the utilization calculation.

Table 73. Modifiable IT Device Token Configurations for Node to Node Utilization Asset (Continued)

IT Device Name	Modifiable Tokens	Default Value[1]	Description
Node to Node Utilization (Bytes per s) Status	Status::Family	All	The IP protocol family. This is the recommended value.
	Status::Protocol	All	The IP protocol. This is the recommended value.
	Status::Application	All	The IP application. This is the recommended value.
	Status::SampleCount	15	The number of samples used to average the utilization calculation.
	Status::Node1		Enter the computer name or IP address of the first computer that is being monitored.
	Status::Node2		Enter the computer name or IP address of the second computer that is being monitored.
Node to Node Utilization (Percent) Status	Status::Family	All	The IP protocol family. This is the recommended value.
	Status::Protocol	All	The IP protocol. This is the recommended value.
	Status::Application	All	The IP application. This is the recommended value.
	Status::SampleCount	15	The number of samples used to average the utilization calculation.
	Status::Node1		Enter the computer name or IP address of the first computer that is being monitored.
	Status::Node2		Enter the computer name or IP address of the second computer that is being monitored.

NOTE:
1.   Blank cells in the **Default Value** column indicate that a **value must be entered**.

Asset - Single Node Utilization

Description: The Single Node Utilization Asset monitors traffic on a single node.

Table 74 lists IT Devices for the Single Node Utilization Asset.

Table 74. Single Utilization Asset IT Device List

Device Name	IT Device	Description
Alarms		
Node Alarm	Node Utilization Alarm	Alarms when the utilization exceeds the nominal bandwidth at three thresholds.
Status		
Node Alert	Node Utilization Alert	Alerts when the utilization exceeds the nominal bandwidth at three thresholds.
Node Utilization (Bytes per s) Status	Node Utilization (Bytes per s)	Node to Node utilization in bytes per sec.
Node Utilization (Percent) Status	Node Utilization (Percent)	Node utilization in percent of nominal bandwidth.

Table 75 lists the IT General Properties for the Single Node Utilization Asset.

Table 75. IT General Properties for Single Node Utilization Asset

Name	Default Value[1,2]	Description
Host		Enter the name or IP address of the host computer that the network monitor is running.
IP Address		Enter the IP address of the network adapter on the host computer that is connected to the target network.
Port		**This must be left blank.** The Port used by the network monitor.

NOTES:
1. Blank cells in the **Default Value** column indicate that a **value must be entered**.
2. Shaded cells in the **Default Value** column indicate that the **value must be left blank.**

Table 76 lists the modifiable IT Device Token Configurations for the Single Node Utilization Asset.

Table 76. Modifiable IT Device Token Configurations for Single Node Utilization Asset

IT Device Name	Modifiable Tokens	Default Value[1]	Description
Node Alarm	CommonTokens::Node		Enter the computer name or IP address that is being monitored.
	CommonTokens::Family	All	The IP protocol family. This is the recommended value.
	CommonTokens::Protocol	All	The IP protocol. This is the recommended value.
	CommonTokens::Application	All	The IP application. This is the recommended value.
	CommonTokens::LowLevel	25%	The low level network utilization threshold, exceeding the default value causes an alarm.
	CommonTokens::MediumLevel	50%	The medium level network utilization threshold, exceeding the default value causes an alarm.
	CommonTokens::HighLevel	75%	The high level network utilization threshold, exceeding the default value causes an alarm.
	CommonTokens::SampleCount	15	The number of samples used to average the utilization calculation.

Table 76. Modifiable IT Device Token Configurations for Single Node Utilization Asset (Continued)

IT Device Name	Modifiable Tokens	Default Value[1]	Description
Node Alert	CommonTokens::Node		Enter the computer name or IP address that is being monitored.
	CommonTokens::Family	All	The IP protocol family. This is the recommended value.
	CommonTokens::Protocol	All	The IP protocol. This is the recommended value.
	CommonTokens::Application	All	The IP application. This is the recommended value.
	CommonTokens::LowLevel	25%	The low level network utilization threshold, exceeding the default value causes an alert.
	CommonTokens::MediumLevel	50%	The medium level network utilization threshold, exceeding the default value causes an alert.
	CommonTokens::HighLevel	75%	The high level network utilization threshold, exceeding the default value causes an alert.
	CommonTokens::SampleCount	15	The number of samples used to average the utilization calculation.

Table 76. Modifiable IT Device Token Configurations for Single Node Utilization Asset (Continued)

IT Device Name	Modifiable Tokens	Default Value[1]	Description
Node Utilization (Bytes per s) Status	Status::Family	All	The IP protocol family. This is the recommended value.
	Status::Protocol	All	The IP protocol. This is the recommended value.
	Status::Application	All	The IP application. This is the recommended value.
	Status::SampleCount	15	The number of samples used to average the utilization calculation.
	Status::Node		Enter the computer name or IP address that is being monitored.
Node Utilization (Percent) Status	Status::Family	All	The IP protocol family. This is the recommended value.
	Status::Protocol	All	The IP protocol. This is the recommended value.
	Status::Application	All	The IP application. This is the recommended value.
	Status::SampleCount	15	The number of samples used to average the utilization calculation.
	Status::Node		Enter the computer name or IP address that is being monitored.

NOTE:

1.   Blank cells in the **Default Value** column indicate that a **value must be entered**.

Asset - Cisco 12-Port Switch

Description: This Asset represents the Cisco 2950 (12-Port Switch). It generates alarms when a port problem occurs or when a port is disconnected. This switch indicates typical switch related data such as port speed, traffic counters, and in and out error counters.

Table 77 lists IT devices for the Cisco 2950 (12-Port Switch) Asset.

Table 77. Cisco 12-Port Switch Asset IT Device List

Device Name	IT Device	Description
Alarms		
Cisco 12-Port Switch Alarm	Cisco 12-Port Switch Alarm	Alarms when any port in the switch is faulty or disconnected.
Status		
Cisco 12-Port Switch Alert	Cisco 12-Port Switch Alert	Alerts when any port in the switch is faulty or disconnected.
Cisco 12-Port Switch Status	Cisco 12-Port Switch Status	Returns the status of key attributes.

Table 78 lists the IT general properties for the Cisco 2950 (12-Port Switch) Asset.

Table 78. IT General Properties for Cisco 12-Port Switch Asset

Name	Default Value[1]	Description
Host	localhost	Change this to the name or IP address of the computer making the status requests to the switch. This is typically the same computer running the monitoring software. **This is not the IP address of the switch.**
IP Address		Enter the IP address of the switch being monitored.
Community		Change the SNMP community name for the device being monitored. This name is equivalent to a password allowing communication. Check with network personnel responsible for configuring this device to determine the name.
AlarmOnOpenPort	false	If true, an alarm will be generated if a port becomes disconnected. If false, disconnected ports are not treated as error conditions. False is the default.
ErrorRateLimit	5	The number of errors per second on a specific port above which the port is identified as being faulty.
ConsecutiveErrorCount	5	The number of consecutive error update periods that a fault port remains at fault before the problem is signaled back to the client as an event.
StartPortIndex	2	This is used to align the internal representation of a port with its external port number that is physically present on the outside of the switch.

NOTE:
1.   Blank cells in the **Default Value** column indicate that a **value must be entered**.

Light Asset - Cisco 12-Port Switch

A Light Cisco 2950 (12-Port Switch) Asset is available providing basic alarm detection for the Cisco 2950 (12-Port Switch) Asset. Status information is not returned. The data is subscribed at a slower rate (60 seconds) when using Light Assets. Follow the configuration procedures for the Asset - Cisco 12-Port Switch on page 150 to set up the Light Cisco 2950 (12-Port Switch) Asset.

Asset - Cisco 24-Port Switch

Description: This Asset represents the Cisco 2950 (24-Port Switch). It generates alarms when a port problem occurs or optionally when a port is disconnected. Indicates typical switch related data such as port speed, traffic counters, and in and out error counters.

Table 79 lists IT Devices for the Cisco 2950 (24-Port Switch) Asset.

Table 79. Cisco 24-Port Switch Asset IT Device List

Device Name	IT Device	Description
Alarms		
Cisco 24-Port Switch Alarm	Cisco 24-Port Switch Alarm	Alarms when any port in the switch is faulty or disconnected.
Status		
Cisco 24-Port Switch Alert	Cisco 24-Port Switch Alert	Alerts when any port in the switch is faulty or disconnected.
Cisco 24-Port Switch Status	Cisco 24-Port Switch Status	Returns the status of key attributes.

Table 80 lists the IT General Properties for the Cisco 2950 (24-Port Switch) Asset.

Table 80. IT General Properties for Cisco 24-Port Switch Asset

Name	Default Value[1]	Description
Host	localhost	Change this to the name or IP address of the computer making the status requests to the switch. This is typically the same computer running the monitoring software. **This is not the IP address of the switch.**
IP Address		Enter the IP address of the switch being monitored.
Community		Change the SNMP community name for the device being monitored. This name is equivalent to a password allowing communication. Check with network personnel responsible for configuring this device to determine the name.
AlarmOnOpenPort	false	If true, an alarm will be generated if a port becomes disconnected. If false, disconnected ports are not treated as error conditions. False is the default.
ErrorRateLimit	5	The number of errors per second on a specific port above which the port is identified as being faulty.
ConsecutiveErrorCount	5	The number of consecutive error update periods that a fault port remains at fault before the problem is signaled back to the client as an event.
StartPortIndex	2	This is used to align the internal representation of a port with its external port number that is physically present on the outside of the switch.

NOTE:
1. Blank cells in the **Default Value** column indicate that a **value must be entered**.

Light Asset - Cisco 24-Port Switch

A Light Cisco 2950 (24-Port Switch) Asset is available providing basic alarm detection for the Cisco 2950 (24-Port Switch) Asset. Status information is not returned. The data is subscribed at a slower rate (60 seconds) when using Light Assets. Follow the configuration procedures for the Asset - Cisco 24-Port Switch on page 152 to set up the Light Cisco 2950 (24-Port Switch) Asset.

Asset - Cisco 48-Port Switch

Description: This Asset represents the Cisco 2950 (48-Port Switch). It generates alarms when a port problem occurs or optionally when a port is disconnected. Indicates typical switch related data such as port speed, traffic counters, and in and out error counters.

Table 81 lists IT Devices for the Cisco 2950 (48-Port Switch) Asset.

Table 81. Cisco 48-Port Switch Asset IT Device List

Device Name	IT Device	Description
Alarms		
Cisco 48-Port Switch Alarm	Cisco 48-Port Switch Alarm	Alarms when any port in the switch is faulty or disconnected.
Status		
Cisco 48-Port Switch Alert	Cisco 48-Port Switch Alert	Alerts when any port in the switch is faulty or disconnected.
Cisco 48-Port Switch Status	Cisco 48-Port Switch Status	Returns the status of key attributes.

Table 82 lists the IT General Properties for the Cisco 2950 (48-Port Switch) Asset.

Table 82. IT General Properties for Cisco 48-Port Switch Asset

Name	Default Value[1]	Description
Host	localhost	Change this to the name or IP address of the computer making the status requests to the switch. This is typically the same computer running the monitoring software. **This is not the IP address of the switch.**
IP Address		Enter the IP address of the switch being monitored.
Community		Change the SNMP community name for the device being monitored. This name is equivalent to a password allowing communication. Check with network personnel responsible for configuring this device to determine the name.
AlarmOnOpenPort	false	If true, an alarm will be generated if a port becomes disconnected. If false, disconnected ports are not treated as error conditions. False is the default.
ErrorRateLimit	5	The number of errors per second on a specific port above which the port is identified as being faulty.
ConsecutiveErrorCount	5	The number of consecutive error update periods that a fault port remains at fault before the problem is signaled back to the client as an event.
StartPortIndex	2	This is used to align the internal representation of a port with its external port number that is physically present on the outside of the switch.

NOTE:
1.   Blank cells in the **Default Value** column indicate that a **value must be entered**.

Light Asset - Cisco 48-Port Switch

A Light Cisco 2950 (48-Port Switch) Asset is available providing basic alarm detection for the Cisco 2950 (48-Port Switch) Asset. Status information is not returned. The data is subscribed at a slower rate (60 seconds) when using Light Assets. Follow the configuration procedures for the Asset - Cisco 48-Port Switch on page 154 to set up the Light Cisco 2950 (48-Port Switch) Asset.

Asset - Hirschmann Mach 3000 Switch

Description: This Asset represents the Hirschmann Mach 3000 switch device. It generates alarms when a port or power problem occur. Indicates typical switch related data such as port speed and traffic counters.

Table 83 lists IT Devices for the Hirschmann Mach 3000 Switch Asset.

Table 83. Hirschmann Mach 3000 Switch Asset IT Device List

Device Name	IT Device	Description
Alarms		
Hirschmann Module 1 Alarm	Hirschmann n-Port Alarm	Generates a single summary alarm if any problems are detected on this module or port range.
Hirschmann PS 1 Alarm	Hirschmann Power Supply Alarm	Generates an alarm if any problems are found on the specified power supply.
Status		
Hirschmann Module 1 Alert	Hirschmann 8-Port Alert	Generates an alert if a problem is detected on this module or an individual port.
Hirschmann PS 1 Alert	Hirschmann Power Supply Alert	Generates an alert if any problems are found on the specified power supply.
Hirschmann Base Status	Hirschmann Mach 3000 Base Status	Returns the basic status attributes.

Table 83. Hirschmann Mach 3000 Switch Asset IT Device List (Continued)

Device Name	IT Device	Description
Hirschmann Module 1 Status	Hirschmann 8-Port Status	Returns the status of module attributes.
Hirschmann PS 1 Status	Hirschmann Power Supply Status	Returns the status of the power supply attributes.

Table 84 lists the IT General Properties for the Hirschmann Mach 3000 Switch Asset.

Table 84. IT General Properties for Hirschmann Mach 3000 Switch Asset

Name	Default Value[1]	Description
Host	localhost	Change this to the name or IP address of the computer making the status requests to the switch. This is typically the same computer running the monitoring software. **This is not the IP address of the switch.**
IP Address		Enter the IP address of the switch being monitored.
Community		Change the SNMP community name for the device being monitored. This name is equivalent to a password allowing communication. Check with network personnel responsible for configuring this device to determine the name.
AlarmOnOpenPort	true	Will enable or disable alarming on a disconnected port.

NOTE:
1.   Blank cells in the **Default Value** column indicate that a **value must be entered**.

Table 85 lists the Modifiable IT Device Token Configurations for the Hirschmann Mach 3000 Switch Asset.

Table 85. Modifiable IT Device Token Configurations for a
Hirschmann Mach 3000 Switch Asset

IT Device Name	Modifiable Tokens	Default Value[1]	Description
Hirschmann Module 1 Alarm	PortHealth::StartPortIndex		Enter the first port index for the module.
	PortHealth::NumberPorts		Enter the number of ports in the module.

Table 85. Modifiable IT Device Token Configurations for a
Hirschmann Mach 3000 Switch Asset (Continued)

IT Device Name	Modifiable Tokens	Default Value[1]	Description
Hirschmann Module 1 Alert	CommonToken::PortIndex-1 - CommonToken::PortIndex-8		Enter the index number of the port in the overall Hirschmann switch.
Hirschmann Module 1 Status	CommonToken::PortIndex-1 - CommonToken::PortIndex-8		Enter the index number of the port in the overall Hirschmann switch.
Hirschmann PS 1 Alarm	Alarm::Enable	True	Enables alarm detection on the specified power supply.
	Alarm::PowerSupplyIndex	1	Indicates the power supply index.
Hirschmann PS 1 Alert	CommonTokens::Enable	True	Enables alarm detection on the specified power supply.
	CommonTokens::PowerSupplyIndex	1	Indicates the power supply index.
Hirschmann PS 1 Status	PowerSupplyStatus:: PowerSupplyIndex	1	Indicates the power supply index.

NOTE:
1.   Blank cells in the **Default Value** column indicate that a **value must be entered**.

Light Asset - Hirschmann Mach 3000 Switch

Description: This Light Asset represents a Hirschmann Mach 3000 Switch device. IT generates alarms when a port or power problem occurs. It indicates typical switch related data such as port speed and traffic counters.

Table 86 lists IT Devices for the Light Hirschmann Mach 3000 Switch Asset.

Table 86. Light Hirschmann Mach 3000 Switch Asset IT Device List

Device Name	IT Device	Description
Alarms		
Hirschmann Module 1 Alarm	Light Hirschmann n-Port Alarm	Generates a single summary alarm if any problems are detected on this module or port range.
Hirschmann PS 1 Alarm	Light Hirschmann Power Supply Alarm	Generates an alarm if any problems are found on the specified power supply.
Status		
Hirschmann Module 1 Alert	Light Hirschmann 8-Port Alert	Generates an alert if a problem is detected on this module or an individual port.
Hirschmann PS 1 Alert	Light Hirschmann Power Supply Alert	Generates an alert if any problems are found on the specified power supply.
Hirschmann Base Status	Hirschmann Mach 3000 Base Status	Returns the basic status attributes.

Table 87 lists the IT General Properties for the Light Hirschmann Mach 3000 Switch Asset.

Table 87. IT General Properties for Light Hirschmann Mach 3000 Switch Asset

Name	Default Value[1]	Description
Host	localhost	Change this to the name or IP address of the computer making the status requests to the switch. This is typically the same computer running the monitoring software. **This is not the IP address of the switch.**
IP Address		Enter the IP address of the switch being monitored.
Community		Change the SNMP community name for the device being monitored. This name is equivalent to a password allowing communication. Check with network personnel responsible for configuring this device to determine the name.
AlarmOnOpenPort	true	Will enable or disable alarming on a disconnected port.

NOTE:
1.   Blank cells in the **Default Value** column indicate that a **value must be entered**.

Table 88 lists the Modifiable IT Device Token Configurations for the Light Hirschmann Mach 3000 Switch Asset.

Table 88. Modifiable IT Device Token Configurations for a Light Hirschmann Mach 3000 Switch Asset

IT Device Name	Modifiable Tokens	Default Value[1]	Description
Hirschmann Module 1 Alarm	PortHealth::StartPortIndex		Enter the first port index for the module.
	PortHealth::NumberPorts		Enter the number of ports in the module.
Hirschmann Module 1 Alert	CommonToken::PortIndex-1 - CommonToken::PortIndex-8		Enter the index number of the port in the overall Hirschmann switch.
Hirschmann PS 1 Alarm	Alarm::Enable	True	Enables alarm detection on the specified power supply.
	Alarm::PowerSupplyIndex	1	Indicates the power supply index.
Hirschmann PS 1 Alert	CommonTokens::Enable	True	Enables alarm detection on the specified power supply.
	CommonTokens::PowerSupplyIndex	1	Indicates the power supply index.

NOTE:

1. Blank cells in the **Default Value** column indicate that a **value must be entered**.

Asset - Hirschmann RS2 Switch

Description: This Asset represents the Hirschmann RS2 switch device. It generates alarms when a port or power problem occur. Indicates typical switch related data such as port speed and traffic counters.

Table 89 lists IT Devices for the Hirschmann RS2 Switch Asset.

Table 89. Hirschmann RS2 Switch Asset IT Device List

Device Name	IT Device	Description
Alarms		
Hirschmann Alarm	Hirschmann RS2 Alarm	Generates alarms on port and power supply problems.
Status		
Hirschmann Alert	Hirschmann RS2 Alert	Generates alerts on port and power supply problems.
Hirschmann Status	Hirschmann RS2 Status	Returns the status of key attributes.

Table 90 lists the IT General Properties for the Hirschmann RS2 Switch Asset.

Table 90. IT General Properties for Hirschmann RS2 Switch Asset

Name	Default Value[1]	Description
Host	localhost	Change this to the name or IP address of the computer making the status requests to the switch. This is typically the same computer running the monitoring software. **This is not the IP address of the switch.**
IP Address		Enter the IP address of the switch being monitored.
Community		Change the SNMP community name for the device being monitored. This name is equivalent to a password allowing communication. Check with network personnel responsible for configuring this device to determine the name.

NOTE:
1.   Blank cells in the **Default Value** column indicate that a **value must be entered**.

Table 91 lists the Modifiable IT Device Token Configurations for the Hirschmann RS2 Switch Asset.

Table 91. Modifiable IT Device Token Configurations for a
Hirschmann RS2 Switch Asset

IT Device Name	Modifiable Tokens	Default Value[1]	Description
Hirschmann Alarm	PowerSupply-1::Enable PowerSupply-2::Enable	True	Enables alarm detection on the specified power supply.
	Port-1-AlarmOnOpen Port-7-AlarmOnOpen	True	Enables alarming on the port when it is not connected. Otherwise, alarms are only generated when problems occur on connected ports.
	Port-1::Enable Port-7::Enable	True	Enables alarm detection on the specified port.
Hirschmann Alert	CommonTokens::Enable-PowerSupply-1 CommonTokens::Enable-PowerSupply-2	True	Enables alert detection on the specified power supply.
	CommonTokens::Enable-Port-1-AlarmOnOpen CommonTokens::Enable-Port-7-AlarmOnOpen	True	Enables alerting on the port when it is not connected. Otherwise, alerts are only generated when problems occur on connected ports.
	CommonTokens::Enable Port-1 CommonTokens::Enable Port-7	True	Enables alert detection on the specified port.

NOTE:
1.   Blank cells in the **Default Value** column indicate that a **value must be entered**.

Light Asset - Hirschmann RS2 Switch

A Light Hirschmann RS2 Switch Asset is available providing basic alarm detection for the Hirschmann RS2 Switch Asset. Status information is not returned. The data is subscribed at a slower rate (60 seconds) when using Light Assets. Follow the configuration procedures for the Asset - Hirschmann RS2 Switch on page 163 to set up the Light Hirschmann RS2 Switch Asset.

IT Device Library

IT Devices are used to compose the IT Assets. They can also be added into existing IT Asset objects when required. There are three distinct IT Devices:

- **Alarm Devices**: Devices that generate alarms when failure conditions exist. Properties defined in Alarm Devices return alarm definition strings for use by Asset Optimization to generate alarms. Alarm Devices are always driven by scripts.

> The returned properties are used for the purpose of being processed into alarms by Asset Optimization.

- **Alert Devices**: Devices that generate alerts when failure conditions exist. Properties defined in Alert Devices return Alert Strings or Alert Numeric Values for use by the Auto-Populate IT Faceplate. The faceplate displays the Alert Strings and uses the Alert Numeric Value to determine the color of the string. Alert Devices are always driven by scripts.

- **Status Devices**: Devices that return only status information, no alarms. Properties defined in Status Devices typically return Boolean, numeric, or string values. Status devices may be driven by either WMI data directly, or through scripts.

The Alarm Devices described in this section are:

- Alarm Device - Generic Interface Alarm on page 169.
- Alarm Device - Generic Interface Alarm on page 169.
- Alarm Device - Network Utilization Alarm on page 171.
- Alarm Device - Node to Node Utilization Alarm on page 173.
- Alarm Device - Node Utilization Alarm on page 175.
- Alarm Device - Performance Counter Alarm (Alarm) on page 177.

The Status Devices described in this section are:

Alarm Device - Generic Interface Alarm

Description: The alarm status of the device.

Table 92 lists the Generic Interface Alarm Conditions/Subconditions.

Table 92. Generic Interface Alarm Conditions/Subconditions

Conditions	Subconditions Generated	Description
Status	Normal	The network adapter is functioning normally.
	Bad	The network interface hardware may have been removed or the remote computer may not be available.

Status Device - Generic Interface Alert

Description: Current value or status of the interface adapter.

Table 93 lists the Generic Interface Alert properties.

Table 93. Generic Interface Alert Properties

Property	Data Type	Description
Status	String	The status of the network interface adapter.
Value-Status	Numeric	A numeric representation of the current state of the network interface adapter.

Status Device - Generic Interface Status

Description: Current value or status of the interface adapter.

Table 94 lists the Generic Interface Status properties.

Table 94. Generic Interface Status Properties

Property	Data Type	Description
Name	String	The string describes the name of the network interface adapter.
AdapterType		The string describes the type of network medium.
Description		The string provides the description of the device.
MACAddress		The string provides the unique 48-bit identifier for the network interface.
DeviceID		This string uniquely identifies the network adapter.
Index	Numeric	The network adapter index on the computer.
Availability		The status of the device.
ConfigManagerErrorCode		The Win32 Config Manager error code.

Alarm Device - Network Utilization Alarm

Description: Generates alarms when there is excessive network utilization on the network segment.

Table 95 lists the Network Utilization Alarm Conditions/Subconditions.

Table 95. Network Utilization Alarm Conditions/Subconditions

Conditions	Subconditions Generated	Description
Utilization	Normal	Network Utilization is running within normal range limits.
	Bad	Bad Input.
	LowUtilization	The network utilization is above the low threshold.
	MediumUtilization	The network utilization is above the medium threshold.
	HighUtilization	The network utilization is above the high threshold.

Status Device - Network Utilization Alert

Description: Current value or status of network utilization

Table 96 lists the Network Utilization Alert properties.

Table 96. Network Utilization Alert Properties

Property	Data Type	Description
ValueUtilization	Numeric	A numeric representation of the current state of the network utilization.
Utilization	String	A string describing the current state of the network utilization.

Status Device - Network Utilization (Bytes per s) Status

Description: Current status of network utilization by bytes per second.

Table 97 lists the Network Utilization (Bytes per s) Status properties.

Table 97. Network Utilization (Bytes per s) Status Properties

Property	Data Type	Description
Network Utilization (Bytes per s) Status	Numeric	A numeric representation of the current status of the network utilization.

Status Device - Network Utilization (Percent) Status

Description: Returns key status values on the utilization of the percentage of nominal bandwidth used.

Table 98 lists the Network Utilization (Percent) Status properties.

Table 98. Network Utilization (Percent) Status Properties

Property	Data Type	Description
Network Utilization (Percent) Status	Numeric	A numeric representation of the current state of the utilization of the network.

Alarm Device - Node to Node Utilization Alarm

Description: Generates alarms when there is excessive network utilization between nodes.

Table 99 lists the Node to Node Utilization Alarm Conditions/Subconditions.

Table 99. Node to Node Utilization Alarm Conditions/Subconditions

Conditions	Subconditions Generated	Description
Between Nodes	Normal	Network Utilization is running within normal range limits.
	Bad	Bad Input.
	LowUtilization	The network utilization is above the low threshold.
	MediumUtilization	The network utilization is above the medium threshold.
	HighUtilization	The network utilization is above the high threshold.

Status Device - Node to Node Utilization Alert

Description: Current value or status of network utilization between nodes.

Table 100 lists the Node to Node Utilization Alert properties.

Table 100. Node to Node Utilization Alert Properties

Property	Data Type	Description
Value-Between Nodes	Numeric	A numeric representation of the current state of the network utilization between nodes.
Between Nodes	String	A string describing the current state of the network utilization between nodes.

Status Device - Node To Node Utilization (Bytes per s) Status

Description: Returns key status values on the utilization of the network between nodes in bytes per second.

Table 101 lists the Node to Node Utilization (Byte per s) Status properties.

Table 101. Node to Node Utilization (Byte per s) Status Properties

Property	Data Type	Description
Status	Numeric	A numeric representation of the current state of the utilization of the network between nodes.

Status Device - Node To Node Utilization (Percent) Status

Description: Returns key status information on the utilization of the network between nodes.

Table 102 lists the Node to Node Utilization (Percent) Status properties.

Table 102. Node to Node Utilization (Percent) Status Properties

Property	Data Type	Description
Status	Numeric	A numeric representation of the current state of the utilization of the network between nodes.

Alarm Device - Node Utilization Alarm

Description: Generates alarms when there is excessive network utilization on a single node.

Table 103 lists the Node Utilization Alarm Conditions/Subconditions.

Table 103. Node Utilization Alarm Conditions/Subconditions

Conditions	Subconditions Generated	Description
Single Node	Normal	Network utilization is running within normal range limits.
	Bad	Bad Input.
	LowUtilization	The network utilization is above the low threshold.
	MediumUtilization	The network utilization is above the medium threshold.
	HighUtilization	The network utilization is above the high threshold.

Status Device - Node Utilization Alert

Description: Current value or status of the network utilization on a single node.

Table 104 lists the Node Utilization Alert properties.

Table 104. Node Utilization Alert Properties

Property	Data Type	Description
ValueSingleNode	Numeric	A numeric representation of the current state of the network utilization on a single node.
SingleNode	String	A string describing the current state of the network utilization on a single node.

Status Device - Node Utilization (Bytes per s) Status

Description: Current status of a single node utilization of bandwidth in bytes per second.

Table 105 lists the Node Utilization (Byte per s) Status properties.

Table 105. Node Utilization (Byte per s) Status Properties

Property	Data Type	Description
Status	Numeric	A numeric representation of the current state of the utilization of the network of a single node.

Status Device - Node Utilization (Percent) Status

Description: Current status of a single node utilization in percent of nominal bandwidth.

Table 106 lists the Node Utilization (Percent) Status properties.

Table 106. Node Utilization (Percent) Status Properties

Property	Data Type	Description
Status	Numeric	A numeric representation of the current state of the utilization of the network of a single node.

Alarm Device - Performance Counter Alarm (Alarm)

Description: Generates alarms when the Windows Performance Counter has exceeded pre-configured alarm limits.

Table 107 lists the Performance Counter Alarm (Alarm) Conditions/Subconditions.

Table 107. Performance Counter Alarm (Alarm) Conditions/Subconditions

Conditions	Subconditions Generated	Description
PerformanceAlarm	Normal	The performance counter is running within normal range limits.
	Bad	Bad Input.
	LowUtilization	The performance counter is above the low threshold.
	MediumUtilization	The performance counter is above the medium threshold.
	HighUtilization	The performance counter is above the high threshold.

Status Device - Performance Counter Alert (Performance Alert)

Description: Generates alerts based on Windows Performance Counter limits.

Table 108 lists the Performance Counter Alert (Performance Alert) properties.

Table 108. Performance Counter Alert (Performance Alert) Properties

Property	Data Type	Description
Value-Alert	Numeric	A numeric representation of the Windows Performance Counter value.
Alert	String	A string describing the alert condition when the value exceeds the limit.

Alarm Device - Performance Counter Alarm (Reversed) (Reversed Alarm)

Description: Generates alarms when the Windows Performance Counter is lower then the pre-configured threshold level.

Table 109 lists the Performance Counter Alarm (Reversed) (Reversed Alarm) Conditions/Subconditions.

Table 109. Performance Counter Alarm (Reversed) (Reversed Alarm) Conditions/Subconditions

Conditions	Subconditions Generated	Description
PerformanceAlarm	Normal	The performance counter is running within normal range limits.
	Bad	Bad Input.
	Warning	The performance counter is above the warning limit.
	Serious	The performance counter is in a serious condition.
	Critical	The performance counter is in a critical condition.

Status Device - Performance Counter (Reversed) Alert (Reversed Performance Alert)

Description: Generates alerts based on Windows Performance Counter limits.

Table 110 lists the Performance Counter (Reversed) Alert (Reversed Performance Alert) properties.

Table 110. Performance Counter (Reversed) Alert (Reversed Performance Alert) Properties

Property	Data Type	Description
Value-Alert	Numeric	A numeric representation of the Windows Performance Counter value.
Alert	String	A string describing when the value falls below the limit.

Status Device - Performance Counter Status (Value)

Description: Current Value of the Windows Performance Monitor Counter.

Table 111 lists the Performance Counter Status (Value) properties.

Table 111. Performance Counter Status (Value) Properties

Property	Data Type	Description
Counter Status	Numeric	A numeric representation of the Windows Performance Counter value.

Alarm Device - Computer CPU Alarm

Description: Generates an alarm when the CPU utilization becomes too high. The usage is averaged over the update period, which is 10 seconds, as a minimum. This means that CPU spikes are automatically leveled.

Table 112 lists the Computer CPU Alarm Conditions/Subconditions.

Table 112. Computer CPU Alarm Conditions/Subconditions

Conditions	Subconditions Generated	Description
CPUOverload	Normal	CPU(s) utilization is within acceptable range.
	Bad	No CPU(s) loading data is available.
	Warning	CPU utilization has reached or exceeded the Low Limit.
	Serious	CPU utilization has reached or exceeded the Medium Limit.
	Critical	CPU utilization has reached or exceeded the High Limit and is in critical overload condition.

Status Device - Computer CPU Alert

Description: Generates alerts based on CPU utilization.

Table 113 lists the Computer CPU Alert properties.

Table 113. Computer CPU Alert Properties

Property	Data Type	Description
CPUOverload	String	A string describing the current state of the computer CPU.
Value-CPUOverload	Numeric	A numeric representation of the current state of the computer CPU.

Status Device - Computer CPU Status

Description: Provides the current value of the CPU load.

Table 114 lists the Computer CPU Status properties.

Table 114. Computer CPU Status Properties

Property	Data Type	Description
CPULoad	Numeric	The CPU load from the given computer. This load is the running average CPU load over 4 update periods. This update period must be a least 15 seconds.

Light Alarm Device - Light Computer CPU Alarm

Description: Generates one or more alarms based on the CPU utilization.

Table 115 lists the Light Computer CPU Alarm Conditions/Subconditions.

Table 115. Light Computer CPU Alarm Conditions/Subconditions

Conditions	Subconditions Generated	Description
CPUOverload	Normal	CPU(s) utilization is within acceptable range.
	Bad	No CPU(s) loading data is available.
	Warning	CPU utilization has reached or exceeded the Low Limit.
	Serious	CPU utilization has reached or exceeded the Medium Limit.
	Critical	CPU utilization has reached or exceeded the High Limit and is in critical overload condition.

Light Status Device - Light Computer CPU Alert

Description: Generates alerts based on CPU utilization.

Table 116 lists the Light Computer CPU Alert properties.

Table 116. Light Computer CPU Alert Properties

Property	Data Type	Description
CPUOverload	String	A string describing the current state of the computer CPU.
Value-CPUOverload	Numeric	A numeric representation of the current state of the computer CPU.

Alarm Device - Computer General Alarm (Auto)

Description: Generates one or more alarms based on checking the individual resource usage of a given software process. This device automatically detects trends in resource usage and generates alarms when it anticipates a problem.

Table 117 lists the Computer General Alarm (Auto) Conditions/Subconditions.

Table 117. Computer General Alarm (Auto) Conditions/Subconditions

Conditions	Subconditions Generated	Description
Handles	Normal	Handle usage is within the acceptable range.
	Bad	No Handle usage data is available.
	Warning	The number of Handles used by the system has reached or exceeded the Handle warning limit.
	Error	The number of Handles used by the system has reached or exceeded the Handle error limit.
VM-Absolute	Normal	Virtual memory (VM) usage is within the acceptable range.
	Bad	No VM usage data is available.
	Warning	VM usage has reached or exceeded the warning limit.
	Error	VM usage has reached or exceeded the error limit.
Threads	Normal	Thread usage is within the acceptable range.
	Bad	No Thread usage data is available.
	Warning	The number of Threads used by the system has reached or exceeded the Thread warning limit.
	Error	The number of Threads used by the system has reached or exceeded the Thread error limit.

Table 117. Computer General Alarm (Auto) Conditions/Subconditions (Continued)

Conditions	Subconditions Generated	Description
VM-Trend	Normal	Virtual memory (VM) usage is within the acceptable range.
	Bad	No VM usage data is available.
	Warning	The system has observed a sustained upward trend in the VM used over the span of 2 ½ hours.
	Error	The system has observed a sustained upward trend in the VM used over the span of 5 hours.

Light Alarm Device - Light Computer General Alarm (Auto)

Table 118 lists the Light Computer General Alarm (Auto) Conditions/Subconditions.

Table 118. Light Computer General Alarm (Auto) Conditions/Subconditions

Conditions	Subconditions Generated	Description
Handles	Normal	Handle usage is within the acceptable range.
	Bad	No Handle usage data is available.
	Warning	The number of Handles used by the system has reached or exceeded the Handle warning limit.
	Error	The number of Handles used by the system has reached or exceeded the Handle error limit.
VM-Absolute	Normal	Virtual memory (VM) usage is within the acceptable range.
	Bad	No VM usage data is available.
	Warning	VM usage has reached or exceeded the warning limit.
	Error	VM usage has reached or exceeded the error limit.

Table 118. Light Computer General Alarm (Auto) Conditions/Subconditions (Continued)

Conditions	Subconditions Generated	Description
Threads	Normal	Thread usage is within the acceptable range.
	Bad	No Thread usage data is available.
	Warning	The number of Threads used by the system has reached or exceeded the Thread warning limit.
	Error	The number of Threads used by the system has reached or exceeded the Thread error limit.
VM-Trend	Normal	Virtual memory (VM) usage is within the acceptable range.
	Bad	No VM usage data is available.
	Warning	The system has observed a sustained upward trend in the VM used over the span of 2 ½ hours.
	Error	The system has observed a sustained upward trend in the VM used over the span of 5 hours.

Light Status Device - Light Computer General Alert

Description: Generates one or more alerts based on checking against absolute limits.

Table 119 lists the Light Computer General Alert properties.

Table 119. Light Computer General Alert Properties

Property	Data Type	Description
Handles	String	A string describing the current state of the Handles.
Threads		A string describing the current state of the Threads.
VM-Absolute		A string describing the current state of the VM-Absolute.
VM-Trend		A string describing the current state of the VM-Trend.

Table 119. Light Computer General Alert Properties (Continued)

Property	Data Type	Description
Value-Handles	Numeric	A numeric representation of the current state of the Handles.
Value-Threads		A numeric representation of the current state of the Threads.
Value-VM-Absolute		A numeric representation of the current state of the VM-Absolute.
Value-VM-Trend		A numeric representation of the current state of the VM-Trend.

Alarm Device - Computer General Alarm

Description: Generates one or more alarms based on checking the individual resource usage of a given software process.

Table 120 lists the Computer General Alarm Conditions/Subconditions.

Table 120. Computer General Alarm Conditions/Subconditions

Conditions	Subconditions Generated	Description
Handles	Normal	Handle usage is within the acceptable range.
	Bad	No Handle usage data is available.
	Warning	The number of Handles used by the system has reached or exceeded the Handle warning limit.
	Error	The number of Handles used by the system has reached or exceeded the Handle error limit.
VM-Absolute	Normal	Virtual memory (VM) usage is within the acceptable range.
	Bad	No VM usage data is available.
	Warning	VM usage has reached or exceeded the warning limit.
	Error	VM usage has reached or exceeded the error limit.
Threads	Normal	Thread usage is within the acceptable range.
	Bad	No Thread usage data is available.
	Warning	The number of Threads used by the system has reached or exceeded the Thread warning limit.
	Error	The number of Threads used by the system has reached or exceeded the Thread error limit.

Status Device - Computer General Alert

Description: Generates one or more alerts based on checking against absolute limits.

Table 121 lists the Computer General Alert properties.

Table 121. Computer General Alert Properties

Property	Data Type	Description
Handles	String	A string describing the current state of the Handles.
Threads		A string describing the current state of the Threads.
VM-Absolute		A string describing the current state of the VM-Absolute.
VM-Trend		A string describing the current state of the VM-Trend.
Value-Handles	Numeric	A numeric representation of the current state of the Handles.
Value-Threads		A numeric representation of the current state of the Threads.
Value-VM-Absolute		A numeric representation of the current state of the VM-Absolute.
Value-VM-Trend		A numeric representation of the current state of the VM-Trend.

Status Device - Computer General Status

Description: Returns several key status values for a given computer.

Table 122 lists the Computer General Status properties.

Table 122. Computer General Status Properties

Property	Data Type	Description
HandleCount	Numeric	The total number of Handles currently in use on this computer.
VM		The total amount of Virtual Memory currently in use on this computer (in bytes).
VMMAX		The total amount of Virtual Memory available on this computer (in bytes).
ThreadCount		The total number of Threads currently in use on this computer.

Alarm Device - Computer Process Alarm

Description: Generates one or more alarms based on checking the individual resource usage of a given software process. This device automatically detects trends in resource usage and generates alarms when it anticipates a problem.

Table 123 lists the Computer Process Alarm Conditions/Subconditions.

Table 123. Computer Process Alarm Conditions/Subconditions

Conditions	Subconditions Generated	Description
Handles	Normal	Handle usage is within the acceptable range.
	Bad	No Handle usage data is available.
	Warning	The system has observed a sustained upward trend in the number of Handles used over the span of 2 ½ hours.
	Error	The system has observed a sustained upward trend in the number of Handles used over the span of 5 hours.
VM	Normal	Virtual Memory (VM) usage is within the acceptable range.
	Bad	No VM usage data is available.
	Warning	The system has observed a sustained upward trend in the VM used over the span of 2 ½ hours.
	Error	The system has observed a sustained upward trend in the VM used over the span of 5 hours.
Threads	Normal	Thread usage is within the acceptable range.
	Bad	No Thread usage data is available.
	Warning	The system has observed a sustained upward trend in the number of Threads used over the span of 2 ½ hours.
	Error	The system has observed a sustained upward trend in the number of Threads used over the span of 5 hours.

Table 123. Computer Process Alarm Conditions/Subconditions (Continued)

Conditions	Subconditions Generated	Description
CPULoad	Normal	CPU(s) utilization is within the acceptable range.
	Bad	No CPU(s) loading data is available.
	Low	CPU utilization has reached or exceeded the Low limit.
	Medium	CPU utilization has reached or exceeded the Medium limit.
	High	CPU utilization has reached or exceeded the High limit.
ProcessExists	Normal	The given process is running.
	Bad	No data is available.
	Error	The process is not running on the specified computer.

Status Device - Computer Process Alert

Description: Returns a set of strings (Normal, Bad, Warning, or Error) indicating the health of several software process attributes.

Table 124 lists the Computer Process Alert properties.

Table 124. Computer Process Alert Properties

Property	Data Type	Description
Handles	String	The string indicating the state of the Handles resource on the given software process.
Memory		The string indicating the state of the Memory resource on the given software process.
Threads		The string indicating the state of the Threads resource on the given software process.
CPULoad		The string indicating the state of the CPU usage by the given software process.
Value-Handles	Numeric	The numeric representation of the current state of the Handles resource on the given software process.
Value-Memory		The numeric representation of the current state of the Memory resource on the given software process.
Value-Threads		The numeric representation of the current state of the Threads resource on the given software process.
Value-CPULoad		The numeric representation of the current state of the CPU usage on the given software process.

Status Device - Computer Process Status

Description: Returns several key status values for a given software process.

Table 125 lists the Computer Process Status properties.

Table 125. Computer Process Status Properties

Property	Data Type	Description
HandleCount	Numeric	The total number of Handles currently in use by this software process.
VM		The total amount of Virtual Memory currently in use by this software process.
ProcessId		The process ID of the given software process.
ThreadCount		The total number of Threads currently in use by this software process.
CPULoad		The percentage load this software process is putting on the CPU.
ProcessName	String	The name of the given process.

Alarm Device - Computer Process Alarm (Compact)

Description: Generates a single alarm based on the combination of several checks done on a given software process. The device automatically detects trends in resource usage and generates alarms when it anticipates a problem.

Table 126 lists the Computer Process Alarm (Compact) Conditions/Subconditions.

Table 126. Computer Process Alarm (Compact) Conditions/Subconditions

Conditions	Subconditions Generated	Description
ProcessHealth	Normal	Process is functioning normally.
	Bad	The device was not properly configured. No process name was given.
	ProcessNotRunning	The given process is not running.
	MemoryLeak	The system has observed a sustained upward trend in the amount of Virtual Memory used by the process.
	HandleLeak	The system has observed a sustained upward trend in the number of Handles used by the process.
	ThreadsLeak	The system has observed a sustained upward trend in the number of Threads used by the process.
	CPUOverLoad	The system has observed a sustained period of high CPU usage.

Alarm Device - Computer Process Alarm (Auto)

Description: Generates one or more alarms based on checking the individual resource usage of a given software process. This device automatically detects trends in resource usage and generates alarms when it anticipates a problem.

Table 127 lists the Computer Process Alarm (Auto) Conditions/Subconditions.

Table 127. Computer Process Alarm (Auto) Conditions/Subconditions

Conditions	Subconditions Generated	Description
Handles	Normal	Handle usage is within the acceptable range.
	Bad	No Handle usage data is available.
	Warning	The system has observed a sustained upward trend in the number of Handles used over the span of 2 ½ hours.
	Error	The system has observed a sustained upward trend in the number of Handles used over the span of 5 hours.
VM	Normal	Virtual Memory (VM) usage is within the acceptable range.
	Bad	No VM usage data is available.
	Warning	The system has observed a sustained upward trend in the VM used over the span of 2 ½ hours.
	Error	The system has observed a sustained upward trend in the VM used over the span of 5 hours.
Threads	Normal	Thread usage is within the acceptable range.
	Bad	No Thread usage data is available.
	Warning	The system has observed a sustained upward trend in the number of Threads used over the span of 2 ½ hours.
	Error	The system has observed a sustained upward trend in the number of Threads used over the span of 5 hours.

Table 127. Computer Process Alarm (Auto) Conditions/Subconditions (Continued)

Conditions	Subconditions Generated	Description
CPULoad	Normal	CPU(s) utilization is within the acceptable range.
	Bad	No CPU(s) loading data is available.
	Low	CPU utilization has reached or exceeded the Low limit.
	Medium	CPU utilization has reached or exceeded the Medium limit.
	High	CPU utilization has reached or exceeded the High limit.
ProcessExists	Normal	The given process is running.
	Bad	No data is available.
	Error	The process is not running on the specified computer.

Alarm Device - Computer Process Alarm (Min)

Description: Generates a single alarm based only on whether or not a given process is running.

Table 128 lists the Computer Process Alarm (Min) Conditions/Subconditions.

Table 128. Computer Process Alarm (Min) Conditions/Subconditions

Conditions	Subconditions Generated	Description
ProcessExists	Normal	The given process is running.
	Bad	There is no data available.
	Error	The process is not running on the specified computer.

Alarm Device - Disk Drive Alarm

Description: Generates a single alarm based on the health of a given hard drive, as computed by the device driver.

Table 129 lists the Disk Drive Alarm Conditions/Subconditions.

Table 129. Disk Drive Alarm Conditions/Subconditions

Conditions	Subconditions Generated	Description
Status	Normal	The given hard drive is functioning normally.
	Bad	There is no hard drive status available.
	Error	The device driver has detected a problem with the hard drive.

Status Device - Disk Drive Alert

Description: Generates a single alert based on the health of a given hard drive, as computed by the device driver.

Table 130 lists the Disk Drive Alert Conditions/Subconditions.

Table 130. Disk Drive Alert Conditions/Subconditions

Property	Data Type	Description
Status	String	A string describing the current state of the physical disk drive.
Value-Status	Numeric	A numeric representation of the current state of the physical disk drive.

Status Device - Disk Drive Status

Description: Returns several key status values for a given disk drive.

Table 131 lists the Disk Drive Status Conditions/Subconditions.

Table 131. Disk Drive Status Conditions/Subconditions

Property	Data Type	Description
Partitions	Numeric	The number of partitions on the given drive.
Model	String	The model number of the given drive.
Manufacturer		The manufacturer of the given drive.
Description		A description of the given drive.
ErrorDescription		A description of the existing error condition on the given drive, if any.
LastErrorCode	Numeric	The error code of the existing error condition on the given drive, if any.
Status	String	The overall status of the given drive.
DeviceId		The windows device identifier for the given drive (e.g. "\.\PHYSICALDRIVE0").
Size	Numeric	The size, in bytes, of a given drive.

Alarm Device - Disk Volume Alarm

Description: Generates an alarm when the amount of available hard disk space goes below a certain limit.

Table 132 lists the Disk Volume Alarm Conditions/Subconditions.

Table 132. Disk Volume Alarm Conditions/Subconditions

Conditions	Subconditions Generated	Description
FreeSpace	Normal	The free space on the given hard drive is within the acceptable range.
	Bad	Hard drive information is not available.
	Warning	The amount of free space available has reached or gone below the warning limit.
	Serious	The amount of free space available has reached or gone below the serious limit.
	Critical	The amount of free space available has reached or gone below the critical limit.

Status Device - Disk Volume Alert

Description: Generates an alert when the amount of available hard disk space goes below a certain limit.

Table 133 lists the Disk Volume Alert properties.

Table 133. Disk Volume Alert Properties

Property	Data Type	Description
FreeSpace	String	A string describing the free space of the logical disk drive.
Value-FreeSpace	Numeric	A numeric representation of the free space of the logical disk drive.

Status Device - Disk Volume Status

Description: Returns the percentage free of a given hard drive partition.

Table 134 lists the Disk Volume Status properties.

Table 134. Disk Volume Status Properties

Property	Data Type	Description
FreeSpace	Numeric	A percentage free of a given hard drive.

Light Alarm Device - Light Disk Volume Alarm

Description: Generates an alarm when the amount of available hard disk space goes below a certain limit.

Table 135 lists the Light Disk Volume Alarm Conditions/Subconditions.

Table 135. Light Disk Volume Alarm Conditions/Subconditions

Conditions	Subconditions Generated	Description
FreeSpace	Normal	The free space on the given hard drive is within the acceptable range.
	Bad	Hard drive information is not available
	Warning	The amount of free space available has reached or gone below the warning limit.
	Serious	The amount of free space available has reached or gone below the serious limit.
	Critical	The amount of free space available has reached or gone below the critical limit.

Light Status Device - Light Disk Volume Alert

Description: Generates an alert when the amount of available hard disk space goes below a certain limit.

Table 136 lists the Light Disk Volume Alert properties.

Table 136. Light Disk Volume Alert Properties

Property	Data Type	Description
FreeSpace	String	A string describing the state of the physical disk drive.
Value-FreeSpace	Numeric	A numeric representation of the current state of the physical disk drive.

Alarm Device - Printer Alarm

Description: Generates several printer alarm possibilities based on the status of a given network printer.

Table 137 lists the Printer Alarm Conditions/Subconditions.

Table 137. Printer Alarm Conditions/Subconditions

Conditions	Subconditions Generated	Description
Available	Normal	The printer can be seen on the network.
	Bad	There is no data available.
	Alarm	The printer cannot be seen on the network.
Service Request	Normal	No Service Request problem has been indicated by the printer.
	Bad	The printer Service Request status cannot be accessed.
	Active	The printer has indicated that service is necessary.

Table 137. Printer Alarm Conditions/Subconditions (Continued)

Conditions	Subconditions Generated	Description
Offline	Normal	No Offline problem has been indicated by the printer.
	Bad	The printer Offline status cannot be accessed.
	Active	The printer has indicated that it is offline.
Jammed	Normal	No Paper Jammed problem has been indicated by the printer.
	Bad	The printer Jammed status cannot be accessed.
	Active	The printer has indicated that it has a paper jam.
DoorOpen	Normal	No DoorOpen problem has been indicated by the printer.
	Bad	The printer DoorOpen status cannot be accessed.
	Active	The printer has indicated that one of its access doors is open preventing proper operation.
NoToner	Normal	There has not been a NoToner problem indicated by the printer.
	Bad	The printer NoToner status cannot be accessed.
	Active	The printer has indicated that it is out of toner.
LowToner	Normal	There has not been a LowToner problem indicated by the printer.
	Bad	The printer LowToner status cannot be accessed.
	Active	The printer has indicated that it is low on toner.
NoPaper	Normal	There has not been a NoPaper problem indicated by the printer.
	Bad	The printer NoPaper status cannot be accessed.
	Active	The printer has indicated that it is out of paper.

Table 137. Printer Alarm Conditions/Subconditions (Continued)

Conditions	Subconditions Generated	Description
LowPaper	Normal	There has not been a LowPaper problem indicated by the printer.
	Bad	The printer LowPaper status cannot be accessed.
	Active	The printer has indicated that it is low on paper.

Status Device - Printer Alert

Description: Generates several printer alert possibilities based on the status of a given network printer.

Table 138 lists the Printer Alert properties.

Table 138. Printer Alert Properties

Property	Data Type	Description
Available	String	A string describing the current state of the printer availability.
DoorOpen		A string describing the current state of the printer DoorOpen.
Jammed		A string describing the current state of the printer Jammed.
LowPaper		A string describing the current state of the printer LowPaper.
LowToner		A string describing the current state of the printer LowToner.
NoPaper		A string describing the current state of the printer NoPaper.
NoToner		A string describing the current state of the printer NoToner.
Offline		A string describing the current state of the printer Offline.
ServiceRequest		A string describing the current state of the printer ServiceRequest.

Table 138. Printer Alert Properties (Continued)

Property	Data Type	Description
Value-Available	Numeric	A numeric representation of the current state of the printer availability.
Value-DoorOpen		A numeric representation of the current state of the printer DoorOpen.
Value-Jammed		A numeric representation of the current state of the printer Jammed.
Value-LowPaper		A numeric representation of the current state of the printer LowPaper.
Value-LowToner		A numeric representation of the current state of the printer LowToner.
Value-NoPaper		A numeric representation of the current state of the printer NoPaper.
Value-NoToner		A numeric representation of the current state of the printer NoToner.
Value-Offline		A numeric representation of the current state of the printer Offline.
Value-ServiceRequest		A numeric representation of the current state of the printer ServiceRequest.

Status Device - Printer Status

Description: Returns the status of key attributes of a given network printer.

Table 139 lists the Printer Status properties.

Table 139. Printer Status Properties

Property	Data Type	Description
SysName	String	The name of the given printer.
SysLocation		The configured location of the given printer.
SysDescription		The description of the given printer.
DeviceStatus		A string describing the current device status (e.g. running).
PrinterStatus		A string describing the current device status (e.g. running).
DetectedErrorState	Numeric	A number indicating the current error condition on the printer, if any (e.g. 00 indicates no error).
szDetectedErrorState	String	The decoded error code of the existing error condition on the printer, if any. This string will contain one or more of the following strings, separated by plus (+) signs: Bad quality, Service Request, Offline, Jammed, Door Open, No Toner, No Paper, Low Paper.

Alarm Device - Cisco 12-Port Switch Alarm

Description: Generates alarms for port failures and optionally for disconnected ports.

Table 140 lists the Cisco 12-Port switch alarm conditions/subconditions.

Table 140. Cisco 12-Port Switch Alarm Conditions/Subconditions

Conditions	Subconditions Generated	Description
SwitchHealth	Normal	The port is functioning normally, or the port is not connected but alarming on this condition is disabled.
	Bad	Bad quality on ports: The status of one or several switch ports cannot be accessed.
	DeviceDown	Device is down: All ports are bad quality and status cannot be accessed on any ports.
	PortError	Errors are detected. One or several ports have input or output errors above the specified error limit.
	PortDisconnected	Port(s) are disconnected: One or more ports are not connected. This only alarms if the switch is configured to alarm on open ports.

Status Device - Cisco 12-Port Switch Alert

Description: Returns the status of key attributes of a given Cisco 12-Port switch.

Table 141 lists the Cisco 12-Port switch alert properties.

Table 141. Cisco 12-Port Switch Alert Properties

Property	Data Type	Description
Port-01 to Port-12	String	A string describing the current state of each port. The string is either Normal or Bad quality.
Value-Port-01 to Value-Port-12	Numeric	A numeric representation of a port failure or disconnection.

Status Device - Cisco 12-Port Switch Status

Description: Returns the status of key attributes of a given Cisco 12-port switch.

Even though this is a 12-Port switch, it actually has 15 ports exposed. Ports 0, 13, and 14 are not used for communication and are internal. They are exposed for completeness.

Table 142 lists the Cisco 12-Port switch status properties.

Table 142. Cisco 12-Port Switch Status Properties

Property	Data Type	Description
SysName	String	The name of the given switch.
SysDescr		The configured description of the switch.
SysUpTime		The amount of time the switch has been running since the last reset, in hundredths of seconds.
IfDescr00 to IfDescr14		A textual string containing information about the interface. This string should include the name of the manufacturer, the product name and the version of the hardware interface.
IfOperStatus00 to IfOperStatus14	Numeric	A string describing the current port status of ports 0 to 14 (e.g. up).
IfInOctets00 to IfInOctets14		The number of bytes received by the switch per port.
IfOutOctets00 to IfOutOctets14		The number of bytes sent by the switch per port.
IfSpeed00 to IfSpeed14		The speed of each port in bytes per second.
IfOutErrors00 to IfOutErrors14		The number of inbound packets that contained errors preventing them from being delivered to a higher-layer protocol.
IfInErrors00 to IfInErrors14		The number of outbound packets that could not be transmitted because of errors.

Light Alarm Device - Light Cisco 12-Port Switch Alarm

Description: Generates alarms for port failures and optionally for disconnected ports.

Table 143 lists the Light Cisco 12-Port switch alarm conditions/subconditions.

Table 143. Cisco 12-Port Switch Alarm Conditions/Subconditions

Conditions	Subconditions Generated	Description
SwitchHealth	Normal	The port is functioning normally, or the port is not connected but alarming on this condition is disabled.
	Bad	Bad quality on ports: The status of one or several switch ports can not be accessed.
	DeviceDown	Device is down: All ports are bad quality and status can not be accessed on any ports.
	PortError	Errors are detected. One or several ports have input or output errors above the specified error limit.
	PortDisconnected	Port(s) are disconnected: One or more ports are not connected. This only alarms if the switch is configured to alarm on open ports.

Light Status Device - Light Cisco 12-Port Switch Alert

Description: Returns the status of key attributes of a given Cisco 12-Port switch.

Table 144 lists the Light Cisco 12-Port switch alert properties.

Table 144. Light Cisco 12-Port Switch Alert Properties

Property	Data Type	Description
Port-01 to Port-12	String	A string describing the current state of each port. The string is either Normal or Bad quality.
Value-Port-01 to Value-Port-12	Numeric	A numeric representation of a port failure or disconnection.

Alarm Device - Cisco 24-Port Switch Alarm

Description: Generates alarms for port failures and optionally for disconnected ports.

Table 145 lists the Cisco 24-Port switch conditions/subconditions.

Table 145. Cisco 24-Port Switch Alarm Conditions/Subconditions

Conditions	Subconditions Generated	Description
SwitchHealth	Normal	The port is functioning normally, or the port is not connected but alarming on this condition is disabled.
	Bad	Bad quality on ports: The status of one or several switch ports can not be accessed.
	DeviceDown	Device is down: All ports are bad quality and status can not be accessed on any ports.
	PortError	Errors are detected. One or several ports have input or output errors above the specified error limit.
	PortDisconnected	Port(s) are disconnected: One or more ports are not connected. This only alarms if the switch is configured to alarm on open ports.

Status Device - Cisco 24-Port Switch Alert

Description: Returns the status of key attributes of a given Cisco 24-Port switch.

Table 146 lists the Cisco 24-Port switch alert properties.

Table 146. Cisco 24-Port Switch Alert Properties

Property	Data Type	Description
Port-01 to Port-24	String	A string describing the current state of each port. The string is either Normal or Bad quality.
Value-Port-01 to Value-Port-24	Numeric	A numeric representation of a port failure or disconnection.

Status Device - Cisco 24-Port Switch Status

Description: Returns the status of key attributes of a given Cisco 24-Port device switch.

Even though this is a 24-Port Switch, it actually has 27 ports exposed. Ports 0, 25 and 26 are not used for communication and are internal. They are exposed for completeness.

Table 147 lists the Cisco 24-Port switch status properties.

Table 147. Cisco 24-Port Switch Status Properties

Property	Data Type	Description
SysName	String	The name of the given switch.
SysDescr		The configured description of the switch.
SysUpTime		The amount of time the switch has been running since the last reset, in hundredths of seconds.
IfDescr00 to IfDescr26		A textual string containing information about the interface. This string should include the name of the manufacturer, the product name and the version of the hardware interface.
IfOperStatus00 to IfOperStatus26	Numeric	A string describing the current port status of ports 0 to 26 (e.g. up).
IfInOctets00 to IfInOctets26		The number of bytes received by the switch per port.
IfOutOctets00 to IfOutOctets26		The number of bytes sent by the switch per port.
IfSpeed00 to IfSpeed26		The speed of each port in bytes per second.
IfOutErrors00 to IfOutErrors26		The number of inbound packets that contained errors preventing them from being delivered to a higher-layer protocol.
IfInErrors00 to IfInErrors26		The number of outbound packets that could not be transmitted because of errors.

Light Alarm Device - Light Cisco 24-Port Switch Alarm

Description: Generates alarms for port failures and optionally for disconnected ports.

Table 148 lists the Light Cisco 24-Port switch alarm conditions/subconditions.

Table 148. Light Cisco 24-Port switch Alarm Conditions/Subconditions

Conditions	Subconditions Generated	Description
SwitchHealth	Normal	The port is functioning normally, or the port is not connected but alarming on this condition is disabled.
	Bad	Bad quality on port(s): The status of one or several switch ports can not be accessed.
	DeviceDown	Device is down: All ports are bad quality and status cannot be accessed on any ports.
	PortError	Errors are detected. One or several ports have input or output errors above the specified error limit.
	PortDisconnected	Port(s) are disconnected: One or more ports are not connected. This only alarms if the switch is configured to alarm on open ports.

Light Status Device - Light Cisco 24-Port Switch Alert

Description: Returns the status of key attributes of a given Cisco 24-Port switch.

Table 149 lists the Light Cisco 24-Port switch alert properties.

Table 149. Light Cisco 24-Port Switch Alert Properties

Property	Data Type	Description
Port-01 to Port-24	String	A string describing the current state of each port. The string is either Normal or Bad quality.
Value-Port-01 to Value-Port-24	Numeric	A numeric representation of a port failure or disconnection.

Alarm Device - Cisco 48-Port Switch Alarm

Description: Generates alarms for port failures and optionally for disconnected ports.

Table 150 lists the Cisco 48-Port switch alarm conditions/subconditions.

Table 150. Cisco 48-Port Switch Alarm Conditions/Subconditions

Conditions	Subconditions Generated	Description
SwitchHealth	Normal	The port is functioning normally, or the port is not connected but alarming on this condition is disabled.
	Bad	Bad quality on port(s): The status of one or several switch ports can not be accessed.
	DeviceDown	Device is down: All ports are bad quality and status can not be accessed on any ports.
	PortError	Errors are detected. One or several ports have input or output errors above the specified error limit.
	PortDisconnected	Port(s) are disconnected: One or more ports are not connected. This only alarms if the switch is configured to alarm on open ports.

Status Device - Cisco 48-Port Switch Alert

Description: Returns the status of key attributes of a given Cisco 48-Port switch.

Table 151 lists the Cisco 48-Port switch alert properties.

Table 151. Cisco 48-Port Switch Alert Properties

Property	Data Type	Description
Port-01 to Port-48	String	A string describing the current state of each port. The string is either Normal or Bad quality.
Value-Port-01 to Value-Port-48	Numeric	A numeric representation of a port failure or disconnection.

Status Device - Cisco 48-Port Switch Status

Description: Returns the status of key attributes of a given Cisco 48-Port switch device.

> Even though this is a 48-Port Switch, it actually has 53 ports exposed. Ports 0, 51 and 52 are not used for communication and are internal. They are exposed for completeness. Ports 49 and 50 are high-speed (GHz) ports.

Table 152 lists the Cisco 48-Port switch status properties.

Table 152. Cisco 48-Port Switch Status Properties

Property	Data Type	Description
SysName	String	The name of the given switch.
SysDescr		The configured description of the switch.
SysUpTime		The amount of time the switch has been running since the last reset, in hundredths of seconds.
IfDescr00 to IfDescr52		A textual string containing information about the interface. This string should include the name of the manufacturer, the product name and the version of the hardware interface.
IfOperStatus00 to IfOperStatus52	Numeric	A string describing the current port status of ports 0 to 52 (e.g. up).
IfInOctets00 to IfInOctets52		The number of bytes received by the switch per port.
IfOutOctets00 to IfOutOctets52		The number of bytes sent by the switch per port.
IfSpeed00 to IfSpeed52		The speed of each port in bytes per second.
IfOutErrors00 to IfOutErrors52		The number of inbound packets that contained errors preventing them from being delivered to a higher-layer protocol.
IfInErrors00 to IfInErrors52		The number of outbound packets that could not be transmitted because of errors.

Light Alarm Device - Light Cisco 48-Port Switch Alarm

Description: Generates alarms for port failures and optionally for disconnected ports.

Table 153 lists the Light Cisco 48-Port switch alert conditions/subconditions.

Table 153. Light Cisco 48-Port Switch Alert Conditions/Subconditions

Conditions	Subconditions Generated	Description
SwitchHealth	Normal	The port is functioning normally, or the port is not connected but alarming on this condition is disabled.
	Bad	Bad quality on port(s): The status of one or several switch ports can not be accessed.
	DeviceDown	Device is down: All ports are bad quality and status can not be accessed on any ports.
	PortError	Errors are detected. One or several ports have input or output errors above the specified error limit.
	PortDisconnected	Port(s) are disconnected: One or more ports are not connected. This only alarms if the switch is configured to alarm on open ports.

Light Status Device - Light Cisco 48-Port Switch Alert

Description: Returns the status of key attributes of a given Cisco 48-Port switch.

Table 154 lists the Light Cisco 48-Port switch alert properties.

Table 154. Light Cisco 48-Port Switch Alert Properties

Property	Data Type	Description
Port-01 to Port-48	String	A string describing the current state of each port. The string is either Normal or Bad quality.
Value-Port-01 to Value-Port-48	Numeric	A numeric representation of a port failure or disconnection.

Alarm Device - Hirschmann 8-Port Alarm

Description: Generates alarms on the port modules of the Hirschmann Mach 3000 switches.

Table 155 lists the Hirschmann 8-Port Alarm conditions/subconditions.

Table 155. Hirschmann 8-Port Alarm Conditions/Subconditions

Conditions	Subconditions Generated	Description
PortHealth	Normal	The port is functioning normally.
	Bad	The port cannot be accessed.
	ModuleDown	The port module is down or not responding.
	PortError	The switch has detected an error on this port module.
	PortDisconnect	A port or ports on the module have been disconnected from the network.

Status Device - Hirschmann 8-Port Alert

Description: Generates alerts on Hirschmann Mach 3000 switches.

Table 156 lists the Hirschmann 8-Port Alert properties.

Table 156. Hirschmann 8-Port Alert Properties

Property	Data Type	Description
Port-1 to Port-8	String	A string describing the current state of the port.
Value-Port-1 to Value-Port-8	Numeric	A numeric representation of the current state of the port. A value of zero (0) in normal and one (1) is Bad Input, greater than one (1) is an abnormal state.

Status Device - Hirschmann 8-Port Status

Description: Returns the status of key attributes of a configurable set of ports on a given Hirschmann Mach 3000 switch.

There are four different port status devices corresponding to the 1, 2, 4, and 8 port modules. Depending on the device used, the range of properties vary.

Table 157 lists the Hirschmann 8-Port status properties.

Table 157. Hirschmann 8-Port Status Properties

Property	Data Type	Description
IfOperStatus1 to IfOperStatus8	Numeric	A string describing the current status of the ports (e.g. up).
IfInOctets1 to IfInOctets8		The number of bytes received by the switch per port.
IfOutOctets1 to IfOutOctets8		The number of bytes sent by the switch per port.
IfSpeed1 to IfSpeed8		The speed of each port in bytes per second.
MediaAvailable1 to MediaAvailable8	String	A string describing the current availability of the port. Possible states include: OTHER, UNKNOWN, AVAILABLE, NOTAVAILABLE, REMOTEFAULT, INVALIDSIGNAL, REMOTEJABBER, REMOTELINKLOSS, REMOTETEST, OFFLINE, AUTONEGERROR.

Light Alarm Device - Light Hirschmann 8-Port Alarm

Description: Generates alarms on the port modules of the Hirschmann Mach 3000 switches.

Table 158 lists the Light Hirschmann 8-Port Alarm conditions/subconditions.

Table 158. Light Hirschmann 8-Port Alarm Conditions/Subconditions

Conditions	Subconditions Generated	Description
PortHealth	Normal	The port is functioning normally.
	Bad	The port cannot be accessed.
	ModuleDown	The port module is down or not responding.
	PortError	The switch has detected an error on this port module.
	PortDisconnect	A port or ports on the module have been disconnected from the network.

Light Status Device - Light Hirschmann 8-Port Alert

Description: Generates alerts on Hirschmann Mach 3000 switches.

Table 159 lists the Light Hirschmann 8-Port Alert properties.

Table 159. Light Hirschmann 8-Port Alert Properties

Property	Data Type	Description
Port-1 to Port-8	String	A string describing the current state of the port.
Value-Port-1 to Value-Port-8	Numeric	A numeric representation of the current state of the port. A value of zero (0) in normal and one (1) is Bad Input, greater than one (1) is an abnormal state.

Alarm Device - Hirschmann n-Port Alarm

Description: Generates alarms on the port modules of the Hirschmann Mach 3000 switches.

Table 160 lists the Hirschmann n-Port Alarm Conditions/Subconditions.

Table 160. Hirschmann n-Port Alarm Conditions/Subconditions

Conditions	Subconditions Generated	Description
PortHealth	Normal	The port is functioning normally.
	Bad	The port cannot be accessed.
	ModuleDown	The port module is down or not responding.
	PortError	The switch has detected an error on this port module.
	PortDisconnect	A port or ports on the module have been disconnected from the network.

Light Alarm Device - Light Hirschmann n-Port Alarm

Description: Generates alarms on the port modules of the Hirschmann Mach 3000 switches.

Table 161 lists the Light Hirschmann n-Port Alarm Conditions/Subconditions.

Table 161. Light Hirschmann n-Port Alarm Conditions/Subconditions

Conditions	Subconditions Generated	Description
PortHealth	Normal	The port is functioning normally.
	Bad	The port cannot be accessed.
	ModuleDown	The port module is down or not responding.
	PortError	The switch has detected an error on this port module.
	PortDisconnect	A port or ports on the module have been disconnected from the network.

Alarm Device - Hirschmann Power Supply Alarm

Description: Generates alarms on power supply problems on Hirschmann Mach 3000 switches.

Table 162 lists the Hirschmann Power Supply Alarm Conditions/Subconditions.

Table 162. Hirschmann Power Supply Alarm Conditions/Subconditions

Conditions	Subconditions Generated	Description
Alarm	Normal	The power supply is functioning normally.
	Bad	The power supply status cannot be accessed.
	Active	The switch has reported a problem with the power supply.

Status Device - Hirschmann Power Supply Alert

Description: Generates alerts on power supply problems on Hirschmann Mach 3000 switches.

Table 163 lists the Hirschmann Power Supply Alert properties.

Table 163. Hirschmann Power Supply Alert Properties

Property	Data Type	Description
Status	String	A string describing the state of the power supply (e.g. failed).
Value-Status	Numeric	A numerical representation of the state of the power supply. A value of 0 is normal, 1 is Bad Input, greater than 1 is abnormal state.

Status Device - Hirschmann Power Supply Status

Description: Returns the status of the Power supplies on given Hirschmann Mach 3000 switches.

Table 164 lists the Hirschmann power supply alert properties.

Table 164. Hirschmann Power Supply Alert Properties

Property	Data Type	Description
PowerSupplyStatus	String	A string describing the state of the power supply (e.g. failed).

Light Alarm Device - Light Hirschmann Power Supply Alarm

Description: Generates alarms on power supply problems on Hirschmann Mach 3000 switches.

Table 165 lists the Light Hirschmann power supply alarm conditions/subconditions.

Table 165. Light Hirschmann Power Supply Alarm Conditions/Subconditions

Conditions	Subconditions Generated	Description
Alarm	Normal	The power supply is functioning normally.
	Bad	The power supply status cannot be accessed.
	Active	The switch has reported a problem with the power supply.

Light Status Device - Light Hirschmann Power Supply Alert

Description: Returns the status of the Power supplies of Hirschmann Mach 3000 switches.

Table 166 lists the Light Hirschmann power supply Alert properties.

Table 166. Light Hirschmann Power Supply Alert Properties

Property	Data Type	Description
Status	String	A string describing the state of the power supply (e.g. failed).
Value-Status	Numeric	A numerical representation of the state of the power supply. A value of 0 is normal, 1 is Bad Input, greater than 1 is abnormal state.

Status Device - Hirschmann Mach 3000 Base Status

Description: Returns the basic status attributes of given Hirschmann Mach 3000 switches.

Table 167 lists the Hirschmann Mach 3000 Base Status properties.

Table 167. Hirschmann Mach 3000 Base Status Properties

Property	Data Type	Description
SysName	String	The name of the given switch.
SysDescr		The configured description of the switch.
SysUpTime	Numeric	The amount of time the switch has been running since the last reset, in hundredths of seconds.

Alarm Device - Hirschmann RS2 Alarm

Description: Generates alarms on port and power supply problems on Hirschmann RS2 switches.

Table 168 lists the Hirschmann RS2 Alarm conditions/subconditions.

Table 168. Hirschmann RS2 Alarm Conditions/Subconditions

Conditions	Subconditions Generated	Description
PowerSupply1 PowerSupply2	Normal	The power supply is functioning normally.
	Bad	The power supply status cannot be accessed.
	Active	The switch has reported a problem with the power supply.

Table 168. Hirschmann RS2 Alarm Conditions/Subconditions (Continued)

Conditions	Subconditions Generated	Description
Port-1 Port-2 Port-3 Port-4 Port-5 Port-6 Port-7	Normal	The port is functioning normally, or the port is not connected but alarming on this condition is disabled.
	Bad	The switch port status cannot be accessed.
	Unknown	The switch has indicated that a problem of type Unknown has occurred.
	NotAvailable	The switch has indicated that a problem of type Not Available has occurred.
	RemoteFault	The switch has indicated that a problem of type Remote Fault has occurred.
	InvalidSignal	The switch has indicated that a problem of type Invalid Signal has occurred.
	RemoteJabber	The switch has indicated that a problem of type Remote Jabber has occurred.
	RemoteLinkLoss	The switch has indicated that a problem of type Remote Link Loss has occurred.
	Remote Test	The switch has indicated that a problem of type Remote Test has occurred.
	Offline	The switch has indicated that a problem of type Offline has occurred.
	AutoNegError	The switch has indicated that a problem of type Auto Neg Error has occurred.
	Unconnected	The switch has indicated that no network connection is currently present on this port.

Status Device - Hirschmann RS2 Alert

Description: Generates alerts on port and power supply problems on Hirschmann RS2 switches.

Table 169 lists the Hirschmann RS2 Alert properties.

Table 169. Hirschmann RS2 Alert Properties

Property	Data Type	Description
PowerSupply-1 PowerSupply-2	String	A string describing the current state of the power supply.
Port-1 to Port-#		A string describing the current state of the port.
Value-PowerSupply-1 Value-PowerSupply-2	Numeric	A numeric representation of the current state of the power supply. A value of zero (0) is normal, one (1) is Bad Input, greater than one (1) is an abnormal state.
Value-Port-1 to Value-Port-#		A numeric representation of the current state of the port. A value of zero (0) is normal, one (1) is Bad Input, greater than one (1) is an abnormal state.

Status Device - Hirschmann RS2 Status

Description: Returns the status of key attributes of Hirschmann RS2 switches.

Table 170 lists the Hirschmann RS2 status properties.

Table 170. Hirschmann RS2 Status Properties

Property	Data Type	Description
SysName	String	The name of the given switch.
SysDescr		The configured description of the switch.

Table 170. Hirschmann RS2 Status Properties (Continued)

Property	Data Type	Description
SysUpTime	Numeric	The amount of time the switch has been running since the last reset, in hundredths of seconds.
IfOperStatus1 to IfOperStatus7		A string describing the current port status of ports 0 to 7 (e.g. up).
IfInOctets1 to IfInOctets7		The number of bytes received by the switch per port.
IfOutOctets1 to IfOutOctets7		The number of bytes sent by the switch per port.
IfSpeed1 to IfSpeed7		The speed of each port in bytes per second.
MediaAvailable1 to MediaAvailable7	String	A string describing the current availability of the port. Possible states include: OTHER, UNKNOWN, AVAILABLE, NOTAVAILABLE, REMOTEFAULT, INVALIDSIGNAL, REMOTEJABBER, REMOTELINKLOSS, REMOTETEST, OFFLINE, AUTONEGERROR.
PowerState1 to PowerState7		A string describing the state of the power supply (e.g. failed).

Light Alarm Device - Light Hirschmann RS2 Alarm

Description: Generates alarms on port and power supply problems on Hirschmann RS2 switches.

Table 171 lists the Light Hirschmann RS2 Alarm conditions/subconditions.

Table 171. Light Hirschmann RS2 Alarm Conditions/Subconditions

Conditions	Subconditions Generated	Description
PowerSupply1 PowerSupply2	Normal	The power supply is functioning normally.
	Bad	The power supply status cannot be accessed.
	Active	The switch has reported a problem with the power supply.
Port-1 Port-2 Port-3 Port-4 Port-5 Port-6 Port-7	Normal	The port is functioning normally, or the port is not connected but alarming on this condition is disabled.
	Bad	The switch port status cannot be accessed.
	Unknown	The switch has indicated that a problem of type Unknown has occurred.
	NotAvailable	The switch has indicated that a problem of type Not Available has occurred.
	RemoteFault	The switch has indicated that a problem of type Remote Fault has occurred.
	InvalidSignal	The switch has indicated that a problem of type Invalid Signal has occurred.
	RemoteJabber	The switch has indicated that a problem of type Remote Jabber has occurred.

Table 171. Light Hirschmann RS2 Alarm Conditions/Subconditions (Continued)

Conditions	Subconditions Generated	Description
	RemoteLinkLoss	The switch has indicated that a problem of type Remote Link Loss has occurred.
	Remote Test	The switch has indicated that a problem of type Remote Test has occurred.
	Offline	The switch has indicated that a problem of type Offline has occurred.
	AutoNegError	The switch has indicated that a problem of type Auto Neg Error has occurred.
	Unconnected	The switch has indicated that no network connection is currently present on this port.

Alarm Device – Symmetricom XLi Clock Alarm

Description: Generates alarms if one of the clock fault conditions enters the fault state.

Table 172 lists the Symmetricom XLi Clock Alarm conditions/subconditions.

Table 172. Symmetricom XLi Clock Alarm Conditions/Subconditions

Conditions	Subconditions Generated	Description
statusPrimaryRefClk	Normal	The clock fault condition is in the normal state.
statusSecondaryRefClk	Bad	The clock fault condition can not be accessed.
statusIrig	Fault	The clock fault condition is in the fault condition.
statusAuxRef		
statusPrimaryPower		
statusSecondaryPower		
statusRbOsc		
statusDac		
statusTimeError		
statusTimeout		

Light Status Device - Light Hirschmann RS2 Alert

Description: Generates alerts on port and power supply problems on Hirschmann RS2 switches.

Table 173 lists the Light Hirschmann RS2 Alert properties.

Table 173. Light Hirschmann RS2 Alert Properties

Property	Data Type	Description
PowerSupply-1 PowerSupply-2	String	A string describing the current state of the power supply.
Port-1 to Port-#		A string describing the current state of the port.
Value-PowerSupply-1 Value-PowerSupply-2	Numeric	A numeric representation of the current state of the power supply. A value of zero (0) is normal, one (1) is Bad Input, greater than one (1) is an abnormal state.
Value-Port-1 to Value-Port-#		A numeric representation of the current state of the port. A value of zero (0) is normal, one (1) is Bad Input, greater than one (1) is an abnormal state.

Status Device – Symmetricom XLi Clock Status

Description: Returns the status of key attributes of Symmetricom XLi Clock.

Table 174 lists the Symmetricom XLi Clock Status properties.

Table 174. Symmetricom XLi Clock Status Properties

Property	Data Type	Description
SysName	String	The name of the clock.
SysLocation	String	The configured location of the clock.
SysDescr	String	The configured description of the clock.
StatusClock	String	The status of the clock. Possible states: locked or unlocked.

Table 174. Symmetricom XLi Clock Status Properties (Continued)

Property	Data Type	Description
statusClockSource	String	The current clock source. Possible states: clockIrigA, clockIrigB, clockIrigG, clockNasa36, clockPrimary, clockSecondary, clockAuxRef or clockNone.
statusPllSynthesizer	String	The current status of the PLL Synthesizer. Possible states: unlocked or locked.
statusLpnPll	String	The current status of the LPN PLL. Possible states: unlocked or locked.
statusPrimaryRefClk	String	The current status of the primary reference clock. Possible States: ok or fault.
statusSecondaryRefClk	String	The current status of the secondary reference clock. Possible states: ok or fault.
statusIrig	String	The current status of the IRIG. Possible states: ok or fault.
statusAuxRef	String	The current status of the auxiliary reference clock. Possible states: ok or fault.
statusPrimaryPower	String	The current status of the primary power. Possible states: ok or fault.
statusSecondaryPower	String	The current status of the secondary power. Possible states: ok or fault.
statusRbOsc	String	The current status of the rubidium oscillator. Possible states: ok or fault.
statusDac	String	The current status of the digital to analog converter. Possible states: ok or fault.

Table 174. Symmetricom XLi Clock Status Properties (Continued)

Property	Data Type	Description
statusFirstTimeLock	String	The current status of the clock since power on. Possible states: firstTimeLockedOnce – indicates the clock has locked at least once since power on. firstTimeLockedOnceWithinTimeout – indicates the clock has locked since power on but is still within the power on suppress timeout. firstTimeNotLocked – indicates the clock has not locked since power on.
statusTimeError	String	The current status of the timer error indicator. Possible states: ok or fault.
statusTimeout	String	The current status of the timeout fault indicator. Possible states: ok or fault.

INDEX

Revision History

Introduction

This section provides information on the revision history of this User Manual.

ℹ️ The revision index of this User Manual is not related to the 800xA 5.1 System Revision.

Revision History

The following table lists the revision history of this User Manual.

Revision Index	Description	Date
-	First version published for 800xA 5.1	June 2010
A	Updated for 800xA 5.1 Rev B	June 2012
B	Updated for 800xA 5.1 Rev E	July 2015

Updates in Revision Index A

The following table shows the updates made in this User Manual for 800xA 5.1 Rev B.

Updated Section/Sub-section	Description of Update
Section 2: ESXi Server Monitoring	New topic added to introduce ESXi Server Monitoring Functionality.

Updates in Revision Index B

The following table shows the updates made in this User Manual for 800xA 5.1 Rev E.

Updated Section/Sub-section	Description of Update
Section 2: IT Device SNMP Configuration	Configuration steps added for the topic.
Section 2: IT Device Traps	Configuration steps added for the topic.
All sections	Removed *Community Name* password from the document.

Contact us

Power and productivity
for a better world™

ABB