Foglight™ for SNMP 5.8.5

User and Reference Guide

If you have any questions regarding your potential use of this material, contact:

Dell Inc.
Attn: LEGAL Dept
5 Polaris Way
Aliso Viejo, CA 92656

Refer to our web site (software.dell.com) for regional and international office information.

Patents

Foglight™ is protected by U.S. Patents # 7,979,245; 8,175,862; and 8,892,415. Additional Patents Pending.

For more information, go to http://software.dell.com/legal/patents.aspx.

Trademarks

Legend

CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

WARNING: A WARNING icon indicates a potential for property damage, personal injury, or death.

IMPORTANT NOTE, **NOTE**, **TIP**, **MOBILE**, or **VIDEO:** An information icon indicates supporting information.

Foglight for SNMP User and Reference Guide
April 2015
Management Server Version 5.7.5
Cartridge Version 5.8.5

Contents

1

Using Foglight for SNMP to Monitor Devices

Foglight for SNMP supports and extends the physical host and device monitoring capabilities of the Foglight for Infrastructure cartridge to a broader set of platforms that the Infrastructure agent does not currently support.

Foglight for SNMP allows you to collect data from all types of devices, such as desktops, servers, routers, and switches, across Microsoft®Windows®, Linux®, Oracle Solaris®, HP® UX, and AIX operating systems. When you enable SNMP on a device and provide the correct credentials, Foglight for SNMP can monitor that device and collect data from it.

When you deploy Foglight for SNMP, you can view the performance of the monitored platforms and devices. Foglight for SNMP gives you the capability to ensure consistent platform and device performance by reviewing the performance statistics. Better management of your hosts and devices can be achieved when you are alerted to potential problems before end users are affected.

Foglight for SNMP relies on the SNMP Agent to collect data. Start by installing the Foglight for SNMP cartridge on the Management Server. The SNMP Agent package is automatically deployed, and agent instances are automatically created. This process may take several minutes to complete.

SNMP Discovery on Linux

Foglight for SNMP running on Linux requires that you allow Foglight Agent Manager root or administrator access to start the Agent Manager's ICMPService.

To enable access, do one of the following. These options are listed in order of preference.

- On more advanced Linux systems, assign the `CAP_NET_RAW` capability to the `ICMPService`.
- Configure `sudo` to allow the `udp2icmp` helper application shipped by Dell to run as root.
- Provide the Foglight Agent Manager with `root` permissions (not recommended).

Foglight for SNMP Navigation Basics

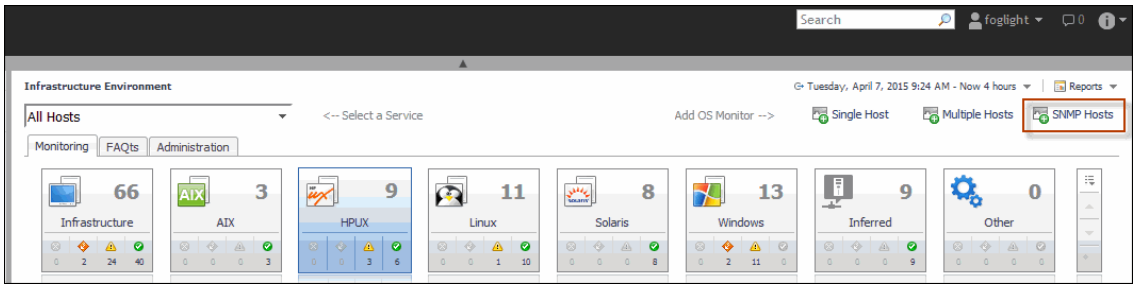
Foglight for SNMP integrates seamlessly into the Infrastructure cartridge workflow. Thus, after you install the Foglight for SNMP cartridge you will not see a separate SNMP dashboard in the navigation panel on the left of the browser interface.

- Infrastructure Environment Dashboard
- Breadcrumbs
- Time range
- Sortable lists
- Exporting SNMP Tables
- Alarms and status indicators
- Mouse-over actions

Infrastructure Environment Dashboard

An SNMP Hosts button is added to the far right of the Infrastructure Environment dashboard.

Figure 1. SNMP Hosts Button on Infrastructure Environment Dashboard



For information on how to discover network devices using the SNMP Hosts button, see **Discovering SNMP Devices on page 11**.

Breadcrumbs

When you drill down into various levels across dashboards, a trail of breadcrumbs is left at the top of the current dashboard. This trail provides you with a simple mechanism for returning to the main Infrastructure Environment view. Click on Infrastructure Environment to return to the main view.

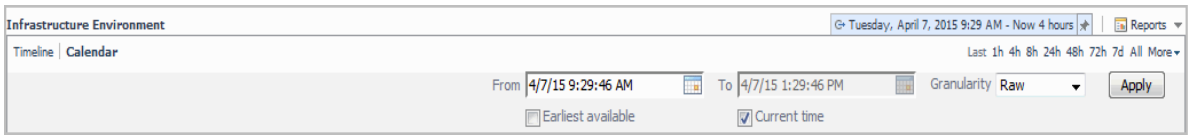
Figure 2. Breadcrumb trail

Time range

The default behavior of Foglight for SNMP is to display metrics, alerts, and messages that have occurred within the last four hours. This time range, however, is configurable.

To configure the time range, use the Time Range popup, which you can access from the upper right corner of the Foglight for SNMP browser interface.

Figure 3. Time range



Using the Time Range popup, you can select from predefined time ranges or you can specify a custom range using calendar precision controls to specify dates and times. When you modify the time range for a dashboard or view, it adjusts the range for all of the views contained within and drill-downs accessed from that dashboard or view. It does not adjust the time range for any parent views.

Sortable lists

Foglight for SNMP tables contain sortable lists. Clicking a column heading once sorts the list in ascending order. Clicking the column heading again re-sorts the list in descending order.

This is handy when you want to have an organized view sorted by name, status, or some other criterion.

Exporting SNMP Tables

If you want to investigate the results in a table or forward them to a third-party, you can export the table.

To export an SNMP table:

1. On the Infrastructure Environment dashboard, select a host monitored by an SNMP agent.
2. Click **Explore**.
3. Select the desired tab to display the table you wish to export.
4. Click the Customizer icon at the top right of the table.
5. On the popup that opens, click **Export**.
6. On this new popup, select an export format.

   The table is exported in the format you selected.

Alarms and status indicators

Foglight for SNMP uses status indicators to show the alarm status of SNMP-managed devices. Four status indicators (fatal, critical, warning, and normal) are used throughout the Foglight for SNMP views.

Mouse-over actions

Many items within the Foglight for SNMP views display additional information when you hover the cursor over them. For example, when you hover the cursor over a graph you are likely to see a specific value or values that correspond to the position of the cursor. When you hover the cursor over an individual metric, you are likely to see a small descriptive popup.

Monitoring with both Host and SNMP Agents

A host can be monitored simultaneously by both an Infrastructure agent and an SNMP agent. For hosts monitored by both Infrastructure and SNMP agents, the two agents will collect different sets of information. The Infrastructure agent will gather data on the processor, network interface, disk, and memory. The SNMP agent will collect additional metrics not available in the Infrastructure cartridge such as 'Windows Installed Programs'.

However, monitoring a host simultaneously using both an Infrastructure and an SNMP agent is not recommended.

SNMP Communities and Credentials

When you run network discovery, selecting the correct credentials is essential in order for Foglight for SNMP to access the devices in a network. When a device is discovered during a scan of the network, Foglight for SNMP will add it to the database. If you incorrectly set the credentials for that device, Foglight for SNMP cannot monitor and collect data from it.

In the **Discover Device(s)** wizard, choose the correct credential for the devices in the network. Select a credential for one of the following protocols:

- SNMP Version 1 Credential
- SNMP Version 2 Credential
- SNMP Version 3 Credential

From the **Discover Device(s)** wizard, you can add new credentials by clicking the Manage all credentials link. For more information, see Accessing the Manage all credentials wizard.

Accessing the Manage all credentials wizard

You should only add or remove credentials via the Manage all credentials wizard.

To access the Manage all credentials wizard

1. On the navigation panel, click **Infrastructure**.
2. On the Infrastructure Environment dashboard, click **SNMP Hosts**.
3. Under **IP Address to Discover**, add either a single IP address and SNMP Port, or a range of IP addresses and SNMP Port.
4. Click **Next**.
5. On the Assign Credential page, click **Manage all credentials**.
6. To add or remove Communities and Credentials, follow the procedures in either Managing SNMP V1 or V2c Community Strings, or Managing the SNMP V3 Credentials.

Managing SNMP V1 or V2c Community Strings

There are two default community strings: public (read-only) and private (write). You can add more community strings. All community strings must be unique. Therefore, you may have to run the **Discover Device(s)** wizard more than once to properly discover all devices in the network.

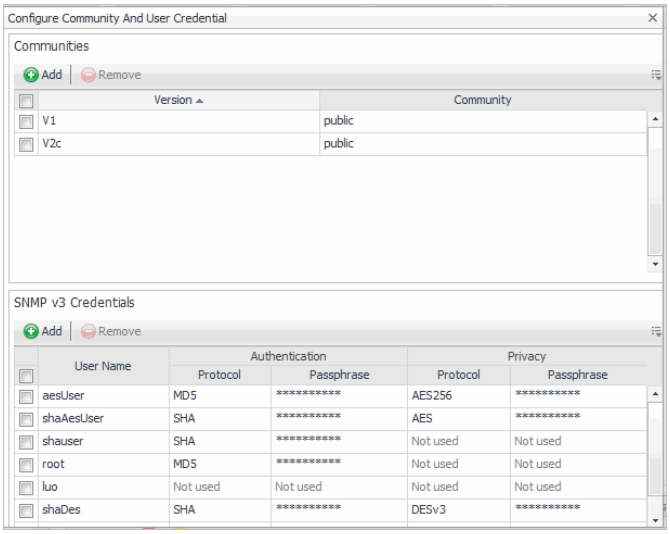
IMPORTANT: Add or remove credentials via the Manage all credentials wizard only.

Adding SNMP V1 or V2c Community Strings

To add an SNMP V1 or V2c community string:

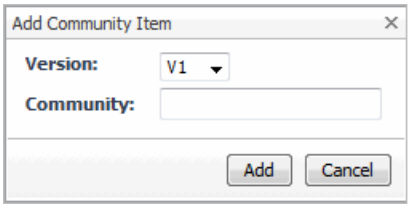
1. Open the Configure Community and User Credential dialog box, as described in Accessing the Manage all credentials wizard.

Figure 4. The Configure Community And User Credential dialog box opens.



2 In the Communities table, click **Add**.

Figure 5. The Add Community Item dialog box opens.



3 Select the version: **V1** or **V2c**.

4 In the **Add Community Item** dialog box, type a unique community string name.

5 Click **Add**.

Removing SNMP V1 or V2c Community Strings

Community strings cannot be removed if they are being used to manage devices.

To remove an SNMP V1 or V2c community string:

1 Open the Configure Community and User Credential dialog box, as described in Accessing the Manage all credentials wizard.

2 In the Communities table, click the check box next to the community string that you want to remove.

The **Remove** button becomes enabled.

3 Click **Remove**.

The **Remove Community Items** dialog box opens.

4 Click **OK**.

Managing the SNMP V3 Credentials

You can add multiple credentials. All credentials must be unique. You may have to run the **Discover Device(s)** wizard more than once to properly discover all devices in the network.

IMPORTANT: Add or remove credentials through the Manage all credentials wizard only.

Adding SNMP V3 Credentials

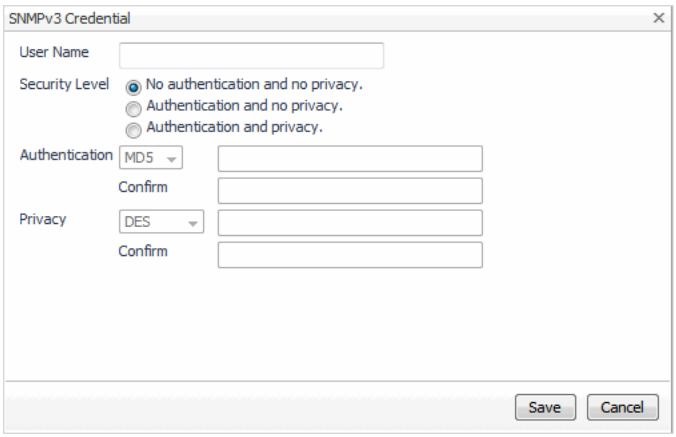
Credentials can be added, edited, and removed.

To add SNMP V3 credentials:

1 Open the Configure Community and User Credential dialog box, as described in Accessing the Manage all credentials wizard.

2 In the **SNMP v3 Credentials** table, click **Add**.

Figure 6. The SNMPv3 Credential dialog box opens.



3 Type the user name that will be used for authentication.

NOTE: Foglight for SNMP does not support multiple SNMP V3 credentials with different passwords for the same user name.

4 Select a **Security Level**:

- **No authentication and no privacy** — the identity of the sender is not verified.
- **Authentication and no privacy** — the identity of the sender is verified, but the information is not encrypted.
- **Authentication and privacy** — the identity of the sender is verified and the information is encrypted.

5 If the **Security Level** that you selected requires authentication, select an authentication protocol and type the passphrase. The passphrase is the password of the specified user name.

6 If the **Security Level** that you selected requires privacy, select a privacy protocol and type the passphrase. The passphrase is the encryption key.

Removing SNMP V3 Credentials

Credentials cannot be removed if they are being used to manage devices.

To remove SNMP V3 credentials

1 Open the Configure Community and User Credential dialog box, as described in Accessing the Manage all credentials wizard.

2 In the **SNMP v3 Credentials** table, click the check box next to the set of credentials that you want to remove.

The **Remove** icon becomes enabled.

3 Click **Remove**.

The **Remove User Credential Items** dialog box opens.

4 Click **OK**.

Changing an SNMP Agent Credential

You can change the credential that is used to monitor a host.

To change a credential

1. Log in to the Foglight browser interface. On the navigation panel, under **Dashboards**, click **Administration > Agents > Agent Status**.
2. Select the agent for which you want to change a credential and, in the toolbar, click **Edit**.
3. Click **Edit Properties**.
4. Click **Modify the private properties for this agent**.
5. Scroll down to locate the Credentials property.
6. Click the **Edit** button on the right side of the **Credentials** property.

   The credentials table opens.
7. Record the ID of the credential and close the table. For example, `default_credential_V1_id`.
8. Click the **Edit** button on the right side of the **Devices** property.

   The devices list table opens.
9. Select the desired device and double click the Credential field.
10. Enter the ID of the credential recorded in Step 7 in the Credential field.
11. Click **Save Changes**.

Managing Monitor Configurations

A monitor is a group of OIDs used to communicate with an SNMP agent. A typical SNMP monitoring environment contains a combination of built-in and user configured OIDs.

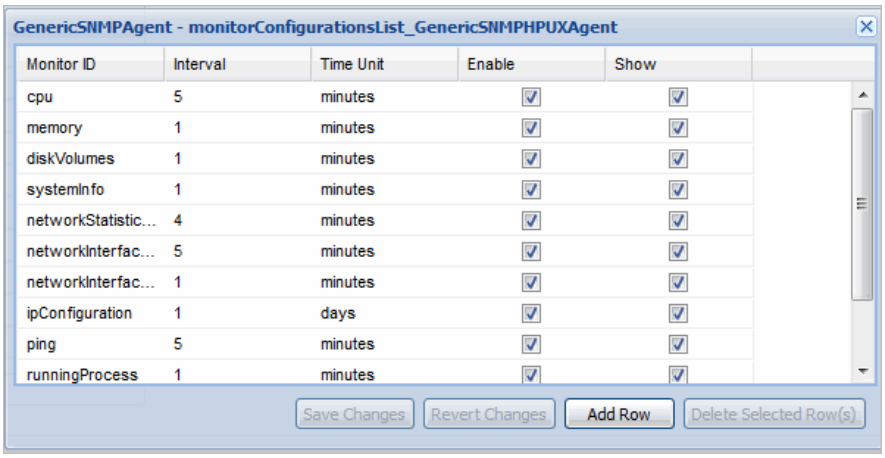
Foglight for SNMP provides pre-defined monitors that collect key data for most of the common devices in a network. When you create a custom SNMP monitor, you can define any Object Identifier (OID) to an MIB node in order to monitor any SNMP device (regardless of the manufacturer or type of device).

For example, you can monitor temperature on a switch, fan speed on a router, and battery status on a UPS. Custom SNMP monitors enable Foglight for SNMP to provide complete SNMP coverage on any network.

To manage monitor configurations:

1. Log in to the Foglight browser interface. On the navigation panel, under **Dashboards**, click **Administration > Agents > Agent Status**.
2. Select the SNMP agent type for which you want to configure an SNMP monitor and, in the toolbar, click **Edit**.
3. Click **Edit Properties**.
4. Click **Modify the private properties for this agent**.
5. In the **Devices and Collection OIDs** section, locate the **Monitor Configurations** property.
6. Click the **Edit** button for this property.

Figure 7. A table of the properties specific to the selected agent type opens.



NOTE: For the **Show** column:

- if the **Show** column is unchecked, the **Enable** column should be unchecked as well.
- if the **Show** column is checked, the **Enable** column can be checked or unchecked.

7 Modify the fields, as necessary:

IMPORTANT: Do NOT modify the Monitor ID.

- Interval — The time during which the agent collects data.
- Time Unit — The time unit associated with the **Interval** property. Supports minutes, hours, days, and `cron`.

  NOTE: For information on how to use `cron`, see the *Foglight Agent Manager Guide*.

- Enable — Indicates whether data collection from the monitor is enabled or disabled.
- Show — Indicates whether the monitor is available for configuring through the UI.

8 Click **Save Changes**.

The new settings are saved for the selected agent.

Discovering SNMP Devices

Foglight for SNMP uses SNMP to discover devices in a network and then to provide a complete set of attributes for each discovered device. This type of network discovery gathers data relating to hardware, software, and processes for each device, and identifies devices by responding status, protocols, type, and operating system.

To discover a device by SNMP, provide the SNMP credentials for the device and make sure that you have the correct port open so that the target machine can accept SNMP packets from that device. Foglight for SNMP uses generic SNMP agent instances to collect information from monitored SNMP devices.

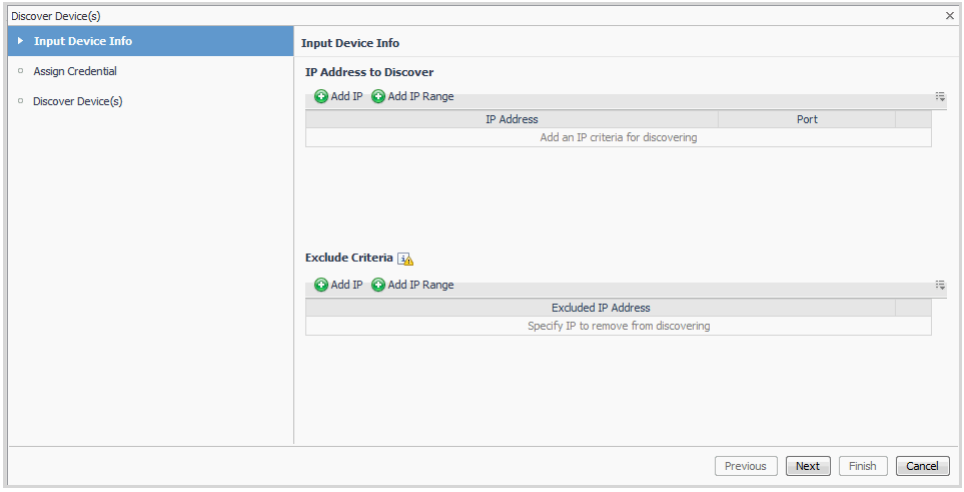
To discover a device and start monitoring it, use the **Discover Device(s)** wizard, which is accessible from the Infrastructure Environment dashboard.

To discover a device:

1 On the navigation panel, under **Dashboards**, click **Infrastructure**.

2 On the Infrastructure Environment dashboard, click **SNMP Hosts**.

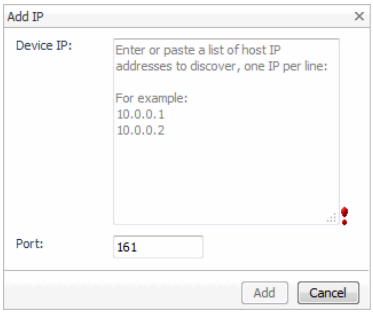
Figure 8. The Discover Device(s) wizard opens.



3 In the **IP Address to Discover** section, add a single IP address or a range of IP addresses to be discovered.

- Click **Add IP** to specify an IP address and SNMP Port.

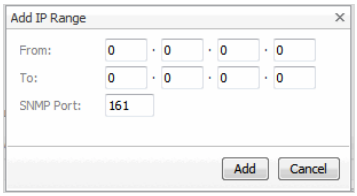
Figure 9. The Add IP dialog box.



or

- Click **Add IP Range** to specify a range of IP addresses and an SNMP Port.

Figure 10. The Add IP Range dialog box.



For example, an IP address range of 10.10.120.1 - 10.10.121.2 adds the following IP addresses: 10.10.120.1, 10.10.120.2, 10.10.121.1, and 10.10.121.2.

4 In the Exclude Criteria table, specify any IP addresses to be excluded from discovery.

- Click **Add IP** to specify the IP address that should be excluded.

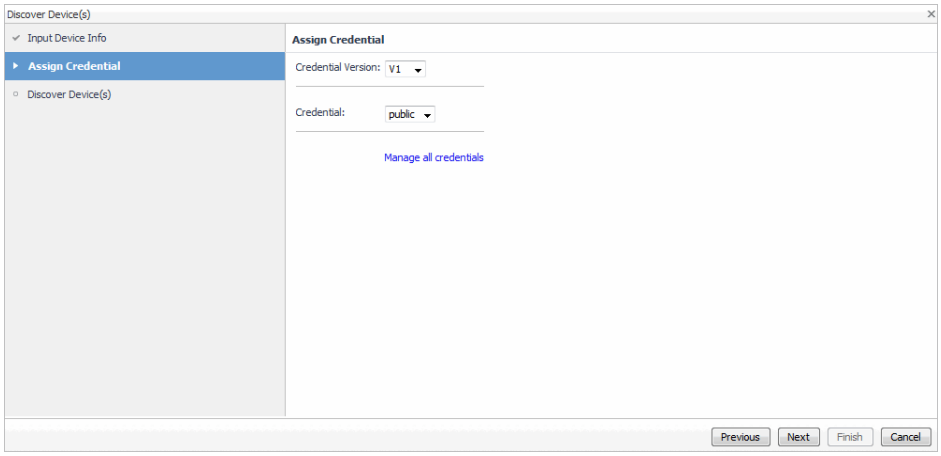
NOTE: Click **Exclude Criteria** to see a list of IP addresses that are excluded by default.

or

- Click **Add IP Range** to specify a range of IP addresses to be excluded.

5 Click **Next**.

Figure 11. The Assign Credential page opens.



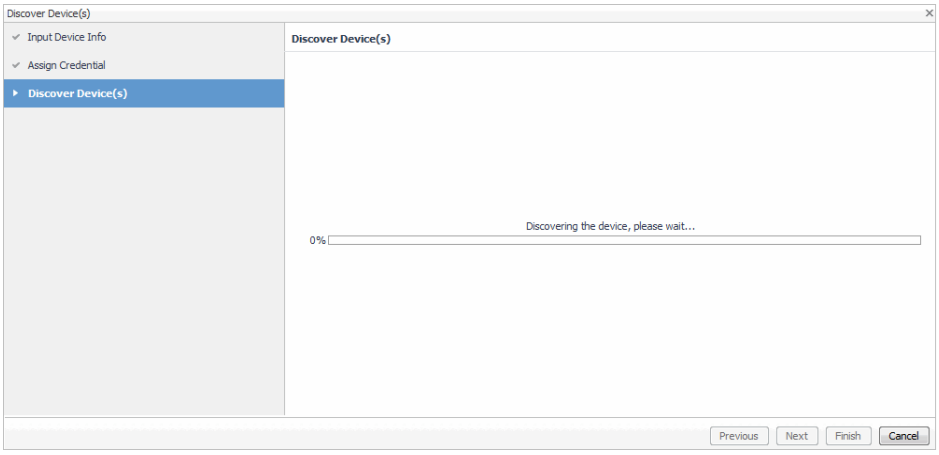
6 On the **Assign Credential** page, specify the SNMP credential version and the community string required to discover devices, and then click **Next**:

- **Credential Version** — The version of SNMP to be used to monitor the host.
- **Credential** — SNMP community string. The default is public.

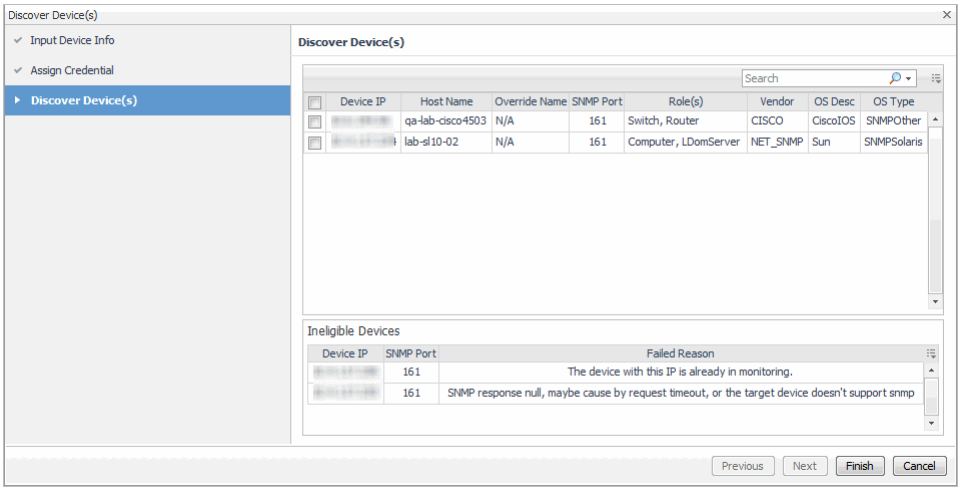
NOTE: Click **Manage all credentials** to add Communities and Credentials. For information on how to add or remove Communities and Credentials, see Managing SNMP V1 or V2c Community Strings on page 7 and Managing the SNMP V3 Credentials on page 8.

7 Click **Next**.

Figure 12. The Discover Device(s) page opens.



The **Discover Device(s)** page refreshes and displays a list of discovered and ineligible devices. For more information on ineligible devices, see Ineligible Devices.



8 Select one or more devices.

> **NOTE:** You can provide an override name by editing the Override Name field. The name you supply will be used as the identity of that host.

9 Click **Finish**.

Ineligible Devices

SNMP devices can be deemed ineligible for one of the following reasons:

- The device is already being monitored.
- The host is unreachable and ICMP ping failed.
- SNMP failed either because of a request timeout or the target device does not support SNMP.
- The target device's host name is empty.

Viewing SNMP Monitored Hosts

SNMP monitored hosts can be viewed from the Infrastructure Environment dashboard.

Viewing Information Collected From SNMP Devices

When you select a monitored host and display its resource utilization views in the Quick View, you can drill down to a detailed view to explore that host's activity. For example, selecting a Windows® host and choosing **Explore** displays a monitoring dashboard that helps you understand the state of the host's resources and how they affect your monitored system as a whole.

To drill down on an SNMP monitored host

To select an SNMP monitored host:

1 On the navigation panel, under **Dashboards**, click **Infrastructure**.

The Infrastructure Environment dashboard opens.

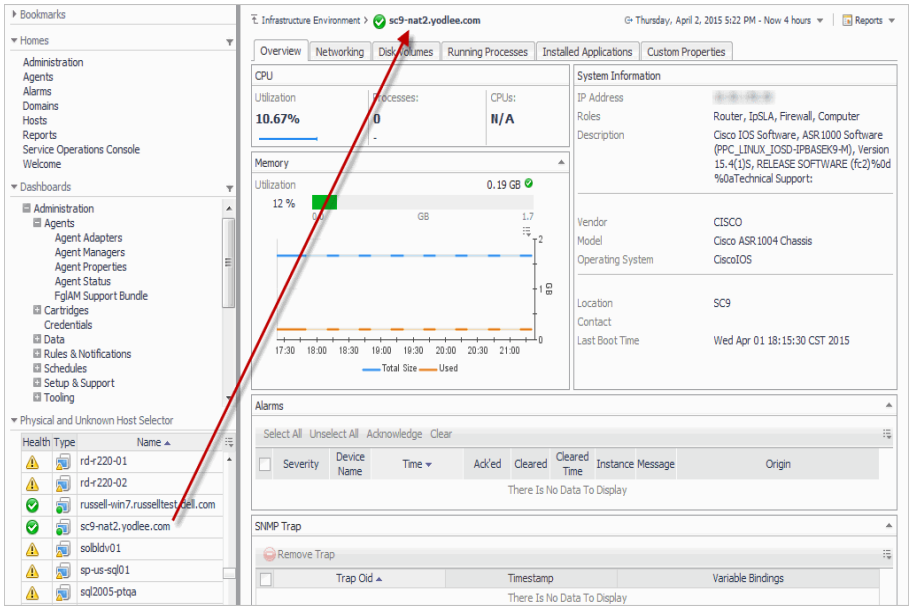
2 Select a monitored host from the list of hosts in the view on the left.

3 In the top-right corner of the **Resource Utilizations on *hostname*** view, click **Explore**.

> **NOTE:** If the host is also monitered by an Infrastructure agent, the Monitor tab appears in addition to SNMP-related tabs.

In addition to the information displayed in the right-hand panel the **Physical and Unknown Host Selector** is displayed on the navigation panel. Selecting a different monitored host refreshes the information displayed.

Figure 13. Physical and Unknown Host Selector in the navigation panel.



When you drill down into various levels across dashboards, a trail of breadcrumbs is left at the top of the current dashboard. This trail provides you with a simple path for returning to the main Infrastructure Environment view.

Click **Infrastructure Environment** in the breadcrumb to return to the main view.

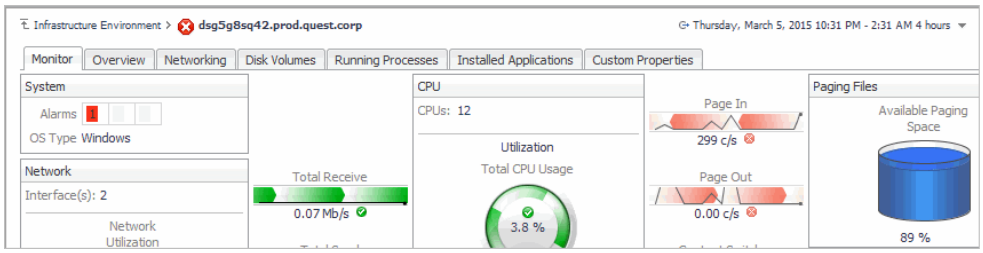
Figure 14. Example of a breadcrumb trail.

Hosts Monitored by both an Infrastructure and SNMP Agent

When a host is monitored by both an Infrastructure and an SNMP agent, you will see an Infrastructure-related Monitor tab as well as various SNMP tabs. SNMP tabs include Overview, Networking, and Disk Volumes.

> **NOTE:** The number of SNMP tabs is dynamic depending on which monitors have been enabled for the operating system selected. For example, if you disable the diskVolumes monitor for Windows, then the **Disk Volumes** tab is hidden.

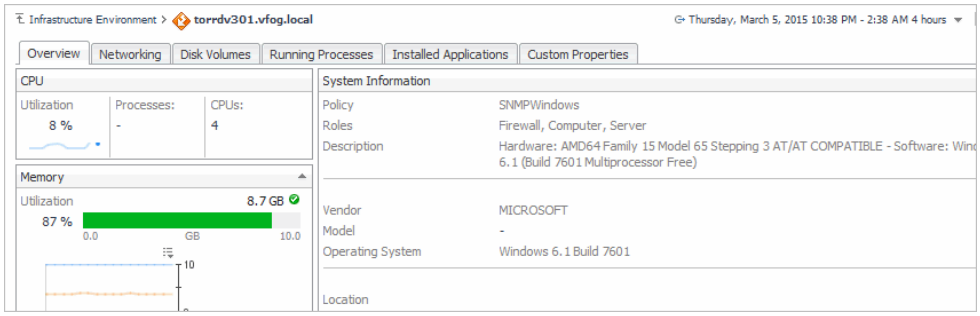
Figure 15. Example of a host monitored by both an Infrastructure and an SNMP agent.



Hosts Monitored only by SNMP

When a host is monitored by an SNMP agent only, just SNMP related tabs will be displayed. SNMP tabs include Overview, Networking, and Disk Volumes.

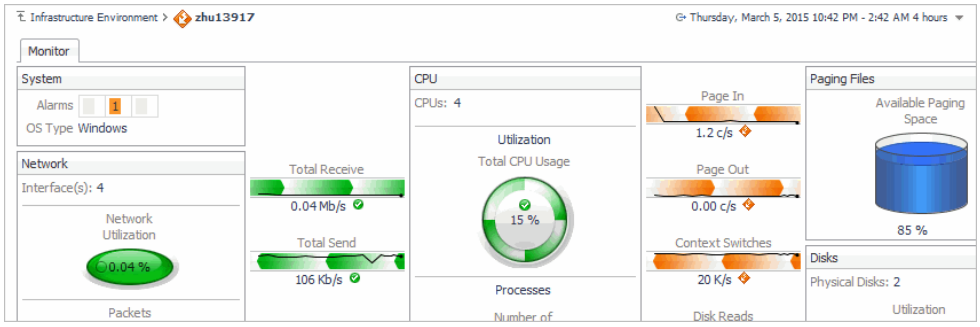
Figure 16. Example of a host monitored only by an SNMP agent.



Hosts Monitored only by an Infrastructure Agent

When a host is monitored by an Infrastructure agent only, one Infrastructure-related Monitor tab is displayed.

Figure 17. Example of a host monitored only by an Infrastructure agent.



For more information on the Monitoring tab, see ‘Exploring the Monitoring Tab’ in the *Foglight for Infrastructure User and Reference Guide*.

Generating Reports

Reports are a convenient way to share data about your monitored SNMP environment with others in your organization.

To run the report associated with the Infrastructure Environment dashboard:

1 On the Infrastructure Environment dashboard, click **Reports** in the upper-right corner.

2 In the list that appears, click **Hosts**. This is the report associated with the Infrastructure Environment dashboard.

3 On the Set Input Parameters page of the Hosts report wizard, select the input parameters for the report from the *Time Range* and the *Service* lists. Click **Next**.

4 On the Set Properties page, type a name for the report, select a format for it, and type the email addresses of the people who should receive this report.

5 Optional — click the **Schedule This Report** check box to schedule the report delivery.

6 In the **Retain** box, specify the number of copies of the report to be retained, then click **Next**.

If you selected to schedule the report, the Select Schedule page appears. Continue with Step 7.

If you did not select to schedule the report, the Summary page appears. Continue with Step 8.

7 On the Select Schedule page, select a schedule type from the list of available options, or click **New Schedule** to define a custom schedule, then click **Next**.

8 On the Summary page, review the settings defined, then click **Finish**.

The report is generated and delivered to the recipients indicated in the report settings.

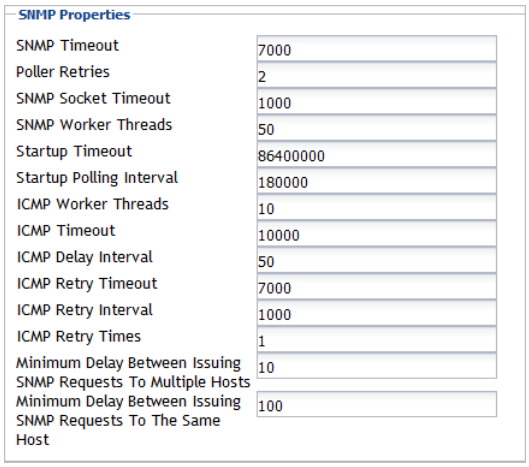
Configuring SNMP Agent Properties

The SNMP agent includes the following groups of agent properties:

- SNMP Properties
- Devices and Collection OIDs
- Credentials

SNMP Properties

Figure 18. SNMP Properties.

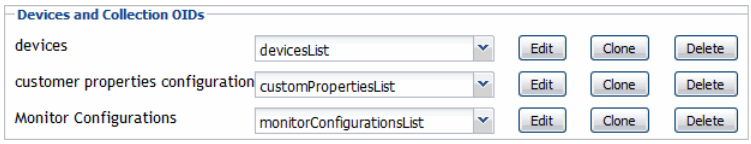


- **SNMP Timeout:** Timeout in milliseconds before a confirmed request from a device is received.
- **Poller Retries:** Retry times for retrieving the data if timeout.

- **SNMP Socket Timeout:** UDP socket timeout for incoming messages in milliseconds. A timeout of zero is interpreted as an infinite timeout.
- **SNMP Worker Threads:** The number of threads used to perform different SNMP collections concurrently.
- **Startup Timeout:** Total time limit trying to start monitoring the device. During this time, the device would be started several times.
- **Startup Polling Interval:** The interval between each attempt to start the device.
- **ICMP Worker Threads:** The number of threads which were used for ICMP Ping when doing the discovery.
- **ICMP Timeout:** The time, in milliseconds, before the call aborts.
- **ICMP Delay Interval:** The delay interval between each ICMP retry.
- **ICMP Retry Timeout:** Timeout for ICMP retry.
- **ICMP Retry Interval:** Retry interval for ICMP.
- **ICMP Retry Times:** Retry times for Internet Control Message Protocol.
- **Minimum delay between issuing SNMP requests to multiple hosts:** Guarantees at least a delay of the set value between subsequent requests to the same host.
- **Minimum delay between issuing SNMP requests to the same host:** Ensures at least a delay of the set value between consecutive requests to any host.

Devices and Collection OIDs

Figure 19. Devices and Collection OID properties.



- **Devices:**

  All properties are read-only, except where noted. Each entry in the list includes the following columns:

  - IP Address: The IP address of the target device.
  - Override Name: The user-supplied name used as the identity of the host.
  - SNMP Port: Port for SNMP discovery and monitoring.
  - Credential: The ID of a credential's secondary property. (Editable).

    NOTE: To obtain the id of an SNMP version, click the **Edit** button to the right of the credentials property.

  - Vendor: The vendor name of the target device.
  - Is Monitoring: A flag indicating whether the target device is monitoring or not. (Editable).
  - Is Monitored By IC: A flag indicating whether the target is monitored by an Infrastructure agent.
- **Custom Properties Configuration:**

  Each entry in the list includes the following columns:

  - OID: User customized OID.
  - Alias: The alias of the OID.
  - OID Type: The OID type. Supports string, metric, and tables.

- Parent ID: The OID of the parent table. Required to maintain the relationship between columns and the table.
- Editable: A flag indicating whether this OID is editable or not. A user added OID is editable.
- Enable: A flag indicating whether this monitor is collecting for this OID or not.

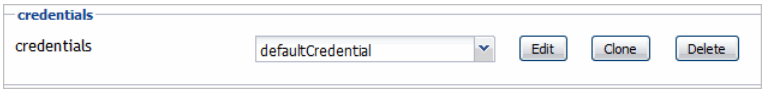
- **Monitor Configurations:**

  Each entry in the list includes the following columns:

  - Monitor ID: The identity of the monitor. Do not edit or change this ID.
  - Interval: Interval for collecting this monitor.
  - Time Unit: The interval time unit.
  - Enable: A flag indicating if this monitor is collecting for this OID or not.
  - Show: False means this monitor is removed from this agent and may not be edited anymore.

Credentials

Figure 20. Credentials properties.



- **Credentials:**

  Each entry in the list includes the following columns:

  - ID: The identity of the credential.
  - Version: SNMP version. Supports V1, V2c, and V3.
  - Community: SNMP community string. The default is public.
  - User ID: System generated ID.
  - User Name: V3 credential user name.
  - Auth Type: Authentication type. Supports MD5 and SHA.
  - Auth Password: Authentication password.
  - Privacy Type: Privacy type. Supports DES, DESv3, AES, AES128, AES192, and AES256.
  - Privacy Password: Privacy password.

Foglight for SNMP Reference

The SNMP Monitored Host view contains the following tabs:

- Overview tab
- Networking tab
- Disk Volumes tab
- Running Processes tab
- Installed Applications tab
- Custom Properties tab

Overview tab

This tab displays only when a host is monitored by an SNMP agent. If a host is not monitored by an SNMP agent then the **Overview** tab does not display.

Purpose

If a host is monitored by an Infrastructure agent, the Overview tab displays system information, alarms, and SNMP traps. If a host is not monitored by an infrastructure agent, CPU and memory information will also be displayed.

Figure 21. Overview tab: Host monitored by SNMP agent AND Infrastructure agent

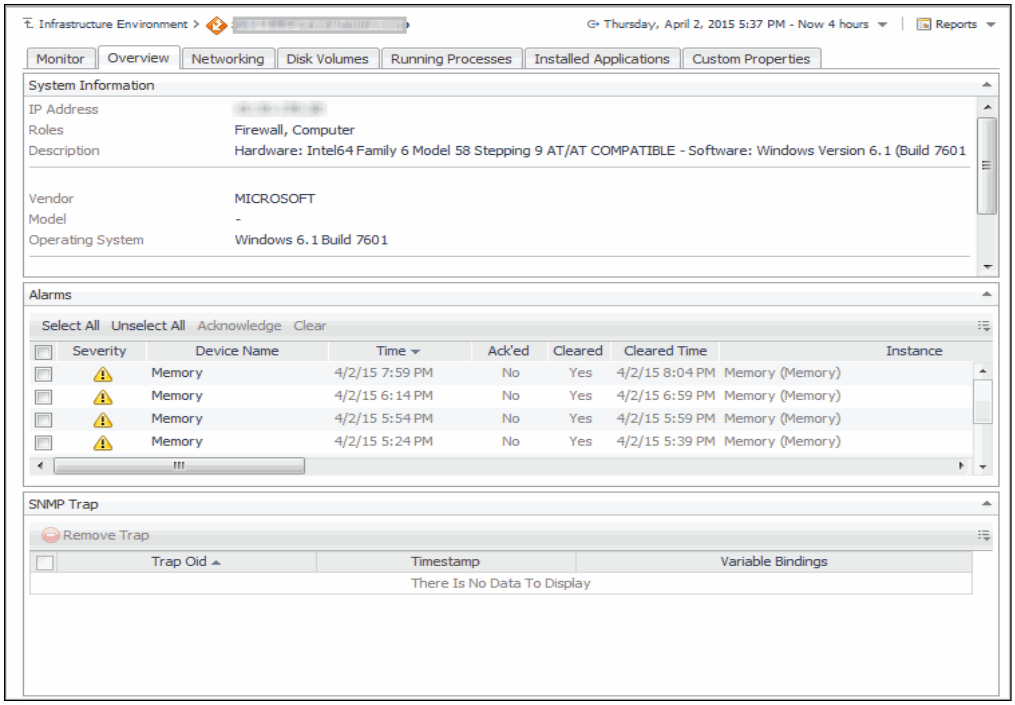
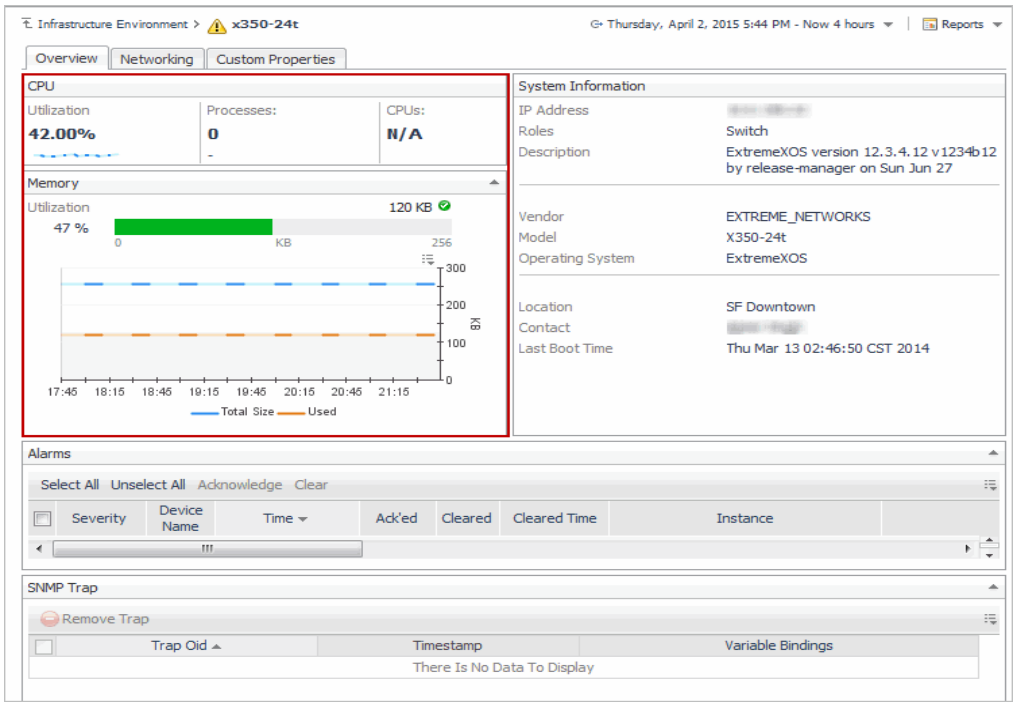


Figure 22. Overview tab: Host monitored by SNMP agent only



How to Get Here

1 On the Infrastructure Environment dashboard, select a host monitored by an SNMP agent.

2 Click **Explore**.

Description of embedded views

This view is made up of the following embedded views:

- Alarms
- CPU
- Memory
- SNMP Trap
- System Information

Alarms

Table 1. Alarms view

Description	This view shows the number of alarms associated with the monitored device.
Data Displayed	• Severity — The alarm severity. • Device Name — The device which generated the alarm. • Time — The date and time the alarm was generated. • Ack'ed — Indicates if the alarm is acknowledged. • Cleared — Indicates if an alarm has been cleared. • Cleared Time — Displays the time the alarm was cleared. • Instance — The object against which the alarm was generated. • Message — A message explaining the reason for this alarm. • Origin — The origin of the alarm.

CPU

Table 2. CPU view

Description	Monitors the number of processors, current usage, and average usage over time from a device.
Data Displayed	• Utilization — The current percentage of time the CPU spends executing both system and user code. • Processes — The number of processes that are waiting in the run queue. • CPUs — The total number of CPUs available.

Memory

Displays the total amount of memory usage for the host.

Table 3. Memory view

Description	Displays the current memory utilization percentage and the utilization percentage over time.
Data Displayed	• Utilization, bar — The current memory utilization of the monitored device. • Utilization, in graph — The total memory available and the memory utilization of the monitored device over the selected time range.

NOTE: Hover the cursor over the lines on the utilization graph to see additional information.

SNMP Trap

Table 4. SNMP Trap view

Description	The notification messages received from SNMP-managed devices.
Data Displayed	• Trap Oid — The Object Identifier (OID) of the trap as defined in the MIB file. • Timestamp — The time elapsed between the last reinitialization of the network and the generation of the trap. • Variable Bindings — The pairing of the name of a variable to the variable's value.

System Information

Table 5. System Information view

Description	Provides device IP address, device type and roles, operating system, and other detailed system information for a device.
Data Displayed	• IP Address — The primary IP address of the host. • Roles — Network device types. For example, printer, switch, router, VMHost, phone, firewall, and LDom server. • Description — A text description of the entity. • Vendor — The name of the manufacturer of the monitored device. • Model — The vendor-specific model name identifier string associated with this physical component. • Operating System — The operating system installed on the host. • Location — The physical location of the monitored device. • Contact — The contact person for this monitored node, together with information on how to contact this person. • Last Boot Time — The time (in hundredths of a second) since the network management portion of the system was last re-initialized.

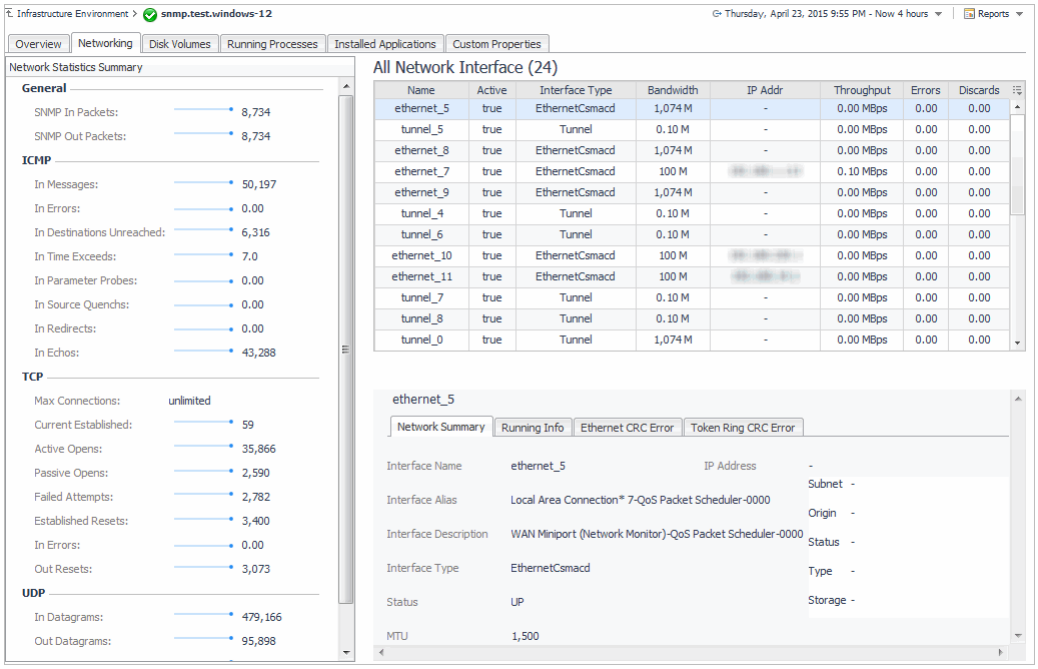
Networking tab

This tab displays only when a host is monitored by an SNMP agent. If a host is not monitored by an SNMP agent then the **Networking** tab does not display.

Purpose

Through two embedded views (All Network Interface (xx) and Network Statistics Summary), the Networking view enables you to view information pertaining to monitored network interfaces.

Figure 23. Networking view



How to Get Here

1. On the Infrastructure Environment dashboard, select a host monitored by an SNMP agent.
2. Click **Explore**.

Description of embedded views

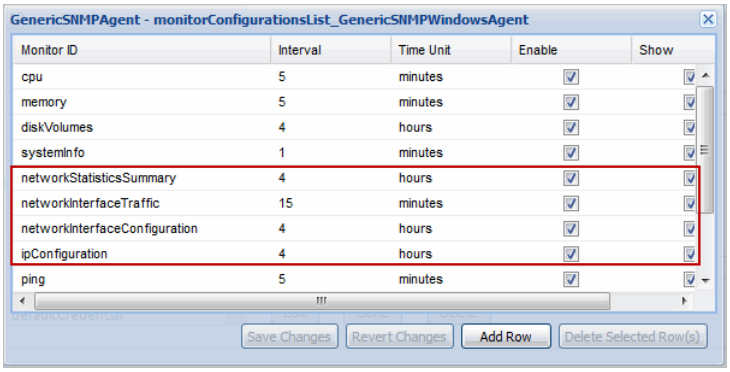
This view is made up of the following embedded views:

- All Network Interface (xx)
- Network Statistics Summary

Pre-defined Foglight for SNMP Network Monitors

The networking tab is populated by four different pre-defined Foglight for SNMP network monitors.

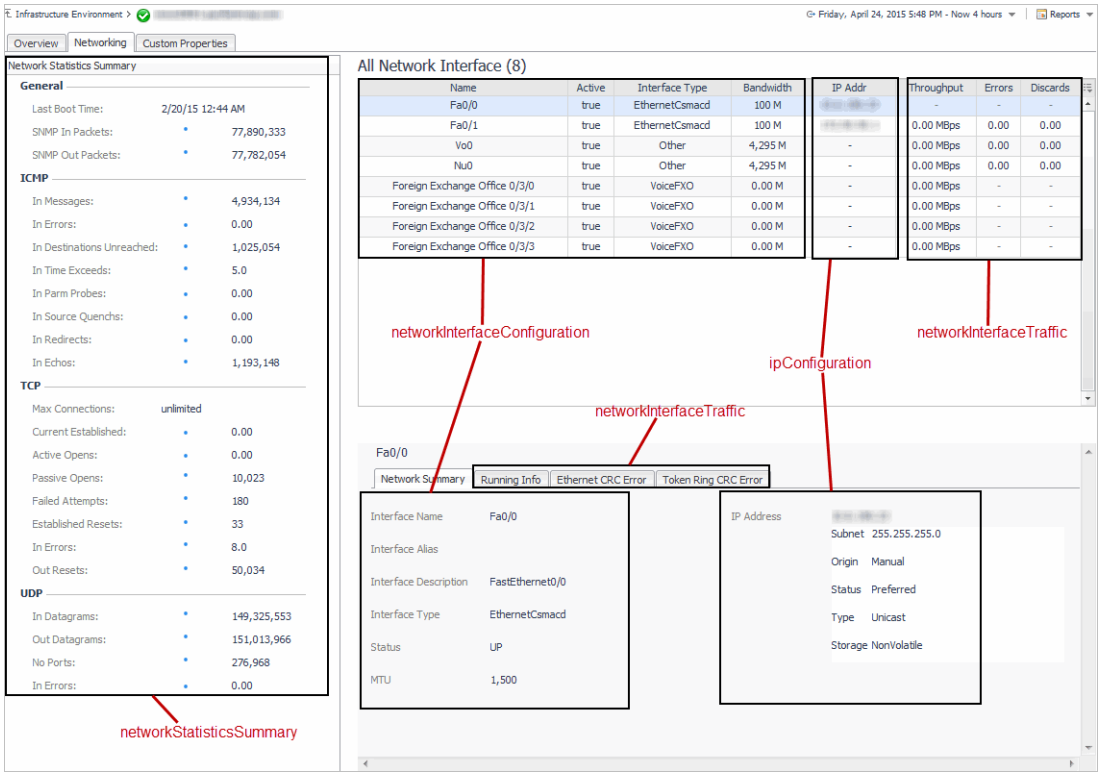
Figure 24. Pre-defined Foglight for SNMP Network Monitors



- networkStatisticsSummary — Collects the network summary data for a host, such as ICMP, UDP, and so on.
- networkInterfaceTraffic — Collects traffic data for each network interface, for example, 'Running Info', 'Ethernet CRC Error', 'Token Ring CRC Error'.
- networkInterfaceConfiguration — Collects network configuration data, such as interface name, type, status, and so on.
- ipConfiguration — Collects network interface IP information, such as IPAddress, Subnet, Storage, and so on.

For information on configuring network monitors, see Configuring SNMP Agent Properties on page 17.

Figure 25. Data Collected by Pre-defined Foglight for SNMP Network Monitors



All Network Interface (xx)

The All Network Interface (xx) view displays a table listing all monitored network interfaces associated with the selected device. Selecting a particular network interface refreshes the view below the table to display detailed information about that network interface.

The view title displays in a numeric format within brackets the number of monitored network interfaces.

Table 6. All Network Interface view

Description	The network data related to the monitored device.
Data Displayed	• Name — The network interface name. • Active — The current operational state of the interface. • Interface Type — The type of interface. • Bandwidth — The maximum data transfer rate of the network interface. • IP Addr — The IP address of the network interface. • Throughput — The average rate of network throughput. • Errors — The number of data packets that contain errors, over the selected time range. • Discards — The number of packets which were chosen to be discarded even though no errors had been detected to prevent their being transmitted.

The detailed view of the selected network interface is made up of the following embedded views

Network Summary tab

Table 7. Network Summary view

Data Displayed	• Interface Name — The network interface name. • Interface Alias — This object is an 'alias' name for the interface as specified by a network manager, and provides a non-volatile 'handle' for the interface. • Interface Description — A textual string containing information about the interface. • Interface Type — The type of interface, designated by the physical link protocols immediately below the network layer in the protocol stack. • Status — The desired state of the interface. • MTU — The size of the largest datagram that can be sent or received on the interface, specified in octets. • IP Address: The IP address of the network interface. - Subnet: The subnet mask associated with the IP address of this entry. - Origin: The origin of the address. - Status: The status of the address, describing if the address can be used for communication. - Type: The type of address, unicast(1), anycast(2), broadcast(3). - Storage: The storage type for this conceptual row. If this object has a value of 'permanent', then no other objects are required to be able to be modified.

Running Info tab

This view displays information about network transmission pertaining to received and sent packets, including errors, discards, unicast, broadcast and multicast packets. With this information, you can easily analyze the network interface's network data transmission.

Table 8. Running Info view

Data Displayed	• Throughput — The average rate of network throughput. • Received — The amount of data received from the network. • Transmitted — The amount of data sent to the network. • In: - In Error: For packet-oriented interfaces, the number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol. For character-oriented or fixed-length interfaces, the number of inbound transmission units that errors preventing them from being deliverable to a higher-layer protocol. - In Discards: The number of inbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. - In Unknown Protocols: For packet-oriented interfaces, the number of packets received via the interface which were discarded because of an unknown or unsupported protocol. For character-oriented or fixed-length interfaces which support protocol multiplexing the number of transmission units received via the interface which were discarded because of an unknown or unsupported protocol. For any interface which does not support protocol multiplexing, this counter will always be 0. - In Ucast Packets: The number of packets, delivered by this sub-layer to a higher (sub-)layer, which were not addressed to a multicast or broadcast address at this sub-layer. - In Multicast Packets: The number of packets, delivered by this sub-layer to a higher (sub-)layer, which were addressed to a multicast address at this sub-layer. For a MAC layer protocol, this includes both Group and Functional addresses. - In Broadcast packets: The number of packets, delivered by this sub-layer to a higher (sub-)layer, which were addressed to a multicast or broadcast address at this sub-layer. • Out: - Out Error: The number of outbound data packets that contain errors, over the selected time range. - Out Discards: The number of outbound packets which were chosen to be discarded even though no errors had been detected to prevent their being transmitted. - Out Queue Length: The length of the output packet queue (in packets). - Out Ucast Packets: The total number of packets that higher-level protocols requested be transmitted, and which were not addressed to a multicast or broadcast address at this sub-layer, including those that were discarded or not sent. - Out Multicast Packets: The total number of packets that higher-level protocols requested be transmitted, and which were addressed to a multicast address at this sub-layer, including those that were discarded or not sent. For a MAC layer protocol, this includes both Group and Functional addresses. - Out Broadcast Packets: The total number of packets that higher-level protocols requested be transmitted, and which were addressed to a broadcast address at this sub-layer, including those that were discarded or not sent.

Ethernet CRC Error tab

When a failure occurs during data transmission on an ethernet network, it is always difficult to determine whether it is a link failure or a port fault. The information displayed on this view helps you analyze ethernet problems.

Table 9. Ethernet CRC Error view

Data Displayed	• IS Hcounter — High Capacity Counter objects. If the dot3HCStatsTable has an entry, this interface will be set as HCounter. • Alignment Errors — A count of frames received on a particular interface that are not an integral number of octets in length and do not pass the FCS check. • FCS Errors — A count of frames received on a particular interface that are an integral number of octets in length but do not pass the FCS check. • Single Collision Frames — A count of frames that are involved in a single collision, and are subsequently transmitted successfully. • Multiple Collision Frames — A count of frames that are involved in more than one collision and are subsequently transmitted successfully. • SQE Test Errors — A count of times that the SQE TEST ERROR is received on a particular interface. The SQE TEST ERROR is set in accordance with the rules for verification of the SQE detection mechanism in the PLS Carrier Sense Function as described in IEEE Std. 802.3, 2000 Edition, section 7.2.4.6. • Deferred Transmissions — A count of frames for which the first transmission attempt on a particular interface is delayed because the medium is busy. • Late Collisions — The number of times that a collision is detected on a particular interface later than one slotTime into the transmission of a packet. • Excessive Collisions — A count of frames for which transmission on a particular interface fails due to excessive collisions. • Internal Mac Transmit Errors — A count of frames for which transmission on a particular interface fails due to an internal MAC sublayer transmit error. • Carrier Sense Errors — The number of times that the carrier sense condition was lost or never asserted when attempting to transmit a frame on a particular interface. • Frame Too Longs — A count of frames received on a particular interface that exceed the maximum permitted frame size. • Internal Mac Receive Errors — A count of frames for which reception on a particular interface fails due to an internal MAC sublayer receive error. • Symbol Errors — For an interface operating at 100 Mb/s, the number of times there was an invalid data symbol when a valid carrier was present. • Rate Control Ability — 'true' for interfaces operating at speeds above 1000 Mb/s that support Rate Control through lowering the average data rate of the MAC sublayer, with frame granularity, and 'false' otherwise. • Rate Control Status — The current Rate Control mode of operation of the MAC sublayer of this interface. • Duplex Status — The current mode of operation of the MAC entity.

Token Ring CRC Error tab

Table 10. Token Ring CRC Error view

Data Displayed	• Line Errors — This counter is incremented when a frame or token is copied or repeated by a station. • Burst Errors — This counter is incremented when a station detects the absence of transitions for five half-bit timers (burst-five error). • AC Errors — This counter is incremented when a station receives an AMP or SMP frame in which A is equal to C is equal to 0, and then receives another SMP frame with A is equal to C is equal to 0 without first receiving an AMP frame. It denotes a station that cannot set the AC bits properly. • Abort Trans Errors — This counter is incremented when a station transmits an abort delimiter while transmitting. • Internal Errors — This counter is incremented when a station recognizes an internal error. • Lost Frame Errors — This counter is incremented when a station is transmitting and its TRR timer expires. • Receive Congestions — This counter is incremented when a station recognizes a frame addressed to its specific address, but has no available buffer space indicating that the station is congested. • Frame Copied Errors — This counter is incremented when a station recognizes a frame addressed to its specific address and detects that the FS field A bits are set to 1 indicating a possible line hit or duplicate address. • Token Errors — This counter is incremented when a station acting as the active monitor recognizes an error condition that needs a token transmitted. • Soft Errors — The number of Soft Errors the interface has detected. It directly corresponds to the number of Report Error MAC frames that this interface has transmitted. Soft Errors are those which are recoverable by the MAC layer protocols. • Hard Errors — The number of times this interface has detected an immediately recoverable fatal error. It denotes the number of times this interface is either transmitting or receiving beacon MAC frames. • Signal Loss — The number of times this interface has detected the loss of signal condition from the ring. • Transmit Beacons — The number of times this interface has transmitted a beacon frame. • Recoverys — The number of Claim Token MAC frames received or transmitted after the interface has received a Ring Purge MAC frame. • Lobe Wires — The number of times the interface has detected an open or short circuit in the lobe data path. The adapter will be closed and dot5RingState will signify this condition. • Removes — The number of times the interface has received a Remove Ring Station MAC frame request. • Singles — The number of times the interface has sensed that it is the only station on the ring. This will happen if the interface is the first one up on a ring, or if there is a hardware problem. • Freq Errors — The number of times the interface has detected that the frequency of the incoming signal differs from the expected frequency by more than that specified by the IEEE 802.5 standard.

Network Statistics Summary

This view displays a summary of network statistics.

Table 11. Network Statistics Summary view

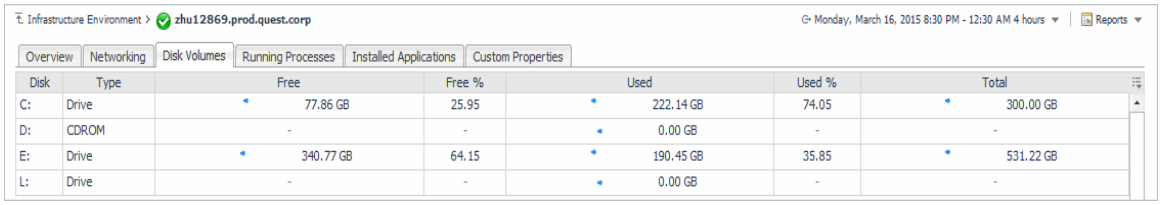
Description		
Data Displayed	General	• Last Boot Time — Time the machine was last booted. • SNMP In Packets — The total number of messages delivered to the SNMP entity from the transport service. • SNMP Out Packets — The total number of SNMP Messages which were passed from the SNMP protocol entity to the transport service.
	ICMP	• In Messages — The total number of ICMP messages that the entity received. This counter includes all ICMP messages counted by icmpInErrors. • In Errors — The number of ICMP messages that the entity received but determined to have ICMP-specific errors. • In Destinations Unreached — The number of ICMP Destination Unreachable messages received. • In Time Exceeds — The number of ICMP Time Exceeded messages received. • In Parameter Probes — The number of ICMP Parameter problem messages received. The ICMP Parameter problem message is generated as a response for any error not specifically covered by another ICMP message. • In Source Quenchs — The number of ICMP Source Quench messages received. The ICMP Source Quench message is a request to decrease the traffic rate of data messages sent to an internet destination. • In Redirects — The number of ICMP Redirect messages received. The ICMP Redirect message is used to notify a remote host to send data packets on an alternative route. • In Echos — The number of ICMP Echo (request) messages received.
	TCP	• Max Connections — The limit on the total number of TCP connections. • Current Established — The number of TCP connections for which the current state is either ESTABLISHED or CLOSE-WAIT. • Active Opens — The number of times TCP connections have made a direct transition to the SYN-SENT state from the CLOSED state. • Passive Opens — The number of times TCP connections have made a direct transition to the SYN-RCVD state from the LISTEN state. • Failed Attempts — The number of times TCP connections have made a direct transition to the CLOSED state from either the SYN-SENT state or the SYN-RCVD state, plus the number of times TCP connections have made a direct transition to the LISTEN state from the SYN-RCVD state. • Established Resets — The number of times TCP connections have made a direct transition to the CLOSED state from either the ESTABLISHED state or the CLOSE-WAIT state. • In Errors — The total number of segments received in error. • Out Resets — The number of TCP segments sent containing the RST flag.
	UDP	• In Datagrams — The total number of UDP datagrams delivered to UDP users. • Out Datagrams — The total number of UDP datagrams sent from this entity. • No Ports — The total number of received UDP datagrams for which there was no application at the destination port. • In Errors — The number of received UDP datagrams that could not be delivered for reasons other than the lack of an application at the destination port.

Disk Volumes tab

This tab displays disk usage and total capacity per volume for a device. Results are available in raw numbers and as percentages.

The **Disk Volumes** tab displays when a host is monitored by an SNMP agent only. If a host is monitored by an Infrastructure agent then the **Disk Volumes** tab does not display.

Figure 26. Disk Volumes view



The table is comprised of the following fields:

- Disk — A disk volume on the monitored host.
- Type — The type of storage. For example, hard drive or CD-ROM.
- Free — Available space on the disk.
- Free % — Percentage of available space on disk.
- Used — Used space on the disk.
- Used % — Percentage of space used on disk.
- Total — The total amount of the logical disk space, including available and used space.

How to Get Here

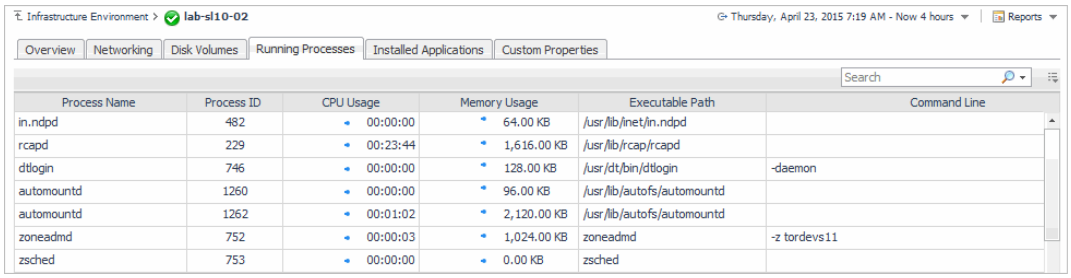
1. On the Infrastructure Environment dashboard, select a host monitored by an SNMP agent.
2. Click **Explore**.

Running Processes tab

This tab displays name, path, CPU, and memory consumption for all the processes running on a device.

The **Running Processes** tab displays only when a host is monitored by an SNMP agent. If a host is not monitored by an SNMP agent then the **Running Processes** tab does not display.

Figure 27. Running Processes view



The table is comprised of the following fields:

- Process Name — The name of the process.
- Process ID — The processes' index ID found in the SNMP table.

- CPU Usage — The CPU resources that the process is using.
- Memory Usage — The memory resources in MB that the process is using.
- Executable Path — The location on long-term storage from which this software was loaded.
- Command Line — The parameters for the process.

To look for a specific running process, you can filter the list using the **Search** box.

Figure 28. The Search box.

How to Get Here

1 On the Infrastructure Environment dashboard, select a host monitored by an SNMP agent.

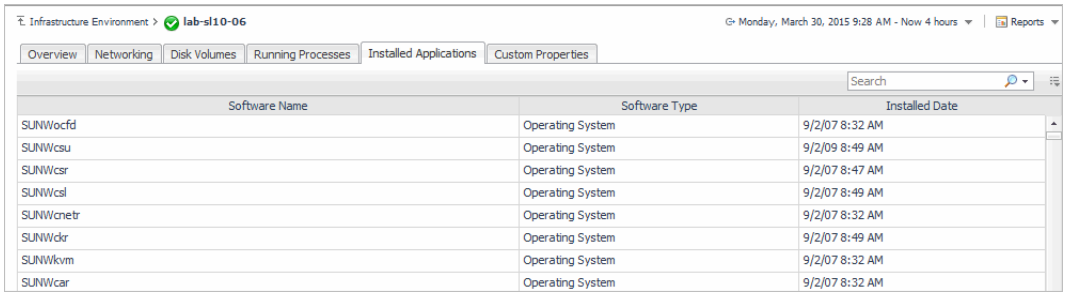
2 Click **Explore**.

Installed Applications tab

This tab displays a list of software applications installed on the selected host.

The **Installed Applications** tab displays only when a host is monitored by an SNMP agent. If a host is not monitored by an SNMP agent then the **Installed Applications** tab does not display.

Figure 29. Installed Applications view



The table is comprised of the following fields:

- Software Name — The name of the installed software.
- Software Type — The type of this software.
- Installed Date — The last-modification date of this application as it would appear in a directory listing.

To look for a specific installed application, use the **Search** box.

How to Get Here

1 On the Infrastructure Environment dashboard, select a host monitored by an SNMP agent.

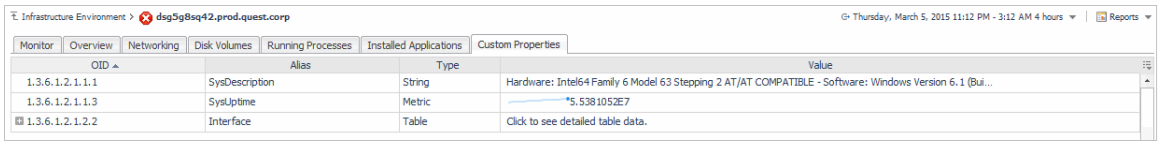
2 Click **Explore**.

Custom Properties tab

This tab displays a list of custom properties on the selected host.

The **Custom Properties** tab displays only when a host is monitored by an SNMP agent. If a host is not monitored by an SNMP agent then the **Custom Properties** tab does not display.

Figure 30. Custom Properties view



The table is comprised of the following fields:

- OID — The vendor specific object identifier that is used to represent a particular device type.
- Alias — The OID's alias.
- Type — The OID type. Supports string, metric, and tables.
- Value — The OID value collected from the device.

NOTE: For more information on a specific column or table, click one of the following links, located in the **Value** column:

- Click to see detailed table data.
- Click to see detailed table column data.

How to Get Here

1. On the Infrastructure Environment dashboard, select a host monitored by an SNMP agent.
2. Click **Explore**.

About Dell

Dell listens to customers and delivers worldwide innovative technology, business solutions and services they trust and value. For more information, visit www.software.dell.com.

Contacting Dell

Technical support:
Online support

Product questions and sales:
(800) 306-9329

Email:
info@software.dell.com

Technical support resources

Technical support is available to customers who have purchased Dell software with a valid maintenance contract and to customers who have trial versions. To access the Support Portal, go to https://support.software.dell.com/.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. In addition, the portal provides direct access to product support engineers through an online Service Request system.

The site enables you to:

- Create, update, and manage Service Requests (cases)
- View Knowledge Base articles
- Obtain product notifications
- Download software. For trial software, go to Trial Downloads.
- View how-to videos
- Engage in community discussions
- Chat with a support engineer