Foglight™ for SNMP 5.8.5.8

User and Reference Guide

The information in this document is provided in connection with Quest Software products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Quest Software products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, QUEST SOFTWARE ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL QUEST SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF QUEST SOFTWARE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Quest Software makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. Quest Software does not make any commitment to update the information contained in this document.

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

Quest Software Inc.
Attn: LEGAL Dept.
4 Polaris Way
Aliso Viejo, CA 92656

Refer to our website (https://www.quest.com) for regional and international office information.

Patents

Quest Software is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at https://www.quest.com/legal.

Trademarks

Quest, the Quest logo, and Join the Innovation are trademarks and registered trademarks of Quest Software Inc. For a complete list of Quest marks, visit https://www.quest.com/legal/trademark-information.aspx. "Apache HTTP Server", Apache, "Apache Tomcat" and "Tomcat" are trademarks of the Apache Software Foundation. Google is a registered trademark of Google Inc. Android, Chrome, Google Play, and Nexus are trademarks of Google Inc. Red Hat, JBoss, the JBoss logo, and Red Hat Enterprise Linux are registered trademarks of Red Hat, Inc. in the U.S. and other countries. CentOS is a trademark of Red Hat, Inc. in the U.S. and other countries. Fedora and the Infinity design logo are trademarks of Red Hat, Inc. Microsoft, .NET, Active Directory, Internet Explorer, Hyper-V, Office 365, SharePoint, Silverlight, SQL Server, Visual Basic, Windows, Windows Vista and Windows Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. AIX, IBM, PowerPC, PowerVM, and WebSphere are trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide. Java, Oracle, Oracle Solaris, PeopleSoft, Siebel, Sun, WebLogic, and ZFS are trademarks or registered trademarks of Oracle and/or its affiliates in the United States and other countries. SPARC is a registered trademark of SPARC International, Inc. in the United States and other countries. Products bearing the SPARC trademarks are based on an architecture developed by Oracle Corporation. OpenLDAP is a registered trademark of the OpenLDAP Foundation. HP is a registered trademark that belongs to Hewlett-Packard Development Company, L.P. Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both. MySQL is a registered trademark of MySQL AB in the United States, the European Union and other countries. Novell and eDirectory are registered trademarks of Novell, Inc., in the United States and other countries. VMware, ESX, ESXi, vSphere, vCenter, vMotion, and vCloud Director are registered trademarks or trademarks of VMware, Inc. in the United States and/or other jurisdictions. Sybase is a registered trademark of Sybase, Inc. The X Window System and UNIX are registered trademarks of The Open Group. Mozilla and Firefox are registered trademarks of the Mozilla Foundation. "Eclipse", "Eclipse Foundation Member", "EclipseCon", "Eclipse Summit", "Built on Eclipse", "Eclipse Ready" "Eclipse Incubation", and "Eclipse Proposals" are trademarks of Eclipse Foundation, Inc. IOS is a registered trademark or trademark of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries. Apple, iPad, iPhone, Mac OS, Safari, Swift, and Xcode are trademarks of Apple Inc., registered in the U.S. and other countries. Ubuntu is a registered trademark of Canonical Ltd. Symantec and Veritas are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. OpenSUSE, SUSE, and YAST are registered trademarks of SUSE LCC in the United States and other countries. Citrix, AppFlow, NetScaler, XenApp, and XenDesktop are trademarks of Citrix Systems, Inc. and/or one or more of its subsidiaries, and may be registered in the United States Patent and Trademark Office and in other countries. AlertSite and DéjàClick are either trademarks or registered trademarks of Boca Internet Technologies, Inc. Samsung, Galaxy S, and Galaxy Note are registered trademarks of Samsung Electronics America, Inc. and/or its related entities. MOTOROLA is a registered trademarks of Motorola Trademark Holdings, LLC. The Trademark BlackBerry Bold is owned by Research In Motion Limited and is registered in the United States and may be pending or registered in other countries. Quest is not endorsed, sponsored, affiliated with or otherwise authorized by Research In Motion Limited. Ixia and the Ixia four-petal logo are registered trademarks or trademarks of Ixia. Opera, Opera Mini, and the O logo are trademarks of Opera Software ASA. Tevron, the Tevron logo, and CitraTest are registered trademarks of Tevron, LLC. PostgreSQL is a registered trademark of the PostgreSQL Global Development Group. MariaDB is a trademark or registered trademark of MariaDB Corporation Ab in the European Union and United States of America and/or other countries. Vormetric is a registered trademark of Vormetric, Inc. Intel, Itanium, Pentium, and Xeon are trademarks of Intel Corporation in the U.S. and/or other countries. Debian is a registered trademark of Software in the Public Interest, Inc. OpenStack is a trademark of the OpenStack Foundation. Amazon Web Services, the "Powered by Amazon Web Services" logo, and "Amazon RDS" are trademarks of Amazon.com, Inc. or its affiliates in the United States and/or other countries. Infobright, Infobright Community Edition and Infobright Enterprise Edition are trademarks of Infobright Inc. POLYCOM®, RealPresence® Collaboration Server, and RMX® are registered trademarks of Polycom, Inc. All other trademarks and registered trademarks are property of their respective

Legend

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

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

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

Foglight User and Reference Guide
Updated - March 2017
Foglight Version - 5.7.5.8
Cartridge Version - 5.8.5.8

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.

Use Foglight for SNMP 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 users are affected.

Starting with version 5.8.5.3, the SNMP agent package that collects data is no longer deployed during installation. Using multiple Foglight Agent Managers is now supported, so after you install the Foglight for SNMP cartridge on the Management Server, run an SNMP discovery to select an Agent Manager. For more information, see Running SNMP discovery.

Getting started with Foglight for SNMP

Review the following topics to learn about the dashboards, understand any requirements, and complete an SNMP Discovery to start monitoring devices and collecting data:

- Installing or upgrading Foglight for SNMP
- Understand monitoring with both host and SNMP agents
- Multiple Foglight Agent Manager instances
- Running SNMP discovery

Installing or upgrading Foglight for SNMP

Foglight for Infrastructure must be installed before installing Foglight for SNMP. For more information, see the *Foglight for Infrastructure Release Notes*.

For information about installing or upgrading Foglight for SNMP, and for system requirements and compatibility, see the *Foglight for SNMP Release Notes*.

For general cartridge installation instructions, see the “Install Foglight cartridges” topic in the *Foglight Administration and Configuration Guide*.

Next step:

- To start monitoring devices, run an SNMP discovery.

Foglight for SNMP navigation basics

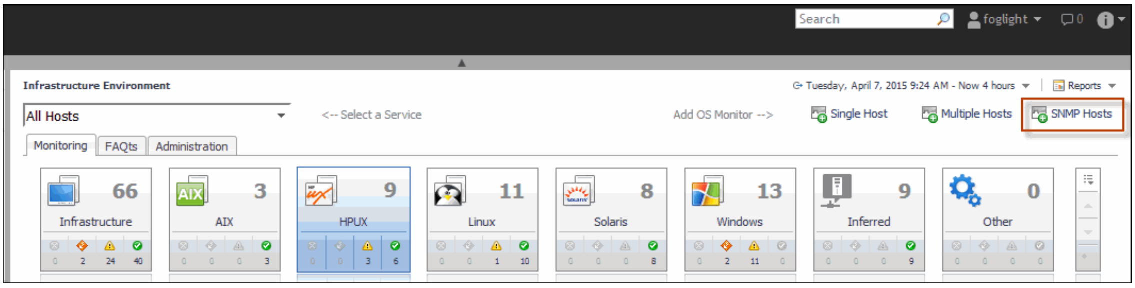
Foglight for SNMP integrates seamlessly into the Infrastructure cartridge workflow. So, after you install the Foglight for SNMP cartridge there is no separate SNMP dashboard in the navigation panel on the left of the browser interface.

To access the Infrastructure Environment dashboard:

1. Log in to Foglight.
2. In the navigation panel, under Dashboards, click **Infrastructure**.

The SNMP Hosts button is in the top-right corner of the Infrastructure Environment dashboard.

Figure 1. SNMP Hosts Button on Infrastructure Environment Dashboard



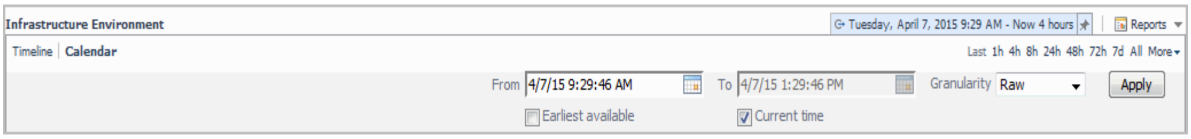
For information on how to discover network devices using the SNMP Hosts button, see Running SNMP discovery.

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 pop-up, which you can access from the upper right corner of the Foglight for SNMP browser interface.

Figure 2. Time range


Infrastructure Environment
Tuesday, April 7, 2015 9:29 AM - Now 4 hours
Reports
Timeline
Calendar
Last 1h 4h 8h 24h 48h 72h 7d All More
Apply

From 4/7/15 9:29:46 AM To 4/7/15 1:29:46 PM Granularity Raw

□ Earliest available ☑ Current time

Using the Time Range pop up, 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 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. Sorting 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 navigation panel, under Dashboards, click **Infrastructure**.
1. On the Infrastructure Environment dashboard, select a host that an SNMP agent monitors.
2. Click Explore.
3. Select the desired tab to display the table you want to export.
4. Click the Customizer icon ☰ at the top right of the table.
5. On the pop-up that opens, click Export.
6. On this new pop-up, 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 pop-up.

Understand monitoring with both host and SNMP agents

A host can be monitored simultaneously by both an Infrastructure agent and an SNMP agent, but it is not recommended.

For hosts monitored by both Infrastructure and SNMP agents, the two agents collect different sets of information. The Infrastructure agent gathers data on the processor, network interface, disk, and memory. The SNMP agent collects additional metrics not available in the Infrastructure cartridge such as ‘Windows Installed Programs’.

For information about the host details on the Infrastructure dashboard, see Hosts monitored by both an Infrastructure and SNMP agent.

Host availability alerting

Foglight for SNMP 5.8.5.5 has changed the way it alerts users about host availability.

If a host is monitored only by the SNMP agent, Foglight for SNMP is able to identify and report the following three states for the monitored host:

- MONITORED. This is the default state. It is set on the *Host* object when the host can be reached via SNMP.

- UNMONITORED. It is set on the *Host* object when the target host cannot be reached via SNMP, but can be reached via ICMP.
- UNAVAILABLE. It is set on the *Host* object when the target host cannot be reached via both SNMP and ICMP.

When the *Host* monitored status changes, the following alarms are triggered: *Warning* (for the UNMONITORED state) and *Critical* (for the UNAVAILABLE state).

If a host is monitored by both the Infrastructure and the SNMP agent, then the host monitored status is identified and reported as described in the *Foglight for Infrastructure User and Reference Guide*, “Host availability alerting” section.

Multiple Foglight Agent Manager instances

Having multiple Foglight Agent Manager instances is supported for Foglight for SNMP.

When you run an SNMP discovery, a specific Foglight Agent Manager is selected to monitor the discovered devices. Each set of devices that you discover can be monitored by a specific Agent Manager. A device can be monitored by one Foglight Agent Manager instance only.

SNMP discovery

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.

Running an SNMP discovery completes the following activities:

- Deploys the agent package to the selected Foglight Agent Manager instance.
- Creates the discovery agent (GenericDiscoveryAgent) on the Foglight Agent Manager instance, if one does not exist.
- Discovers devices in a network.
- Creates SNMP monitoring agent instances based on the OS types of the devices selected for discovery. For example, if you choose discovered devices that have Linux® and Windows® operating systems, a `GenericSNMPWindowsAgent` instance and a `GenericSNMPLinuxAgent` instance is created in that Foglight Agent Manager to monitor those devices respectively.

Next step:

- Running SNMP discovery.

SNMP discovery on Linux requirements

Foglight for SNMP running on Linux requires that you allow Foglight Agent Manager root or administrator access to start the Agent Manager’s ICMPService. Perform one of the following in this order of preference.

- On a more advanced Linux system, assign CAP_NET_RAW capability to the ICMPService to allow this access.
- Configure sudo to allow udp2icmp helper application to run as *root*.

    - Edit the sudoers file for your system to allow `<fglam_home>/client/*/bin/udp2icmp` to be run as root by the Foglight user. For detailed steps, see Using sudo to configure Secure Launcher permissions.

- Provide Foglight Agent Manager with root permissions (not recommended).

Using sudo to configure Secure Launcher permissions

This section contains instructions for using *sudo* to give agents elevated permissions. Use one of the following two methods: the configuration interface or the `fglam.config.xml` file.

To set up secure launcher permissions using the configuration interface and sudo:

1. Follow the instructions in the Launching the Agent Manager Installation Interface or Configuring the Agent Manager from the Command-Line topics in the *Foglight Agent Manager Guide*.
2. Navigate to the **Configure Secure Launcher** or **Secure Launcher** step.
3. Set the path to point to the *sudo* executable. This executable is typically located in */usr/bin/sudo* (the default path provided by the Agent Manager installer).
4. Exit from the configuration interface as described in Launching the Agent Manager Installation Interface or Configuring the Agent Manager from the Command-Line topics in the *Foglight Agent Manager Guide*.
5. Edit the *sudoers* file for your system to allow *<fglam_home>/client/<fglam_version>/bin/fog4_launcher* to be run as root by a specific user, without requiring a password, and only for the agents that require root privileges.

   For example, to allow the user *foglight* to run *fog4_launcher* for two specific agents without being prompted for a password:

   ```
   foglight    ALL = NOPASSWD:  \

   /<fglam_home>/client/*/bin/fog4_launcher
   /<fglam_home>/state/default/<cartridge>/*/bin/<agent> ?*@?* bin/<agent>, \

   /<fglam_home>/client/*/bin/fog4_launcher
   /<fglam_home>/state/default/<cartridge>/*/bin/<agent2> ?*@?* bin/<agent2>
   ```

   The example above also limits the acceptable arguments to match the expected pattern when the Agent Manager runs the agents.
6. Edit the *sudoers* file for your system to allow *<fglam_home>/client/*/bin/udp2icmp* to be run as root by a specific user, without requiring a password. This is required for ICMP ping service.

   See the *Foglight for Infrastructure User and Reference Guide* for detailed examples of how to edit the *sudoers* file to restrict the granted permissions to a specific set of agents.

> **TIP:** For *sudo* configuration, it is a best practice to use a wildcard for the version-specific Agent Manager and cartridge directories, as shown in the example above. Using a wildcard in a path is described in the *Sudoers Manual* at:
>
> http://www.gratisoft.us/sudo/man/sudoers.html#wildcards
>
> Using a wildcard for the version-specific directories allows you to avoid updating each *sudoers* file that references these directories when you upgrade the Agent Manager or the agents.

If these permissions are no longer needed, remove the lines that you added to run *fog4_launcher* or *udp2icmp* with root permissions.

To set up secure launcher permissions using fglam.config.xml and sudo:

1. Navigate to *<fglam_home>/state/default/config*.
2. Open the *fglam.config.xml* file for editing.

3 Edit the `<config:path>` element under `<config:secure-launcher>` to point to the *sudo* executable. This executable is typically located in */usr/bin/sudo* (the default path provided by the Agent Manager installer).

4 Edit the *sudoers* file for your system to allow *<fglam_home>/client/<fglam_version>/bin/fog4_launcher* to run as root by a specific user, without requiring a password, and only for the agents that require root privileges.

For example, to allow the user *foglight* to run *fog4_launcher* for two specific agents without being prompted for a password:

```
foglight    ALL = NOPASSWD:  \

/<fglam_home>/client/*/bin/fog4_launcher
/<fglam_home>/state/default/<cartridge>/*/bin/<agent> ?*@?* bin/<agent>, \

/<fglam_home>/client/*/bin/fog4_launcher
/<fglam_home>/state/default/<cartridge>/*/bin/<agent2> ?*@?* bin/<agent2>
```

The example above also limits the acceptable arguments to match the expected pattern when the Agent Manager runs the agents.

5 Edit the *sudoers* file for your system to allow *<fglam_home>/client/*/bin/udp2icmp* to be run as root by a specific user, without requiring a password. This is required for ICMP ping service.

See the *Foglight for Infrastructure User and Reference Guide* for detailed examples of how to edit the *sudoers* file to restrict the granted permissions to a specific set of agents.

i **TIP:** For *sudo* configuration, it is a best practice to use a wildcard for the version-specific Agent Manager and cartridge directories, as shown in the example above. Using a wildcard in a path is described in the *Sudoers Manual* at:

http://www.gratisoft.us/sudo/man/sudoers.html#wildcards

Using a wildcard for the version-specific directories allows you to avoid updating each *sudoers* file that references these directories when you upgrade the Agent Manager or the agents.

Running SNMP discovery

Prerequisites:

- SNMP discovery on Linux requirements.
- The SNMP credentials for the device being discovered.
- The ports for the SNMP protocol (by default, 161) and SNMP traps (by default, 162) must be open, and not blocked by a firewall.

  The SNMP protocol port can be changed during the discovery process. The SNMP trap port on the GenericSNMPTrapAgent can be changed in the agent properties. For more information, see Changing the GenericSNMPTrapAgent port

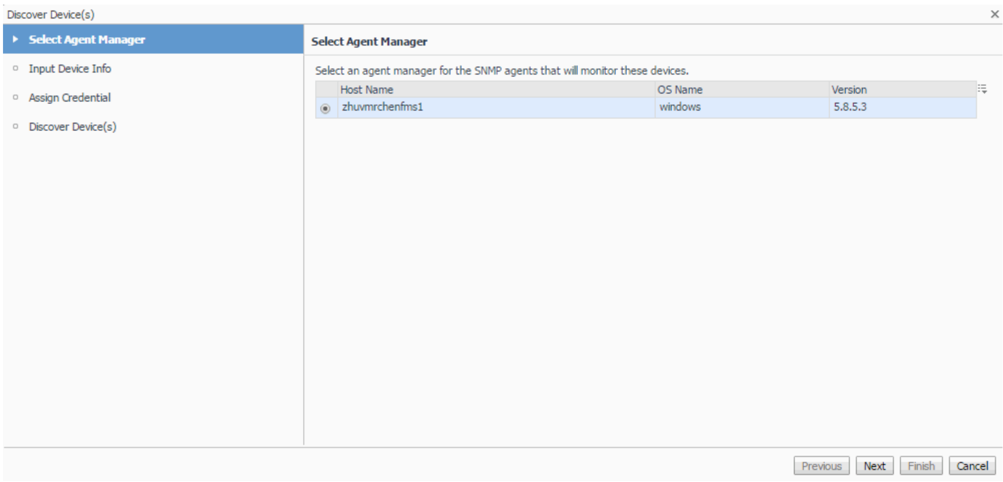
  i **IMPORTANT:** On Linux® hosts, non-root users cannot bind to ports below 1024. The default port number for the SNMP traps is 162, so the port number must be changed.

To complete the agent configuration and discover devices:

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

2 On the Infrastructure Environment dashboard, click SNMP Hosts.

The **Discover Device(s)** interactive UI opens.



Discover Device(s)

- Select Agent Manager
- Input Device Info
- Assign Credential
- Discover Device(s)

Select Agent Manager

Select an agent manager for the SNMP agents that will monitor these devices.

	Host Name	OS Name	Version
●	zhuvmrchenfms1	windows	5.8.5.3

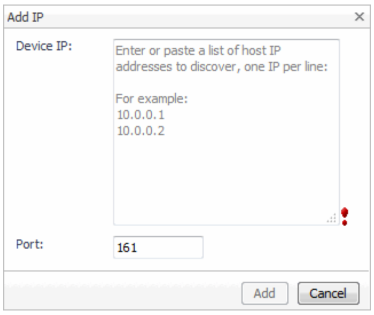
3 On the **Select an Agent Manager** page, select the Foglight Agent Manager instance that you want to use to monitor devices.

The SNMP discovery deploys the agent package to this Foglight Agent Manager instance. If a discovery agent does not exist on this Foglight Agent Manager instance, the `GenericDiscoveryAgent` is created.

4 On the **Input Device Info** page, discover the devices that you want to monitor with the selected Foglight Agent Manager.

a In the IP Address to Discover section, add a single IP address or a range of IP addresses for discovery.

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



Add IP

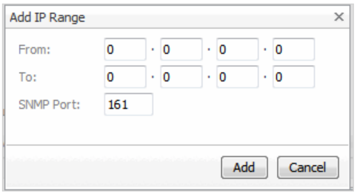
Device IP: Enter or paste a list of host IP addresses to discover, one IP per line:

For example:
10.0.0.1
10.0.0.2

Port: 161

Or

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



Add IP Range

From: 0 . 0 . 0 . 0
To: 0 . 0 . 0 . 0
SNMP Port: 161

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.

The SNMP port is the port number for the SNMP protocol on the device. The default is 161, but it can be changed to the value that was set when SNMP was configured on the device.

b In the Exclude Criteria table, specify any IP addresses to exclude from discovery.

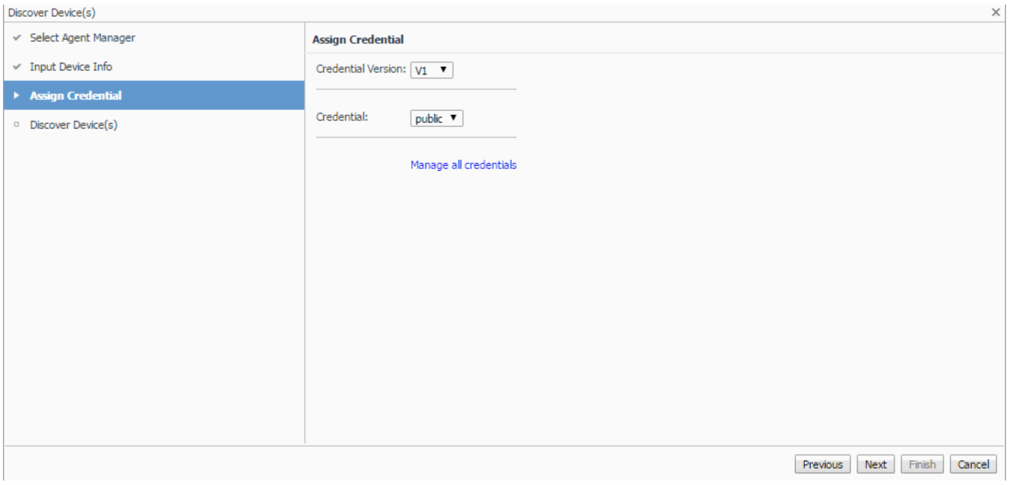
- Click ⊕ Add IP to specify the IP address that should be excluded.

> **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 exclude.

5 On the Assign Credential page, specify the SNMP credential version and the community string required to discover devices



Assign Credential

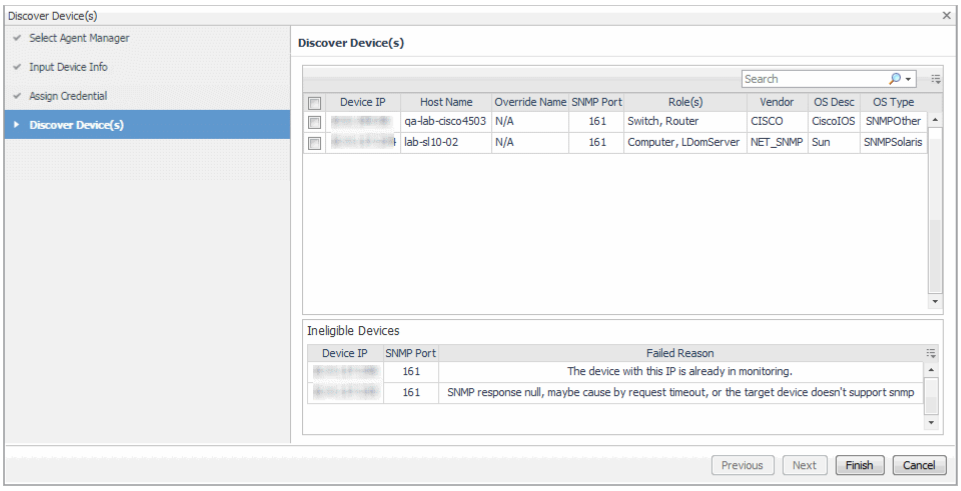
Credential Version: V1 ▾

Credential: public ▾

- Credential Version — The version of SNMP 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 and Managing the SNMP V3 credentials.

6 The Discover Device(s) page opens refreshes to display a list of discovered and ineligible devices. For more information on ineligible devices, see Ineligible devices.



Discover Device(s)

□	Device IP	Host Name	Override Name	SNMP Port	Role(s)	Vendor	OS Desc	OS Type
□	[redacted]	qa-lab-cisco4503	N/A	161	Switch, Router	CISCO	CiscoIOS	SNMPOther
□	[redacted]	lab-sl10-02	N/A	161	Computer, LDomServer	NET_SNMP	Sun	SNMPSolaris

Ineligible Devices

Device IP	SNMP Port	Failed Reason
[redacted]	161	The device with this IP is already in monitoring.
[redacted]	161	SNMP response null, maybe cause by request timeout, or the target device doesn't support snmp

7 Select one or more devices for this Agent Manager to monitor.

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

8 Click Finish.

At this step in the discovery, the following agents are created on the Foglight Agent Manager:

- The `GenericSNMPTrapAgent` is created for the Foglight Agent Manger (if one did not exist).

> ℹ **IMPORTANT:** Linux non-root users cannot bind to ports below 1024. The default port number for the `GenericSNMPTrapAgent` is *162*, so the port number must be changed for Linux hosts before devices can be monitored. For detailed information, see Changing the GenericSNMPTrapAgent port.

- Monitoring agent instances for the OS types of the chosen discovered devices.
  The following seven agents may be created, depending on the OS type of the discovered devices:

Table 1. Monitoring agent instances created during discovery

Agent name	Created for	Collector settings
`GenericSNMPWindowsAgent`	devices with Windows OS	**Default enabled:** cpu, memory, diskVolumes, systemInfo, runningProcess, networkStatisticSummary, networkInterfacTraffic, networkInterfaceConfiguration, ipConfiguration,availability, programInstalled, customProperties
`GenericSNMPSolarisAgent`	devices with Solaris OS	cpu, memory, diskVolumes, systemInfo, runningProcess, networkStatisticSummary, networkInterfacTraffic, networkInterfaceConfiguration, ipConfiguration,availability, programInstalled, customProperties
`GenericSNMPHPUXAgent`	devices with HP-UX OS	cpu, memory, diskVolumes, systemInfo, runningProcess, networkStatisticSummary, networkInterfacTraffic, networkInterfaceConfiguration, ipConfiguration,availability, customProperties **Disabled by default:** programInstalled
`GenericSNMPAIXAgent`	devices with AIX OS	cpu, memory, diskVolumes, systemInfo, runningProcess, networkStatisticSummary, networkInterfacTraffic, networkInterfaceConfiguration, ipConfiguration,availability, programInstalled, customProperties
`GenericSNMPLinuxAgent`	devices with Linux OS	cpu, memory, diskVolumes, systemInfo, runningProcess, networkStatisticSummary, networkInterfacTraffic, networkInterfaceConfiguration, ipConfiguration,availability, programInstalled, customProperties

Table 1. Monitoring agent instances created during discovery

Agent name	Created for	Collector settings
`GenericSNMPOtherAgent`	Created if a host with an OS type is detected during discovery but the OS is not Windows, Linux, HPUX, Solaris, or AIX. The host is added to this agent for collection.	cpu, memory, systemInfo, availability customProperties, networkStatisticSummary, networkInterfacTraffic, networkInterfaceConfiguration, ipConfiguration **Disabled by default:** programInstalled, runningProcess, diskVolumes
`GenericSNMPInferredAgent`	Created if an OS type for a host is not detected during discovery. The host is added to this agent for collection	cpu, memory, diskVolumes, systemInfo, customProperties, networkStatisticSummary, networkInterfacTraffic, networkInterfaceConfiguration, ipConfiguration, availability **Disabled by default:** programInstalled, runningProcess

Next steps:

- To see the devices that you have discovered, see Viewing SNMP monitored hosts.
- To investigate devices that could not be discovered, see Ineligible devices.

Ineligible devices

SNMP devices that are not discovered can be deemed ineligible for one of the following reasons:

- The device is already being monitored by a Foglight Agent Manager.
  For more information, see Multiple Foglight Agent Manager instances.
- The host is unreachable and ICMP ping failed.
  For more information, see SNMP discovery on Linux requirements.
- SNMP failed either because of a request time out (for example, the specified credential is incorrect) or the target device does not support SNMP.
  For more information, see SNMP communities and credentials.

SNMP communities and credentials

When you run SNMP discovery, specifying the correct device 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 adds it to the database. If the credentials are incorrectly set for that device, Foglight for SNMP cannot discover the device so that it can be monitored.

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 2c 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

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

To access the Manage all credentials wizard:

1 On the navigation panel, click Infrastructure.

2 On the Infrastructure Environment dashboard, click SNMP Hosts.

The Discover Device(s) wizard opens.

3 On the Select an Agent Manager page, select the Foglight Agent Manager instance that is monitoring the devices.

4 On the Input Device Info page, under IP Address to Discover, add either a single IP address and SNMP Port, or a range of IP addresses and SNMP Port.

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

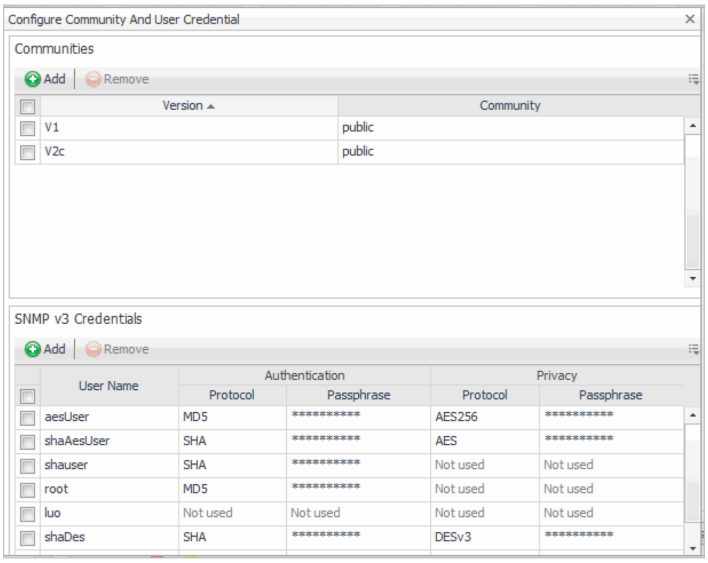
Foglight for SNMP uses public (read-only) community strings. You can add more public community strings. All community strings must be unique for each version. Therefore, you may have to run the Discover Device(s) wizard more than once to properly discover all devices in the network.

> **IMPORTANT:** Add or remove credentials using 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.



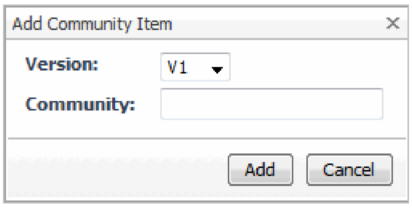
Communities

□	Version ▲	Community
□	V1	public
□	V2c	public

SNMP v3 Credentials

□	User Name	Authentication		Privacy	
		Protocol	Passphrase	Protocol	Passphrase
□	aesUser	MD5	**********	AES256	**********
□	shaAesUser	SHA	**********	AES	**********
□	shauser	SHA	**********	Not used	Not used
□	root	MD5	**********	Not used	Not used
□	luo	Not used	Not used	Not used	Not used
□	shaDes	SHA	**********	DESv3	**********

2 In the Communities table, click Add.



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.

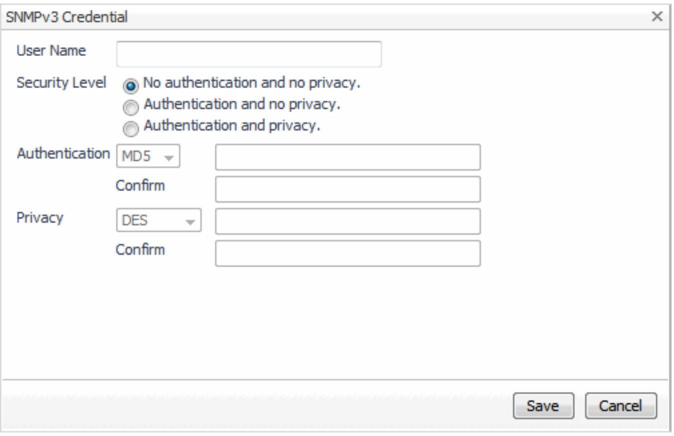
Adding SNMP V3 credentials

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.



SNMPv3 Credential

User Name

Security Level
● No authentication and no privacy.
○ Authentication and no privacy.
○ Authentication and privacy.

Authentication MD5

Confirm

Privacy DES

Confirm

3 Type the user name that is 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 device credential

After a device has been discovered and is being monitored, you can associate the device with a different existing SNMP credential.

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 Object Identifiers (OIDs) used to communicate with an SNMP agent. A typical SNMP monitoring environment contains a combination of built-in and user configured OIDs.

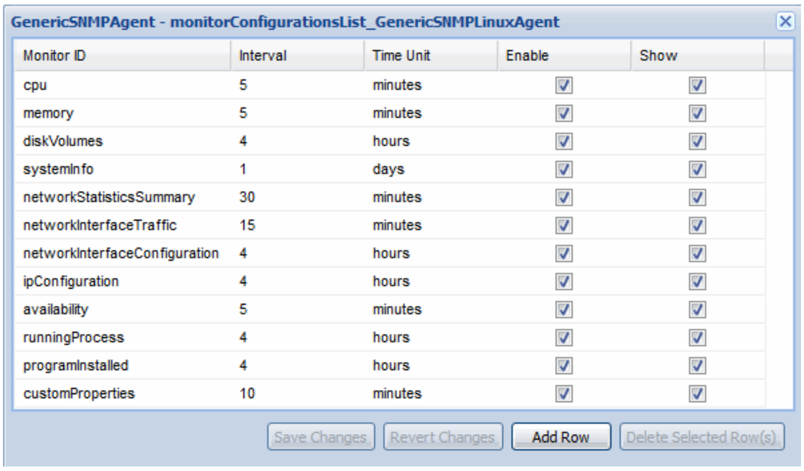
Foglight for SNMP provides pre-defined monitors that collect key data for most of the common devices in a network. When you create a custom SNMP monitor, you can define any OID to an management information base (MIB) node to monitor any SNMP device (regardless of the manufacturer or type of device).

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.

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


GenericSNMPAgent - monitorConfigurationsList_GenericSNMPLinuxAgent

Monitor ID	Interval	Time Unit	Enable	Show
cpu	5	minutes	☑	☑
memory	5	minutes	☑	☑
diskVolumes	4	hours	☑	☑
systemInfo	1	days	☑	☑
networkStatisticsSummary	30	minutes	☑	☑
networkInterfaceTraffic	15	minutes	☑	☑
networkInterfaceConfiguration	4	hours	☑	☑
ipConfiguration	4	hours	☑	☑
availability	5	minutes	☑	☑
runningProcess	4	hours	☑	☑
programInstalled	4	hours	☑	☑
customProperties	10	minutes	☑	☑

7 Double-click on the value to change the fields, as necessary:

> i | **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`.

> i | **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 — Disregard — this field is no longer used.

8 Click Save Changes.

The new settings are saved for the selected agent.

Configuring SNMP agent properties

The SNMP agent includes the following groups of agent properties:

- SNMP properties
- Devices and collection OIDs
- Credentials

SNMP properties

To configure the SNMP agent properties:

1 On the navigation panel, under Dashboards, click **Administration > Agents > Agent Status**.

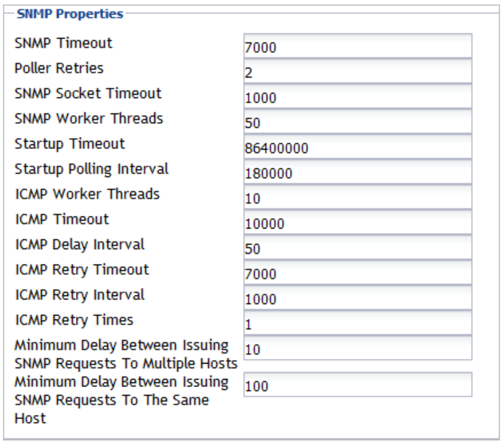
2 Select the SNMP agent. For example, *GenericSNMPLinuxAgent*.

3 On the toolbar, click Edit > Edit Properties.

4 Click Modify the private properties for this agent.

5 In the SNMP Properties section, make your changes and click **Save**.

Figure 3. SNMP properties.



SNMP Properties

SNMP Timeout	7000
Poller Retries	2
SNMP Socket Timeout	1000
SNMP Worker Threads	50
Startup Timeout	86400000
Startup Polling Interval	180000
ICMP Worker Threads	10
ICMP Timeout	10000
ICMP Delay Interval	50
ICMP Retry Timeout	7000
ICMP Retry Interval	1000
ICMP Retry Times	1
Minimum Delay Between Issuing SNMP Requests To Multiple Hosts	10
Minimum Delay Between Issuing SNMP Requests To The Same Host	100

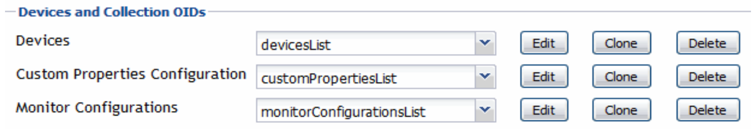
- SNMP Timeout: Timeout in milliseconds before a confirmed request from a device is received.
- Poller Retries: Retry times for retrieving the data if timeout.
- SNMP Socket Timeout: UDP socket timeout for incoming messages in milliseconds. A timeout of zero is interpreted as an infinite timeout.
- SNMP 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 cancels.
- 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

To configure the device and collection IODs:

1. On the navigation panel, under Dashboards, click **Administration > Agents > Agent Status**.
2. Select the SNMP agent. For example, *GenericSNMPLinuxAgent*.
3. On the toolbar, click Edit > Edit Properties.
4. Click Modify the private properties for this agent.
5. Make any required changes and click **Save**.

Figure 4. Devices and collection OID properties



Devices and Collection OIDs

Devices: devicesList

Custom Properties Configuration: customPropertiesList

Monitor Configurations: monitorConfigurationsList

Devices

Each entry in the list includes the following columns:

> **IMPORTANT:** Device properties must be added or edited using the SNMP Discovery. All properties listed below should be considered read-only, except where noted. For more information, see Running SNMP discovery on page 10.

- 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. (Editable)
- 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 that this monitor is removed from this agent and may not be edited anymore.

Credentials

You can change the credentials for an SNMP agent, for example, if a credential becomes compromised.

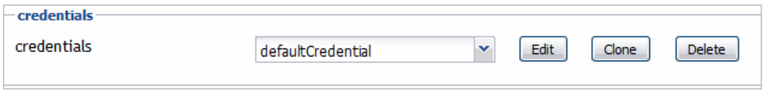
There are two options for changing this global credential.

- Use the **Administration** > **Agents** > **Agent Properties** dashboard. Select the SNMP agent from the **Namespace** > **Type** list.

  Or

- Use the **Administration > Agents > Agent Status** dashboard. Select the SNMP agent. For example, *GenericSNMPLinuxAgent*. On the toolbar, click Edit > Edit Properties and click **Modify the properties for all GenericSNMPAgent** agents.

Figure 5. Credentials properties.



credentials

credentials: defaultCredential

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.

Changing the GenericSNMPTrapAgent port

A GenericSNMPTrapAgent is created for each Agent Manager that you are using to monitor SNMP devices.

The default port number for a GenericSNMPTrapAgent is *162*, but it can be changed.

On Linux, non-root users cannot bind to ports below 1024 on Linux hosts (by default), so this port number must be changed.

The `GenericSNMPTrapAgent` has two properties:

- **snmpTrapPort** - Used to configure the port for the agent to receive SNMP traps from monitored SNMP devices. The port is opened on the agent side and is used to listen to the SNMP traps sent from the monitored devices.
- **devices** - Do Not Change. The items in this table are populated by the `GenericSNMPTrapAgent` cartridge which is used to help the SNMPTrap agent decide if the agent should report the trap sent from an SNMP device. Only when the SNMP device sending the trap is in this monitored devices list, the agent will then report it and show it in the corresponding SNMP device dashboard.

The only property that should be changed for the `GenericSNMPTrapAgent` is the **snmpTrapPort**.

To change the port number:

1. Log in to the Foglight browser interface. On the navigation panel, under Dashboards, click Administration > Agents > Agent Status.

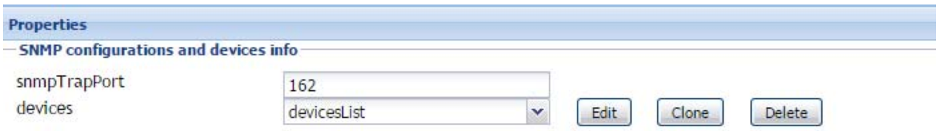
2 Select the **GenericSNMPTrapAgent**.

3 On the toolbar, click Edit > Edit Properties.

4 Click Modify properties for this agent only.

5 In the **SNMP configurations and devices info** section, change the **snmpTrapPort** number.

> **IMPORTANT:** The **devices** property is configured automatically by the agent. It identifies the device that is sending the trap. It should not be changed.


Properties

SNMP configurations and devices info

snmpTrapPort: 162

devices: devicesList

6 Click Save.

Viewing SNMP monitored hosts

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

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 select an SNMP monitored host:

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

The Infrastructure Environment dashboard opens.

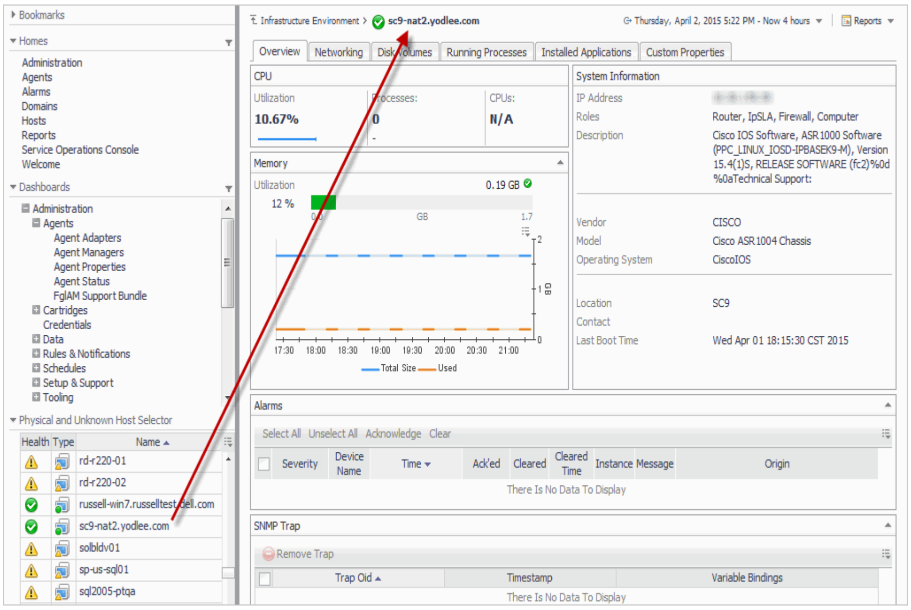
2 Select a monitored host from the list of hosts in the view on the left.

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

> **NOTE:** If the host is also monitored 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 6. 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.

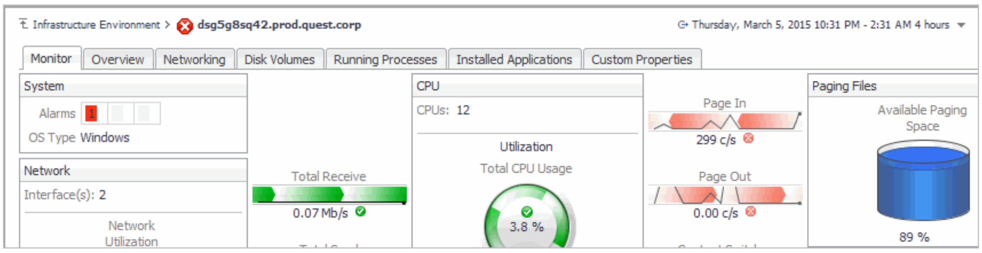
Click I**nfrastructure Environment** in the breadcrumb to return to the main view.

Hosts monitored by both an Infrastructure and SNMP agent

When a host is monitored by both an Infrastructure and an SNMP agent, you see an Infrastructure-related Monitor tab and 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.

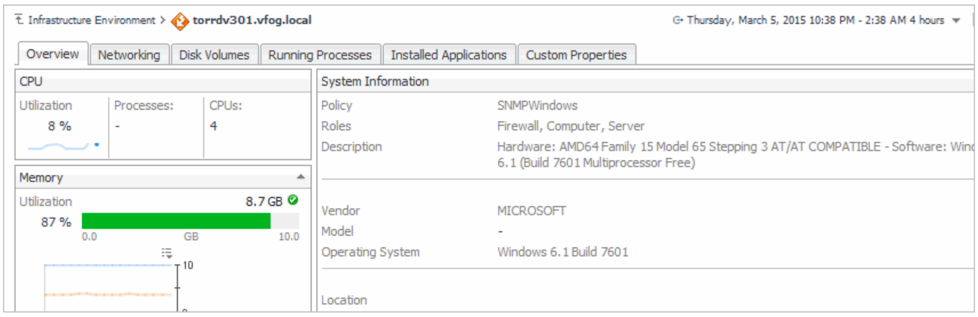
Figure 7. Example of a host monitored by both an Infrastructure and an SNMP agent.



Hosts monitored only by SNMP

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

Figure 8. Example of a host monitored only by an SNMP agent.



Infrastructure Environment > torrdv301.vfog.local

Thursday, March 5, 2015 10:38 PM - 2:38 AM 4 hours

CPU

Utilization: 8 %

Processes: -

CPUs: 4

Memory

Utilization: 87 % 8.7 GB

System Information

Policy: SNMPWindows

Roles: Firewall, Computer, Server

Description: Hardware: AMD64 Family 15 Model 65 Stepping 3 AT/AT COMPATIBLE - Software: Wind
6.1 (Build 7601 Multiprocessor Free)

Vendor: MICROSOFT

Model: -

Operating System: Windows 6.1 Build 7601

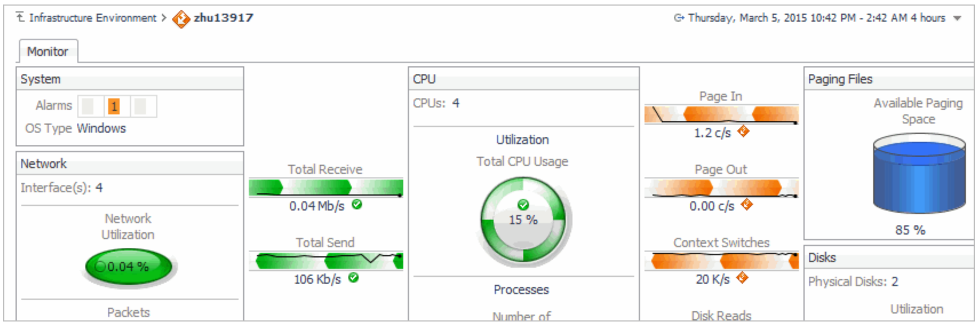
Location

For more information about the detail displayed on the SNMP tabs, see Foglight for SNMP reference.

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 9. Example of a host monitored only by an Infrastructure agent.



Infrastructure Environment > zhu13917

Thursday, March 5, 2015 10:42 PM - 2:42 AM 4 hours

System

Alarms 1

OS Type Windows

Network

Interface(s): 4

Network Utilization 0.04 %

Packets

Total Receive 0.04 Mb/s

Total Send 106 Kb/s

CPU

CPUs: 4

Utilization

Total CPU Usage 15 %

Processes

Number of

Page In 1.2 c/s

Page Out 0.00 c/s

Context Switches 20 K/s

Disk Reads

Paging Files

Available Paging Space 85 %

Disks

Physical Disks: 2

Utilization

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** 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.

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

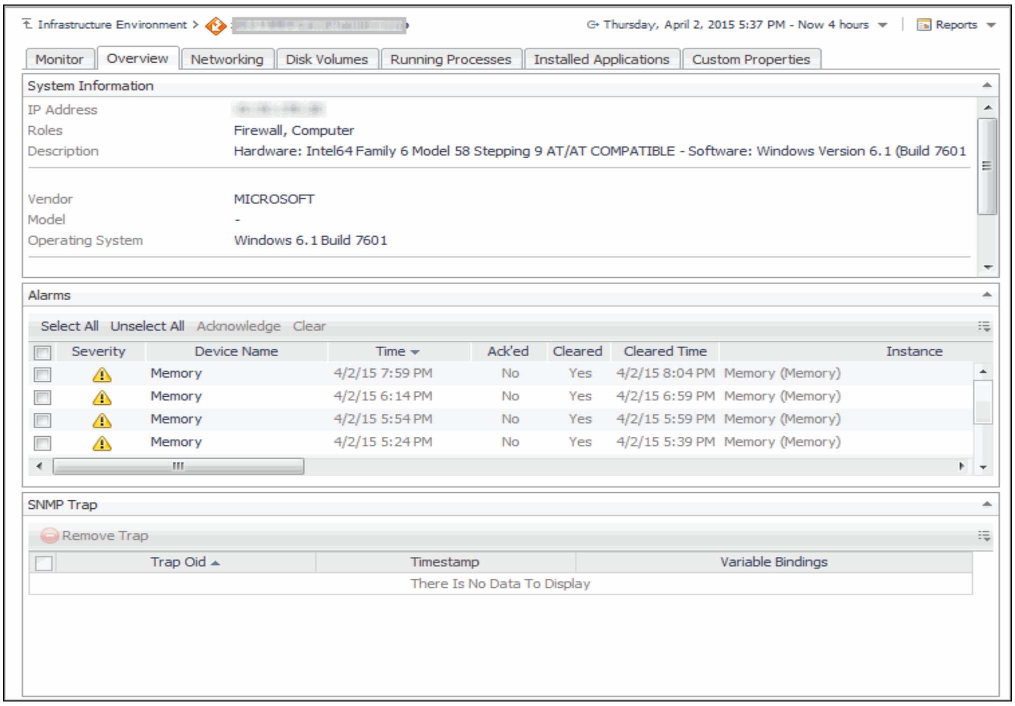
Overview tab

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 also displays.

Figure 10. Overview tab: Host monitored by SNMP agent AND Infrastructure agent



Infrastructure Environment > [redacted]

Thursday, April 2, 2015 5:37 PM - Now 4 hours | Reports

System Information

IP Address	[redacted]
Roles	Firewall, Computer
Description	Hardware: Intel64 Family 6 Model 58 Stepping 9 AT/AT COMPATIBLE - Software: Windows Version 6.1 (Build 7601
Vendor	MICROSOFT
Model	-
Operating System	Windows 6.1 Build 7601

Alarms

Select All Unselect All Acknowledge Clear

□	Severity	Device Name	Time	Ack'ed	Cleared	Cleared Time	Instance
□	⚠	Memory	4/2/15 7:59 PM	No	Yes	4/2/15 8:04 PM	Memory (Memory)
□	⚠	Memory	4/2/15 6:14 PM	No	Yes	4/2/15 6:59 PM	Memory (Memory)
□	⚠	Memory	4/2/15 5:54 PM	No	Yes	4/2/15 5:59 PM	Memory (Memory)
□	⚠	Memory	4/2/15 5:24 PM	No	Yes	4/2/15 5:39 PM	Memory (Memory)

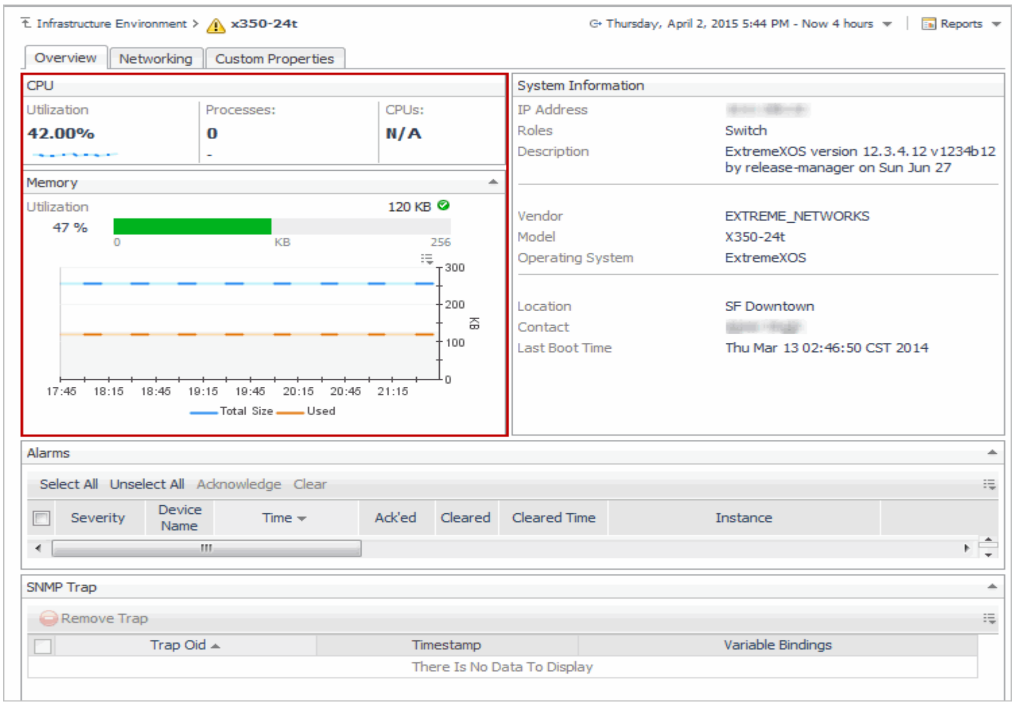
SNMP Trap

Remove Trap

□	Trap Oid	Timestamp	Variable Bindings

There Is No Data To Display

Figure 11. Overview tab: Host monitored by SNMP agent only



Infrastructure Environment > x350-24t

Thursday, April 2, 2015 5:44 PM - Now 4 hours | Reports

CPU

Utilization	Processes:	CPUs:
42.00%	0	N/A

Memory

Utilization 47 % 120 KB

System Information

IP Address	[redacted]
Roles	Switch
Description	ExtremeXOS version 12.3.4.12 v1234b12 by release-manager on Sun Jun 27
Vendor	EXTREME_NETWORKS
Model	X350-24t
Operating System	ExtremeXOS
Location	SF Downtown
Contact	[redacted]
Last Boot Time	Thu Mar 13 02:46:50 CST 2014

Alarms

Select All Unselect All Acknowledge Clear

□	Severity	Device Name	Time	Ack'ed	Cleared	Cleared Time	Instance

SNMP Trap

Remove Trap

□	Trap Oid	Timestamp	Variable Bindings

There Is No Data To Display

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 2. 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 3. 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 running 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 4. 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 5. 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 6. 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.

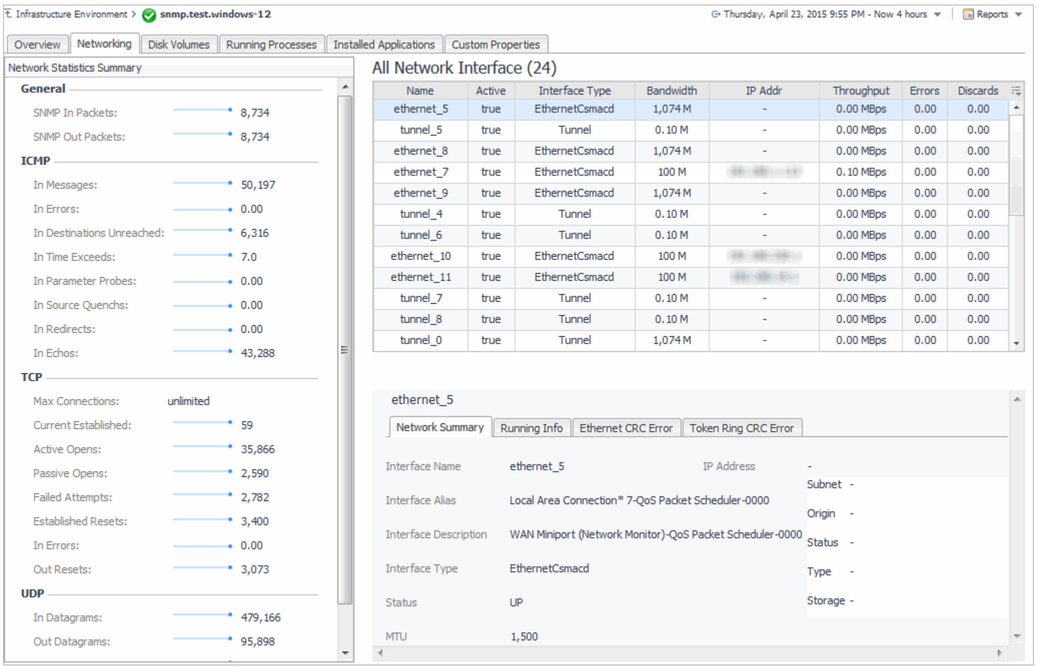
Networking tab

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 12. Networking view



Infrastructure Environment > snmp.test.windows-12
Thursday, April 23, 2015 9:55 PM - Now 4 hours
Reports
Overview
Networking
Disk Volumes
Running Processes
Installed Applications
Custom Properties

Network Statistics Summary

General

SNMP In Packets:	8,734
SNMP Out Packets:	8,734

ICMP

In Messages:	50,197
In Errors:	0.00
In Destinations Unreached:	6,316
In Time Exceeds:	7.0
In Parameter Probes:	0.00
In Source Quenchs:	0.00
In Redirects:	0.00
In Echos:	43,288

TCP

Max Connections:	unlimited
Current Established:	59
Active Opens:	35,866
Passive Opens:	2,590
Failed Attempts:	2,782
Established Resets:	3,400
In Errors:	0.00
Out Resets:	3,073

UDP

In Datagrams:	479,166
Out Datagrams:	95,898

All Network Interface (24)

Name	Active	Interface Type	Bandwidth	IP Addr	Throughput	Errors	Discards
ethernet_5	true	EthernetCsmacd	1,074 M	-	0.00 MBps	0.00	0.00
tunnel_5	true	Tunnel	0.10 M	-	0.00 MBps	0.00	0.00
ethernet_8	true	EthernetCsmacd	1,074 M	-	0.00 MBps	0.00	0.00
ethernet_7	true	EthernetCsmacd	100 M	[redacted]	0.10 MBps	0.00	0.00
ethernet_9	true	EthernetCsmacd	1,074 M	-	0.00 MBps	0.00	0.00
tunnel_4	true	Tunnel	0.10 M	-	0.00 MBps	0.00	0.00
tunnel_6	true	Tunnel	0.10 M	-	0.00 MBps	0.00	0.00
ethernet_10	true	EthernetCsmacd	100 M	[redacted]	0.00 MBps	0.00	0.00
ethernet_11	true	EthernetCsmacd	100 M	[redacted]	0.00 MBps	0.00	0.00
tunnel_7	true	Tunnel	0.10 M	-	0.00 MBps	0.00	0.00
tunnel_8	true	Tunnel	0.10 M	-	0.00 MBps	0.00	0.00
tunnel_0	true	Tunnel	1,074 M	-	0.00 MBps	0.00	0.00

ethernet_5

Interface Name	ethernet_5	IP Address	-
		Subnet	-
Interface Alias	Local Area Connection* 7-QoS Packet Scheduler-0000	Origin	-
Interface Description	WAN Miniport (Network Monitor)-QoS Packet Scheduler-0000	Status	-
Interface Type	EthernetCsmacd	Type	-
Status	UP	Storage	-
MTU	1,500		

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

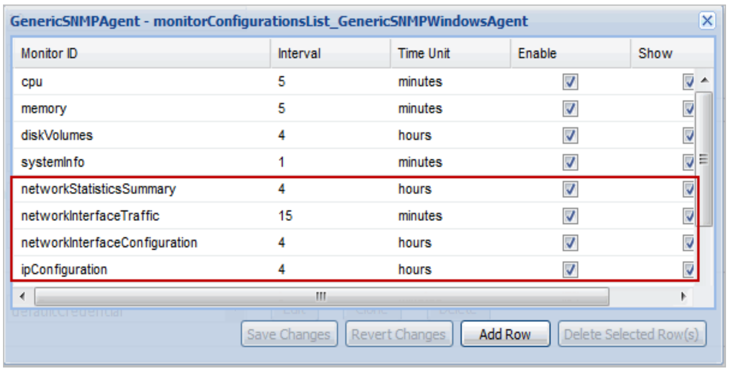
This view is made up of the following embedded views:

- 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 13. Pre-defined Foglight for SNMP network monitors


GenericSNMPAgent - monitorConfigurationsList_GenericSNMPWindowsAgent

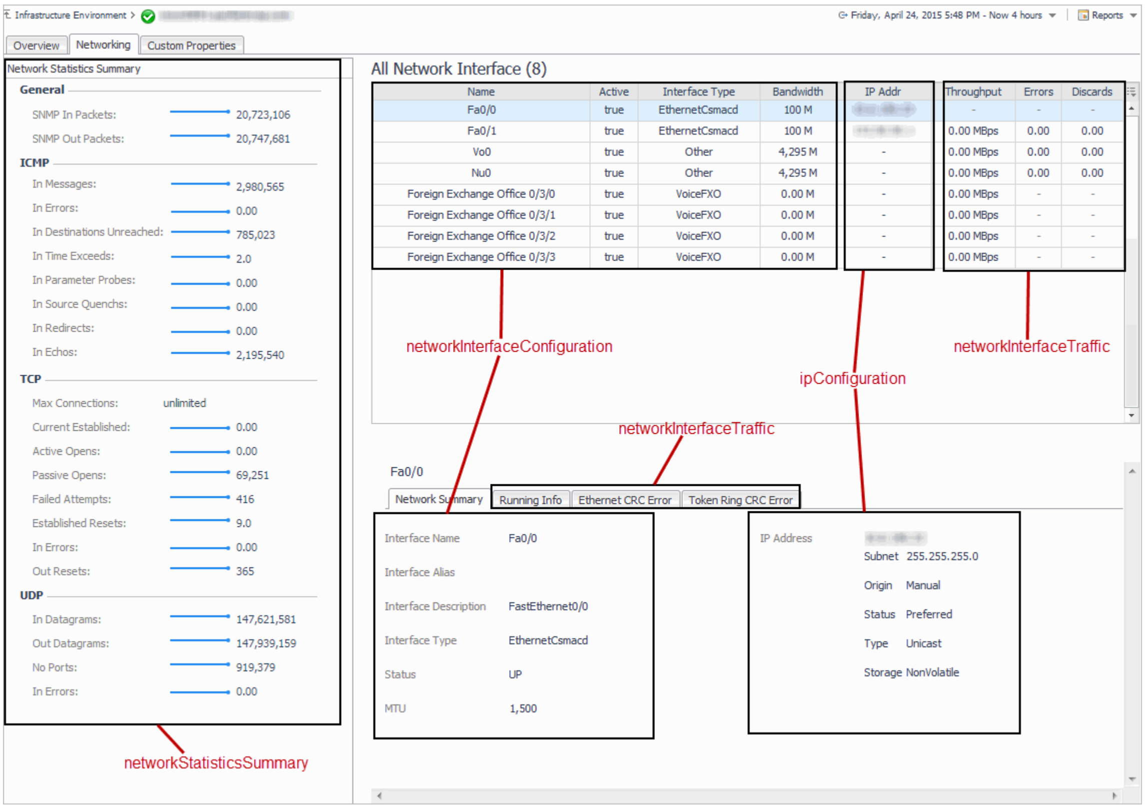
Monitor ID	Interval	Time Unit	Enable	Show
cpu	5	minutes	☑	☑
memory	5	minutes	☑	☑
diskVolumes	4	hours	☑	☑
systemInfo	1	minutes	☑	☑
networkStatisticsSummary	4	hours	☑	☑
networkInterfaceTraffic	15	minutes	☑	☑
networkInterfaceConfiguration	4	hours	☑	☑
ipConfiguration	4	hours	☑	☑

- networkStatisticsSummary — Collects the network summary data for a host, such as ICMP, UDP.

- 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.
- ipConfiguration — Collects network interface IP information, such as IPAddress, Subnet, Storage.

For information on configuring network monitors, see Configuring SNMP agent properties on page 19.

Figure 14. Data Collected by Pre-defined Foglight for SNMP network monitors



Network Statistics Summary

General

SNMP In Packets:	20,723,106
SNMP Out Packets:	20,747,681

ICMP

In Messages:	2,980,565
In Errors:	0.00
In Destinations Unreached:	785,023
In Time Exceeds:	2.0
In Parameter Probes:	0.00
In Source Quenchs:	0.00
In Redirects:	0.00
In Echos:	2,195,540

TCP

Max Connections:	unlimited
Current Established:	0.00
Active Opens:	0.00
Passive Opens:	69,251
Failed Attempts:	416
Established Resets:	9.0
In Errors:	0.00
Out Resets:	365

UDP

In Datagrams:	147,621,581
Out Datagrams:	147,939,159
No Ports:	919,379
In Errors:	0.00

All Network Interface (8)

Name	Active	Interface Type	Bandwidth	IP Addr	Throughput	Errors	Discards
Fa0/0	true	EthernetCsmacd	100 M	[redacted]	-	-	-
Fa0/1	true	EthernetCsmacd	100 M	[redacted]	0.00 MBps	0.00	0.00
Vo0	true	Other	4,295 M	-	0.00 MBps	0.00	0.00
Nu0	true	Other	4,295 M	-	0.00 MBps	0.00	0.00
Foreign Exchange Office 0/3/0	true	VoiceFXO	0.00 M	-	0.00 MBps	-	-
Foreign Exchange Office 0/3/1	true	VoiceFXO	0.00 M	-	0.00 MBps	-	-
Foreign Exchange Office 0/3/2	true	VoiceFXO	0.00 M	-	0.00 MBps	-	-
Foreign Exchange Office 0/3/3	true	VoiceFXO	0.00 M	-	0.00 MBps	-	-

Fa0/0

Network Summary | Running Info | Ethernet CRC Error | Token Ring CRC Error

Interface Name	Fa0/0
Interface Alias	
Interface Description	FastEthernet0/0
Interface Type	EthernetCsmacd
Status	UP
MTU	1,500

IP Address [redacted]

Subnet	255.255.255.0
Origin	Manual
Status	Preferred
Type	Unicast
Storage	NonVolatile

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 7. 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 8. 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 9. 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 is always 0. - In Unicast 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 Unicast 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 10. Ethernet CRC Error view

Data Displayed	• IS Hcounter — High Capacity Counter objects. If the dot3HCStatsTable has an entry, this interface is 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 then transmitted successfully. • Multiple Collision Frames — A count of frames that are involved in more than one collision and are then 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 11. 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. • Recovery — 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 happens 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 12. Network Statistics Summary view

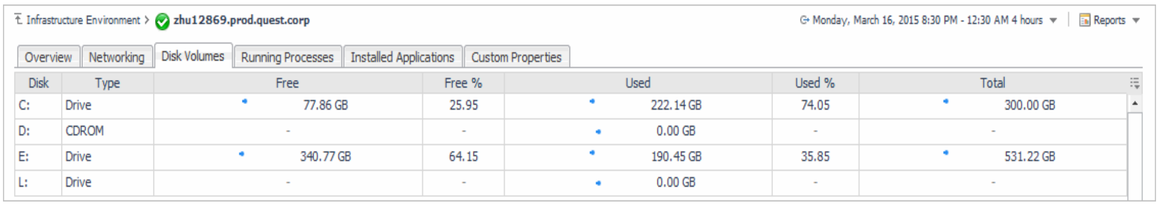
Data Displayed	General	• SNMP In Packets — The total number of messages delivered to the SNMP entity from the transport service. • SNMP Out Packets — The total number of SNMP Messages which were passed from the SNMP protocol entity to the transport service.
	ICMP	• In Messages — The total number of ICMP 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 15. Disk Volumes view


Infrastructure Environment > zhu12869.prod.quest.corp
Monday, March 16, 2015 8:30 PM - 12:30 AM 4 hours
Reports
Overview
Networking
Disk Volumes
Running Processes
Installed Applications
Custom Properties

Disk	Type	Free	Free %	Used	Used %	Total
C:	Drive	77.86 GB	25.95	222.14 GB	74.05	300.00 GB
D:	CDROM	-	-	0.00 GB	-	-
E:	Drive	340.77 GB	64.15	190.45 GB	35.85	531.22 GB
L:	Drive	-	-	0.00 GB	-	-

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.

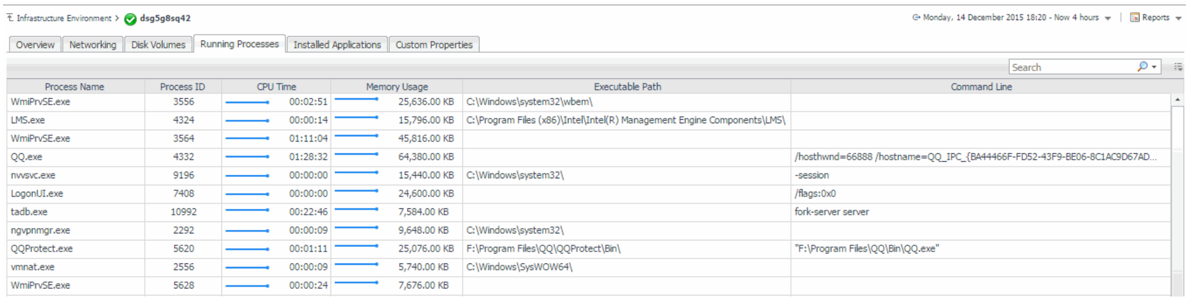
2 Click Explore.

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 16. Running Processes view



Process Name	Process ID	CPU Time	Memory Usage	Executable Path	Command Line
WmiPrvSE.exe	3556	00:02:51	25,636.00 KB	C:\Windows\system32\wbem\	
LMS.exe	4324	00:00:14	15,796.00 KB	C:\Program Files (x86)\Intel\Intel(R) Management Engine Components\LMS\	
WmiPrvSE.exe	3564	01:11:04	45,816.00 KB		
QQ.exe	4332	01:28:32	64,380.00 KB		/hosthwnd=66888 /hostname=QQ_IPC_{BA44466F-FD52-43F9-BE06-8C1AC9D67AD...
nvvsvc.exe	9196	00:00:00	15,440.00 KB	C:\Windows\system32\	-session
LogonUI.exe	7408	00:00:00	24,600.00 KB		/flags:0x0
tadb.exe	10992	00:22:46	7,584.00 KB		fork-server server
ngvpnmgr.exe	2292	00:00:09	9,648.00 KB	C:\Windows\system32\	
QQProtect.exe	5620	00:01:11	25,076.00 KB	F:\Program Files\QQ\QQProtect\Bin\	"F:\Program Files\QQ\Bin\QQ.exe"
vmnat.exe	2556	00:00:09	5,740.00 KB	C:\Windows\SysWOW64\	
WmiPrvSE.exe	5628	00:00:24	7,676.00 KB		

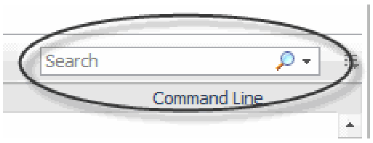
The table is comprised of the following fields:

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

- CPU Time — The total CPU time used for the process.
- 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 17. The Search box.



How to get here

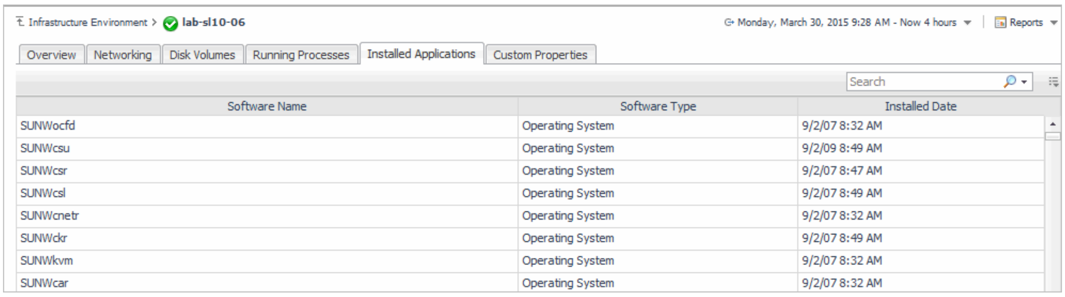
1. On the Infrastructure Environment dashboard, select a host monitored by an SNMP agent.
2. Click Explore.

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 18. Installed Applications view



Software Name	Software Type	Installed Date
SUNWocfd	Operating System	9/2/07 8:32 AM
SUNWcsu	Operating System	9/2/09 8:49 AM
SUNWcsr	Operating System	9/2/07 8:47 AM
SUNWcsl	Operating System	9/2/07 8:49 AM
SUNWcnetr	Operating System	9/2/07 8:32 AM
SUNWckr	Operating System	9/2/07 8:49 AM
SUNWkvm	Operating System	9/2/07 8:32 AM
SUNWcar	Operating System	9/2/07 8:32 AM

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

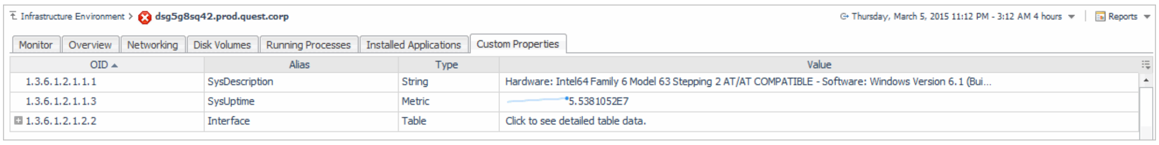
1. On the Infrastructure Environment dashboard, select a host monitored by an SNMP agent.
2. Click Explore.

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 19. Custom Properties view



Infrastructure Environment > dsg5g8sq42.prod.quest.corp
Thursday, March 5, 2015 11:12 PM - 3:12 AM 4 hours
Reports
Monitor
Overview
Networking
Disk Volumes
Running Processes
Installed Applications
Custom Properties

OID ▲	Alias	Type	Value
1.3.6.1.2.1.1.1	SysDescription	String	Hardware: Intel64 Family 6 Model 63 Stepping 2 AT/AT COMPATIBLE - Software: Windows Version 6.1 (Bui...
1.3.6.1.2.1.1.3	SysUptime	Metric	5.5381052E7
⊞ 1.3.6.1.2.1.2.2	Interface	Table	Click to see detailed table data.

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 Us

We are more than just a name

We are on a quest to make your information technology work harder for you. That is why we build community-driven software solutions that help you spend less time on IT administration and more time on business innovation. We help you modernize your data center, get you to the cloud quicker and provide the expertise, security and accessibility you need to grow your data-driven business. Combined with Quest's invitation to the global community to be a part of its innovation, and our firm commitment to ensuring customer satisfaction, we continue to deliver solutions that have a real impact on our customers today and leave a legacy we are proud of. We are challenging the status quo by transforming into a new software company. And as your partner, we work tirelessly to make sure your information technology is designed for you and by you. This is our mission, and we are in this together. Welcome to a new Quest. You are invited to Join the Innovation™.

Our brand, our vision. Together.

Our logo reflects our story: innovation, community and support. An important part of this story begins with the letter Q. It is a perfect circle, representing our commitment to technological precision and strength. The space in the Q itself symbolizes our need to add the missing piece—you—to the community, to the new Quest.

Contacting Quest

For sales or other inquiries, visit https://www.quest.com/company/contact-us.aspx or call +1-949-754-8000.

Technical support resources

Technical support is available to Quest customers with a valid maintenance contract and customers who have trial versions. You can access the Quest Support Portal at https://support.quest.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. The Support Portal enables you to:

- Submit and manage a Service Request.
- View Knowledge Base articles.
- Sign up for product notifications.
- Download software and technical documentation.
- View how-to-videos.
- Engage in community discussions.
- Chat with support engineers online.
- View services to assist you with your product.