

Foglight® Infrastructure Utilities User and Reference Guide 7.1.0



© 2023 Quest Software Inc.

ALL RIGHTS RESERVED.

This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of Quest Software Inc.

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 Where next meets now 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 LLC 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 trademark 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. Tevtron, the Tevtron logo, and CitraTest are registered trademarks of Tevtron, 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 owners.

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 for Infrastructure Foglight® Infrastructure Utilities User and Reference Guide
Updated - 2023
Foglight Version - 7.1.0
Cartridge Version - 7.1.0

Contents

Introduction to this guide	6
Monitoring Web transactions	7
Configuring credentials for Web sites requiring user or proxy authentication	7
Configuring credentials to access Web sites requiring user authentication	9
Configuring credentials for accessing Web sites through proxy servers	12
Monitoring HTTPs URLs in FIPS-compliant mode	16
Monitoring URLs that require a client certificate	16
Exploring your collection of monitored Web sites	17
Expanding your collection of monitored sites	18
Removing Web sites from the existing collection	21
Moving multiple transactions as a group	21
Removing stale transactions from the Performance Browser dashboard	22
Viewing and editing individual Web transaction details	23
Investigating the performance of Web transactions and monitoring locations	26
Exploring the FAQs tab	27
Drilling down on transactions	27
Drilling down on locations via the Locations tab	29
Exploring Web Monitor services	30
Generating reports	33
Configuring Web Monitor agent properties	34
Settings	34
Data Collection Scheduler	35
View reference	36
Web Monitor Performance Browser views	36
Web Monitor Transaction Management views	59
Web Monitor Service Operation Console and Foglight for APM Transactions views	63
Monitoring network devices	67
Configuring the ICMP service for monitoring	67
Configuring the Agent Manager ICMP service	68
Configuring OS-Level ICMP services	69
Managing monitored network devices	69
Expanding your collection of monitored network devices	71
Removing network devices from the existing collection	74
Viewing and editing individual network device details	74
Investigating the performance of network devices	77
Exploring individual network devices	78
Tracing data packets between monitoring locations and network devices	79
Exploring the FAQ tab	80
Generating reports	81
Configuring the agent properties	81
Configuring Net Monitor agent properties	82
View reference	84

Net Monitor Devices Management views	84
Net Monitor Performance Browser views	86
About Us	104
We are more than just a name	104
Our brand, our vision. Together.	104
Contacting Quest	104
Technical support resources	104

Introduction to this guide

Welcome to the Infrastructure Utilities User and Reference Guide.

This User and Reference Guide provides agent configuration instructions and information on investigating the performance of monitored Web sites and monitored network devices. It describes the dashboards included with Foglight Web Monitor and Foglight Net Monitor, and contains instructions for configuring monitoring agents that collect information from monitored systems.

This guide is intended for any user who wants to know more about the monitoring agent properties and the dashboards included with these utilities. It is also meant for those users that want to learn about the rules that are included with the Infrastructure utilities.

Foglight Log Monitor is an infrastructure utility shipped with Foglight for Infrastructure which monitors log files and identifies activities that can potentially lead to performance issues. For more information about Foglight Log Monitor, see the *Foglight for Infrastructure Release Notes* and *User and Reference Guide*.

Monitoring Web transactions

Foglight Web Monitor allows you to monitor Web site response times and to investigate service levels that show the signs of potential performance problems, when monitored from specific points in your environment.

When you deploy Foglight Web Monitor, a set of predefined dashboards enables you to view the performance of the monitored Web sites. They allow you to ensure consistent Web server performance by reviewing the performance statistics. Better management of your Web sites can be achieved when you are alerted of potential problems before end users are affected.

Foglight Web Monitor relies on the Web Monitor Agent to collect data. The agent collects transaction information from specified URLs. Given a collection of URLs and a pre-defined collection schedule, the Web Monitor Agent attempts to connect to these Web sites, gathering response time data and sending it back to the Management Server on each data collection attempt.

Start by installing Foglight Web Monitor on the Management Server, deploying the Web Monitor Agent package, and creating agent instances on one or more hosts. For installation instructions, see the *Foglight Infrastructure Utilities Release Notes*.

If you are planning to monitor transactions from any Web sites that require user authentication, you need to configure appropriate user credentials. For more information, see [Configuring credentials for Web sites requiring user or proxy authentication](#).

At this point you have an option of providing to the agent the list of URLs that you want to monitor, or you can do that later using the Transaction Management dashboard. In addition to managing the collection of monitored Web sites, this dashboard allows you to drill down on individual Web site transaction details, edit the settings that control alarm generation, and provide authentication details, when needed. For more information, see [Exploring your collection of monitored Web sites](#).

Next, navigate to the Performance Browser. This dashboard displays the state of your system performance, providing a visual representation of the status of the monitored transactions and locations. Using this dashboard on a daily basis you can obtain an in-depth understanding of the state of your monitored environment. Monitoring the same collection of Web sites from different agent locations allows you to rule out any issues that may be related to host connectivity rather than Web site response issues. For more information, see [Investigating the performance of Web transactions and monitoring locations](#).

The Web Monitor Agent is equipped with a set of properties that affect its running state. You can make changes to them, as required. For more information about the Web Monitor Agent properties, see [Configuring Web Monitor agent properties](#).

For additional information, see the following topics:

- [Exploring Web Monitor services](#)
- [Generating reports](#)
- [View reference](#)

Configuring credentials for Web sites requiring user or proxy authentication

Monitoring Web sites that require user or proxy authentication requires some additional configuration. To successfully access these sites with the Web Monitoring Agent and collect response time metrics, you must provide the credentials these pages need to access them. A valid credential contains a user name and password that enables the Web Monitoring Agent to access the monitored Web site. You can create credentials using the Manage Credentials dashboard.

NOTE: Only Foglight Administrators are granted privileges to view and manage credentials. To access the Manage Credentials dashboard, your user account must have the Administrator role. To obtain this role, contact your Foglight Administrator.

To get started with managing credentials:

- 1 Log in to the Foglight browser interface.
- 2 On the navigation panel, under **Dashboards**, click **Administration > Credentials**.

The Credentials page appears in the display area.

Credentials

Credential management is a reliable way to control user access to various system components taking into account your organization's security policies. Use this page to maintain user credentials and the related lockboxes, monitor credential events, and view the status of all registered credential clients.

- Manage Credentials**
 - A credential is the information needed to gain access to a system. Credentials are stored in lockboxes.
 - There are 4 credentials.
 - Add, edit and delete credentials.
- Monitor Credential Alarms**
 - There are 7 credential alarms.
 - Monitor credential alarms.
- Manage Lockboxes**
 - A lockbox contains a collection of encrypted credentials and the keys used for their encryption and decryption.
 - There are 1 lockboxes.
 - Add and delete lockboxes.
- View Clients**
 - There are 3 credential clients.
 - Monitor credential clients.

Domain Specific Credential Views

There are 0 customized domain specific credential views provided by the currently installed cartridges.

- 3 On the Credentials page, click **Manage Credentials**.

The Manage Credentials dashboard appears in the display area.

Manage Credentials

A credential is the information that gains access to system resources. Credentials are stored in lockboxes. Use this page to configure credentials to enable access to selected monitored resources. This workflow supports a set of commonly used credentials. Map each credential to one or more resources, choosing the parameters and patterning criteria that best suit your needs. For example, map a credential to a target port number or host address using string, regular expression, or IP address matching. The validity of a credential is determined by its policies. A credential can have none, one or several policies.

Edit	Lockbox	Name	Alarms	Valid Until	Relative Order	Type	Resource Mappings	Policies
	System	Database Server Access			400	Domain, User Name, and Password (Windows)	2 (Usage equals 'OS Monitoring...)	2 Use Count=5, Cache Tim...
	System	Production Server Access			300	Domain, User Name, and Password (Windows)	1 Usage equals 'OS Monitoring...	1 Use Count=5
	System	Local Account for Monitoring UnixOS			200	Use Client's Login At Connection Time	1 Usage equals 'OS Monitoring...	
	System	Local Account for Monitoring Window...		2	100	Use Client's Login At Connection Time	1 Usage equals 'OS Monitoring...	

For complete information about credentials, see the *Administration and Configuration Help*.

For more information, see the following topics:

- [Configuring credentials to access Web sites requiring user authentication](#)
- [Configuring credentials for accessing Web sites through proxy servers](#)
- [Monitoring HTTPs URLs in FIPS-compliant mode](#)
- [Monitoring URLs that require a client certificate](#)

Configuring credentials to access Web sites requiring user authentication

Web Monitor Agent instances that monitor Web sites requiring user authentication need to have credentials that supply this information. A valid credential needed to access a password-protected page requires all of the following information, all encapsulated in a single credential:

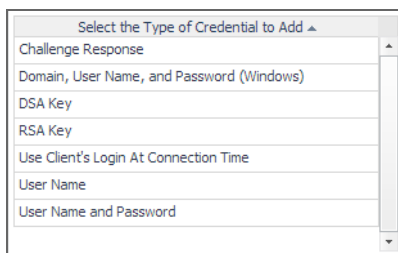
- Web site address
- User name
- Password

To get started, create a new credential of the *User Name and Password* type containing a resource mapping with the *Web Monitor Authentication* usage. Next, provide the URL address that requires these credentials, and save changes to the credential.

To create a credential needed to access a password-protected Web site:

- 1 Log in to the Foglight browser interface.
- 2 On the navigation panel, under **Dashboards**, click **Administration > Credentials**.
- 3 On the Credentials page that appears in the display area, click **Manage Credentials**.
- 4 On the Manage Credentials dashboard that appears in the display area, click **Add**.

The **Select the Type of Credential to Add** list appears.



- 5 In the **Select the Type of Credential to Add** list, click the credential appropriate for your authentication type.
 - **User Name and Password** for Basic authentication.
 - **Domain, User Name, and Password (Windows)** for NTLM authentication.

The **Add A New Credential** wizard appears with the **Credential Properties** page open.

- 6 On the **Credential Properties** page, type the required properties, and click Next.

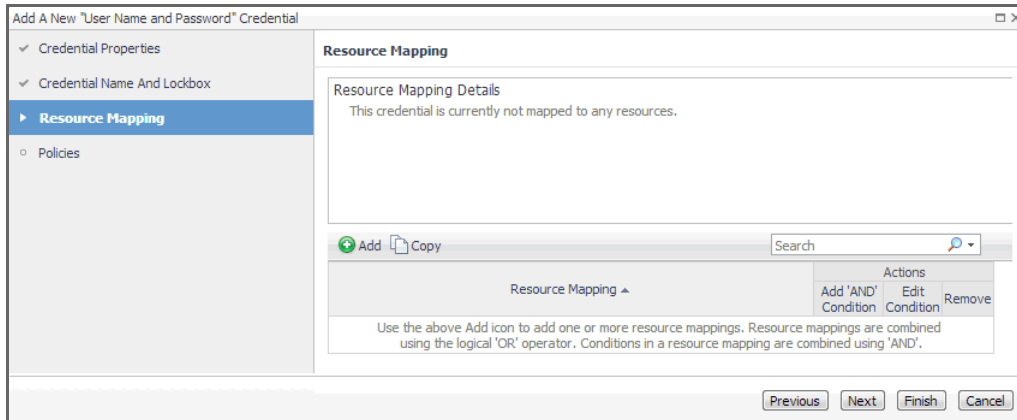
The **Credential Name and Lockbox** page appears.

- 7 On the **Credential Name and Lockbox** page, select the lockbox in which you want to store the Web Monitor credential, and optionally change the credential name.

TIP: If you do not find a suitable lockbox in the list, click **Add** to create a new one.

Click **Next**.

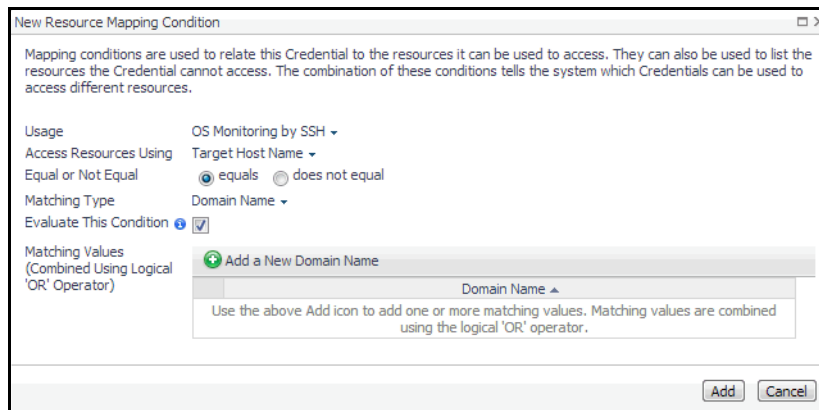
The **Resource Mapping** page appears.



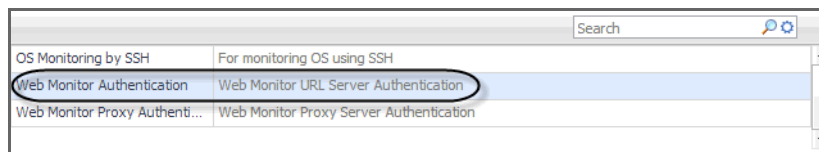
8 Provide the URL of the Web site that requires user authentication.

a On the **Resource Mapping** page, click **Add**.

The **New Resource Mapping Condition** dialog box appears.



b In the **New Resource Mapping Condition** dialog box, click **Usage**, and select **Web Monitor Authentication** from the popup that appears.



The popup closes and the **Access Resources Using** setting is automatically set to **Web Monitoring URL**, indicating that the credential is used when accessing the URL address you are about to specify.

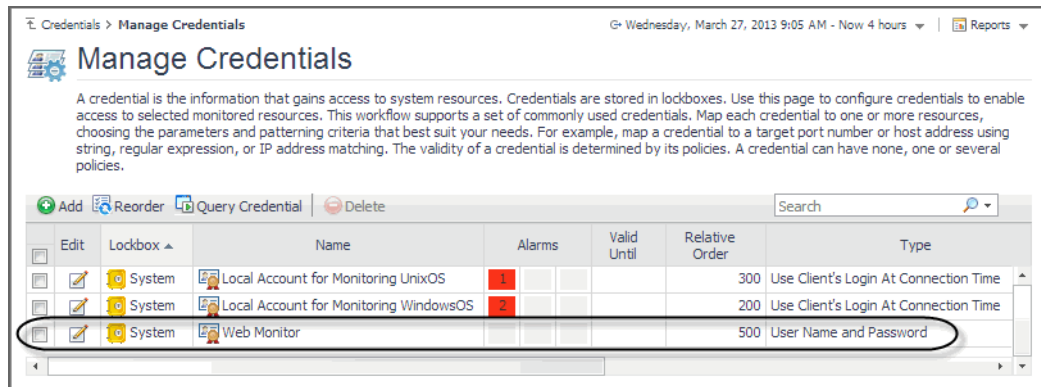
- c Ensure that **equals** and **Evaluate This Condition** are selected.
- d Click **Add a New String** and type the URL into the highlighted cell appearing in the **String** column.

You can specify multiple URLs, if required. During the evaluation, they are combined into an expression using the logical OR operator.

- e Click **Add**.
- f The **New Resource Mapping Condition** dialog box closes and the Resource Mapping page refreshes, showing the newly specified resource mapping.

- g **Optional**—At this point you can refine your credential settings to specify, for example, the time during which the credential is valid, the number of failed attempts after which the credential is locked, the number of times the credential can be used, or the period of time during which the credential data is cached on the server. For complete information, see the *Administration and Configuration Help*.
- h Click **Finish**.

The **Add A New “User Name and Password” Credential** wizard closes and the Manage Credentials dashboard refreshes, showing the newly added Web Monitor credential in the list.



Configuring credentials for accessing Web sites through proxy servers

Web Monitor Agent instances that monitor Web sites through a proxy server need to have credentials supplying that information. A valid credential needed to access a URL page through a proxy server requires the host name or the IP address of the proxy server along with the port number it uses to listen for incoming requests.

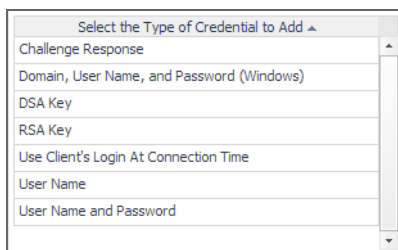
To get started, create a new credential of the *User Name and Password* type containing a resource mapping with the *Web Monitor Proxy Authentication* usage. Next, specify the host name or IP address of the proxy server and the port number, and save your changes.

NOTE: Only Foglight Administrators are granted privileges to view and manage credentials. To access the Manage Credentials dashboard, your user account must have the Administrator role. To obtain this role, contact your Foglight Administrator.

To create a credential for accessing a Web site through a proxy server:

- 1 Log in to the Foglight browser interface.
- 2 On the navigation panel, under **Dashboards**, click **Administration > Credentials**.
- 3 On the Credentials page that appears in the display area, click **Manage Credentials**.
- 4 On the Manage Credentials dashboard that appears in the display area, click **Add**.

The **Select the Type of Credential to Add** list appears.



- 5 In the **Select the Type of Credential to Add** list, click the credential appropriate for your authentication type.
 - **User Name and Password** for Basic authentication.
 - **Domain, User Name, and Password (Windows)** for NTLM authentication.

The **Add A New Credential** wizard appears with the **Credential Properties** page open.

- 6 On the **Credential Properties** page, type the required properties, and click **Next**.

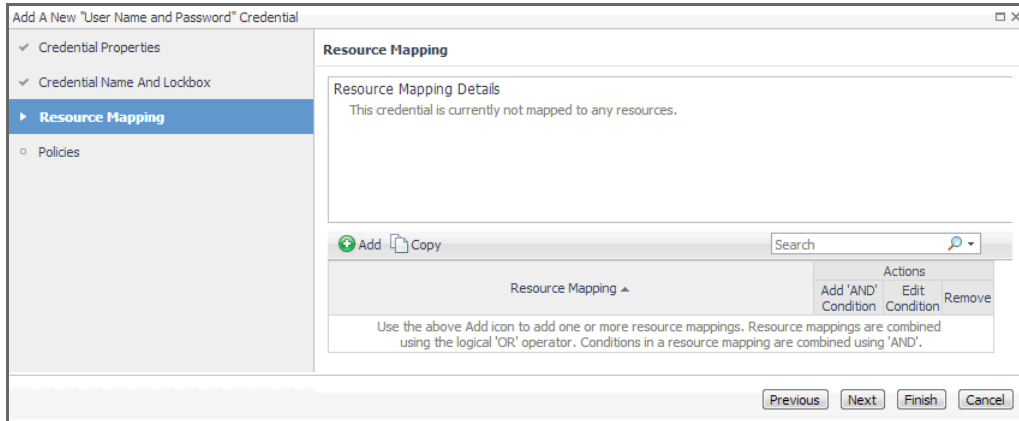
The **Credential Name and Lockbox** page appears.

- 7 On the **Credential Name and Lockbox** page, select the lockbox in which you want to store the Web Monitor credential, and optionally change the credential name.

TIP: If you do not find a suitable lockbox in the list, click **Add** to create a new one.

Click **Next**.

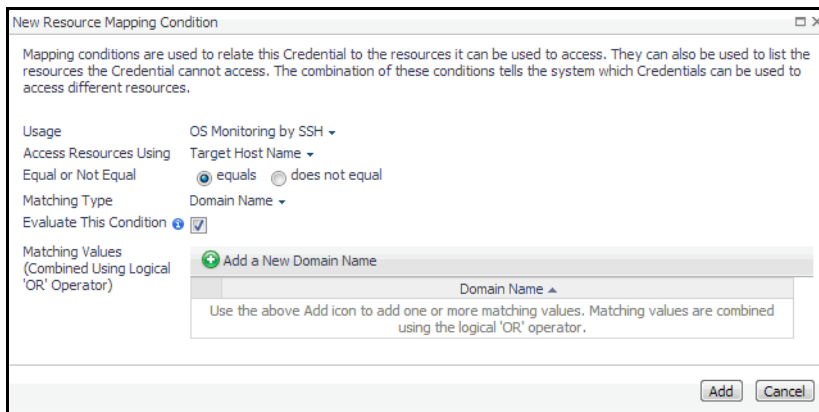
The **Resource Mapping** page appears.



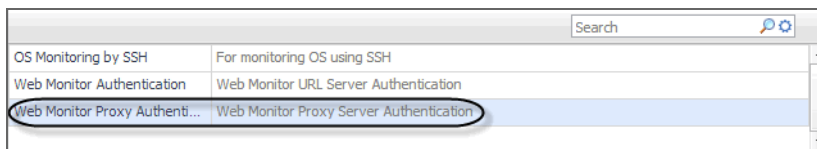
- 8 Specify the name or IP address of the proxy server that you want to use.

- a On the **Resource Mapping** page, click **Add**.

The **New Resource Mapping Condition** dialog box appears.




- b In the **New Resource Mapping Condition** dialog box, click **Usage**, and select **Web Monitor Proxy Authentication** from the popup that appears.



- c Specify the host name or IP address of the proxy server. Click **Access Resources Using**, and in the popup that appears, select one of the following options, as required:
 - **Target Host Name**
 - **Target Host Address**
 - d Ensure that **equals** and **Evaluate This Condition** are selected.

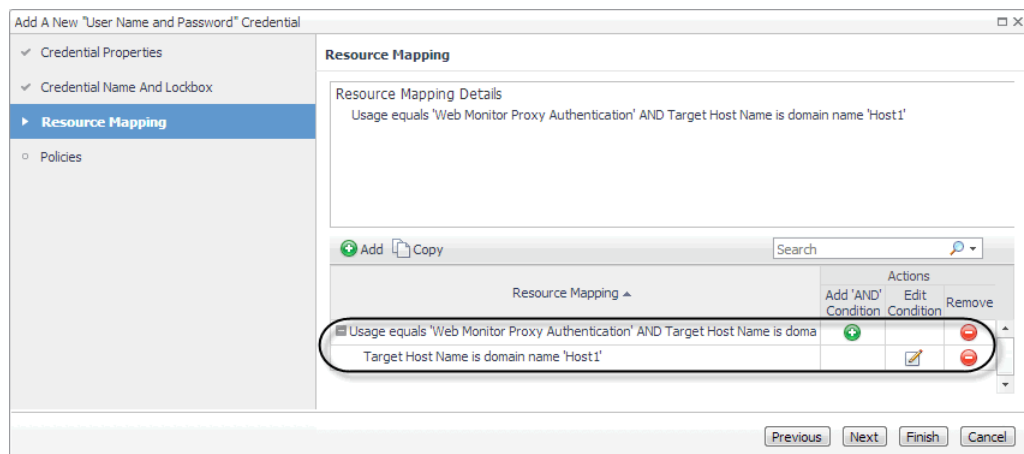
- e Indicate if you want to use a literal or regular expression to specify the host name or IP address. Using regular expressions in general gives you more flexibility in that you can specify multiple servers than using a single expression mapping.

Click **Matching Type**, and in the popup that appears, select one of the following options:


- **Domain Name:** Select this option if you want to use a literal expression to specify the host name or IP address.
- **Regular Expression:** Select this option if you want to use a regular expression to specify the host name or IP address.
- f Click  and in the highlighted cell that appears, type the literal or regular expression (as selected in Step e) that resolves to the desired proxy server name or IP address (as selected in Step c).

You can specify multiple servers, if required. During the evaluation, they are combined into an expression using the logical OR operator.

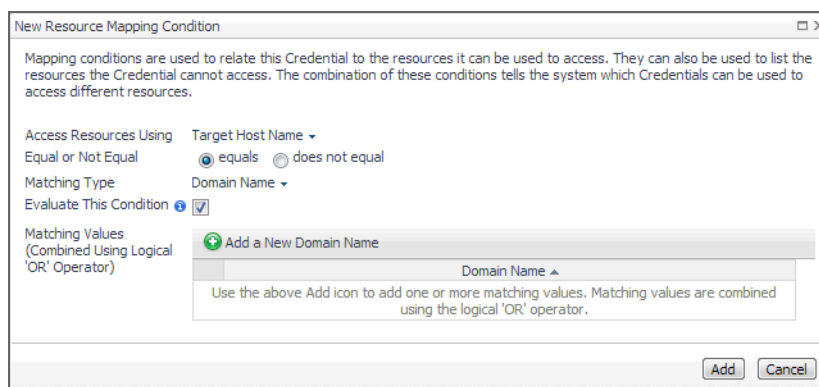
- g Click **Add**.
- h The **New Resource Mapping Condition** dialog box closes and the Resource Mapping page refreshes, showing the newly specified proxy server.



- 9 Specify the port number of the proxy server that you want to use.

- a On the Resource Mapping page, in the row containing the newly specified proxy server, click  in the Add 'AND' Condition column.

The **New Resource Mapping Condition** dialog box appears.




- b Specify the port number the proxy server uses to listen for incoming requests. Click **Access Resources Using in the New Resource Mapping Condition dialog box**, and in the popup that appears, select **Target Port**.

Target Host Name	Access a resource using the name of the host where it resides.
Target Port	Access a resource using the port number of the host where it resides.
Target Host Address	Access a resource using the IP of the host where it resides.

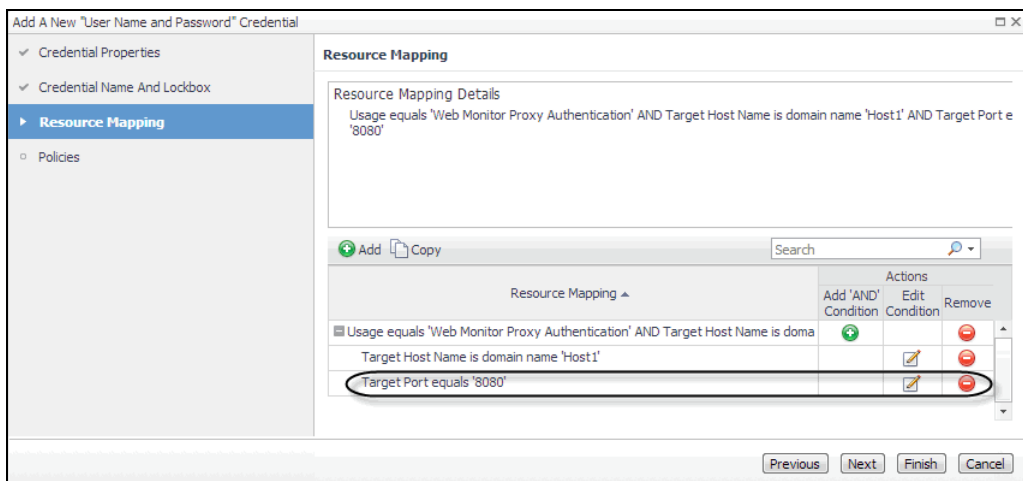
- c Ensure that **equals** and **Evaluate This Condition** are selected.
- d Indicate if you want to use a literal or regular expression to specify the port number. Using regular expressions in general gives you more flexibility in that you can specify multiple port numbers than using a single expression mapping.

Click **Matching Type**, and in the popup that appears, select one of the following options:

- **Exact Match (Case Sensitive):** Select this option if you want to use a literal expression to specify the port number.
 - **Regular Expression:** Select this option if you want to use a regular expression to specify the port number.
- e Click  and in the highlighted cell that appears, type the regular or literal expression (as selected in Step e) that resolves to the desired port number.

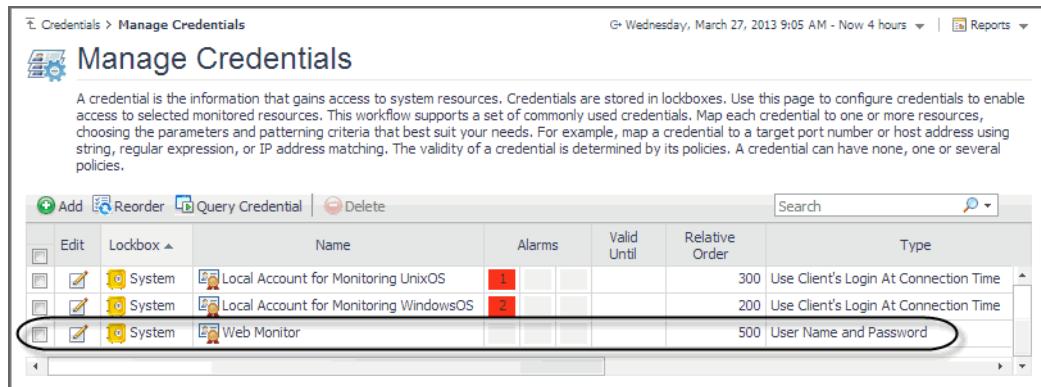
You can specify multiple servers, if required. During the evaluation, they are combined into an expression using the logical **OR** operator.

- f Click **Add**.
- g The **New Resource Mapping Condition** dialog box closes and the Resource Mapping page refreshes, showing the newly specified port number.



- h **Optional**—At this point you can refine your credential settings to specify, for example, the time during which the credential is valid, the number of failed attempts after which the credential is locked, the number of times the credential can be used, or the period of time during which the credential data is cached on the server. For complete information, see the *Administration and Configuration Help*.
- i Click **Finish**.

The **Add A New "User Name and Password" Credential** wizard closes and the Manage Credential dashboard refreshes, showing the newly added Web Monitor credential in the list.



Monitoring HTTPs URLs in FIPS-compliant mode

Foglight Web Monitor agent supports to run in FIPS-compliant mode, depending on the Agent Manager where it is deployed on. That is to say if the Agent Manager runs in FIPS-compliant mode, the Web Monitor agent will be configured to be FIPS-compliant automatically, and vice versa.

When Foglight Web Monitor agent runs in FIPS-compliant mode, and tries to access a Web site with HTTPs connection, the Web Monitor agent requires to authenticate the Web site's certificate. In order to successfully access these URLs and collect response time metrics, you need to import the Web site's certificates to Agent Manager's certificate store.

To import the Web site's certificate to the Agent Manager certificate store:

- 1 Launch a command shell on the Agent Manager machine, and navigate to the `<fglam_home>/bin` directory.
- 2 Import the Web site's certificate with the following command:

```
fglam --add-certificate <alias=/path/to/certificate>
```

For example:

```
fglam --add-certificate your_alias_name=C:\Certificates\test\ServerSSL.cer
```

Monitoring URLs that require a client certificate

Monitoring URLs that require client authentication requires some additional configuration. To successfully access these URLs with the Web Monitoring Agent and collect response time metrics, you must import the certificates for URLs.

To support the monitoring of URLs that require a client certificate:

- 1 Deploy the *WebMonitor* Agent to the Foglight Agent Manager.
- 2 Open the command line and switch to the following path:
`{fglam_home}/agents/WebMonitorAgent/{version}/lib`
- 3 Run this command to import the client certificate for some URLs:

For Windows®:

```
importKeystore.bat "-keystore {filepath} -pwd {password} -urls {ip}:{port} -createKeyStoreFile true"
```

For Linux®:


```
./importKeystore.sh "-keystore {filepath} -pwd {password} -urls {ip}:{port} -createKeyStoreFile true"
```

For example:

```
importKeystore.bat "-keystore D:\echen5\issue\ESC\ESC-1784\sha1\Sha1ClientCert.pfx -pwd Test1234 -urls 10.154.10.168:443 10.154.10.168:6443 -createKeyStoreFile true"
```

i **NOTE:** Ensure you have read and write rights for the following path:
`{fglam_home}/state/default/certificates`

NOTE: The tool for importing the client authentication depends on the JRE being used. Ensure that the JRE exists in one of the following locations:

- When Fglam is external, the JRE should be found in `{fglam_home}`.
- When the Fglam is embedded, the JRE should be found in `{foglight_home}`.
- When the JRE is neither in `{fglam_home}` nor `{foglight_home}`, the path to the JRE should be found in the environment variable `JAVA_HOME`.

The Microsoft® Internet Information Server (IIS) by default enables the TLSv1 and disables the TLSv1.2 protocols. The JDK 1.7+ (included in Foglight Agent Manager 5.7.4 and later) by default handles handshake with TLSv1.2. If the server side and the client side do not include the same supported TLS version, this causes the HTTPs request to fail. The following workarounds are available in this case:

- **Workaround #1**

- 1 Force the client side to handle handshake with TLSv1, by setting the "Force TLSv1" agent property to "True" (for details, see [Settings](#)).
- 2 Ensure that all the Web server whose URLs you are monitoring support TLSv1.

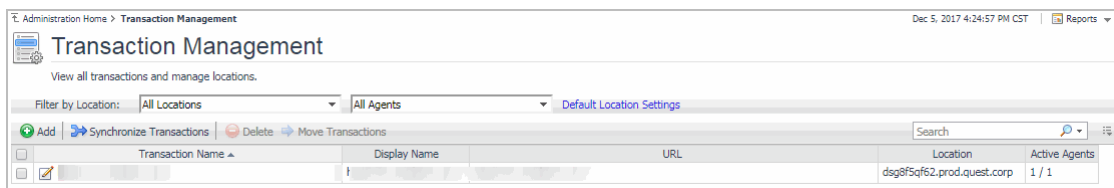
- **Workaround #2**

- 1 Enable TLSv1.2 for your IIS server. (Refer to the [best practice](#) to configure IIS with SSL/TLS.)
- 2 Set the "Force TLSv1" agent property to "False" (for details, see [Settings](#)).
- 3 If your IIS server enabled TLSv1.2 and disabled TLSv1, and you use sha512 certificates, then make sure you applied the following update to your server: <https://support.microsoft.com/en-us/kb/2973337>.

Exploring your collection of monitored Web sites

The Transaction Management dashboard displays a list of monitored Web sites and the locations from which they are monitored. One Web site can be monitored from one or more locations. This can give you a good understanding of the complexity of your monitored environment and the locations from which a specific Web site is monitored.

Figure 1. Transaction Management dashboard

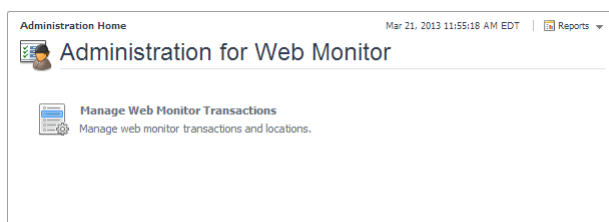


For complete details about the data appearing on this dashboard, see the [Transaction Management table](#).

To explore the collection of monitored Web sites:

- 1 Log in to the Foglight browser interface.
- 2 On the navigation panel, under **Dashboards**, click **Web Monitor > Administration Home**.

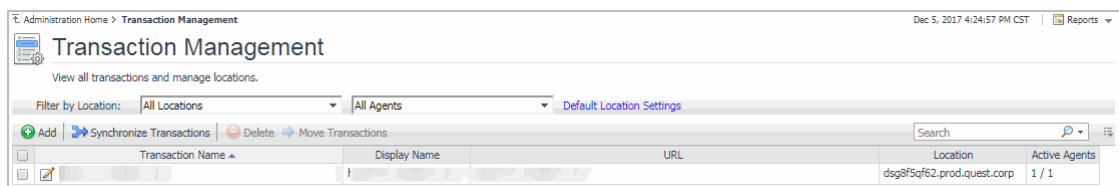
The Administration for Web Monitor page appears in the display area.



- 3 Navigate to the Transaction Management dashboard.

On the Administration Home page, click **Manage Web Monitor Transactions**.

The Transaction Management dashboard appears in the display area.



For more information, see the following topics:

- [Expanding your collection of monitored sites](#)
- [Removing Web sites from the existing collection](#)
- [Moving multiple transactions as a group](#)
- [Removing stale transactions from the Performance Browser dashboard](#)
- [Viewing and editing individual Web transaction details](#)

Expanding your collection of monitored sites

The Transaction Management dashboard allows you to add URLs to the existing collections of monitored sites. Adding a new URL causes the Web Monitor Agent to start collecting information about that URL in the next collection period.

This assumes that you already have the agent package deployed to the Foglight Agent Manager host, and one or more active Web Monitor Agent instances in place. For complete information on how to deploy an agent package, and to create and activate agent instances, see the *Administration and Configuration Help*.

To start monitoring a Web site:

- 1 On the Transaction Management dashboard, click **Add**.

The **Add Transactions** dialog box appears.

URL	Transaction Name	Get Page Header Only	Expected Content	Unexpected Content
		<input type="checkbox"/>		

Deploy to Locations:

Location (FgIAM)	Agent Name
dsg8f5qf62.prod.quest.corp	WebMonitorAgent@dsg8f5qf62.prod.quest.corp
fglam1	WebMonitorAgent@fglam1

Only active WebMonitor agents that has associated locations will be listed. You may need to [Set up Agents](#)

[Optional Advanced Settings](#)

Save Cancel

The **Add Transactions** dialog box shows a list of the Web sites whose transactions you want to monitor, a list of all Web Monitor Agent locations in your environment, and links to additional configuration settings.


- 2 In the **Add Transactions** dialog box, provide information about the Web site whose transactions you want to start monitoring.

- **URL:** The URL of the Web site that you want to monitor.
 - **TIP:** The Web Monitor Agent validates the URL address in the background, to prevent you from adding the duplicate URL address that has been monitored.
- **Transaction Name:** The name you want to associate with the transactions with this Web site.
 - **NOTE:** It is not allowed to associate multiple URL addresses with a same transaction.
- **Get Page Header Only:** Indicates whether you want to collect the page header only.
- **Expected Content:** If content validation is enabled for the agent instance that you want to monitor this URL, and the expected content type is HTML-based, type `html` in this column. Also, a text string could be used such as "laptop" and type `laptop` into this column. In case the monitoring agent detects binary content or the text string at this address, the validation fails and the agent logs an error message.

Content validation can be enabled using the **URL List** secondary agent properties. For more information, see [Settings](#).

- **Unexpected Content:** If unexpected content validation is enabled for the agent instance that you want to monitor this URL, and the unexpected content type is HTML-based, type `html` in this column. Also, a text string could be used such as "laptop" and type `laptop` into this column. In case the monitoring agent detects binary content or the text string at this address, the validation fails and the agent logs an error message. If this column is empty, that means the agent is not required to perform unexpected content validation.

Unexpected Content validation can be enabled using the **URL List** secondary agent properties. For more information, see [Settings](#).

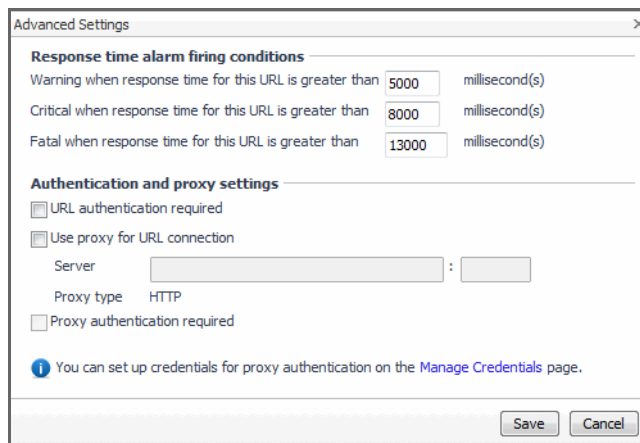
- 3 To add more URLs to the list, click **Add**, and populate the row that appears. To remove a row from the list, click .
- 4 In the **Deploy to Locations** area, select one or more Web Monitor Agent locations that you want to use to monitor the transactions with the newly specified Web sites.

If the host from which you want to configure transaction monitoring does not appear on the list, that is because it does not have a running instance of the Web Monitor Agent. To create a Web Monitor Agent instance on that host, click **Set up Agents** and configure the agent instance on that host. For more information about installing and configuring agent instances, see the *Administration and Configuration Help*.

i | **TIP:** The Web Monitor Agent requires a running instance of the Foglight Agent Manager on the same host. For details on installing and running the Agent Manager, see the *Agent Manager Guide*.

- 5 **Optional**—Specify thresholds for alarm generation, authentication, and proxy settings. If the URL requires user authentication, you need to supply credentials for accessing that URL.
 - a Click **Optional Advanced Settings**.

The **Advanced Settings** dialog box appears.



The image shows the 'Advanced Settings' dialog box. It has two main sections. The first section, 'Response time alarm firing conditions', contains three rows of settings: 'Warning when response time for this URL is greater than' with a value of 5000, 'Critical when response time for this URL is greater than' with a value of 8000, and 'Fatal when response time for this URL is greater than' with a value of 13000. All values are in 'millisecond(s)'. The second section, 'Authentication and proxy settings', contains several checkboxes: 'URL authentication required' (unchecked), 'Use proxy for URL connection' (checked), 'Proxy authentication required' (unchecked), and 'Server' (with a text input field). Below these is a 'Proxy type' dropdown set to 'HTTP'. At the bottom, there is a blue information icon and a message: 'You can set up credentials for proxy authentication on the Manage Credentials page.' There are 'Save' and 'Cancel' buttons at the bottom right.

- b In the **Advanced Settings** dialog box, in the **Response time alarm firing conditions** area, review the thresholds for alarm generation, and edit them, if required.
 - c In the **Authentication and proxy settings** area, specify the following information, as required.
 - **URL authentication required:** Select this check box only if the URL requires user authentication. If that is the case, you need to ensure that you have proper credentials in place to enable the Web Monitor Agent to access it. Click **Manage Credentials** to review the existing credentials, or to create new ones, as required. For more information, see [Configuring credentials to access Web sites requiring user authentication](#).

i | **TIP:** When finished, you can return to this dialog box using the breadcrumb trail.

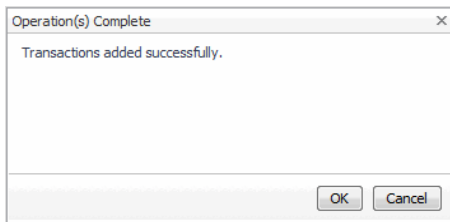
- **Use proxy for URL connection:** Select this check box only if the Web Monitor needs to use a proxy to access the specified URL. Click **Manage Credentials** to review the existing credentials, and create new ones, as required. For more information, see [Configuring credentials to access Web sites requiring user authentication](#).
- **Server:** If you need to configure proxy access, type the name of the proxy server followed by the port number.
- **Proxy authentication required:** Select this check box if the proxy requires authentication.

Click **Save**.

The **Advanced Settings** dialog box closes.

- 6 In the **Add Transactions** dialog box, click **Save**.

The **Operation(s) Complete** message box appears.



Click **OK** to close it.

- 7 In the Transaction Management dashboard, review the list of monitored transactions.

The newly added Web site is added to the list.

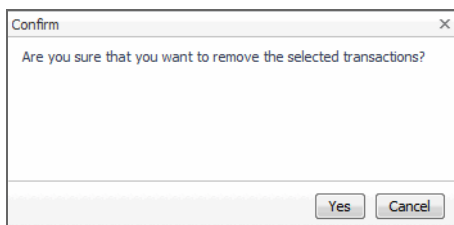
Removing Web sites from the existing collection

The Transaction Management dashboard allows you to remove URLs from the existing collection of monitored sites. Removing a URL from the list causes the Web Monitor Agent to stop collecting Web site transaction information about that URL. The data collected from a removed URL is kept in the Foglight database in accordance with the existing persistence settings. For more information, refer to the *Administration and Configuration Help*.

To stop monitoring a Web site:

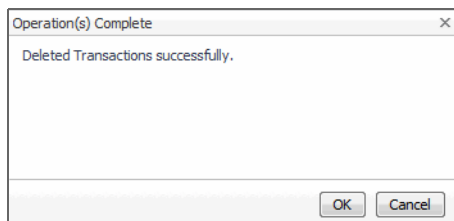
- 1 On the Transaction Management dashboard, select the Web site that you no longer want to monitor, and click **Delete**.

The **Confirm** message box appears.



- 2 Click **Yes** to confirm the removal and close the message box.

The **Operation(s) Complete** message box appears.



Click **OK** to close it.

- 3 In the Transaction Management dashboard, review the list of monitored transactions.

The newly removed Web site no longer appears in the list.

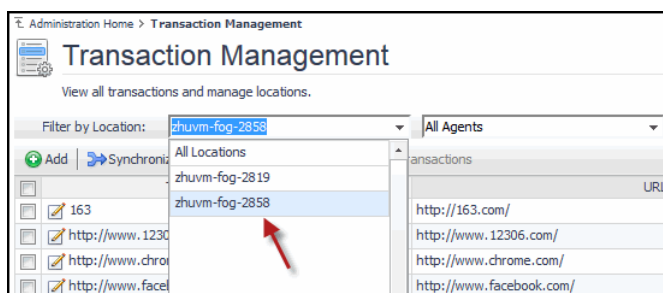
Moving multiple transactions as a group

Moving multiple transactions in a single operation may be accomplished via the Transaction Management dashboard.

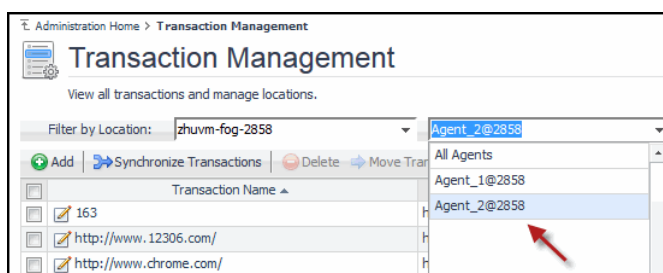
NOTE: You may not deploy the same transaction to multiple agents within the same location.

To move multiple transactions in a single operation:

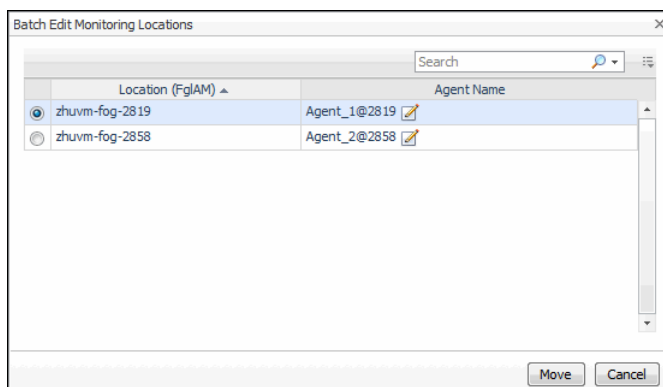
- 1 On the Transaction Management dashboard, filter the transactions by location.



- 2 On the Transaction Management dashboard, filter the transactions by agent.



- 3 Select the transactions you wish to move.
The Move Transactions button is enabled.
- 4 Click **Move Transactions**.
The Batch Edit Monitoring Locations dialog box is displayed.



- 5 Select an agent on another Foglight Agent Manager.
- 6 Click **Move**.


The Operation(s) Complete message box appears once the selected transactions have been redeployed from the original agent to the new selected agent.

Removing stale transactions from the Performance Browser dashboard

Occasionally, the list of transactions in the Performance Browser dashboard Quick View may contain a stale transaction that does not appear on the Transaction Management dashboard. You may remove stale transactions from the Performance Browser dashboard Quick View via the Foglight Data Management dashboard.

To delete a transaction from the Performance Browser Quick View:

- 1 Stop the Foglight Agent Manager that is installed on the host where the Web Monitor agent is running

 **NOTE:** If you do not stop the Foglight Agent Manager first, the Web Monitor agent instance will still reside on the host. For details on stopping the Foglight Agent Manager, refer to the Agent Manager Guide.
- 2 On the navigation panel, under **Dashboards**, click Management Server > Servers > Data Management.
- 3 Click All Services > Services > WebMonitor Pivot Service > Definition.
- 4 Select the Transaction you wish to delete, click Delete.
The Delete Topology Objects message box appears.
- 5 Click Delete to confirm the removal.
The Delete TopologyObjects Progress message box appears.
- 6 Click OK.
- 7 Restart the Foglight Agent Manager installed on the host.

Viewing and editing individual Web transaction details

Every monitored Web site is associated with a number of transaction-related settings. You can view and edit these settings using the Transaction Detail dashboard.

Figure 2. Transaction Detail dashboard

Administration Home > Transaction Management > Transaction Detail

Tuesday, December 5, 2017 12:08 PM - 4:08 PM 4 hours Reports

Transaction Detail

View and edit transaction details.

Transaction name: <http://www.baidu.com/>

Search

URL	Get Page Header Only	Expected Content	Unexpected Content	Display Name
http://www.baidu.com/	<input type="checkbox"/>			http://www.baidu.com/

Edit

Monitoring Locations

Search

Location (FgIAM)	Agent Name
<input checked="" type="checkbox"/> dsq8f5qf62.prod.quest.corp	WebMonitorAgent@dsq8f5qf62.prod.quest.corp

Edit

Advanced Settings

Response time alarm firing conditions

Warning when response time for this URL is greater than 5,000 millisecond(s)
Critical when response time for this URL is greater than 8,000 millisecond(s)
Fatal when response time for this URL is greater than 13,000 millisecond(s)

Authentication and proxy settings

☐ URL authentication required
☐ Use proxy for URL connection

Server: 80
Port: 80
Proxy type: HTTP
☐ Proxy authentication required

Edit

To access the Transaction Detail dashboard, click on a transaction name on the Transaction Management dashboard.

Figure 3. Transaction Name on Transaction Management Dashboard

Administration Home > Transaction Management

Dec 5, 2017 4:24:57 PM CST Reports

Transaction Management

View all transactions and manage locations.

Filter by Location: All Locations All Agents Default Location Settings

Add Synchronize Transactions Delete Move Transactions

Search

Transaction Name	Display Name	URL	Location	Active Agents
<input type="checkbox"/>			dsq8f5qf62.prod.quest.corp	1 / 1

For more information about the Transaction Management dashboard, see [Exploring your collection of monitored Web sites](#). For complete details about the data appearing on this dashboard, see [Transaction Detail view](#).

You can make changes to any transaction details that appear on this dashboard by clicking the appropriate **Edit** button and making the required changes.

Any changes you make to transaction alarm thresholds results in creating topology-scoped values of the registry variables that control these thresholds, and the other way around. The topology type used to contain Web transaction definitions is Internal Synthetic Transaction (Webmonitor), and the Internal Synthetic Transaction (Webmonitor) topology object names are the configured transactions names.

Figure 4. Synthetic_Transaction_MET_Warning Registry Variable

Edit Registry Variable: Synthetic_Transaction_MET_Warning

Name: Synthetic_Transaction_MET_Warning
Variable Type Classname: Double
Description: This is a benchmark to judge whether the response time of a transaction or transaction step is up the baseline, meanwhile, it's a threshold for warning alarms. Change...
Cartridge Name: WebMonitor-JIT
Cartridge Version: 5.7.2
Global Default: 5000.0 Change... Remove...

Performance Calendars List

Move		Schedule Name	Value
Up	Down		
<input type="checkbox"/>	<input type="checkbox"/>	Business week	Ref: NumberOfAlarmsWarning
<input type="checkbox"/>	<input type="checkbox"/>	Off-Hours Database Maintenance	Ref: ResponseTimeThreshold

Registry Values

Topology Type	Topology Object Name	Value
Internal Synthetic Transaction (Webmonitor)		Ref: AvailabilityCritical

NOTE: Access to Foglight registry variables, requires the Administrator role.

For more information about the Foglight registry, see the *Administration and Configuration Help*.

To edit transaction details:

- On the Transaction Detail dashboard, locate the settings that you want to edit.
 - To edit basic transaction information, such as its URL, in the **Basic Information** view, click **Edit**. The **Update Basic Transaction Information** dialog box appears.

Update Basic Transaction Information

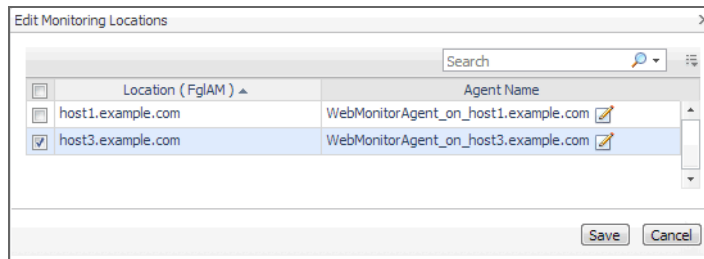
Transaction name: <http://www.baidu.com/>

URL	Get Page Header Only	Expected Content	Unexpected Content	Display Name
	<input type="checkbox"/>			

Save Cancel

Click the column that you want to update, and type the desired values.

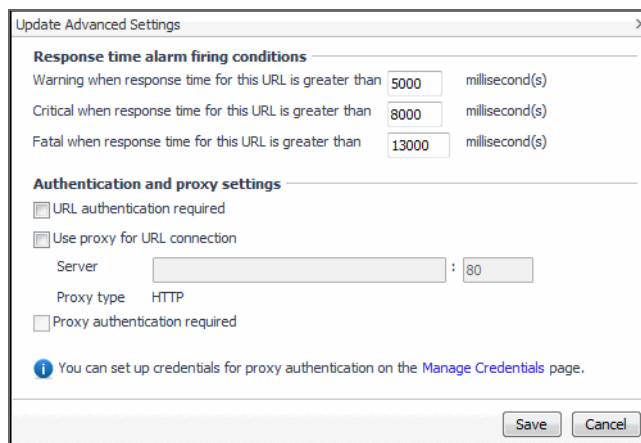
- To start monitoring this Web site with a new set of monitoring agents, in the **Monitoring Location** view, click **Edit**. The **Edit Monitoring Locations** dialog box appears.



Make your selections by selecting or clearing the check boxes next to the names of hosts on which the Web Monitor Agent is installed, as required.

- To specify different thresholds for alarm generation, or authentication and proxy settings, in the **Advanced Settings** view, click **Edit**.

The **Update Advanced Settings** dialog box appears.



To specify different thresholds for alarm generation, in the **Response time alarm firing conditions** area, type the desired values.

To change the authentication or proxy settings, in the **Authentication and proxy settings** area, select and type the desired values.

URL authentication required: Select this check box only if the specified URL requires user authentication. If that is the case, you need to ensure that you have proper credentials in place to enable the Web Monitor Agent to access this URL. Click **Manage Credentials** to review the existing credentials, or to create new ones, as required. For more information, see [Configuring credentials to access Web sites requiring user authentication](#).

When finished, you can return to this dialog box using the breadcrumb trail.

Use proxy for URL connection: Select this check box only if the Web Monitor needs to use a proxy to access the specified URL. Click **Manage Credentials** to review the existing credentials, and create new ones, as required. For more information, see [Configuring credentials to access Web sites requiring user authentication](#).

Server: If you need to configure proxy access, type the name of the proxy server followed by the port number.

Proxy authentication required: Select this check box if the proxy requires authentication.

- 2 Click **Save**.

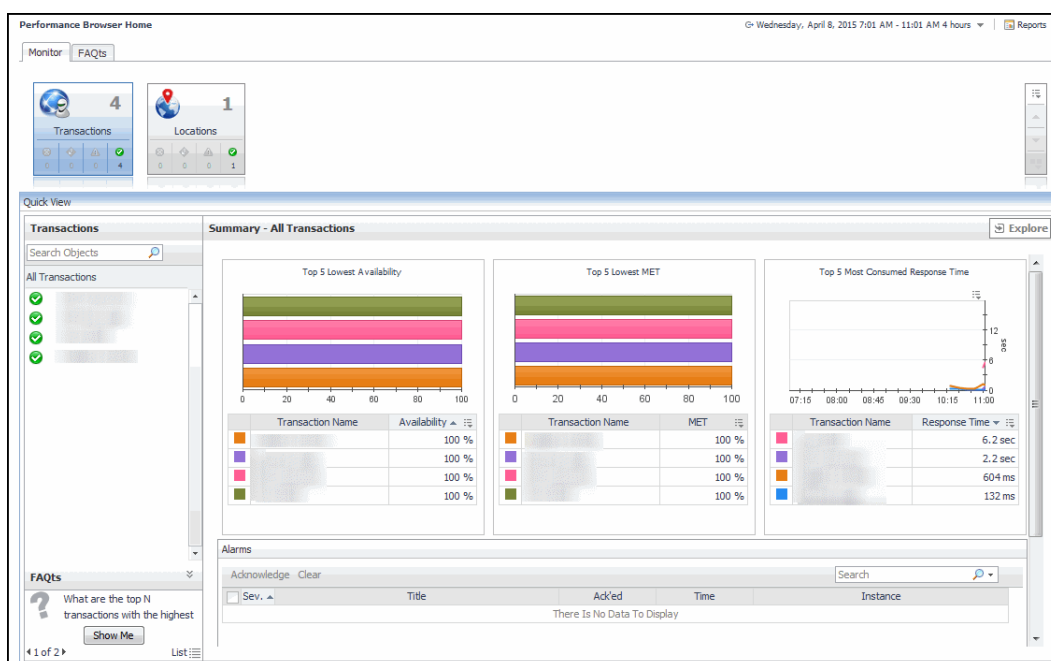
The dialog box closes.

- 3 The view containing newly updated information refreshes, showing the new values.

Investigating the performance of Web transactions and monitoring locations

A typical monitoring environment includes a set of monitored Web sites and the Web Monitor agents that monitor them. These components are displayed on the Performance Browser dashboard. This dashboard provides an overall summary of your entire Web monitoring environment. Use it to see the state of individual Web transactions, and to understand the end users' experience when visiting monitored Web sites.

Figure 5. Performance Browser dashboard



You can access this dashboard from the navigation panel. Under **Dashboards**, click **Web Monitor > Performance Browser**.

When you navigate to the Performance Browser for the first time, the **Monitor** tab, described in this topic, appears open. This tab provides an overall summary of your monitored environment. The **FAQs** tab is also available. For more information about this tab, see [Exploring the FAQs tab](#).

Start by indicating the type of objects you want to investigate. To do that, select the appropriate tile at the top of the **Monitor** tab, **Transactions** or **Locations**. This causes the Quick View to display information about the selected objects. Next, select an object or group of objects in the **Quick View**, such as **All Transactions** or **All Locations**, to display additional information about that selection. For example, selecting all transactions identifies the locations with the lowest availability, the lowest MET (met expected time) data, and the highest consumed response time. For complete information about the data appearing on the Performance Browser, see [Web Monitor Performance Browser views](#).

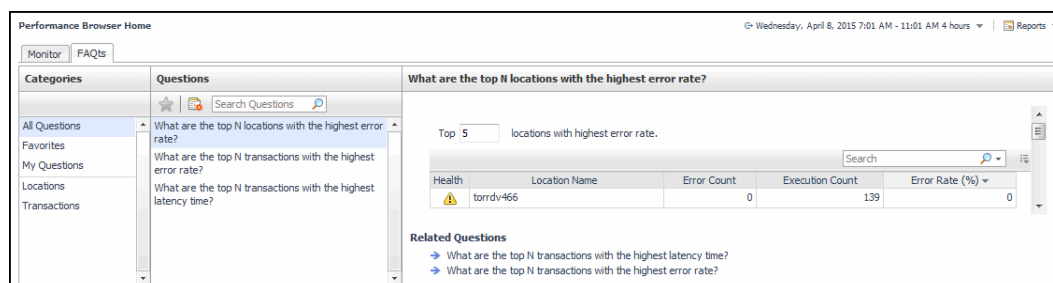
For more information, see the following topics:

- [Drilling down on transactions](#)
- [Drilling down on locations via the Locations tab](#)

Exploring the FAQs tab

The **FAQts** tab available on the Performance Browser allows you to review frequently asked questions about your monitored systems and their answers. The **Categories** view shows several question categories. Selecting a category shows the questions belonging to that category in the **Questions** pane. From there, clicking a question shows the answer on the right.

Figure 6. FAQts Tab View

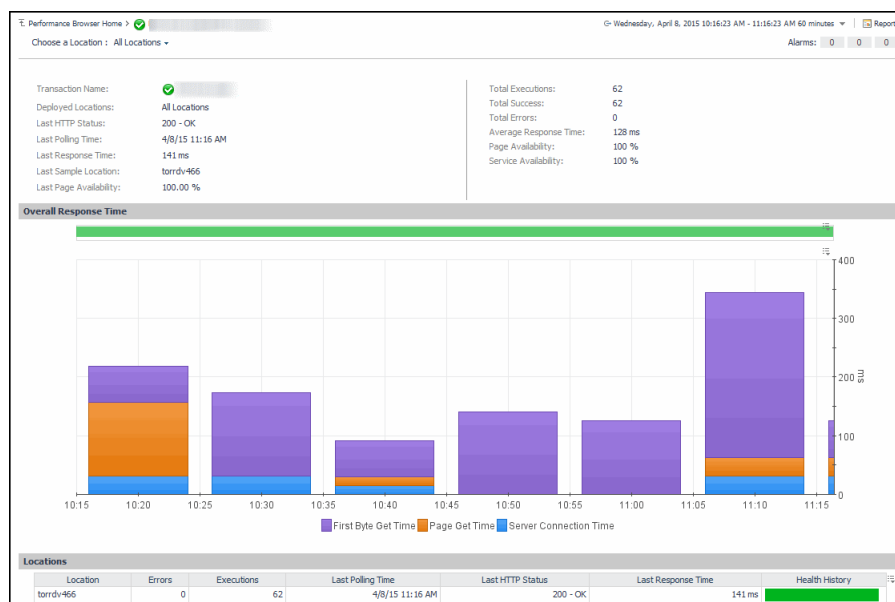


For complete information about the data appearing on this tab, see [FAQts tab](#).

Drilling down on transactions

When you select a transaction in the Quick View, you can see details indicating the overall state of that transaction, the associated response metrics, and any alarms generated against it. To display additional details about that transaction, click **Explore**.

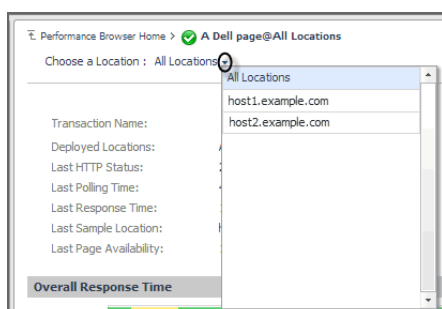
Figure 7. Transaction Additional Details



The **All Locations** drilldown view, displayed by default, allows you to review a larger set of metrics about the selected transaction, and to see how well that transaction is performing when monitored from different locations. Comparing the performance metrics collected from different locations can give you a general view of the responsiveness of your Web sites, and to indicate potential problems at locations that show response issues, and as such might require further investigation. For complete information about the data appearing on this view, see [Transaction at All Locations drilldown view](#).

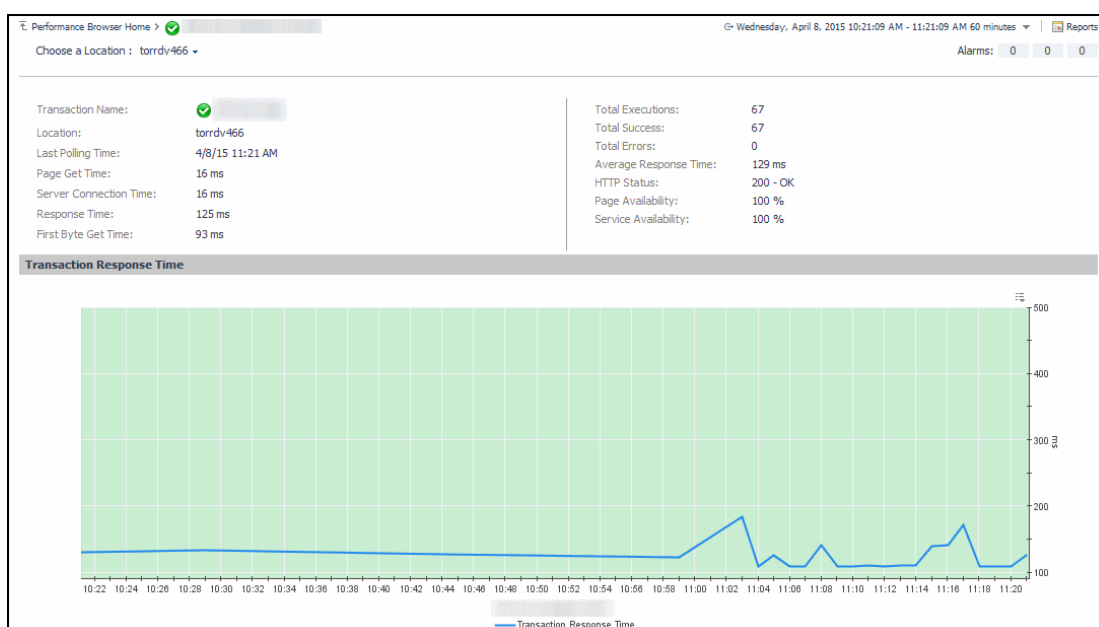
From here, you can drill down on a particular location and review its overall performance. To do that, click the down-facing arrow on the right of **Choose a Location**, and select a location from the list that appears.

Figure 8. Choose a Location



The Location drill down view shows the details of a transaction monitored from a particular location.

Figure 9. Location Drill Down View



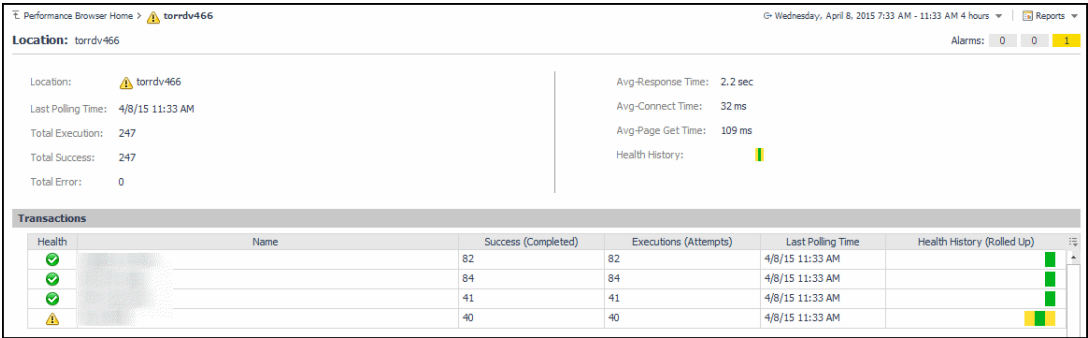
The top part of this view shows a number of metrics resulted from monitoring that transaction from the selected location. The bottom part of this view shows a graph indicating the total transaction response times over the selected time range. High peaks in the graph often suggest potential bottlenecks and likely need to be investigated. For complete information about the data appearing on this view, see [Transaction at a Selected Location drilldown view](#).

In some scenarios you can choose to monitor a Web transaction from multiple locations in your monitored environment. Drilling down on a specific location that shows the signs of performance degradation can either indicate a problem with the monitored location or the monitored Web transaction. Comparing the performance metrics collected from multiple locations can, for example, indicate potential problems with a particular location, rather than with the monitored transaction.

Drilling down on locations via the Locations tab

When you select a location in the Locations Tab Quick View, you can see details indicating the overall state of the transactions monitored from that location, the associated response metrics, and any alarms generated against it. To display additional details about that location, click **Explore**.

Figure 10. Location Additional Details



The **Location** drilldown view provides additional details about the selected location such as its response time and data collection metrics, and indicates its overall health during the monitored time range. For complete information about the data appearing on this view, see [Location drilldown view](#).

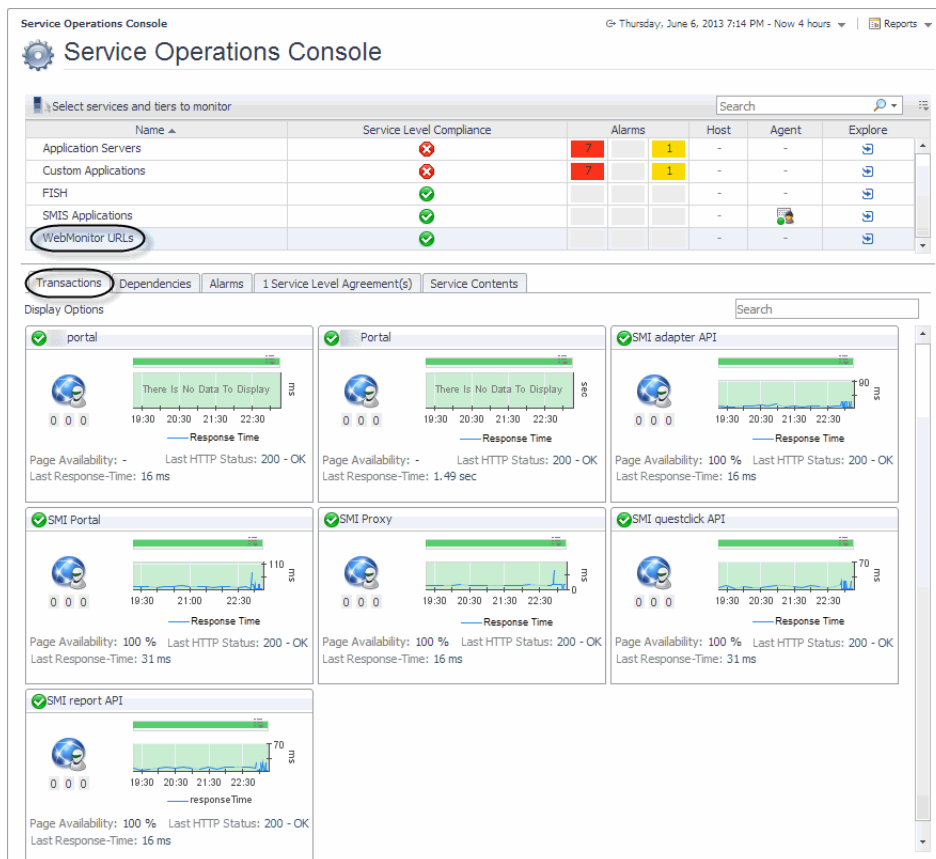
Exploring Web Monitor services

The service mechanism in Foglight allows you to organize your monitoring components into logical groups. A primary use case for this is for a multi-tier application where objects are organized into service tiers and visualized in the Service Operations Console.

Foglight Web Monitor extends the Service Operations Console. When a Web Monitor service is defined and you also have Foglight for APM installed, you can visualize the Web Monitor transactions visualized in the Service Operations Console and on the Transactions dashboard, available with Foglight for APM. For more information about the Service Operations Console, see the *Foglight User Guide*. For details about Foglight for APM, see the *Foglight Monitoring Application Performance User and Reference Guide*.

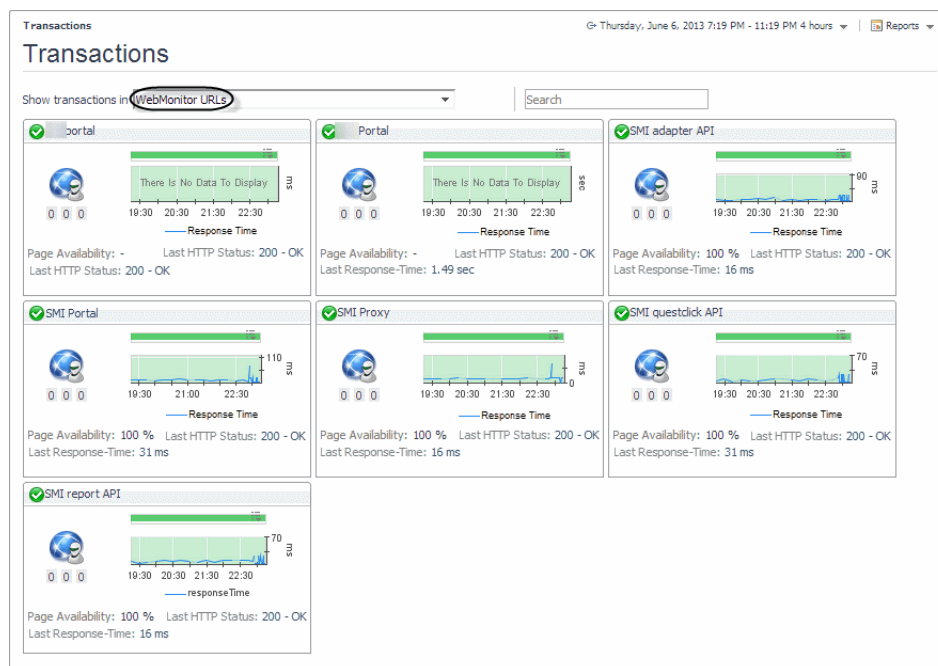
Start by navigating to the Service Operations Console dashboard and select a Web Monitor service. The Web Monitor tiles appear on the **Transactions** tab. The information displayed on these tiles helps you visualize how your Web transactions are performing, and to predict potential bottlenecks.

Figure 11. Service Operations Console



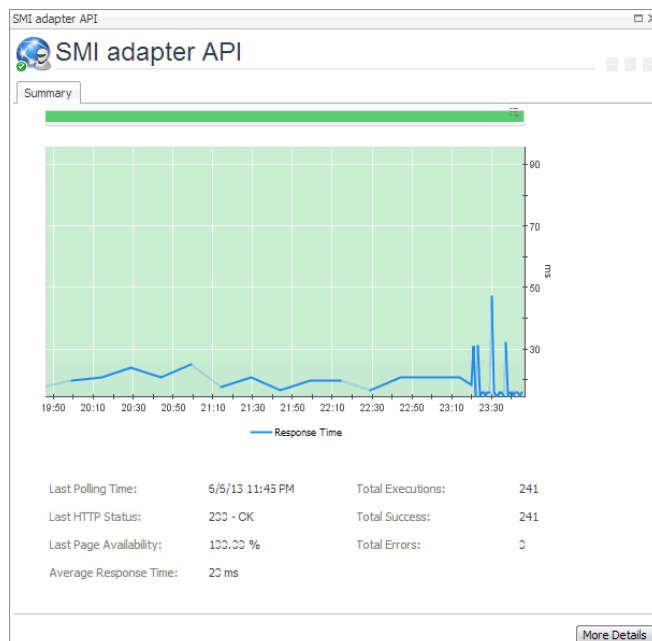
Another way to navigate to these tiles is using the Transactions dashboard included with Foglight for APM. When you select a Web Monitor service on this dashboard, the Web Monitor tiles are displayed.

Figure 12. Web Monitor Tiles



From there, you drill down on the individual Web transaction tiles to obtain more information about their performance.

Figure 13. Individual Web Transaction Tile



Explore the charts displaying the response tile metrics for the selected Web site. This can give you a better idea of how the selected Web site is performing, providing indicators about potential performance problems, if they exist. For example, high response times often suggests higher loads that may require further investigation.

For more information about these views, see [Web Monitor Service Operation Console and Foglight for APM Transactions views](#).

To explore Web transaction tiles:

1 Complete one of the following steps:

- On the navigation panel, click **Services > Service Operations Console**.

On the Service Operations Console that appears in the display area, select a Web Monitor service, and ensure that the **Transaction** tab is open.

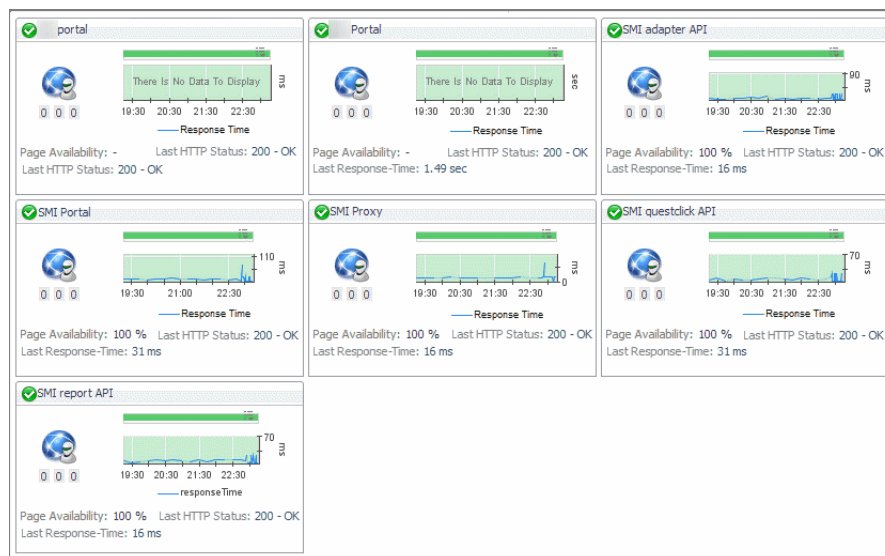
or

- On the navigation panel, click **APM > Transactions**.

On the Transactions dashboard that appears in the display area, select a Web Monitor service.

One or more transaction tiles appear in the display area.

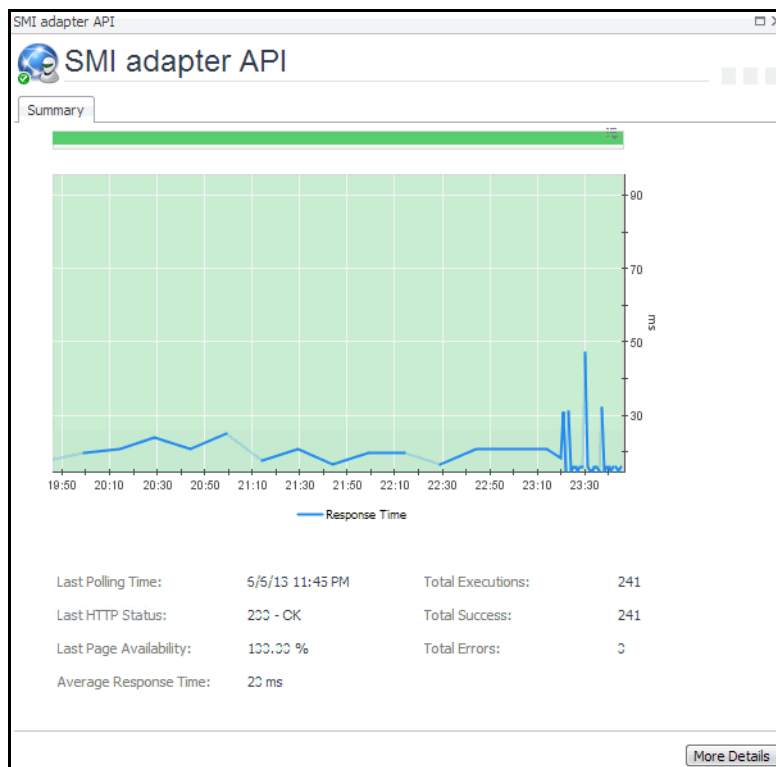
Figure 14. Transaction Tiles



2 Drill down on a transaction. Click the title bar of the transaction tile.

A dialog box appears, showing additional information about the selected transaction.

Figure 15. Selected Transaction Additional Information



Generating reports

Foglight provides a report generation ability. This allows you to create reports using predefined templates to report on the various aspects of your Web monitoring environment. Foglight Web Monitor includes a set of predefined report templates that can help you share data about your monitored environment with others in your organization. Web Monitor reports are accessible from the **Reports** menu.

For complete information about Foglight reports, see the *Foglight User Guide*.

Table 1. Predefined Reports

Report	Purpose
All Transactions Summary	Use this report to understand the overall state of your monitored Web sites and to obtain a general understanding of the responsiveness of your Web sites, and to identify any potential problems that might require further investigation.
All Transactions Daily Outage	Use this report to review the health of the monitored Web sites, and to investigate any reported outages.
Single Transaction	Use this report to see how well a transaction is performing. Comparing the performance metrics collected from different locations can give you a general view of the responsiveness of your Web sites, and to indicate potential problems at locations that show response issues, and as such might require further investigation.

Configuring Web Monitor agent properties

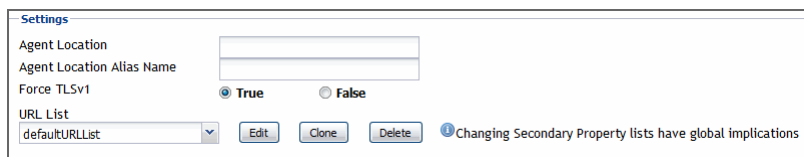
CAUTION: With the exception of “Force TLSv1” and “Data Collection Scheduler” agent properties, you must NOT change any properties through the Agent Status dashboard, unless instructed by Quest Customer Support. You should always go to Web Monitor > Administration Home > Transaction Management dashboard to manage your collection of monitored web sites.

The Web Monitor Agent includes the following groups of agent properties:

- [Settings](#)
- [Data Collection Scheduler](#)

Settings

The **Settings** properties specify general settings the Web Monitor agent needs to start collecting data from monitored Web sites.



- **Agent Location:** The name of the host on which the Foglight Agent Manager associated with this Web Monitor Agent instance is running.
- **Agent Location Alias Name:** The alias name of the host on which the Foglight Agent Manager is running.
- **Force TLSv1:** Indicates whether to use the TLSv1 or TLSv1.2 protocol. When set to “True”, the TLSv1 protocol is used (default value).
- **URL List:** This list also appears on the Transaction Management dashboard. Any changes you make to that collection in the Web Monitor Agent properties is automatically reflected on the Transaction Management dashboard and the other way around. For more information about this dashboard, see [Exploring your collection of monitored Web sites](#).

IMPORTANT: You must leave the default list selected. Do not make any changes to columns in this list, unless instructed by Quest Support.

Each entry in the list includes the following columns:

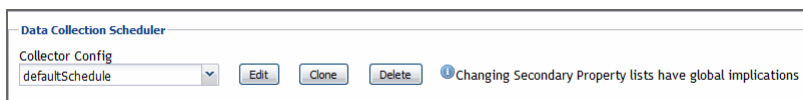
- **URL:** The URL of the monitored Web site.
- **Alias Name:** The name you want to associate with the transactions with this Web site.
- **Display Name:** The display name of the transaction.
- **Connection Time Out:** The maximum amount of time in milliseconds the agent instance can wait for establishing an HTTP connection to the monitored Web site. The value 0 indicates the agent will take the default connection time out. The default is 5 seconds.
- **Read Time Out:** The maximum amount of time in milliseconds the agent instance can wait to receive the data from the monitored URL. For instance, If “Is Page Get Header Only” is enabled, the value specified in “Read Time out” value will be used to read the header only (this is what “Is Page Header” does). If “Is Page Get Header Only” is disabled and “Read Timeout” is kept as 0, the

timeout to read content will be 10 seconds. If “Read Timeout” is 30 seconds, the timeout to read the content will be 30 seconds.

- **Is Get Page Header Only:** Indicates to the Web Monitor Agent whether to collect the page header only.
- **Custom Header:** The custom URL header. Also, multiple custom header is supported. If you have more than one custom headers in the URL you are monitoring, you may use the following in the **Customer Header** column: *property=value, property=value*
- **Enable Content Validation:** Instructs to the Web Monitor Agent whether to enable or disable content validation.
- **Expect Content:** If content validation is enabled for the agent instance that monitors this URL, and the expected content type is HTML-based, type html into this column. Also, a text string could be used such as “laptop” and type `laptop` into this column. When the monitoring agent detects binary content or the text string at this address, the validation fails and the agent logs an error message. If you do not want to enable content validation, leave this column empty.
- **Enable Unexpected Content Validation:** Instructs to the Web Monitor Agent whether to enable or disable unexpected content validation.
- **Unexpected Content:** If unexpected content validation is enabled for the agent instance that monitors this URL, and the unexpected content type is HTML-based, type html into this column. Also, a text string could be used such as “laptop” and type `laptop` into this column. When the monitoring agent detects binary content or the text string at this address, the validation fails and the agent logs an error message. If you do not want to enable unexpected content validation, leave this column empty.
- **Enable Auth:** Indicates to the Web Monitor Agent whether to enable user authentication. If enabled, you must create a credential to provide the agent with a user name and password needed to access this Web site. For more information, see [Configuring credentials to access Web sites requiring user authentication](#).
- **Enable Proxy:** Indicates to the Web Monitor Agent whether to use a proxy server to access this URL. If enabled, you need to create a credential to provide the agent with a user name and password needed to access this proxy server. For more information, see [Configuring credentials for accessing Web sites through proxy servers](#).
- **Proxy Server:** The server handling incoming requests from clients.
- **Proxy Type:** The protocol used to access the proxy server. Currently the only supported protocol is HTTP.
- **Proxy Port:** The port number the proxy server listens on for incoming requests.
- **Enable Proxy Auth:** Indicates if the proxy needs authentication.

Data Collection Scheduler

The **Datacenter Collection Scheduler** agent properties specify the data frequency settings the Web Monitor agent uses to collect metrics from the monitored Web sites.



- **Collector Config:** A list containing the data collectors the agent uses. Each entry in the list includes the following columns:
 - **Collector Name:** The name of the collector the Web Monitor Agent uses to gather data.
 - **Default Collection Interval:** The number of milliseconds, seconds, minutes, hours, or days during which the Web Monitor Agent collects data.
 - **Time Unit:** The time unit associated with the **Default Collection Interval**.

- **Fast-Mode Collection Interval:** The number of milliseconds, seconds, minutes, hours, or days during which the Web Monitor Agent collects data when working in the fast collection mode.
- **Fast-Mode Time Unit:** The time unit associated with the **Fast-Mode Collection Interval**.
- **Fast-Mode Max Count:** The maximum number of the times the Web Monitor Agent can stay in fast collection mode.

View reference

Foglight displays monitoring data in views that group, format, and display data. The main types are described below.

Dashboards are top-level views that contain lower-level views. The dashboards supplied with Foglight, as well as those created by users, are accessible from the navigation panel.

Lower-level views in Foglight can be added to dashboards or can be accessed by drilling down from a dashboard. They receive and display data directly from the Management Server or from other views. Some views filter or select data that appears in other views in the same dashboard. Some are tree views with expandable nodes for selecting servers, applications, or data.

Foglight Web Monitor ships with several dashboards that allow you to monitor and configure your virtual environment. Each of these dashboards contains a number of views. This section describes these views in more detail. For more information about the available dashboards, see [Exploring your collection of monitored Web sites](#), [Investigating the performance of Web transactions and monitoring locations](#), and [Exploring Web Monitor services](#).

This cartridge includes the following groups of views:

- [Web Monitor Performance Browser views](#)
- [Web Monitor Transaction Management views](#)
- [Web Monitor Service Operation Console and Foglight for APM Transactions views](#)

Web Monitor Performance Browser views

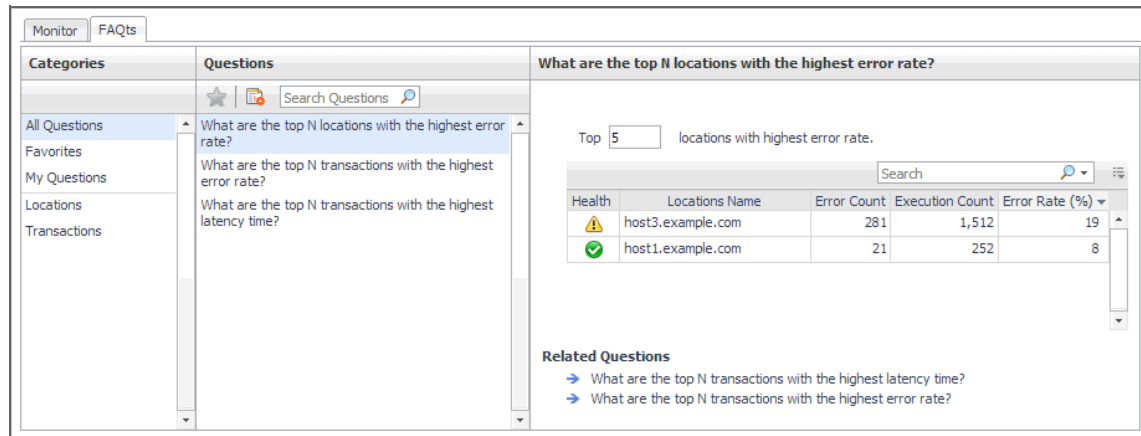
The Performance Browser contains the following views:

- [FAQts tab](#)
- [FAQts view](#)
- [Location drilldown view](#)
- [Location view](#)
- [Locations view](#)
- [Monitor tab](#)
- [Quick View](#)
- [Summary - All Locations view](#)
- [Summary - All Transactions view](#)
- [Transaction at a Selected Location drilldown view](#)
- [Transaction at All Locations drilldown view](#)
- [Transaction view](#)
- [Transactions view](#)
- [Web Monitor Environment view](#)

FAQts tab

Purpose

The **FAQts** tab shows answers to common questions related to your transactions or locations.



How to get here

Navigate to the Performance Browser, and open the **FAQts** tab.

Description of embedded views

This view is made up of the following embedded views:

- [Answer](#)
- [Categories](#)
- [Questions](#)

Answer

This view provides an answer to the question selected in the [Questions](#) view. The answer appears in the following form:

Top x <objects of category>...

where x is the number of objects of the category you provided in the [Categories](#) view.

Specify x by entering a number.

Categories

This view lists the categories for which questions can be answered for you by Foglight.

Click a category in the list to select it.

Questions

This view lists the questions, for the category selected in the [Categories](#), that can be answered for you by Foglight.

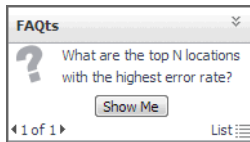
Click a question in the list to select it.

If the list of questions is long and you want to narrow it down, search for a particular text string using the **Search Questions** box.

FAQts view

Purpose

The **FAQts** view shows answers to common questions related to your transactions or locations. The collection of available questions depends on the tile selected in the [Web Monitor Environment view](#). If you select the Transaction tile, this view displays the questions related to your transactions. If you select the Locations tile, the view displays the questions related to your locations.



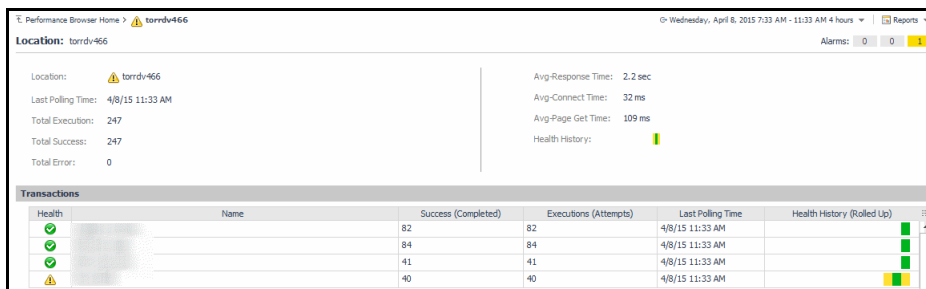
How to get here

In the Performance Browser, in the [Quick View](#), the **FAQts** view appears in the bottom-left corner.

Location drilldown view

Purpose

The **Location** drilldown view provides details about a monitoring location. use this view to investigate the overall state of the transactions monitored from that location, the associated response metrics, response-time and data collection metrics, its overall health during the monitored time range, and the state of transactions monitored from this location.



How to get here

- 1 In the Performance Browser, in the [Web Monitor Environment view](#), select the **Locations** tile.
- 2 In the [Quick View](#), in the [Locations view](#), select a location.
- 3 In the [Location view](#), click **Explore**.

The [Locations view](#) appears in the display area.

Description of embedded views

This view is made up of the following embedded views:

- [Alarms](#)
- [Location](#)
- [Transactions](#)

Alarms

Table 2. Alarms view

Description	Shows the numbers of alarms generated against the selected monitoring location, broken down by alarm type (Normal, Warning, Critical, Fatal).
--------------------	---





Location

Table 3. Location view

Description	Displays details about the selected location.
Data displayed	<ul style="list-style-type: none">• Avg-Connect Time. The average amount of time the agent used to establish connections to the monitored Web site.• Avg-Page Get Time. The average amount of time the agent needs to retrieve the data from the monitored Web site.• Avg-Response Time. The average amount of time the agent waits for a response from the monitored Web site.• Health History. A color-coded bar, representing the alarm state of the monitored location over the selected time range. The color of the bar changes depending on the alarm state. Red indicates a Fatal state, orange indicates Critical, yellow means Warning, and green is the Normal State.• Last Polling Time. The date and time of the most recent data collection.• Location. The name of the host on which the Web Monitor Agent is running.• Total Error. The total number of execution attempts that resulted in errors the Web Monitor Agent encountered during the selected time range.• Total Execution. The total number of execution attempts the Web Monitor Agent performed during the selected time range.• Total Success. The total number of successful executions the Web Monitor Agent performed during the selected time range.

Transactions

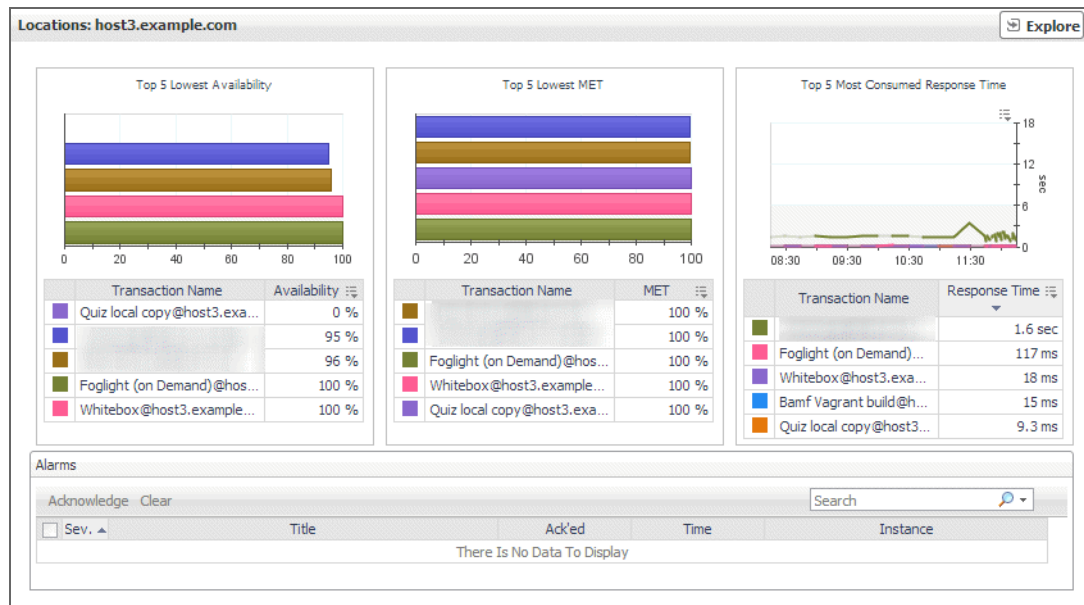
Table 4. Transactions view

	Displays details about each transaction monitored by the Web Monitor Agent that is deployed to the selected location
Description	<ul style="list-style-type: none">• Executions (Attempts). The number of execution attempts the Web Monitor Agent performed to monitor this Web site since it started collecting data.• Health History (Rolled Up). A color-coded bar, representing the alarm state of the monitored Web site over the selected time range. The color of the bar changes depending on the alarm state. Red indicates a Fatal state, orange indicates Critical, yellow means Warning, and green is the Normal State.• Health. The highest severity alarms generated against this Web site: Normal , Warning , Critical , or Fatal .• Last Polling Time. The most recent date and time the Web Monitor Agent made an attempt to collect data from this Web site.• Name. The transaction name, associated with the monitored URL.• Success (Completed). The number of successful executions the Web Monitor Agent performed to monitor this Web site since it started collecting data.
	Drill down on:
Where to go next	<ul style="list-style-type: none">• Any row in this table. For more information, see Transaction at a Selected Location drilldown view.

Location view

Purpose

The **Location** view displays overall response and availability information for the transactions monitored from the selected location. It also identifies the transactions with the lowest availability, lowest MET (met expected time), and highest response time, showing the top five transactions in each of these categories. Use this view to identify the Web sites with degraded performance, and to perform further investigation.



How to get here

- 1 In the Performance Browser, in the [Web Monitor Environment view](#), select the **Locations** tile.
 - 2 In the [Quick View](#), in the [Locations view](#), select a location.
- The [Location view](#) appears on the right.

Description of embedded views

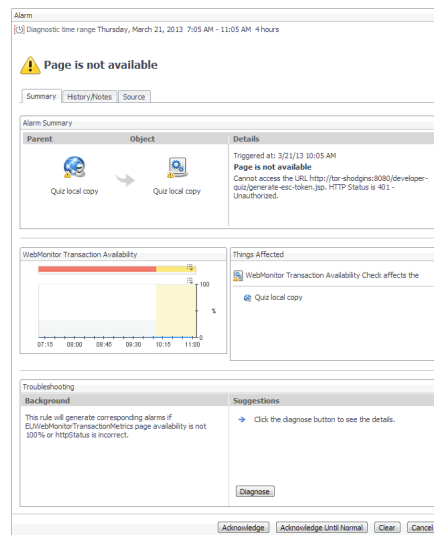
This view is made up of the following embedded views:

- [Alarms](#)
- [Top 5 Lowest Availability](#)
- [Top 5 Lowest MET](#)
- [Top 5 Most Consumed Response Time](#)

Alarms

Table 5. Alarms view

	Lists the alarms generated against the selected location.
Description	<p>NOTE: To acknowledge or clear one or more alarms appearing in this table, select them and click Acknowledge or Clear, as required. For more information about alarms in Foglight, see the <i>Foglight User Guide</i>.</p>
Data displayed	<ul style="list-style-type: none"> • Ack'ed. Indicates if the alarm is acknowledged: <code>true</code> or <code>false</code>. • Instance. The name of the transaction against which the alarm is generated. • Severity. Indicates the alarm severity: Warning ⚠️, Critical 🔴, or Fatal ☠️. • Time. The time at which the alarm is generated. • Title. The name of the rule that generated the alarm.
Where to go next	<p>Drill down on:</p> <ul style="list-style-type: none"> • Any row in this table. Displays the Alarm dialog box, showing additional information about the alarm. For more information about alarms in Foglight, see the <i>Foglight User Help</i>.



Top 5 Lowest Availability

Table 6. Top 5 Lowest Availability view

Description	Shows the top five transactions with the lowest availability.
Data displayed	<ul style="list-style-type: none"> • Availability. The percentage of times the Web site was available when the Web Monitor Agent attempted to collect information from it. • Transaction Name. The transaction name, associated with the monitored URL.
Where to go next	<p>Drill down on:</p> <ul style="list-style-type: none"> • Any row in this table. For more information, see Location drilldown view.

Top 5 Lowest MET

Table 7. Top 5 Lowest MET view

Description	Shows the top five transactions with the lowest MET.
Data displayed	<ul style="list-style-type: none"> • MET. The percentage of times the Web site meets its acceptable time expected by the end user. • Transaction Name. The transaction name, associated with the monitored URL.

Table 7. Top 5 Lowest MET view

Where to go next Drill down on:

- **Any row in this table.** For more information, see [Location drilldown view](#).

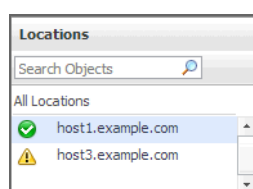
Top 5 Most Consumed Response Time

Table 8. Top 5 Most Consumed Response Time view

Description	Shows the top five transactions with the highest response time.
Data displayed	<ul style="list-style-type: none"> • Response Time. The amount of time the Web site takes to respond to the Web Monitor Agent request. • Transaction Name. The transaction name, associated with the monitored URL.
Where to go next	<p>Drill down on:</p> <ul style="list-style-type: none"> • Any row in this table. For more information, see Location drilldown view.

Locations view

The **Locations** view lists the hosts that are running instances of the Web Monitor Agent, and shows their states.



Selecting **All Locations** shows a list of all host names in the [Summary - All Locations view](#) on the right. Similarly, selecting a location in the list shows location-specific metrics in the [Location view](#) on the right.

How to get here

- In the Performance Browser, in the [Web Monitor Environment view](#), select the **Locations** tile.
The [Locations view](#) appears in the [Quick View](#) on the left.

Description of the view

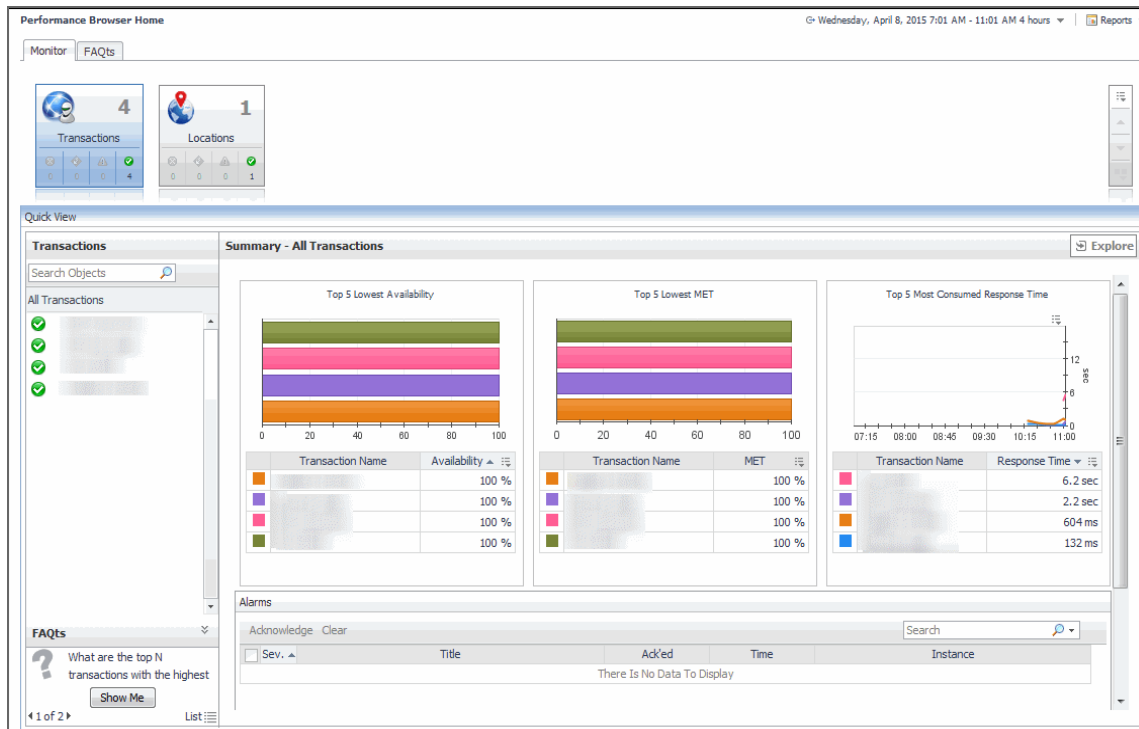
Table 9. Locations view

Data displayed	<ul style="list-style-type: none"> • Alarm severity. The state of the most recent alarm raised against the associated location: Warning ⚠, Critical 🔥, or Fatal ☠. • All Locations. A parent node for the location object instances that appear in this view. • Location. The name of the host on which the Web Monitor Agent is running.
Where to go next	<p>Drill down on:</p> <ul style="list-style-type: none"> • All Locations. Shows the Summary - All Locations view in the Quick View. • Location. Shows the Location view in the Quick View.

Monitor tab

Purpose

The **Monitor** tab is a container view. It displays a combination of location or transaction information, depending on your selection in the [Web Monitor Environment view](#) and the [Quick View](#). Use it to understand the level of user experience offered by the monitored Web sites, and to investigate any issues that they may be experiencing.



How to get here

- Navigate to the Performance Browser.
The **Monitor** tab appears open.

Embedded views

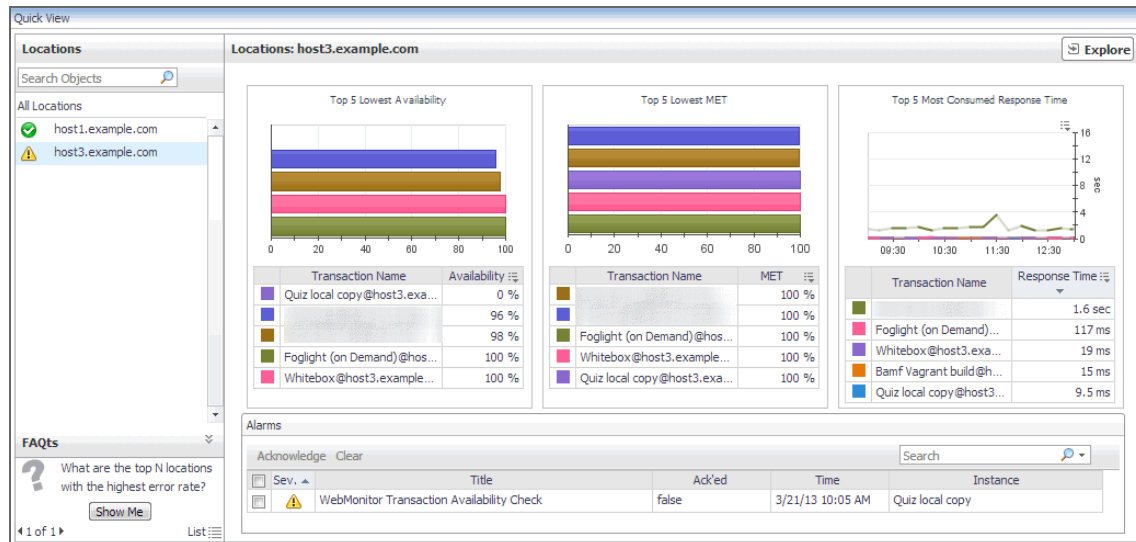
This view is made up of the following views:

- [Quick View](#)
- [Web Monitor Environment view](#)

Quick View

Purpose

The **Quick View** is a container view. It contains a combination of location or transaction views, depending on your selection in the [Web Monitor Environment view](#) and the pane on the left. Use it to understand the level of user experience offered by the monitored Web sites, and to investigate any issues that they may be experiencing.



How to get here

This view appears in the Performance Browser, just below the [Web Monitor Environment view](#).

Embedded views






This view contains a combination of some of the following views, depending on your previous selections:

- [FAQts view](#)
- [Location view](#)
- [Locations view](#)
- [Summary - All Locations view](#)
- [Summary - All Transactions view](#)
- [Transaction view](#)
- [Transactions view](#)

Summary - All Locations view

Purpose

The **Summary - All Locations** view displays a list of existing locations, and shows any alarms generated against them.

Summary - All Locations						Explore
All Locations						
Health	Name	Success (Completed)	Total Execution	Last Polling Time	Health History	
	host3.example.com	1,183	1,440	4/2/13 1:00 PM		
	host1.example.com	225	240	4/2/13 1:00 PM		
Alarms						
Acknowledge Clear		Search				
<input type="checkbox"/>	Sev. ▲	Title	Ack'd	Time	Instance	
<input type="checkbox"/>		WebMonitor Transaction Availability Check	false	3/21/13 10:05 AM	Quiz local copy	

How to get here

- 1 Navigate to the Performance Browser.
- 2 On the [Monitor tab](#), in the [Web Monitor Environment view](#), select the **Locations** tile.
- 3 In the [Quick View](#), in the embedded [Locations view](#), click **All Locations**.

The [Summary - All Locations view](#) appears on the right.

Description of embedded views

This view is made up of the following embedded views:

- [Alarms](#)
- [All Locations](#)

Alarms

Table 10. Alarms view

	Lists the alarms generated against the monitored locations.
Description	<p>NOTE: To acknowledge or clear one or more alarms appearing in this table, select them and click Acknowledge or Clear, as required. For more information about alarms in Foglight, see the <i>Foglight User Guide</i>.</p>

Table 10. Alarms view

	<ul style="list-style-type: none"> • Ack'ed. Indicates if the alarm is acknowledged: <code>true</code> or <code>false</code>. • Instance. The name of the transaction against which the alarm is generated.
Data displayed	<ul style="list-style-type: none"> • Severity. Indicates the alarm severity: Warning ⚠️, Critical 🔴, or Fatal ❌. • Time. The time at which the alarm is generated. • Title. The name of the rule that generated the alarm.
	Drill down on: <ul style="list-style-type: none"> • Any row in this table. Displays the Alarm dialog box, showing additional information about the alarm. For more information about alarms in Foglight, see the <i>Foglight User Help</i>.

Where to go next

All Locations

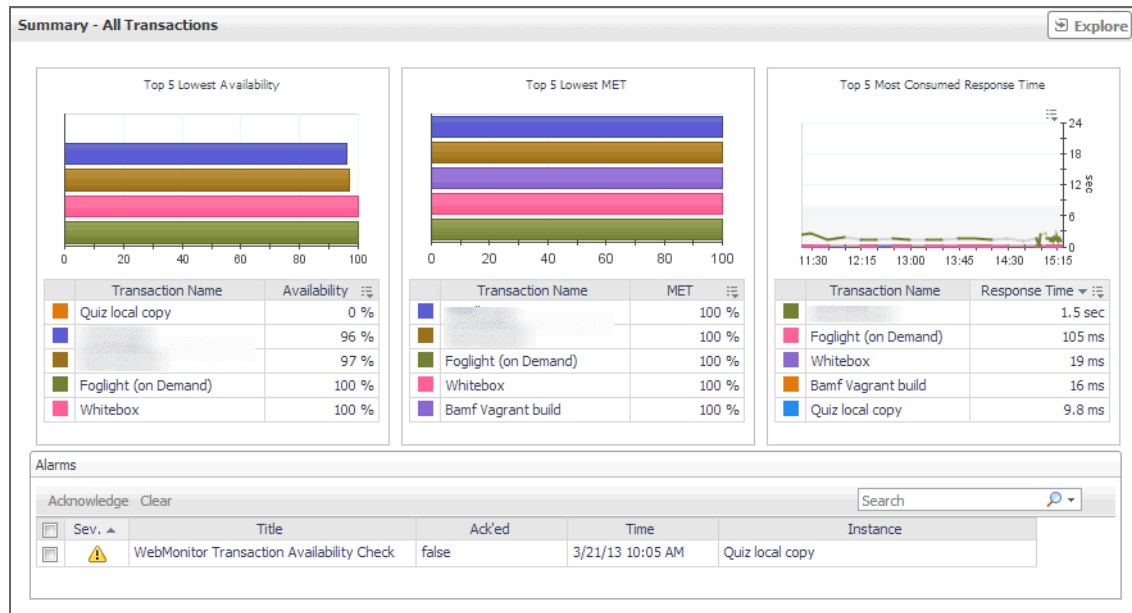
Table 11. All Locations view

Description	Shows a list of all hosts from which Web Monitor Agent instances are running and the related statistics.
Data displayed	<ul style="list-style-type: none"> • Health. The highest severity alarms generated against this Web site: Normal ✅, Warning ⚠️, Critical 🔴, or Fatal ❌. • Name. The name of the host on which the Web Monitor Agent instance is running. • Success (Completed). The number of successful executions the Web Monitor Agent performed since it started collecting data. • Total Execution. The number of execution attempts the Web Monitor Agent performed during the selected time range. • Last Polling Time. The most recent date and time the Web Monitor Agent made an attempt to collect data. • Health History (Rolled Up). A color-coded bar, representing the alarm state of the Web Monitor Agent running on this host over the selected time range. The color of the bar changes depending on the alarm state. Red indicates a Fatal state, orange indicates Critical, yellow means Warning, and green is the Normal State.
Where to go next	Drill down on: <ul style="list-style-type: none"> • Any row in this table. For more information, see Location drilldown view.

Summary - All Transactions view

Purpose

The **Summary - All Transaction** view displays overall response and availability information for the monitored transactions. It also identifies the transactions with the lowest availability, lowest MET (met expected time), and highest response time, showing the top five transactions in each of these categories.



How to get here

- 1 Navigate to the Performance Browser.
- 2 On the **Monitor** tab, in the **Web Monitor Environment** view, select the **Locations** tile.
- 3 In the **Quick View**, in the **Transaction** view, click **All Transactions**.

The **Summary - All Transactions** view appears on the right.

Description of embedded views

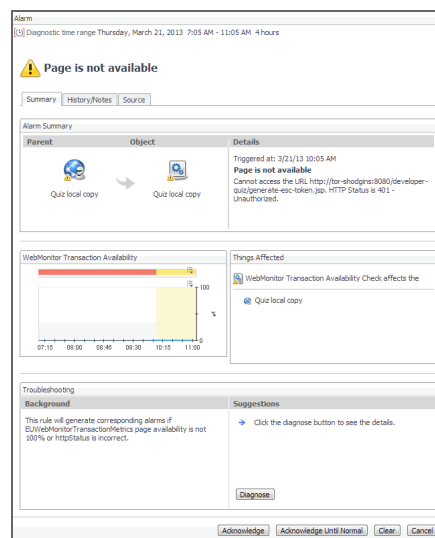
This view is made up of the following embedded views:

- **Alarms**
- **Top 5 Lowest Availability**
- **Top 5 Lowest MET**
- **Top 5 Most Consumed Response Time**

Alarms

Table 12. Alarms view

	Lists the alarms generated against the monitored transactions.
Description	<p>NOTE: To acknowledge or clear one or more alarms appearing in this table, select them and click Acknowledge or Clear, as required. For more information about alarms in Foglight, see the <i>Foglight User Guide</i>.</p>
Data displayed	<ul style="list-style-type: none"> • Ack'ed. Indicates if the alarm is acknowledged: <code>true</code> or <code>false</code>. • Instance. The name of the transaction against which the alarm is generated. • Severity. Indicates the alarm severity: Warning ⚠️, Critical ⚡️, or Fatal ☠️. • Time. The time at which the alarm is generated. • Title. The name of the rule that generated the alarm.
Where to go next	<p>Drill down on:</p> <ul style="list-style-type: none"> • Any row in this table. Displays the Alarm dialog box, showing additional information about the alarm. For more information about alarms in Foglight, see the <i>Foglight User Help</i>.



Top 5 Lowest Availability

Table 13. Top 5 Lowest Availability view

Description	Shows the top five transactions with the lowest availability.
Data displayed	<ul style="list-style-type: none"> • Availability. The percentage of times the Web site was available when the Web Monitor Agent attempted to collect information from it. • Transaction Name. The transaction name, associated with the monitored URL.
Where to go next	<p>Drill down on:</p> <ul style="list-style-type: none"> • Any row in this table. For more information, see Location drilldown view.

Top 5 Lowest MET

Table 14. Top 5 Lowest MET view

Description	Shows the top five transactions with the lowest MET.
--------------------	--

Table 14. Top 5 Lowest MET view

Data displayed	<ul style="list-style-type: none"> • MET. The percentage of times the Web site meets its acceptable response times, expected by the end user. • Transaction Name. The transaction name, associated with the monitored URL.
Where to go next	<p>Drill down on:</p> <ul style="list-style-type: none"> • Any row in this table. For more information, see Location drilldown view.

Top 5 Most Consumed Response Time

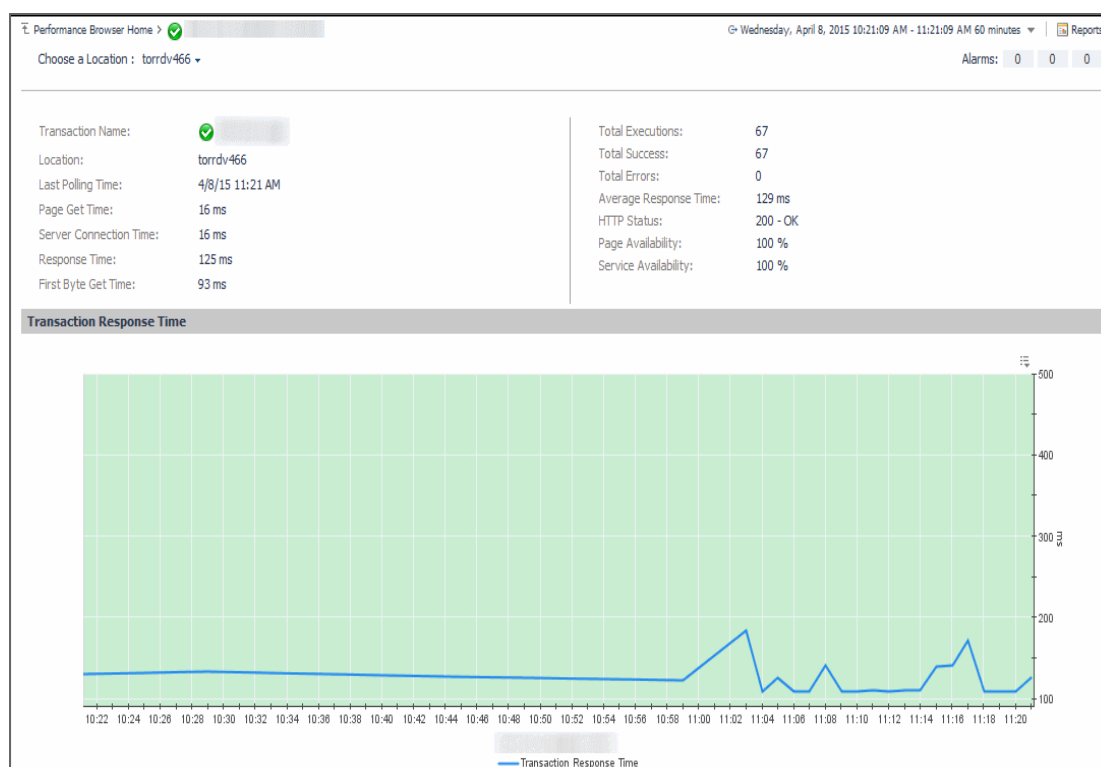
Table 15. Top 5 Most Consumed Response Time view

Description	Shows the top five transactions with the highest response time.
Data displayed	<ul style="list-style-type: none"> • Response Time. The amount of time the Web site takes to respond to the Web Monitor Agent request. • Transaction Name. The transaction name, associated with the monitored URL.
Where to go next	<p>Drill down on:</p> <ul style="list-style-type: none"> • Any row in this table. For more information, see Location drilldown view.

Transaction at a Selected Location drilldown view

Purpose

The **Transaction at a Selected Location** drilldown view provides details about the performance of a transaction monitored from a specific location. This view describe the overall state of the most recent monitoring attempt and response-times recorded during the selected time range, along with its overall health during the monitored time range. Use it to find out how well your Web sites are performing when being monitored from a specific location in your monitoring environment.



How to get here

- 1 In the Performance Browser, in the [Web Monitor Environment view](#), select the **Transactions** tile.
- 2 In the [Quick View](#), in the [Transactions view](#), select a transaction.
- 3 In the [Transaction view](#), click **Explore**.
- 4 In the [Transaction at All Locations drilldown view](#) that appears in the display area, click the down-facing arrow on the right of **Choose a Location**, and select a location from the list that appears.

The [Transaction at All Locations drilldown view](#) appears in the display area.

Description of embedded views

This view is made up of the following embedded views:

- [Alarms](#)
- [Location](#)
- [Transaction Response Time](#)

Alarms

Table 16. Alarms view

Description	Shows the numbers of alarms generated against the selected transaction, broken down by alarm type (Normal, Warning, Critical, Fatal).
--------------------	---

Location

Table 17. Location view

Description	Displays details about the selected location.
Data displayed	<ul style="list-style-type: none">• Average Response Time. The average amount of time the Web Monitor Agent waits for a response from the monitored Web site.• First Byte Get Time. The time between the Web Monitor Agent detects the first byte of the response from the monitored Web site.• HTTP Status. The HTTP status code, indicating the result of the most recent transaction with the monitored Web site.• Last Polling Time. The date and time of the most recent data collection.• Location. The name of the host on which the Web Monitor Agent is running.• Page Availability. The percentage of time the Web site was available when the Web Monitor Agent attempted to collect information from it.• Page Get Time. The amount of time the agent needs to retrieve the data form the monitored Web site.• Response Time. The amount of time the Web Monitor Agent waits for a response from the monitored Web site.• Server Connection Time. The length of time the Web Monitor Agent used to connect to the monitored Web site.• Service Availability. The percentage of time the service was available when the Web Monitor Agent attempted to collect information about this Web site.• Total Errors. The total number of execution attempts that resulted in errors the Web Monitor Agent encountered during the selected time range.• Total Executions. The total number of execution attempts the Web Monitor Agent performed during the selected time range.• Total Executions. The total number of execution attempts the Web Monitor Agent performed during the selected time range.• Total Success. The total number of successful executions the Web Monitor Agent performed during the selected time range.• Transaction Name. The transaction name, associated with the monitored URL.

Transaction Response Time

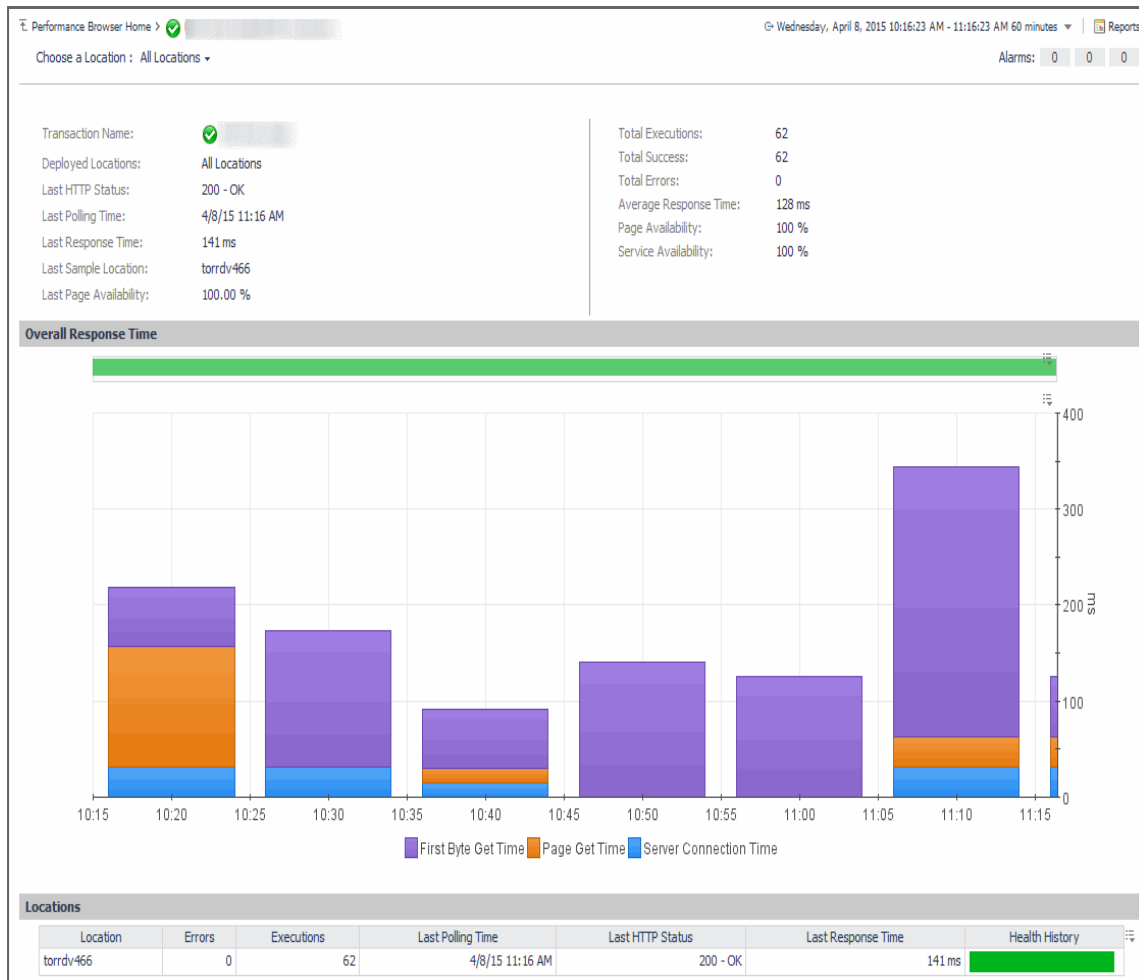
Table 18. Transaction Response Time view

Description	<p>Displays the transaction response times over the selected time range.</p> <ul style="list-style-type: none">• Health History. A color-coded bar, representing the alarm state of the monitored location over the selected time range. The color of the bar changes depending on the alarm state. Red indicates a Fatal state, orange indicates Critical, yellow means Warning, and green is the Normal State.• Transaction Response Time. The amount of time the Web site takes to respond to the Web Monitor Agent request, over the selected time range period. High values in the graph can indicate potential bottlenecks that likely need to be investigated.
--------------------	--

Transaction at All Locations drilldown view

Purpose

The **Transaction at All Locations** drilldown view provides details about the performance of a transaction monitored from all locations to which the Web Monitor Agent is deployed. This view describes how well the Web site responded to monitoring attempts, and shows the response-times recorded during the selected time range. It also lists all of the locations from which this Web site is monitored and indicates the related performance metrics.



How to get here

- 1 In the Performance Browser, in the [Web Monitor Environment view](#), select the **Transactions** tile.
- 2 In the [Quick View](#), in the [Transactions view](#), select a transaction.
- 3 In the [Transaction view](#), click **Explore**.
- 4 In the [Transaction at All Locations drilldown view](#) that appears in the display area, click the down-facing arrow on the right of **Choose a Location**, and select **All Locations** from the list that appears.

The [Transaction at All Locations drilldown view](#) appears in the display area.

Description of embedded views

This view is made up of the following embedded views:

- [Alarms](#)
- [All Locations](#)
- [Overall Response Time](#)
- [Locations](#)

Alarms

Table 19. Alarms view

Description	Shows the numbers of alarms generated against the selected transaction, broken down by alarm type (Normal, Warning, Critical, Fatal).
--------------------	---

All Locations

Table 20. All Locations view

Description	Displays details about all of the locations from which the selected Web site is monitored.
Data displayed	<ul style="list-style-type: none">• Average Response Time. The average amount of time all instances of the Web Monitor Agent configured to monitor this Web site wait for a response from the monitored Web site.• Deployed Locations. The names of the hosts running the instances of the Web Monitor Agent configured to monitor this Web site.• Last HTTP Status. The most recent HTTP status code, indicating the result of the most recent transaction with the monitored Web site.• Last Page Availability. The percentage of time the Web site was available when the Web Monitor Agent attempted to collect information from it during the most recent data collection attempt.• Last Polling Time. The date and time of the most recent data collection.• Last Response Time. The amount of time the Web Monitor Agent waited for a response from the monitored Web site during the most recent data collection attempt.• Last Sample Location. The name of the host running the Web Monitor Agent instance that performed the most recent data collection from this Web site.• Page Availability. The percentage of time the Web site was available when the Web Monitor Agent instances configured to monitor this Web site attempted to collect information.• Service Availability. The percentage of time the service was available when the Web Monitor Agent instances configured to monitor this Web site attempted to collect information.• Total Errors. The total number of execution attempts that resulted in errors all instances of the Web Monitor Agent configured to monitor this Web site encountered during the selected time range.• Total Executions. The total number of execution attempts all instances of the Web Monitor Agent configured to monitor this Web site performed during the selected time range.• Total Success. The total number of execution attempts that resulted in success all instances of the Web Monitor Agent configured to monitor this Web site encountered during the selected time range.• Transaction Name. The transaction name, associated with the monitored URL.

Overall Response Time

Table 21. Overall Response Time view

Displays the transaction response times over the selected time range.	
Description	<ul style="list-style-type: none">• Health History. A color-coded bar, representing the alarm state of the monitored Web site over the selected time range. The color of the bar changes depending on the alarm state. Red indicates a Fatal state, orange indicates Critical, yellow means Warning, and green is the Normal State.
	<ul style="list-style-type: none">• First Byte Get Time. The time between the Web Monitor Agent detects the first byte of the response from the monitored Web site, during the selected time range.
	<ul style="list-style-type: none">• Page Get Time. The average amount of time the monitoring agents take to retrieve the data from the monitored Web site, during the selected time range.
	<ul style="list-style-type: none">• Server Connection Time. The average amount of time the monitoring agents used to connect to the monitored Web sites, during the selected time range.

Locations

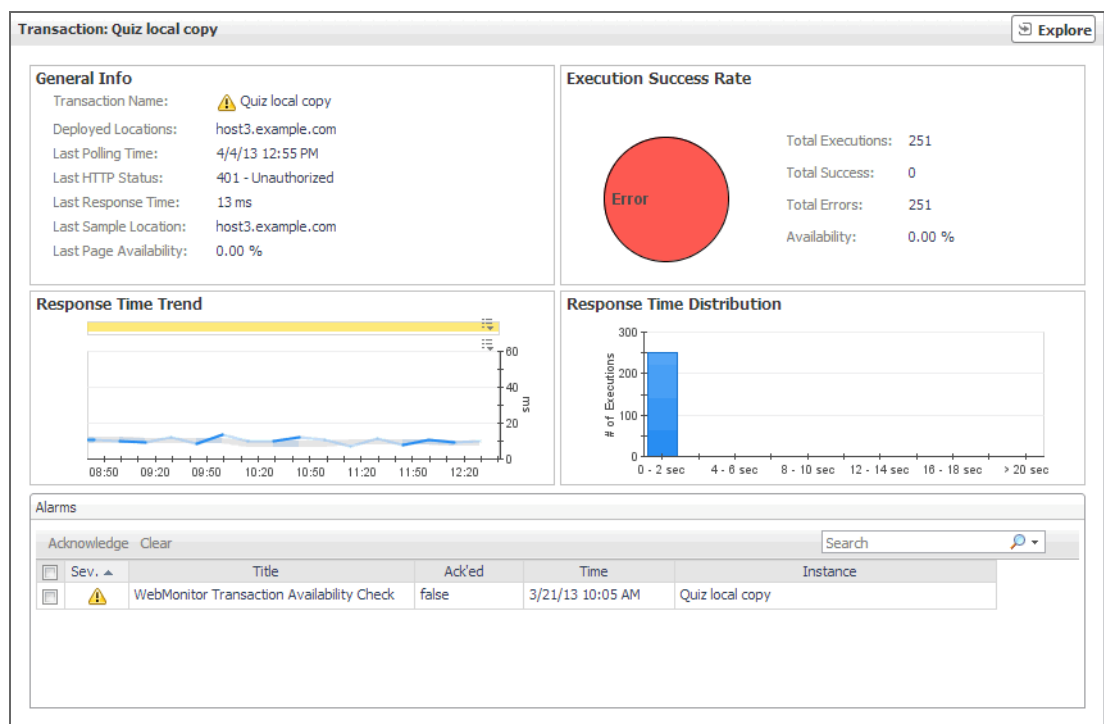
Table 22. Locations view

Displays the transaction response times over the selected time range.	
Description	<ul style="list-style-type: none">• Health History. A color-coded bar, representing the alarm state of the monitored location over the selected time range. The color of the bar changes depending on the alarm state. Red indicates a Fatal state, orange indicates Critical, yellow means Warning, and green is the Normal State.
	<ul style="list-style-type: none">• Location. The name of the host on which the Web Monitor Agent is running.
	<ul style="list-style-type: none">• Errors. The number of execution attempts that resulted in errors the Web Monitor Agent configured to monitor this Web site encountered since it started monitoring this Web site.
	<ul style="list-style-type: none">• Executions. The number of execution attempts the Web Monitor Agent configured to monitor this Web site performed since it started monitoring this Web site.
	<ul style="list-style-type: none">• Last Polling Time. The date and time of the most recent data collection attempt the Web Monitor Agent configured to monitor this Web site performed.
	<ul style="list-style-type: none">• Last HTTP Status. The most recent HTTP status code encountered by the Web Monitor Agent configured to monitor this Web site.
	<ul style="list-style-type: none">• Last Response Time. The amount of time the Web Monitor Agent configured to monitor this Web site waited for a response from the monitored Web site during the most recent data collection attempt.
	Drill down on:
Where to go next	<ul style="list-style-type: none">• Any row in this table. For more information, see Transaction at a Selected Location drilldown view.

Transaction view

Purpose

The **Transaction** view displays overall response and availability information for the selected transaction. Use it to get a better idea of how well this Web site is performing and to investigate potential bottlenecks.



How to get here

- 1 In the Performance Browser, in the [Web Monitor Environment view](#), select the **Transactions** tile.
 - 2 In the [Quick View](#), in the [Transactions view](#), select a transaction.
- The [Transaction view](#) appears on the right.

Description of embedded views

This view is made up of the following embedded views:

- [Alarms](#)
- [General Info](#)
- [Execution Success Rate](#)
- [Response Time Trend](#)
- [Response Time Distribution](#)

Alarms

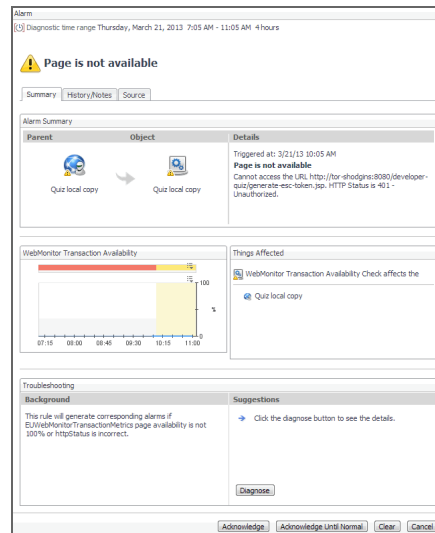
Table 23. Alarms view

	Lists the alarms generated against the selected transaction.
Description	NOTE: To acknowledge or clear one or more alarms appearing in this table, select them and click Acknowledge or Clear , as required. For more information about alarms in Foglight, see the <i>Foglight User Guide</i> .

Table 23. Alarms view

	<ul style="list-style-type: none"> • Ack'ed. Indicates if the alarm is acknowledged: <code>true</code> or <code>false</code>. • Instance. The name of the transaction against which the alarm is generated.
Data displayed	<ul style="list-style-type: none"> • Severity. Indicates the alarm severity: Warning ⚠️, Critical 🚨, or Fatal 🛑. • Time. The time at which the alarm is generated. • Title. The name of the rule that generated the alarm.
	<p>Drill down on:</p> <ul style="list-style-type: none"> • Any row in this table. Displays the Alarm dialog box, showing additional information about the alarm. For more information about alarms in Foglight, see the <i>Foglight User Help</i>.

Where to go next



General Info

Table 24. General Info view

Description	Shows general details about the most recent collection attempt.
Data displayed	<ul style="list-style-type: none"> • Deployed Locations. The names of the hosts running the instances of the Web Monitor Agent configured to monitor this Web site. • Last HTTP Status. The most recent HTTP status code, indicating the result of the most recent transaction with the monitored Web site. • Last Page Availability. The percentage of time the Web site was available when the Web Monitor Agent attempted to collect information from it during the most recent data collection attempt. • Last Polling Time. The date and time of the most recent data collection. • Last Response Time. The amount of time the Web Monitor Agent waited for a response from the monitored Web site during the most recent data collection attempt. • Last Sample Location. The name of the host running the Web Monitor Agent instance that performed the most recent data collection from this Web site. • Transaction Name. The transaction name, associated with the monitored URL.

Execution Success Rate

Table 25. Execution Success Rate view

Description	Indicates the general success rate the monitoring agents encountered during data collection.
Data displayed	<ul style="list-style-type: none">• Availability. The percentage of time the Web site was available when the Web Monitor Agent instances configured to monitor this Web site attempted to collect information.• Total Errors. The total number of execution attempts that resulted in errors all instances of the Web Monitor Agent configured to monitor this Web site encountered during the selected time range.• Total Executions. The total number of execution attempts all instances of the Web Monitor Agent configured to monitor this Web site performed during the selected time range.• Total Successes. The total number of successful execution attempts all instances of the Web Monitor Agent configured to monitor this Web site encountered during the selected time range.

Response Time Trend

Table 26. Response Time Trend view

Description	Indicates the time the Web site takes for responding to monitoring requests and its health.
Data displayed	<ul style="list-style-type: none">• Health History. A color-coded bar, representing the alarm state of the monitored location over the selected time range. The color of the bar changes depending on the alarm state. Red indicates a Fatal state, orange indicates Critical, yellow means Warning, and green is the Normal State.• Response Time. The amount of time the Web site takes to respond to monitoring requests, over the selected time range. High values in the graph can indicate potential bottlenecks that likely need to be investigated. The grey-shaded area indicates baseline values for this metric, representing the expected value range during the selected time period.

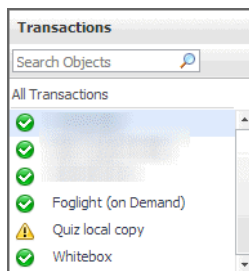
Response Time Distribution

Table 27. Response Time Distribution view

Description	Shows the distribution of transaction response times. Each rectangle in the histogram represent the number of execution attempts that resulted with the response time in the given range.
--------------------	---

Transactions view

The **Transactions** view lists the names of transactions that are currently monitored, and shows their states.



Selecting **All Transactions** shows the overall response and availability information for the monitored transactions in the [Summary - All Transactions view](#) on the right. Similarly, selecting a transaction in the list shows transaction-specific metrics in the [Transaction view](#) on the right.

How to get here

- In the Performance Browser, in the [Web Monitor Environment view](#), select the **Transactions** tile.
- The [Transactions view](#) appears in the [Quick View](#) on the left.

Description of the view

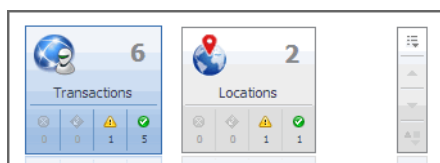
Table 28. Transactions view

Data displayed	<ul style="list-style-type: none"> Alarm severity. The state of the most recent alarm raised against the associated transaction: Warning ⚠️, Critical ⚡, or Fatal ☒. All Transactions. A parent node for the transaction object instances that appear in this view. Transaction. The name of the transaction associated with this Web site.
	Drill down on:
Where to go next	<ul style="list-style-type: none"> All Transactions. Shows the Summary - All Transactions view in the Quick View. Transaction. Shows the Transaction view in the Quick View.


Web Monitor Environment view

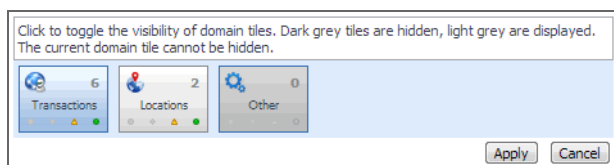
Purpose

The Web Monitor Environment view displays a high-level overview of your monitored environment. The view has two tiles, each representing the monitored objects of interest **Transactions** and **Locations**.



Each tile shows how many of the corresponding object instances there are in your monitored infrastructure, as well as the count of objects of that type in each of the alarm states Normal 🟢, Warning ⚠️, Critical ⚡, or Fatal ☒. For example, the following image shows six transactions: none in the Fatal or Critical states, one in Warning, and one the Normal state.

You can move the tiles by dragging and dropping until you achieve the desired layout. To hide one or more tiles, on the tool bar on the right, click , and in the popup that appears, click a tile that you want to hide.



Clicking the object type icon, the object type name, or the object count, shows summary information for that object type in the [Quick View](#). Clicking an alarm state (for example, Warning) on a tile displays summary information in the [Quick View](#) for the objects of that type that are in the selected alarm state. If an alarm state has a count of zero, then you can not drill down on the alarm state.

How to get here

This view appears in the upper part of the Performance Browser, just above the [Quick View](#).

Description of embedded views

This view is made up of the following embedded views:

- [Locations](#)
- [Transactions](#)

Locations

Table 29. Locations view

Description	Shows the number of locations in your environment from which Web sites are monitored, and total alarm counts associated with those locations.
Data displayed	<ul style="list-style-type: none">• Alarm counts. The total counts of alarms generated against the existing monitoring locations, broken down by alarm types (Normal, Warning, Critical, Fatal).• Location count. The number of locations in your environment.
Where to go next	<p>Drill down on:</p> <ul style="list-style-type: none">• Alarm counts. Lists the locations associated with the alarms in the Locations view, appearing in the Quick View.• Location count. Displays location-related combination of views in the Quick View.

Transactions

Table 30. Transactions view

Description	Shows the number of monitored Web sites in your environment and total alarm counts associated with them.
Data displayed	<ul style="list-style-type: none">• Alarm counts. The total counts of alarms associated with the monitored transactions, broken down by alarm types (Normal, Warning, Critical, Fatal).• Transaction count. The number of monitored Web sites in your environment.
Where to go next	<p>Drill down on:</p> <ul style="list-style-type: none">• Alarm counts. Lists the Web sites associated with the alarms in the Transactions view, appearing in the Quick View.• Transaction count. Displays transaction-related combination of views in the Quick View.

Web Monitor Transaction Management views

The Transaction Management dashboard contains the following views:

- [Transaction Detail view](#)
- [Transaction Management table](#)

Transaction Detail view

Purpose

The **Transaction Detail** view provides details about the selected transaction. Use it to find out the URL of the monitored Web site, the type of monitored content, the locations from which this Web site is monitored, and to review and adjust some advanced settings, if needed.

Administration Home > Transaction Management > Transaction Detail

Tuesday, December 5, 2017 12:08 PM - 4:08 PM 4 hours Reports

Transaction Detail

View and edit transaction details.

Basic Information

Transaction name: <http://www.baidu.com/>

Search

URL	Get Page Header Only	Expected Content	Unexpected Content	Display Name
http://www.baidu.com/	<input type="checkbox"/>			http://www.baidu.com/

Edit

Monitoring Locations

Search

Location (FQDN)	Agent Name
<input checked="" type="checkbox"/> dsg8f9f62.prod.quest.corp	WebMonitorAgent@dsg8f9f62.prod.quest.corp

Edit

Advanced Settings

Response time alarm firing conditions

Warning when response time for this URL is greater than 5,000 milliseconds

Critical when response time for this URL is greater than 10,000 milliseconds

Fatal when response time for this URL is greater than 15,000 milliseconds

Authentication and proxy settings

☐ URL authentication required

☐ Use proxy for URL connection

Server: 80

Port: 80

Proxy type: HTTP

☐ Proxy authentication required

Edit

How to get here

- 1 On the Administration Home page, click **Manage Web Monitor Transactions**.
- 2 On the Transaction Management dashboard that appears, in the [Transaction Management table](#), click a transaction name.

The [Transaction Detail view](#) appears in the display area.

Description of embedded views

This view is made up of the following embedded views:

- [Basic Information](#)
- [Monitoring Locations](#)
- [Advanced Settings](#)

Basic Information

Table 31. Basic Information view

Description	Shows the URL of the monitored Web site. It also indicates whether the agent should retrieve the page header only, and the expected content.
Data displayed	<ul style="list-style-type: none">• Expected Content: If content validation is enabled for the agent instance that monitors this URL, and the expected content type is HTML-based, this is indicated in this column. Also, a text string could be used such as "laptop" and type <code>laptop</code> into this column. In case the monitoring agent detects binary content or the text string at this address, the validation fails and the agent logs an error message. If this column is empty, that means the agent is not required to perform content validation. Content validation can be enabled using the URL List secondary agent properties. For more information, see Settings.• Unexpected Content: If unexpected content validation is enabled for the agent instance that monitors this URL, and the unexpected content type is HTML-based, this is indicated in this column. Also, a text string could be used such as "laptop" and type <code>laptop</code> into this column. In case the monitoring agent detects binary content or the text string at this address, the validation fails and the agent logs an error message. If this column is empty, that means the agent is not required to perform unexpected content validation. Unexpected Content validation can be enabled using the URL List secondary agent properties. For more information, see Settings.• Get Page Header Only. Indicates whether the monitoring agents collect only the page header.• Display Name. The display name of the transaction.• URL. The URL of the monitored Web site.

Monitoring Locations

Table 32. Monitoring Locations view

	Lists one or more hosts on which the monitoring Web Monitor Agent and Foglight Agent Manager are installed.
Description	<ul style="list-style-type: none">• Agent Name. The name of the Web Monitor Agent instance that gathers information about this transaction.• Location (FglAM). The name of the host on which the Agent Manager is installed.

Advanced Settings

Table 33. Advanced Settings view

	Displays thresholds for alarm generation and any authentication settings, if they exist.
Description	<ul style="list-style-type: none">• Authentication and proxy settings. These settings specify user authentication and proxy connection settings that may be required to monitor some transactions. For additional details about these settings and instructions on how to edit them, see Viewing and editing individual Web transaction details.• Response time alarm firing conditions. These settings control alarm generation. The default values are set in the Foglight registry: Synthetic_Transaction_MET_Warning: Controls the global default value of the threshold for generating Warning alarms. WebMonitor_Transaction_Response_Time_Critical: Controls the global default value of the threshold for generating Critical alarms. WebMonitor_Transaction_Response_Time_Fatal: Controls the global default value of the threshold for generating Fatal alarms. <p>For additional details about these settings and instructions on how to edit them, see Viewing and editing individual Web transaction details.</p>

Transaction Management table

Purpose

The **Transaction Management** table displays a list of monitored Web sites and helps you understand which locations monitor them. It provides insight into the complexity of your monitored environment.

Transaction Name	Display Name	URL	Location	Active Agents
			dsg8f5qf62_prod.quest.corp	1 / 1

How to get here

- On the Administration Home page, click **Manage Web Monitor Transactions**.
On the Transaction Management dashboard that appears, the [Transaction Management table](#) appears across the middle section of the display area.

Description of the view

Table 34. Transaction Management table

	<ul style="list-style-type: none">• Active Agents. The number of active Web Monitor Agent instances that currently monitor this Web site out of the total number of agents configured to collect data from it. For example, 1 / 2 means that only one active agent currently monitors this transaction out of two configured agents.
Data displayed	<ul style="list-style-type: none">• Locations. The names of the hosts running the Web Monitor Agent instances that currently monitor this Web site.• Transaction Name. The transaction name associated with the monitored Web site.• Display Name. The display name of the transaction.• URL. The URL of the monitored Web site.
Where to go next	<p>Drill down on:</p> <ul style="list-style-type: none">• Any row in this table. For more information, see Transaction Detail view.

Web Monitor Service Operation Console and Foglight for APM Transactions views

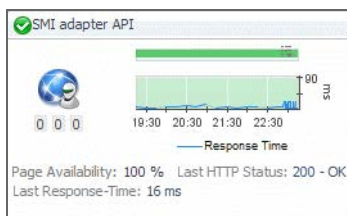
The Service Operations Console and Foglight for APM display the following Foglight Web Monitor views:

- [Transaction tile](#)
- [Transaction dialog box](#)

Transaction tile

Purpose

The Network Device tile shows summarized information about the performance of a network device. The tile bar indicates the device name.



How to get here

- On the navigation panel, click **Services > Service Operations Console**.
On the Service Operations Console that appears in the display area, select a Web Monitor service, and ensure that the **Transaction** tab is open.
- On the navigation panel, click **APM > Transactions**.
On the Transactions dashboard that appears in the display area, select a Web Monitor service.

One or more transaction tiles appear in the display area.

Description of the view

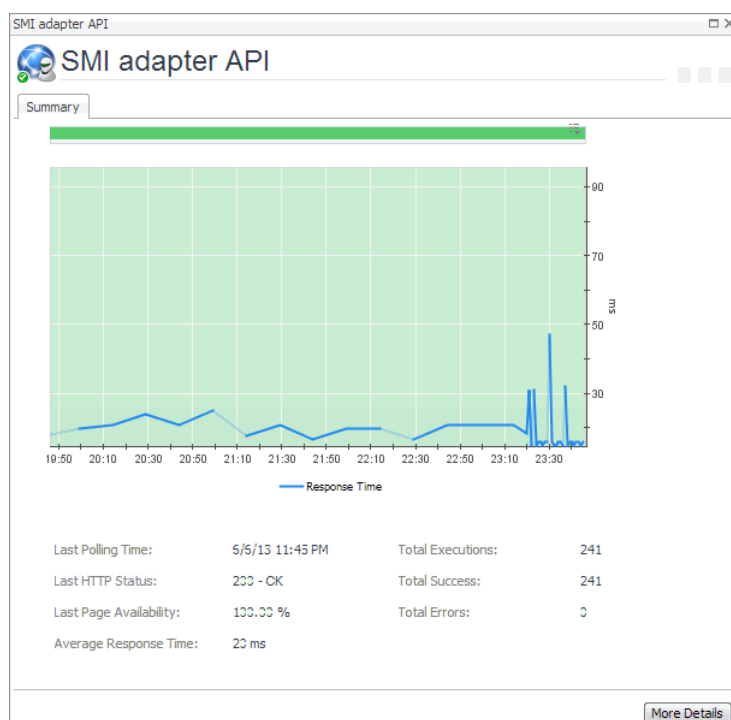
Table 35. Description of the view

Data displayed	<ul style="list-style-type: none">• Alarms. The counts of Fatal, Critical, and Warning alarms.• Health history bar. The color-coded bar represents the alarm state of the monitored application over the time range period selected in the Service Operations Console dashboard. The color of the bar changes over that period depending on the alarm state. Red indicates that the monitored application is in Fatal state, orange indicates Critical, yellow means Warning, and green is for the Normal State.• Last HTTP Status. The most recent HTTP status code, indicating the result of the most recent transaction with the monitored Web site.• Last Response-Time. The amount of time the Web Monitor Agent waited for a response from the monitored Web site during the most recent data collection attempt.• Page Availability. The percentage of time the Web site was available when the Web Monitor Agent instances configured to monitor this Web site attempted to collect information.• Response Time. The amount of time the Web site takes to respond to monitoring requests, over the selected time range. High values in the graph can indicate potential bottlenecks that likely need to be investigated.• Title bar. The name of the Web transaction.
Where to go next	<p>Drill down on:</p> <ul style="list-style-type: none">• Title bar. For more information, see Transaction dialog box.

Transaction dialog box

Purpose

The transaction dialog box shows a series of charts displaying the response time statistics of the selected transactions, accompanied with additional performance indicators, such as the number of errors and the most recent HTTP status. This can give you a better idea of how the selected Web site is performing and alerts you about potential performance problems, if they exist. For example, high response times often suggests higher loads that may require further investigation.



How to get here

- 1 Complete one of the following steps:

- On the navigation panel, click **Services > Service Operations Console**.

On the Service Operations Console that appears in the display area, select a Web Monitor service, and ensure that the **Transaction** tab is open.

- On the navigation panel, click **APM > Transactions**.

On the Transactions dashboard that appears in the display area, select a Web Monitor service.

One or more transaction tiles appear in the display area.

- 2 Click the title bar of a transaction tile.

The transaction dialog box appears.

Description of the view

Table 36. Description of the View

Data displayed	<ul style="list-style-type: none"> • Alarms. The counts of Fatal, Critical, and Warning alarms. • Average Response Time. The average amount of time all instances of the Web Monitor Agent configured to monitor this Web site wait for a response from the monitored Web site. • Health history bar. The color-coded bar represents the alarm state of the monitored application over the time range period selected in the Service Operations Console dashboard. The color of the bar changes over that period depending on the alarm state. Red indicates that the monitored application is in Fatal state, orange indicates Critical, yellow means Warning, and green is for the Normal State. • Last HTTP Status. The most recent HTTP status code, indicating the result of the most recent transaction with the monitored Web site.
-----------------------	--

Table 36. Description of the View

	<ul style="list-style-type: none"> • Last Page Availability. The percentage of time the Web site was available when the Web Monitor Agent attempted to collect information from it during the most recent data collection attempt.
	<ul style="list-style-type: none"> • Last Polling Time. The date and time of the most recent data collection.
	<ul style="list-style-type: none"> • Response Time. The amount of time the Web site takes to respond to monitoring requests, over the selected time range. High values in the graph can indicate potential bottlenecks that likely need to be investigated.
	<ul style="list-style-type: none"> • Title bar. The name of the Web transaction.
	<ul style="list-style-type: none"> • Total Errors. The total number of execution attempts that resulted in errors all instances of the Web Monitor Agent configured to monitor this Web site encountered during the selected time range.
	<ul style="list-style-type: none"> • Total Executions. The total number of execution attempts all instances of the Web Monitor Agent configured to monitor this Web site performed during the selected time range.
	<ul style="list-style-type: none"> • Total Success. The total number of execution attempts that resulted in success all instances of the Web Monitor Agent configured to monitor this Web site encountered during the selected time range.

Where to go next Drill down on:

- **More Details.** For more information, see [Transaction at All Locations drilldown view](#).

Monitoring network devices

Foglight Net Monitor provides device availability and packet loss monitoring between monitoring locations and network devices. Use it to:

- Monitor the network against service level agreements.
- Check for the presence of devices that are critical to your operating environment.

When you deploy Foglight Net Monitor, a set of predefined dashboards enables you to view the performance of the monitored network devices. This allows you to ensure consistent network device performance by re the collected statistics. Better management of your network devices can be achieved when you are alerted to potential problems before end users are affected.

Foglight Net Monitor relies on the Net Monitor Agent to collect data. The agent collects transaction information from monitored devices and visualizes the collected data in Foglight. You need to configure one agent instance on each monitored location.

Start by installing Foglight Net Monitor on the Management Server, deploying the Net Monitor Agent package, and creating agent instances on one or more hosts. For installation instructions, see the *Foglight Net Monitor Release Notes*.

Foglight Net Monitor uses the ICMP (Internet Control Message Protocol) service to monitor network devices. You need to configure this service to enable communication with network devices. For more information, see [Configuring the ICMP service for monitoring](#).

As a next step, you can specify the devices that you want to monitor using the Devices Management dashboard. In addition to managing the collection of monitored network devices, this dashboard allows you to edit the data collection settings. For more information, see [Managing monitored network devices](#).

Next, navigate to the Performance Browser. This dashboard displays the state of your system performance, providing a visual representation of the status of the monitored network devices and locations. Using this dashboard on a daily basis you can obtain an in-depth understanding of the state of your monitored network devices. Monitoring the same collection of network devices from different agent locations allows you to rule out any issues that may be related to host connectivity rather than device responsiveness. For more information, see [Investigating the performance of network devices](#).

The Net Monitor Agent is equipped with a set of properties that affect its running state. You can make changes to them, as required. For more information about the Net Monitor Agent properties, see [Configuring the agent properties](#).

For additional information, see the following topics:

- [Generating reports](#)
- [View reference](#)

Configuring the ICMP service for monitoring

Foglight Net Monitor uses the ICMP (Internet Control Message Protocol) service to communicate with network devices. There are two versions of this service that are available for use:

- *Foglight Agent Manager ICMP service* uses the `udp2icmp` application, that is installed with the Agent Manager, and can be used to issue ICMP messages to target devices.
- *OS-specific ICMP services* use the following OS-level commands to issue ICMP messages to target devices:
 - `ping`
 - `tracert` (Microsoft Windows only) or `traceroute` (Linux only)

Both types of ICMP services are started through an executable application and require proper permissions to execute. For more information, see [Configuring the Agent Manager ICMP service](#) and [Configuring OS-Level ICMP services](#).

By default, Foglight Net Monitor uses the Agent Manager ICMP service for monitoring. OS-level ICMP services can be configured, if needed, using the following option

```
-Dnetmonitor.icmpprovider=OS
```

There are two ways to specify this option:

- On the command line, when you start up the Agent Manager. For example:
`fglam -s -Dnetmonitor.icmpprovider=OS`
- As a JVM system property, in the `<fglam_home>/state/default/config/baseline.jvmargs.config` file. For example:
`-Dnetmonitor.icmpprovider=OS`

Other options are available. For more information, see [ICMP service command-line options](#).

ICMP service command-line options

The following table describes the Foglight Net Monitor parameters that can be used to configure the ICMP service. You can specify these options on the command line, or in an Agent Manager configuration file. For more information, see [Configuring the Agent Manager ICMP service](#).

Table 1. Foglight Net Monitor parameters used to configure the ICMP service

Option	Description
netmonitor.icmpprovider	All agent instances managed by this Agent Manager uses the OS-level ICMP service. This type of ICMP service uses <code>ping</code> and <code>traceroute/tracert</code> commands. The login user must have proper permissions to execute these commands, without providing a password.
netmonitor.ping.path	Unix/Linux only. If the login user does not have the permissions to execute the <code>ping</code> command, use this option to specify the command path.
netmonitor.traceroute.path	Unix/Linux only. If the login user does not have the permissions to execute the <code>traceroute</code> command, use this option to specify the command path.
netmonitor.threadpool.size	Unix/Linux only. Sets the thread pool size. You should specify at least 10.

Configuring the Agent Manager ICMP service

Windows configuration

- The user account launching the Agent Manager application must be an Administrator.
- To prevent time-outs in the trace route responses for all hops except the first and the last when the firewall is on, configure the firewall to enable inbound ICMP network traffic. For more information, visit <http://technet.microsoft.com/en-us/library/cc972926%28v=ws.10%29.aspx>.

Specifically, for IPv4, you need to use the following configuration:

```
ICMP Echo Request (Type 8, Code 8)
ICMP Echo Reply (Type 0, Code 0)
ICMP TTL Expired (Type 11, Code 0)
ICMP Port Unreachable (Type 3, Code 3)
```

UNIX/Linux configuration

- If the user account launching the Agent Manager application is not the root user, they must be granted permissions to execute the `<fglam_home>/client/<build id>/bin/udp2icmp` application without providing a password.
- If the Agent Manager secure-launcher is configured with a sudo path, `requiretty` must **not** be set.

Configuring OS-Level ICMP services

Windows configuration

- Ensure that the `ping` and `tracert` commands are available.
- The user account launching the Agent Manager application must have permissions to execute both `ping` and `tracert` commands.

UNIX/Linux configuration

- Ensure that the `ping` and `traceroute` commands are available.
- The user account launching the Agent Manager application must have permissions to execute both `ping` and `traceroute` commands.
- For Suse Linux with the `apparmor` module, enable `traceroute` to execute with the `-I` option. For example:

```
# Execute blow commands to enable traceroute -I option
complain /usr/sbin/traceroute
/etc/init.d/boot.apparmpr restart
```

Managing monitored network devices

The Devices Management dashboard displays a list of the monitored network devices. It allows you to add or remove network devices from the collection, and to edit their data collection parameters.

NOTE: Before adding new network devices for the first time using this dashboard, you must ensure that the following steps are completed:

- Deploy the Net Monitor Agent package to one or more desired monitoring locations (hosts).
- Create one or more Net Monitor Agent instances.
- Set the running mode for the newly agent created instances (Quick Check more or Normal mode).
- Configure data collection intervals for the newly created agent instances.
- Activate the newly created agent instances, and start their data collection. If you need to monitor the same collection of sub-network devices, you can specify private network properties, as required.

You can add one or more network devices using the Devices Management dashboard, and select desired agents (monitoring locations). Use this dashboard to gain an understanding of the complexity of your monitored environment and to review any alarms associated with the monitored devices.

Devices Management

View all devices and manage locations.

Device Status	Device Name	Device Name Override	NetworkID	Expected Response Time	Trace Route?	Monitor Location	Edit
<input type="checkbox"/>	www.mlook.mobi			300 ms	Yes		
<input checked="" type="checkbox"/>	www.567zw.com			300 ms	Yes		
<input checked="" type="checkbox"/>	www.zh-sport.com			300 ms	Yes		
<input checked="" type="checkbox"/>	rd-aixlp13			500 ms	Yes		
<input checked="" type="checkbox"/>	rd-ia64-03			500 ms	Yes		
<input checked="" type="checkbox"/>	rd-aix03			500 ms	Yes		

Agent Alarms

Severity	Time	Agent Name	Device Name	Alarm Message
	2/25/14 5:44 PM	centos6071_netm	www.mlook.mobi	Network Device Not Found. Failed to resolve IP address with device name(www.mlook.mobi)
	3/4/14 2:46 PM	centos6071_netm	www.567zw.com	Network Device Not Found. Failed to resolve IP address with device name(www.567zw.com)
	2/25/14 5:43 PM	apmw_netm	www.mlook.mobi	Network Device Not Found. Failed to resolve IP address with device name(www.mlook.mobi)

For complete details about the views appearing on this dashboard, see [Net Monitor Devices Management views](#).

To explore the collection of monitored network devices:

- 1 Log in to the Foglight browser interface.
- 2 On the navigation panel, under **Dashboards**, click **Infrastructure > NetMonitor > Devices Management**.
The Devices Management dashboard appears in the display area.

Devices Management

Mar 5, 2014 5:13:57 AM CST | Reports

Devices Management

View all devices and manage locations.

Add

Delete

Search

<input type="checkbox"/>	Device Status	Device Name	Device Name Override	NetworkID	Expected Response Time	Trace Route?	Monitor Location	Edit
<input type="checkbox"/>		www.mlook.mobi			300 ms	Yes		
<input type="checkbox"/>		www.567zw.com			300 ms	Yes		
<input type="checkbox"/>		www.zh-sport.com			300 ms	Yes		
<input type="checkbox"/>		rd-aixp13			500 ms	Yes		
<input type="checkbox"/>		rd-ia64-03			500 ms	Yes		
<input type="checkbox"/>		rd-aix03			500 ms	Yes		

Agent Alarms

Acknowledge Clear

Search

<input type="checkbox"/>	Severity	Time	Agent Name	Device Name	Alarm Message
<input type="checkbox"/>		2/25/14 5:44 PM	centos6071_netm	www.mlook.mobi	Network Device Not Found. Failed to resolve IP address with device name(www.mlook.mobi)
<input type="checkbox"/>		3/4/14 2:46 PM	centos6071_netm	www.567zw.com	Network Device Not Found. Failed to resolve IP address with device name(www.567zw.com)
<input type="checkbox"/>		2/25/14 5:43 PM	apmw_netm	www.mlook.mobi	Network Device Not Found. Failed to resolve IP address with device name(www.mlook.mobi)

For more information, see the following topics:

- [Expanding your collection of monitored network devices](#)
- [Removing network devices from the existing collection](#)
- [Viewing and editing individual network device details](#)

Expanding your collection of monitored network devices

The Devices Management dashboard allows you to expand your collection of monitored network devices by adding new devices to the list. Adding a new network device prompts the Net Monitor Agent to start collecting information about it in the next collection period.

This assumes that you already have the agent package deployed to the Foglight Agent Manager host, and one or more active Net Monitor Agent instances are in place. For complete information on how to deploy an agent package, and how to create and activate agent instances, see the *Administration and Configuration Help*.

To start monitoring a network device:

- 1 On the Devices Management dashboard, click **Add**.

The **Add Device(s)** dialog box appears.

2 In the **Add Device(s)** dialog box, provide information about the network device that you want to monitor.

- **Device(s) Name:** Type the names of one or more network devices that you want to monitor. This can be a host name or a host IP address. If a host name is specified, Foglight Net Monitor resolves it using DNS.
- **Above devices belong to a private network of:** If the hosts on which these devices are installed belong to a private network, select this check box and type the network name.

NOTE: Devices belonging to a private network should be monitored from one monitoring location (agent) only. You should specify only one location per monitored device in that case.

- **Expected Response Time.** Specify the expected amount of round-trip response time in milliseconds between the monitored location and the network device.
- **Trace Route (Enable):** Select this check box if you want to trace the route from the monitoring station to the device. If you do not select this option, you can execute a trace route in real time on the Trace Route page. For more information, see [Tracing data packets between monitoring locations and network devices](#).
- **Monitor by:** Specify one or more rules for collecting information about the monitored devices.

Location: Select the host from which you want to collect information about the monitored devices.

TIP: The list of all running Net Monitor Agent instances is available for selection in the Location box.


To add a new monitoring host, you must first create a Net Monitor Agent instance on that host, activate it, and start its data collection. To do that, click **Create new agent**. For more information about creating and activating agent instances and starting their data collection, see the *Administration and Configuration Help*.

Interval: Specify the collection interval for this device. The values in the list reflect the data collection intervals that are configured for all Net Monitor Agent instances that are running on the selected location. For example, if there are two agents with collection intervals of 10 and 15 minutes, these intervals appear in the list.

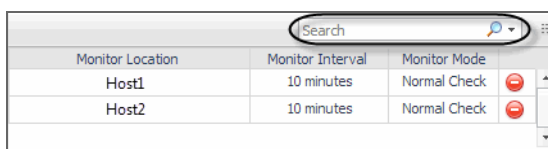
Mode: Specify the collection mode that you want to use for this device. The values in the list reflect the collection modes that are configured for all Net Monitor Agent instances that are running on the selected location. For example, if there are two agents with one running in *Quick Check* mode, and another in *Normal* mode, both collection modes appear in the list.

TIP: Quick Check mode verifies whether a device is alive; it does not instruct the agent to collect data unless it fails to detect the devices you have told it to monitor. Use Quick Check mode when you want to frequently verify that devices are up and running.

Normal Check mode collects data from the device during the specified collection intervals. This mode allows the agent to send the specified packet size and number of packets to collect and can use trace route to collect paths from one location to the monitored device, when the trace route option is enabled. Quick Check mode just sends packets with specific packet size and does not use trace route. When an agent is run in Quick Check mode, the agent can monitor more devices than in Normal Check mode. If you just want to monitor the device availability and are not interested in the device performance statistics, use Quick Check mode instead of Normal mode.

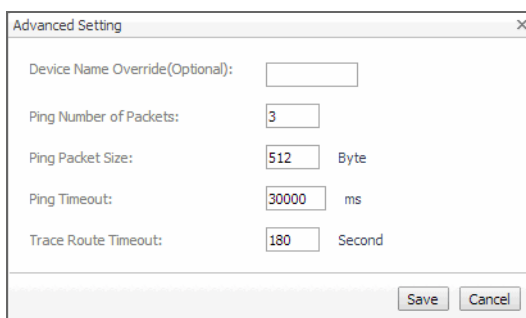
Click  Add to add the selected monitoring location to the table. If you want to collect information about the specified devices from a different location, or using a different mode or interval, you can specify additional monitoring locations.

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



Monitor Location	Monitor Interval	Monitor Mode
Host1	10 minutes	Normal Check
Host2	10 minutes	Normal Check

- **Advanced Settings:** To specify advanced settings such as the device name override, the number of packets to ping, the packet size when pinging, ping timeout, or trace route timeout, click **Advanced Settings** and override the default values, as required.



Advanced Setting

Device Name Override(Optional):

Ping Number of Packets:

Ping Packet Size: Byte

Ping Timeout: ms

Trace Route Timeout: Second

Device Name Override (Optional): Type the device name override, as required. Device name override can be used if you monitor two network devices that share an IP address. You can override the name of one of those devices to identify it. If specified, the device override name appears as that device's name in the browser interface. Another reason why you might need to override a device name is when a device is a host object in the Management Server. In that case, if you do not override the device name, its status reflects the host object status, instead of the device status.

Ping Number of Packets: Type the number of ICMP (Internet Control Message Protocol) or UDP (Universal Datagram Protocol) packets to send to the device.

Ping Packet Size: Type the size of the data portion of the packet in bytes.

Trace Route Timeout: Type the amount of time in seconds after which a route trace times out.

When done, click **Save** in the **Advanced Settings** dialog box.

- 3 In the **Add Device(s)** dialog box, click **Save**.

The **Add Device(s)** dialog box closes, and the Devices Management dashboard refreshes, showing the newly added device in the list.

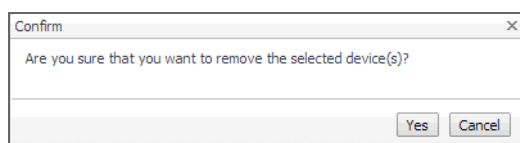
Removing network devices from the existing collection

The Devices Management dashboard allows you to remove network devices from the existing collection of monitored devices. Removing a device from the list causes the Net Monitor Agent to stop collecting information about that device. The data previously collected from a removed device is kept in the Foglight database in accordance with the existing persistence settings. For more information about persistence policies, refer to the *Administration and Configuration Help*.

To stop monitoring a network device:

- 1 On the Devices Management dashboard, select the network device that you no longer want to monitor, and click **Delete**.

The **Confirm** message box appears.




- 2 Click **Yes** to confirm the removal and close the message box.
A message box appears, indicating that the operation is complete.
- 3 Click **OK** to close it.
- 4 In the Devices Management dashboard, review the list of monitored devices.
The newly removed network device no longer appears in the list.

Viewing and editing individual network device details

You can view and edit the monitoring settings associated with individual network devices, when required. For example, you can start monitoring a network device using a different host, or change the data collection periods for specific locations.

To view and edit network device details:

- 1 On the Devices Management dashboard, in the row containing the network device whose settings you want to review, in the Edit column, click Edit .

The **Edit Device** dialog box appears.

Edit Device

Device Name:

☐ Above devices belong to a **private** network of

Expected Response Time: ms

Trace Route: ☐ Enable (This option takes effect only when agent runs in Normal Check mode.)

Monitor by:

Location	Interval	Mode
<input type="text"/>	<input type="text"/>	<input type="text" value="Normal Check"/>

Search

Monitor Location	Monitor Interval	Monitor Mode
Host1	10 minutes	Normal Check
Host2	10 minutes	Normal Check

Can not find the agent? [Create new agent](#)

[Advanced Setting](#)

2 In the **Edit Device** dialog box, review the device settings, and make any changes, as required.

- **Device Name:** Type the names of one or more network devices that you want to monitor. This can be a host name or a host IP address. If a host name is specified, Foglight Net Monitor resolves it using DNS.
- **Above devices belong to a private network of:** If the hosts on which these devices are installed belong to a private network, select this check box and type the network name.

NOTE: Devices belonging to a private network should be monitored from one monitoring location (agent) only. You should specify only one location per monitored device in that case.

- **Expected Response Time.** Specify the expected amount of round-trip response time in milliseconds between the monitored location and the network device.
- **Trace Route (Enable):** Select this check box if you want to trace the route from the monitor station to the device. If you do not select this option, you can execute a trace route in real time on the Trace Route page. For more information, see [Tracing data packets between monitoring locations and network devices](#).
- **Monitor by:** Specify one or more rules for collecting information about the monitored devices.

Location: Select the host from which you want to collect information about the monitored devices.

TIP: The list of all running Net Monitor Agent instances is available for selection in the **Location** box.


To add a new monitoring host, you must first create a Net Monitor Agent instance on that host, activate it, and start its data collection. To do that, click **Create new agent**. For more information about creating and activating agent instances and starting their data collection, see the *Administration and Configuration Help*.

Interval: Specify the collection interval for this device. The values in the list reflect the data collection intervals that are configured for all Net Monitor Agent instances that are running on the selected location. For example, if there are two agents with the collection intervals of 10 and 15 minutes, these intervals appear in the list.

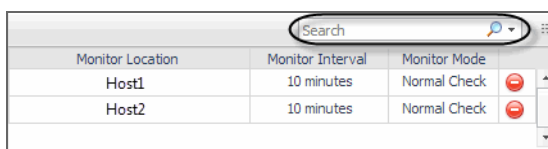
Mode: Specify the collection mode that you want to use for this device. The values in the list reflect the collection modes that are configured for all Net Monitor Agent instances that are running on the selected location. For example, if there are two agents with one running in *Quick Check* mode, and another in *Normal* mode, both collection modes appear in the list.

TIP: Quick Check mode verifies whether a device is alive; it does not instruct the agent to collect data unless it fails to detect the devices you have told it to monitor. Use Quick Check mode when you want to frequently verify that devices are up and running.

Normal Check mode collects data from the device during the specified collection intervals. This mode allows the agent to send the specified packet size and number of packets to collect and can use trace route to collect paths from one location to the monitored device, when the trace route option is enabled. Quick Check mode just sends a fixed number of small-size packets and does not use trace route. When an agent is run in Quick Check mode, the agent can monitor more devices than in Normal Check mode. If you just want to monitor the device availability and are not interested in the device performance statistics, use Quick Check mode instead of Normal mode.

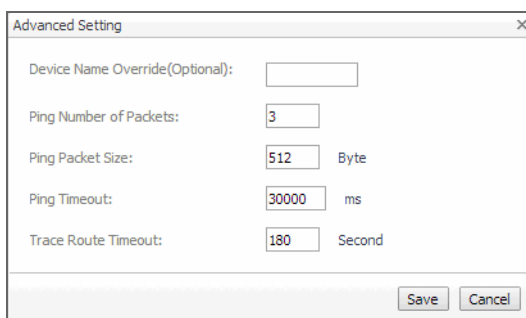
Click  Add to add the selected monitoring location to the table. If you want to collect information about the specified devices from a different location, or using a different mode or interval, you can specify additional monitoring locations.

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



Monitor Location	Monitor Interval	Monitor Mode
Host1	10 minutes	Normal Check
Host2	10 minutes	Normal Check

- **Advanced Settings:** To specify advanced settings such as the device name override, the number of packets to ping, the packet size when pinging, ping timeout, or trace route timeout, click **Advanced Settings** and override the default values, as required.



Advanced Setting

Device Name Override(Optional):

Ping Number of Packets:

Ping Packet Size: Byte

Ping Timeout: ms

Trace Route Timeout: Second

Device Name Override (Optional): Type the device name override, as required. Device name override can be used if you monitor two network devices that share an IP address. You can override the name of one of those devices to identify it. If specified, the device override name appears as that device's name in the browser interface. Another reason why you might need to override a device name is when a device is a host object in the Management Server. In that case, if you do not override the device name, its status reflects the host object status, instead of the device status.

Ping Number of Packets: Type the number of ICMP (Internet Control Message Protocol) or UDP (Universal Datagram Protocol) packets to send to the device.

Ping Packet Size: Type the size of the data portion of the packet in bytes.

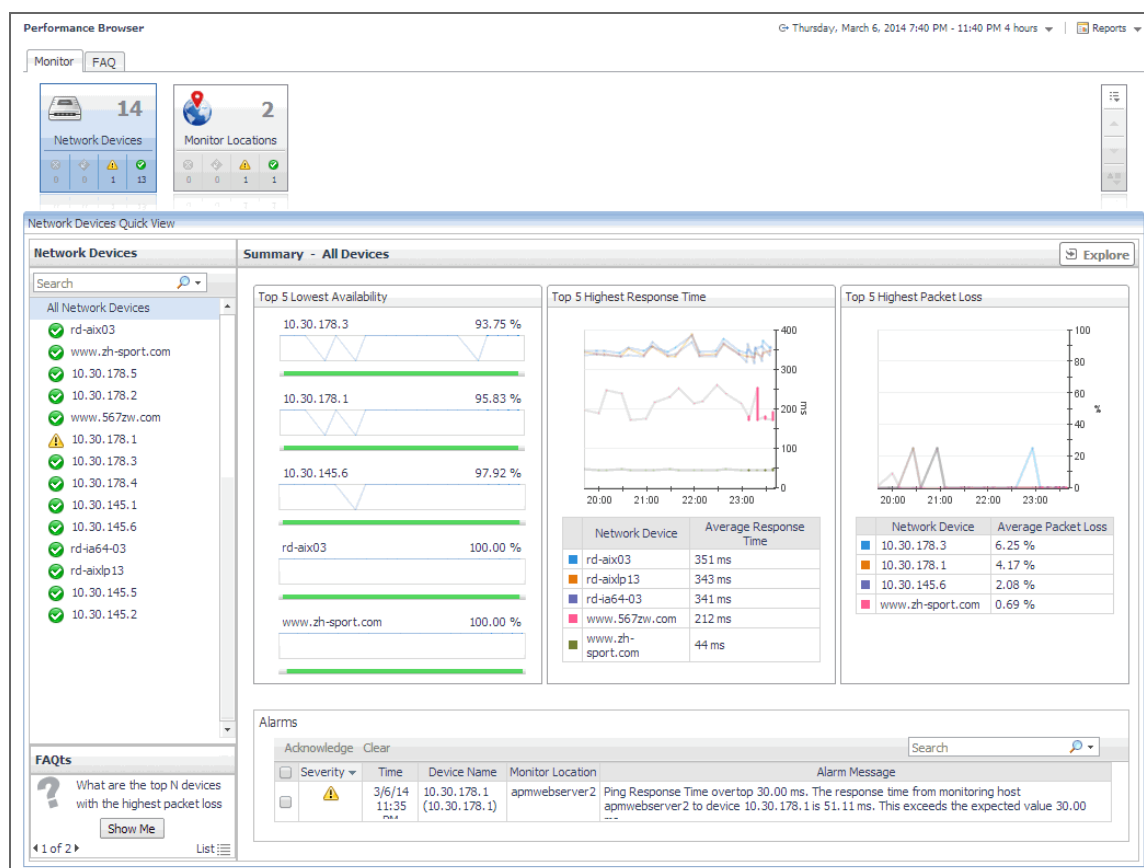
Trace Route Timeout: Type the amount of time in seconds after which a route trace times out.

When done, click **Save** in the **Advanced Settings** dialog box.

- 3 In the **Edit Device** dialog box, click **Save**.

Investigating the performance of network devices

A typical monitored environment includes a set of monitored network devices and Net Monitor Agents that collect data about these devices. These components are displayed on the Performance Browser dashboard. Use this dashboard to see the state of individual network devices when monitored from one or multiple locations.

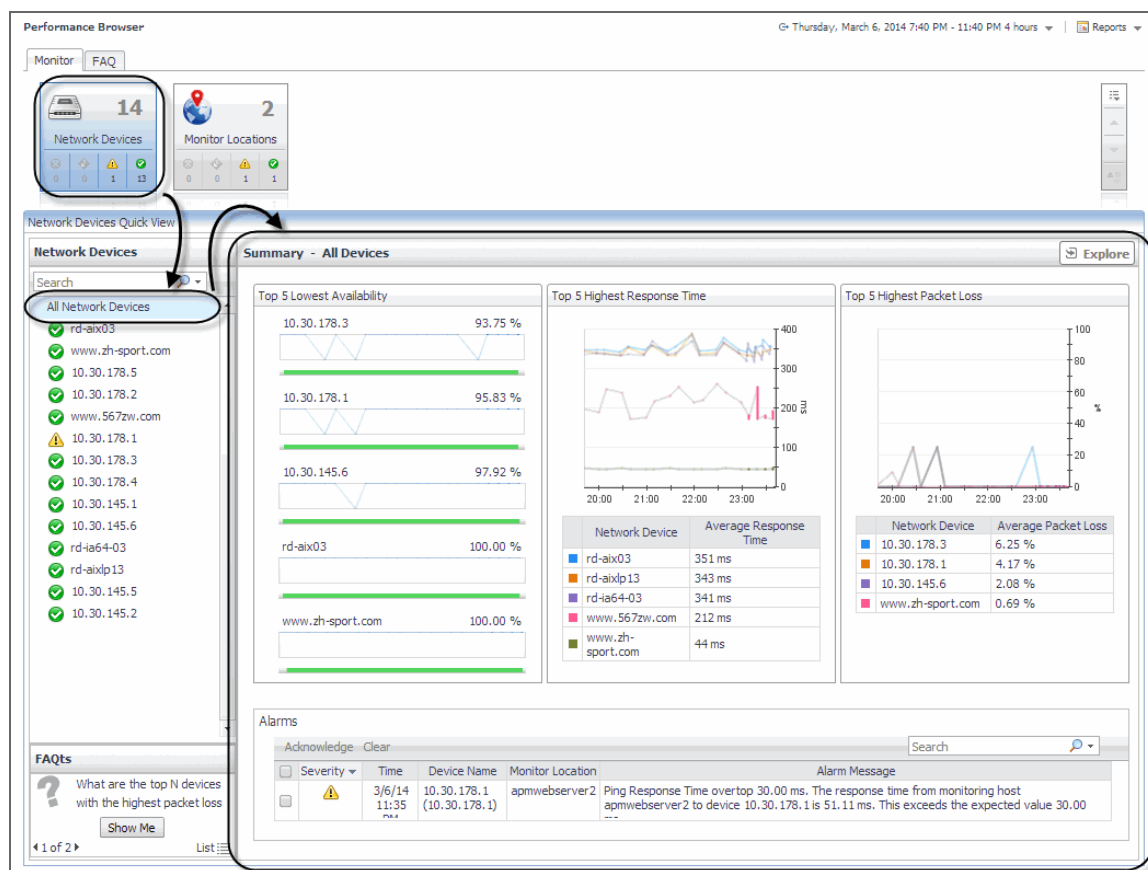


You can access this dashboard from the navigation panel. Under **Dashboards**, click **Infrastructure > NetMonitor > Performance Browser**.

When you navigate to the Performance Browser for the first time, the **Monitoring** tab appears open. This tab provides an overall summary of your monitored network devices.

TIP: In addition to the Monitoring tab, the Performance Browser also offers the FAQ tab. For more information, see [Exploring the FAQ tab](#).

Start by indicating the type of objects that you want to investigate. To do that, select the appropriate tile at the top of the **Monitoring** tab: **Network Devices** or **Monitor Locations**. This causes the Quick View to display information about the selected objects. Next, select an object or group of objects in the Quick View, such as **All Network Devices** or **All Monitor Locations**, to display additional information about that selection.



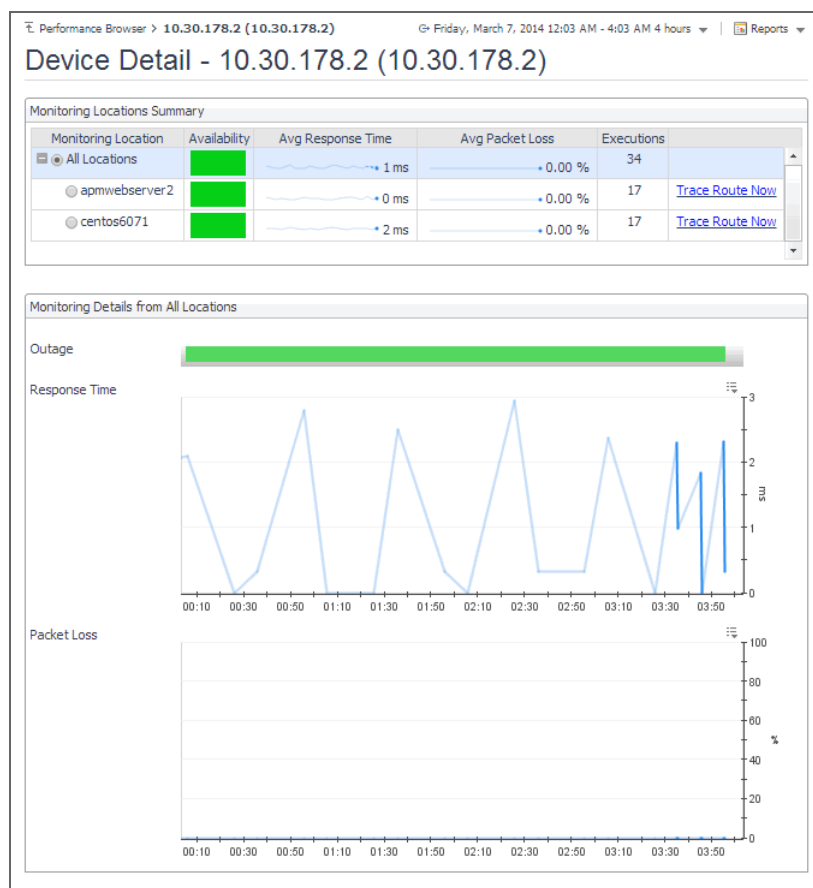
For complete details about the views appearing on this dashboard, see [Net Monitor Performance Browser views](#).

For more information, see the following topics:

- [Exploring individual network devices](#)
- [Tracing data packets between monitoring locations and network devices](#)
- [Exploring the FAQ tab](#)

Exploring individual network devices

When you select a network device in the **Summary - All Devices** view, you can see additional information, such as response times and packet loss values, in the **Device Detail** view. High levels of these indicators typically point to network congestion, and may require additional investigation.



For complete details about the data appearing on this view, see [Device Detail view](#).

To drill down on a network device:

- 1 On the Performance Browser dashboard, select the **Network Devices** tile.
- 2 In the **Network Devices Quick View**, in the **Network Devices** panel on the left, select a network device.
- 3 In the **Summary - Single Device Summary** on the right, click **Explore**.

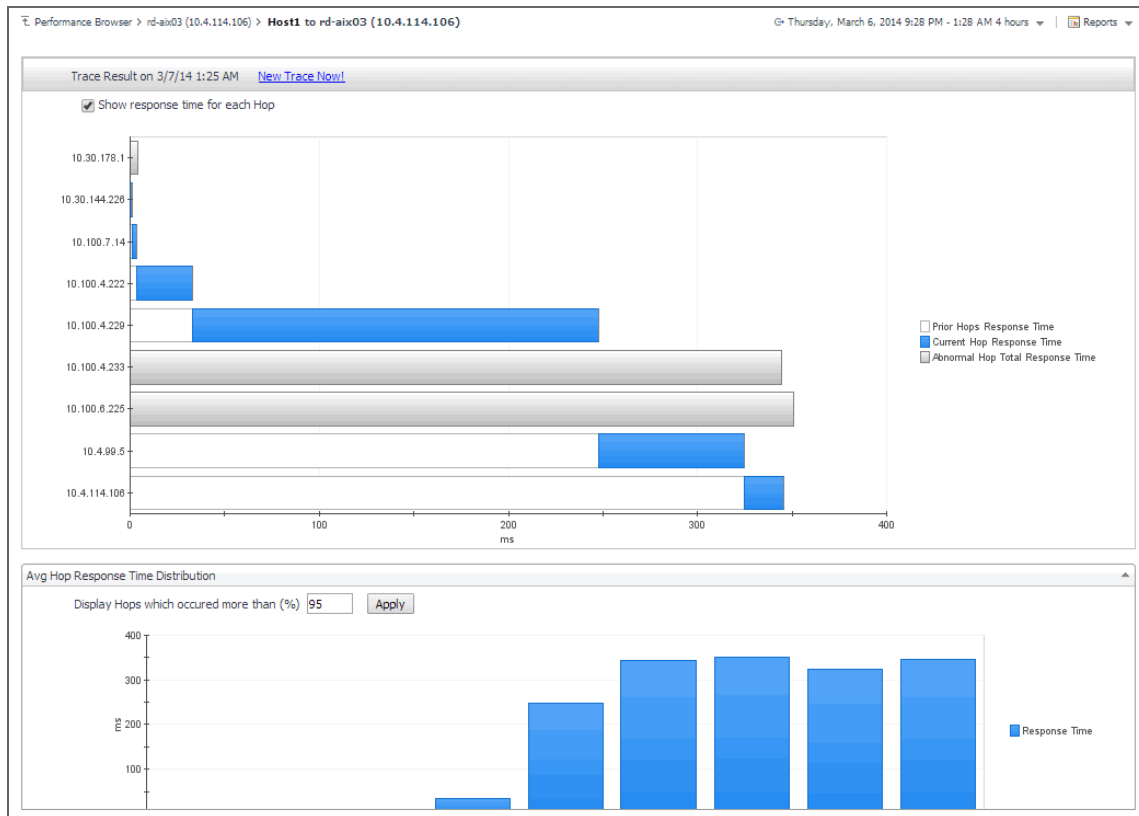
The **Device Detail** view appears in the display area.

Tracing data packets between monitoring locations and network devices

When you monitor a network device from a monitoring location, the monitoring agent sends a configured number of data packets to the device. The complete path of each data packet, from the monitoring location to the network device, represents a route. On the way to its destination, a data packet often runs through a number of other devices, so the route consists of one or more *hops*, where each device it passes through is counted as one hop.

The **Trace Result** view allows you to trace a route between a monitoring location and a network device, and review the time a data packet spends at each individual hop. This can help you investigate signs of performance degradation. For example, if your system reports higher than usual response times and frequent time-outs, you can trace the route of data packets to determine what is causing the bottlenecks.

Another example is when a device ping times out, this may be related to a possible wrong network route which can be seen on this page. For instance, if the expected trace route consists of ten hops, but the trace route in the chart appears to consist of five hops, you can identify the IP address associated with the broken hop in the chart. This can help you to quickly identify the root cause of a broken network.



For complete details about the data appearing on this view, see [Trace Result view](#).

To trace a data packet route:

- 1 On the Performance Browser dashboard, select the **Network Devices** tile.
- 2 In the **Network Devices Quick View**, in the **Network Devices** panel on the left, select a network device.
- 3 In the **Summary - Single Device Summary** on the right, click **Explore**.
- 4 On the Device Detail dashboard, in the **Monitoring Locations Summary** view, in the row containing the monitoring host from which data packets are sent to the device, click **Trace Route Now**.

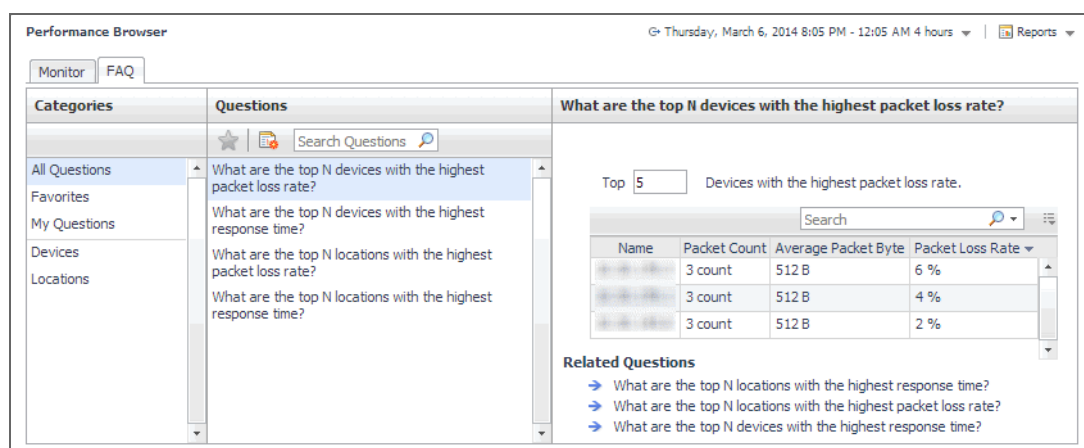
The **Trace Result** view appears in the display area.

The trace route request runs in the background and takes several minutes to complete. Instead of waiting for it to complete, you can navigate to other dashboards, and then return to this page to review the trace route.

IMPORTANT: If the trace route option is disabled in the device settings (see [Viewing and editing individual network device details](#)), this page is not populated with data. You can quickly execute a trace route in real time on this page by clicking **Trace Route Now**.

Exploring the FAQ tab

The **FAQ** tab available on the Performance Browser allows you to look at frequently asked questions about your monitored devices and review the answers. The **Categories** view shows several question categories. Selecting a category shows the questions belonging to that category in the **Questions** pane. From there, clicking a question shows the answer on the right.



Generating reports

Foglight Net Monitor supports the report generation ability. This allows you to create reports using a set of predefined templates to report on the various aspects of your monitored environment. Foglight Net Monitor includes a collection of predefined report templates.

You can generate, copy, and edit reports using the Reports dashboard included with the Foglight Management Server. For more information about this dashboard, see the *Foglight User Help*.

Report templates

Table 2. Predefined report templates

Report Template	Description
All Device Daily Outage Report	Shows network device availability over the specified time range, per monitoring location.
All Device Summary Report	Shows network device performance statistics over the specified time range, per monitoring location. The statistics include the device availability, average response time, average packet loss, hop count, and the number of executions.
Single Device Report	Shows the performance details for a selected network device during the specified time range, per monitoring location. The statistics include the monitoring host availability, average response time, average packet loss, hop count, and the number of executions. It also provides trace route summary details for each host.

Configuring the agent properties

The Net Monitor Agent collects data about monitored network devices and sends it to the Management Server. Monitoring agents keep track of resource utilization metrics and alert you when certain pre-defined thresholds are reached.

When an agent connects to Foglight, it is provided with sets of properties that it uses to configure its correct running state. Each agent is provided with a combination of two types of properties: agent properties and shareable properties.

Default versions of these properties are installed with Foglight for Net Monitor. However, you can edit the default shareable and agent properties, configure agent properties that apply only to a specific agent instance, and create edited clones of shareable properties that are used by a subset of agents of a certain type.

For complete information about working with agent properties, see the *Administration and Configuration Help*.

To configure agent properties:

- 1 Log in to the Foglight browser interface.
- 2 Ensure that the navigation panel is open.
To open the navigation panel, click the right-facing arrow on the left.
- 3 Open the Agent Status dashboard and navigate to the agent properties.
 - a On the navigation panel, under **Dashboards**, choose **Administration > Agents > Agent Status**.

i **IMPORTANT:** Another way of editing agent properties is through the Agent Properties dashboard. The properties you specify on this dashboard apply to all instances of the selected agent type, excluding any of the existing agents. To be certain that you are editing the properties of a particular agent instance and to prevent overwriting of properties of another agent instance, use the Agent Status dashboard instead of the Agent Properties dashboard.
 - b On the Agent Status dashboard, select the instance of the Net Monitor Agent whose properties you want to modify and click **Edit Properties**.
 - c Indicate that you want to edit the properties of the selected agent instance.
A list of agent properties appears in the display area.

Configuring Net Monitor agent properties

When you first install Foglight Net Monitor, you must deploy the Net Monitor Agent package on one or more hosts (monitoring locations). Then, create new agent instances, and set the running mode on those instances (Quick Check mode or Normal mode), and data collection intervals using the Net Monitor Agent properties.

Next, activate the agent instances, and start the data collection. If you monitor the same collection of sub-network devices, you can specify private network properties, as required. The Net Monitor Agent includes the following groups of agent properties that control its behavior:

- [NetMonitor Devices Settings](#)
- [Data Collection Scheduler](#)

When you finish configuring the Net Monitor Agent instances and their agent properties, you can specify the network devices that you want to monitor, and associate them with appropriate monitoring agents, as required. This can be done using the Devices Management dashboard. For more information about this dashboard, see [Managing Monitored Network Devices](#).

NetMonitor Devices Settings

The **Settings** properties specify the collection mode, any private networks to which the monitored network devices belong, and identify the monitored network devices.

NetMonitor Devices Settings

Run Quick Check Mode ? ☐ True ☒ False

Private Network Config Item: privateNetworkConfigList [Edit] [Clone] [Delete]

Device Item: deviceItemList [Edit] [Clone] [Delete]

Data Collection Scheduler

Collector Config: defaultSchedule [Edit] [Clone] [Delete]

- **Run Quick Check Mode:** Quick Check is a utility included with the Net Monitor Agent. It verifies whether a device is alive. It instructs the agent to collect data only if it fails to detect the devices that the agent is configured to monitor. Use Quick Check mode when you want to verify that devices are up and running.

If Quick Check detects the devices in the currently monitored list, Foglight continues to collect data according to the sample frequency. However, if it fails to detect the devices, it immediately initiates a data collection cycle and triggers the *Network Device Not Found* rule which sends an email to the system administrator.

To have the agent run in Quick Check mode, select **True**.

- **Private Network Config Item:** A list identifying private networks to which the monitored network devices belong, if applicable. Each entry in the list includes the following columns:
 - **Private network ID:** The ID of the private network.
 - **Private Ip Pattern:** An expression representing the pattern of the private network IP. This property is used in combination with the network ID. Any IP addresses that match the specified pattern are in same network. For example, if the network ID is `private network 1` and the IP pattern is `10.30.178.1-10.30.178.254`, the agent monitors all devices in `private network 1` that are in the `10.30.178.1-10.30.178.254` range.

Examples of private IP pattern ranges include:

```
192.168.0.1-192.168.0.254
192.168.0.1-192.168.0.254, 192.168.1.1-192.168.1.254
```

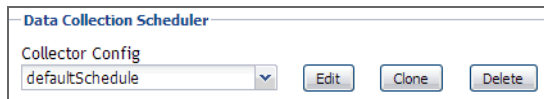
- **Device Item:** A list identifying the devices monitored by the agent instance. Each entry in the list includes the following columns:

i **IMPORTANT:** Do not use this list to specify monitored devices. Instead, use the Devices Management dashboard. For more information about this dashboard, see [Managing monitored network devices](#).

- **Device name:** The name of the monitored network device.
- **Device's network ID:** The ID of the network associated with the network device. Configure this property if you want the agent to monitor more than one device with the same IP address but with different network IDs.
- **Device Type:** The type of the network device: **Host** (if the device is used by a host system), or **Other** (if the device is used by a different machine type, such as a printer).
- **Device name override:** The device name override, if applicable.
- **Ping Timeout (Milliseconds):** The amount of time in milliseconds after which a ping request times out.
- **Trace Route?:** Select if you want to trace routes to this network device.
- **Trace Route Timeout (Seconds):** Type the amount of time in seconds after which a route trace times out.
- **Number of Packets:** The number of ICMP (Internet Control Message Protocol) or UDP (Universal Datagram Protocol) packets to send to monitored network devices.
- **Data Size (Bytes):** The size of the data portion of the packet in bytes.
- **Expected Response Time (Milliseconds):** The expected amount of round-trip response time in milliseconds between the monitoring location and monitored network devices.

Data Collection Scheduler

The **Data Collection Scheduler** agent properties specify the data frequency settings that the Net Monitor Agent uses to collect metrics from the monitored websites.



- **Collector Config:** A list containing the data collectors the agent uses. Each entry in the list includes the following columns:
 - **Collector Name:** The name of the collector the uses to gather data.
 - **Default Collection Interval:** The number of milliseconds, seconds, minutes, hours, or days during which the Net Monitor Agent collects data.
 - **Time Unit:** The time unit associated with the **Default Collection Interval:** **milliseconds, seconds, minutes, hours, or days.**
 - **Fast-Mode Collection Interval:** The number of milliseconds, seconds, minutes, hours, or days during which the Net Monitor Agent collects data when working in the fast collection mode.
 - **Fast-Mode Time Unit:** The time unit associated with the **Fast-Mode Collection Interval:** **milliseconds, seconds, minutes, hours, or days.**
 - **Fast-Mode Max Count:** The maximum number of the times the Net Monitor Agent can stay in fast collection mode.

View reference

Foglight displays monitoring data in views that group, format, and display data. The main types are described below.

Dashboards are top-level views that contain lower-level views. The dashboards supplied with Foglight, as well as those created by users, are accessible from the navigation panel.

Lower-level views in Foglight can be added to dashboards or can be accessed by drilling down from a dashboard. They receive and display data directly from the Management Server or from other views. Some views filter or select data that appears in other views in the same dashboard. Some are tree views with expandable nodes for selecting servers, applications, or data.

Foglight Net Monitor ships with several dashboards that allow you to monitor and configure your monitored environment. Each of these dashboards contains a number of views. This section describes these views in more detail. For more information about the available dashboards, see [Managing monitored network devices](#) and [Investigating the performance of network devices](#).

This cartridge includes the following groups of views:

- [Net Monitor Devices Management views](#)
- [Net Monitor Performance Browser views](#)

Net Monitor Devices Management views

The Devices Management dashboard contains the following views:

- [Agent Alarms view](#)
- [Devices Management table](#)

Agent Alarms view



Purpose

The **Agent Alarms** view displays the alarms generated against the existing agents.

Agent Alarms

Acknowledge Clear

Search




<input type="checkbox"/>	Severity ▾	Time	Agent Name	Device Name	Alarm Message
<input type="checkbox"/>		2/25/14 5:44 PM	centos6071_netm	www.mlook.mobi	Network Device Not Found. Failed to resolve IP address with device name(www.mlook.mobi)
<input type="checkbox"/>		2/25/14 5:43 PM	apmw_netm	www.mlook.mobi	Network Device Not Found. Failed to resolve IP address with device name(www.mlook.mobi)

How to get here

On the Devices Management dashboard, this view appears just below the [Devices Management table](#).

Description of the View

Table 3. Agent Alarms view

Description	Lists the alarms generated against the monitored locations.	
	NOTE: To acknowledge or clear one or more alarms appearing in this table, select them and click Acknowledge or Clear , as required. For more information about alarms in Foglight, see the <i>Foglight User Guide</i> .	
Data displayed	<ul style="list-style-type: none"> • Ack'ed. Indicates if the alarm is acknowledged: <code>true</code> or <code>false</code>. • Device Name. The name of the device against which the alarm is generated, as configured on the Devices Management dashboard. For more information, see Managing monitored network devices. • Severity. Indicates the alarm severity: Warning , Critical , or Fatal . • Time. The date and time when the alarm is generated. • Alarm Message. The alarm message. 	
	Drill down on: <ul style="list-style-type: none"> • Any row. Displays the Alarm Created dialog box, showing additional information about the alarm. For more information about alarms in Foglight, see the <i>Foglight User Help</i>. 	

Where to go next

Alarm Created at 2/25/14 5:44 PM

Diagnostic time range Tuesday, February 25, 2014 2:44 PM - 6:44 PM 4 hours

Host

n/a

Instance

www.mlook.mobi(NetMonitorAgent/5.7.0/NetMonitorAgent/centos6071_netm)

Agent

n/a

Origin (By Rule)

Network Device Not Found

Agent Type

n/a

Default Drilldown

n/a

Message and Help

Network Device Not Found. Failed to resolve IP address with device name(www.mlook.mobi)

Has Service Level Impact on 0 Services

Service Name

SLC

There are no services impacted by this alarm.

History

All Notes

Created Time	Sev	Dur	Ack'd Info	Clearing Info	Notes
Status	By User	Status	By		
2/25/14 5:44 PM	Warning	9.4 d	Not Ack'd		No
					0

Acknowledge

Acknowledge Until Normal

Clear

Find Historic Occurrences

Cancel

Devices Management table

Purpose

The **Devices Management** view displays the monitored network devices.

Add Delete		Search						
<input type="checkbox"/>	Device Status	Device Name	Device Name Override	NetworkID	Expected Response Time	Trace Route?	Monitor Location ?	Edit
<input type="checkbox"/>	✓	10.30.145.6			30 ms	No	● ●	
<input type="checkbox"/>	✓	10.30.145.5			30 ms	No	● ●	
<input type="checkbox"/>	✓	10.30.145.2			30 ms	No	● ●	
<input type="checkbox"/>	✓	10.30.145.1			30 ms	No	● ●	
<input type="checkbox"/>	✓	10.30.178.5			30 ms	No	● ●	
<input type="checkbox"/>	✓	10.30.178.4			30 ms	No	● ●	
<input type="checkbox"/>	✓	10.30.178.3			30 ms	No	● ●	
<input type="checkbox"/>	✓	10.30.178.2			30 ms	No	● ●	
<input type="checkbox"/>	✓	10.30.178.1			30 ms	No	● ●	
<input type="checkbox"/>	✓	www.360.cn.com			300 ms	Yes	● ●	
<input type="checkbox"/>	✓	www.zhihu.com			300 ms	Yes	● ●	
<input type="checkbox"/>	✓	nt-wd-03			500 ms	Yes	● ●	
<input type="checkbox"/>	✓	nt-wd-03			500 ms	Yes	● ●	
<input type="checkbox"/>	✓	nt-wd-03			500 ms	Yes	● ●	

How to get here

On the Devices Management dashboard, this view appears just above the [Agent Alarms view](#).

Description of the View

Table 4. Devices Management view

Data displayed	<ul style="list-style-type: none"> • Device Name Override. The device name override, if one is specified. • Device Name. The name of the monitored device. • Device Status. The state of the highest severity alarm raised against the network device: Warning ⚠, Critical ⚡, or Fatal ☠. • Expected Response Time. The expected round-trip response time between the host on which the Net Monitor Agent is installed and the network device.
	<ul style="list-style-type: none"> • Monitor Location. A color-coded indicator of the data collection state for each location from which this network device is monitored. Green indicates Normal, yellow Warning, orange Critical, and red the Fatal state. • NetworkID. The ID of the private network to which the network device belongs, if applicable. • Trace Route?. Indicates if the route from the monitoring agent to the network device is traced.

Net Monitor Performance Browser views

The Performance Browser contains the following views:

- [Alarms view](#)
- [Device Detail view](#)
- [FAQ tab](#)
- [FAQts view](#)
- [Net Monitor Environment view](#)
- [Network Devices view](#)
- [Monitor tab](#)
- [Monitor Locations view](#)
- [Quick View](#)
- [Single Location Summary view](#)

- [Summary - All Devices view](#)
- [Summary - All Monitor Locations view](#)
- [Summary - Single Device Summary view](#)
- [Trace Result view](#)

Alarms view

Purpose

The **Alarms** view lists the alarms generated against the selected object or group of objects in the [Quick View](#).

TIP: To acknowledge or clear one or more alarms appearing in this table, select them and click Acknowledge or Clear, as required. For more information about alarms in Foglight, see the Foglight User Guide.

Alarms					
Acknowledge Clear		Search			
<input type="checkbox"/>	Severity	Time	Device Name	Monitor Location	Alarm Message
<input type="checkbox"/>	Warning	3/10/14 10:40 PM	10.30.178.3 (10.30.178.3)	Host1	Device is unavailable. Network device 10.30.178.3 is not reachable from Host1
<input type="checkbox"/>	Warning	3/10/14 10:40 PM	10.30.178.1 (10.30.178.1)	Host1	Device is unavailable. Network device 10.30.178.1 is not reachable from Host1
<input type="checkbox"/>	Warning	3/10/14 10:40 PM	10.30.178.5 (10.30.178.5)	Host1	Device is unavailable. Network device 10.30.178.5 is not reachable from Host1




How to get here

- 1 Navigate to the Performance Browser.
- 2 On the [Monitor tab](#), in the [Net Monitor Environment view](#), select the **Network Devices** or **Locations** tile.
- 3 In the [Quick View](#), in the panel on the left, select **All Network Devices**, a network device, or a monitoring location.

The **Alarms** view appears at the bottom of the panel on the right.

Description of the view

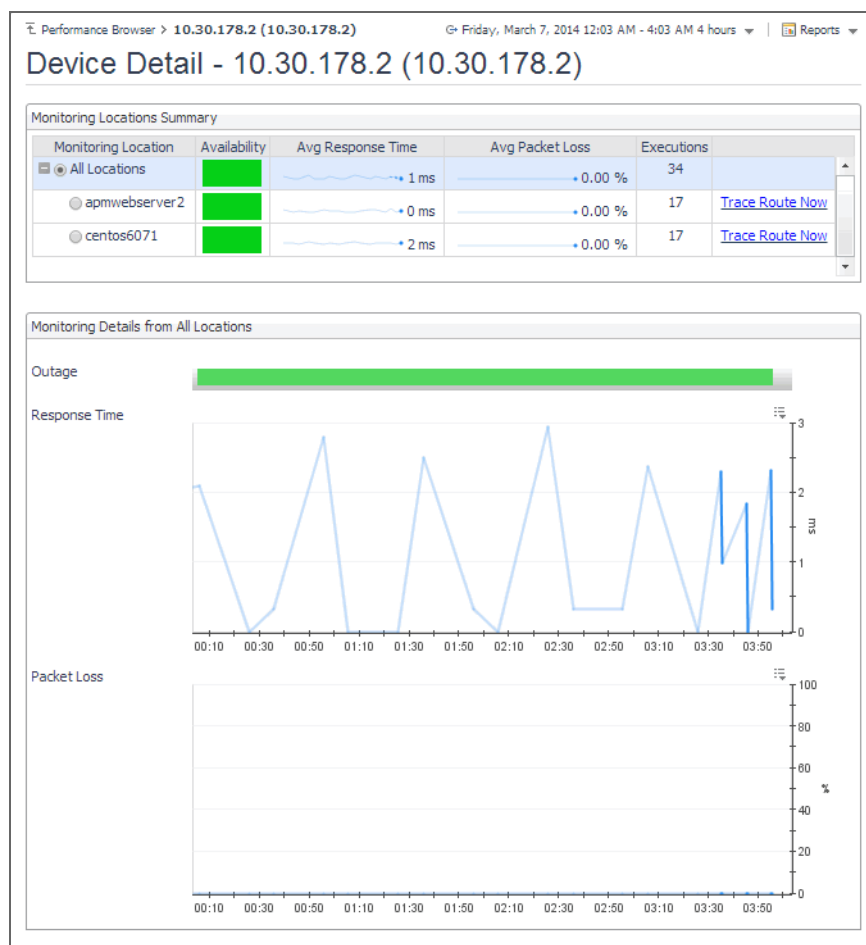
Table 5. Alarms view

Data displayed	<ul style="list-style-type: none"> • Alarm Message. The alarm message, explaining the reason for this alarm. • Device Name. The name of the monitored device against which the alarm is generated.
	<ul style="list-style-type: none"> • Monitor Location. The name of the host running the instance of the Net Monitor Agent that monitors this device.
	<ul style="list-style-type: none"> • Severity. Indicates the alarm severity: Warning , Critical , or Fatal .
	<ul style="list-style-type: none"> • Time. The time at which the alarm is generated.

Device Detail view

Purpose

The **Device Detail** view provides details about the selected network device. Use it to find out the average response times of this device from different monitoring locations, and to review its overall health.



How to get here

- 1 Navigate to the Performance Browser.
- 2 On the [Monitor tab](#), in the [Net Monitor Environment view](#), select the **Network Devices** tile.
- 3 In the [Quick View](#), in the [Network Devices view](#), select a network device.
- 4 In the [Summary - Single Device Summary view](#), click **Explore**.

The **Device Detail** view appears in the display area.

Description of embedded views

This view is made up of the following embedded views:

- [Monitoring Locations Summary](#)
- [Monitoring Details from All Locations](#)

Monitoring Locations Summary

Table 6. Monitoring Locations Summary view

Description	Lists the hosts from which the selected network device is monitored.
Data displayed	<ul style="list-style-type: none">• Availability. A color-coded bar, representing the availability of the device over the selected time range. The color of the bar changes depending on the alarm state. Red indicates the Fatal state, orange indicates Critical, yellow means Warning, and green is the Normal state.• Avg Packet Loss. The average percentage of time the data packets sent to the monitored device are not echoed back. By default, the monitoring agent sends five data packets to the monitored network device. The number of data packets the Net Monitor Agent sends to monitored devices is specified in the Net Monitor Agent properties.• Avg Response Time. The average round-trip response time between the monitoring agent and the network device.• Executions. The number of times the Net Monitor Agent sends data packets to the selected network device.• Monitoring Location. The name of the host from which the selected network device is monitored.
Where to go next	Drill down on: Trace Route Now. For more information, see Trace Result view .

Monitoring Details from All Locations

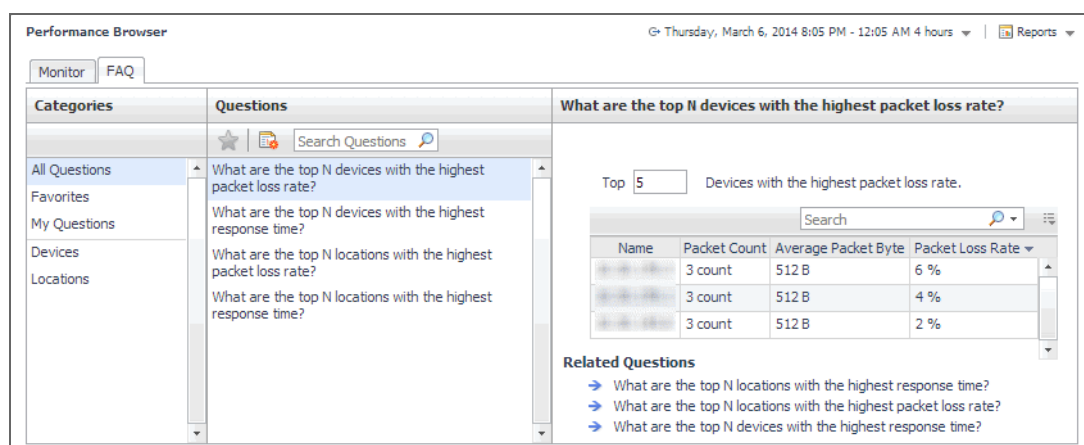
Table 7. Monitoring Details from All Locations view

Description	Shows how well the selected network device is responding to the data collection requests from all of the monitoring locations.
Data displayed	<ul style="list-style-type: none">• Outage. A color-coded bar, representing the availability of the monitored network device over the selected time range. The color of the bar reflects the percentage of time the device is unresponsive.• Packet Loss. The percentage of time the data packets sent to the monitored device are not echoed back, over the selected time range. By default, the monitoring agent sends five data packets to the monitored network device. The number of data packets the Net Monitor Agent sends to monitored devices is specified in the Net Monitor Agent properties.• Response Time. The round-trip response time between the monitoring agent and the network device, over the selected time range.

FAQ tab

Purpose

The **FAQ** tab shows answers to common questions related to your network devices or monitoring locations.



How to get here

Navigate to the Performance Browser, and open the **FAQs** tab.

Description of embedded views

This view is made up of the following embedded views:

- [Answer](#)
- [Categories](#)
- [Questions](#)

Answer

This view provides an answer to the question selected in the [Questions](#) view. The answer appears in the following form:

Top x <objects of category>...

Where x is the number of objects of the category you provided in the [Categories](#) view.

Specify x by entering a number.

Categories

This view lists the categories for which questions can be answered for you by Foglight.

Click a category in the list to select it.

Questions

This view lists the questions, for the category selected in the [Categories](#), that can be answered for you by Foglight.

Click a question in the list to select it.

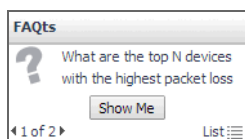
If the list of questions is long and you want to narrow it down, search for a particular text string using the **Search Questions** box.

FAQs view

Purpose

The **FAQs** view shows answers to common questions related to your transactions or locations. The collection of available questions depends on the tile selected in the [Net Monitor Environment view](#). If you select the **Network**

Devices tile, this view displays the questions related to the monitored network devices. Selecting the **Monitor Locations** tile causes the view to display the questions related to your monitoring locations.



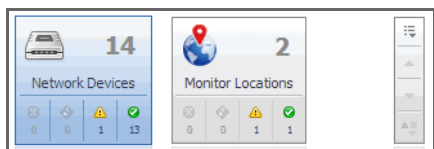
How to get here

In the Performance Browser, in the [Quick View](#), the **FAQs** view appears in the bottom-left corner.


Net Monitor Environment view

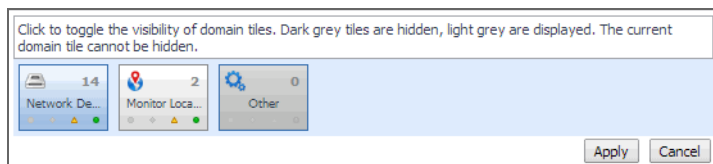
Purpose

The Net Monitor Environment view displays a high-level overview of your monitored environment. The view has two tiles, each representing the monitored objects of interest: **Network Devices** and **Monitor Locations**.



Each tile shows how many of the corresponding object instances there are in your monitored infrastructure, as well as the count of objects of that type in each of the alarm states Normal (green check), Warning (yellow triangle), Critical (orange diamond), or Fatal (red X). For example, the following image shows 14 network devices: none in the Fatal or Critical states, one in Warning, and 13 in the Normal state.

You can move the tiles by dragging and dropping until you achieve the desired layout. To hide one or more tiles, on the tool bar on the right, click , and in the popup that appears, click a tile that you want to hide.



Clicking the object type icon, the object type name, or the object count, shows summary information for that object type in the [Quick View](#). Clicking an alarm state (for example, Warning) on a tile displays summary information in the [Quick View](#) for the objects of that type that are in the selected alarm state. If an alarm state has a count of zero, then you can not drill down on the alarm state.

How to get here

This view appears in the upper part of the Performance Browser, just above the [Quick View](#).

Description of embedded views

This view is made up of the following embedded views:

- [Monitor Locations](#)
- [Network Devices](#)

Monitor Locations

Table 8. Monitor Locations view

Description	Shows the number of locations in your environment from which websites are monitored, and total alarm counts associated with those locations.
Data displayed	<ul style="list-style-type: none">• Alarm counts. The total counts of alarms generated against the existing monitoring locations, broken down by alarm types (Normal, Warning, Critical, Fatal).• Location count. The number of locations in your environment.
Where to go next	<p>Drill down on:</p> <ul style="list-style-type: none">• Alarm counts. Lists the locations associated with the alarms in the Monitor Locations view, appearing in the Quick View.• Location count. Displays a combination of location views in the Quick View.

Network Devices

Table 9. Network Devices view

Description	Shows the number of monitored network devices in your environment and total alarm counts associated with them.
Data displayed	<ul style="list-style-type: none">• Alarm counts. The total counts of alarms associated with the monitored network devices, broken down by alarm types (Normal, Warning, Critical, Fatal).• Device count. The number of monitored network devices in your environment.
Where to go next	<p>Drill down on:</p> <ul style="list-style-type: none">• Alarm counts. Lists the network devices associated with the alarms in the Network Devices view, appearing in the Quick View.• Device count. Displays a combination of device views in the Quick View.

Network Devices view

The **Network Devices** view lists the monitored network devices and shows their alarm states.

If a device name override is specified, this name appears in the list. If a device belongs to a private network, the private network ID is appended to the device.

Selecting **All Network Devices** shows the overall response and availability information for the monitored devices in the [Summary - All Devices view](#) on the right. Similarly, selecting a device in the list shows device-specific metrics in the [Summary - Single Device Summary view](#) on the right.

How to get here

- In the Performance Browser, in the [Net Monitor Environment view](#), select the **Network Devices** tile.
The [Network Devices view](#) appears in the [Quick View](#) on the left.

Description of the view

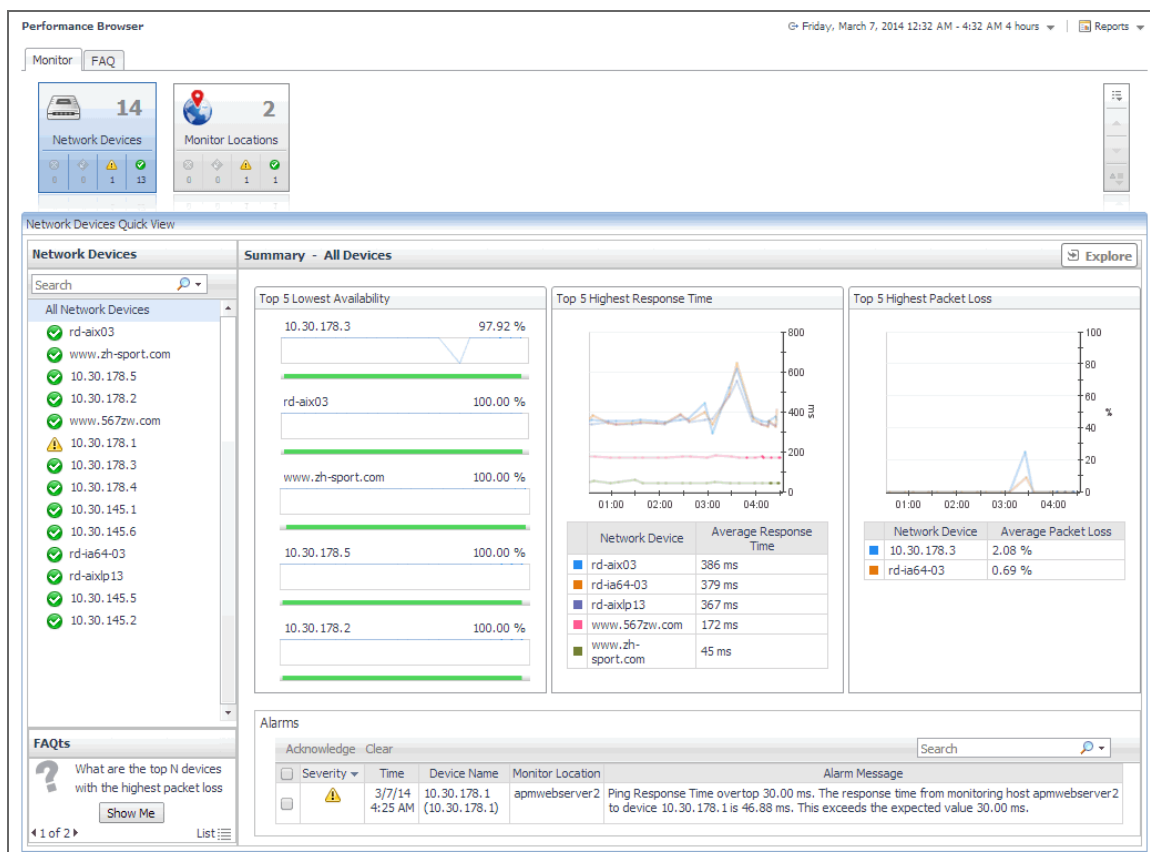
Table 10. Network Devices view

Data displayed	<ul style="list-style-type: none">• Alarm severity. The state of the most recent alarm raised against the associated network device: Warning ⚠, Critical ⚡, or Fatal ☠.• All Network Devices. A parent node for the network device object instances that appear in this view.• Network Device. The network device name.
	Drill down on:
Where to go next	<ul style="list-style-type: none">• All Network Devices. Shows the Summary - All Devices view in the Quick View.• Network Device. Shows the Summary - Single Device Summary view in the Quick View.

Monitor tab

Purpose

The **Monitor** tab is a container view. This tab displays a combination of location- or device-related information, depending on your selection in the [Net Monitor Environment view](#) and the [Quick View](#). Use it to gain an understanding of how well your monitored network devices are performing, and to investigate any potential issues.



How to get here

- Navigate to the Performance Browser.
The **Monitor** tab appears open.

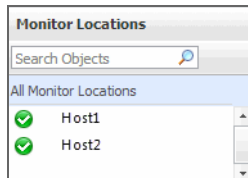
Embedded views

This view is made up of the following views:

- [Net Monitor Environment view](#)
- [Quick View](#)

Monitor Locations view

The **Monitor Locations** view lists the hosts that are running instances of the Net Monitor Agent, and shows their states.



Selecting **All Monitor Locations** shows a list of all host names in the [Summary - All Monitor Locations view](#) on the right. Similarly, selecting a location in the list shows location-specific metrics in the [Single Location Summary view](#) on the right.

How to get here

- In the Performance Browser, in the [Net Monitor Environment view](#), select the Monitor **Locations** tile.
The [Monitor Locations view](#) appears in the [Quick View](#) on the left.

Description of the View

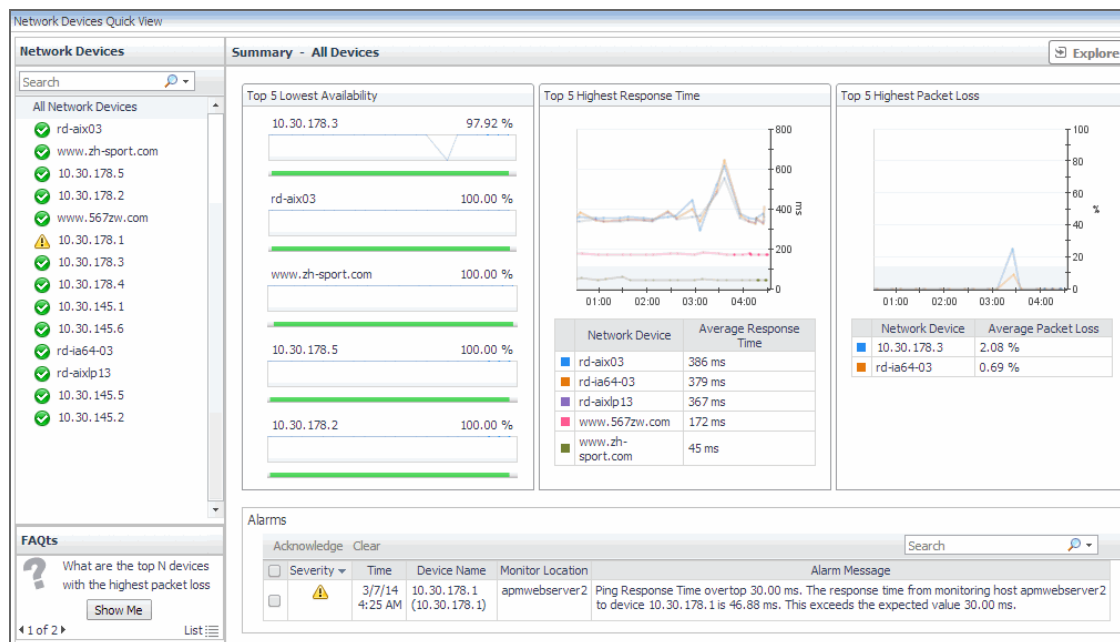
Table 11. Monitor Locations view

Data displayed	<ul style="list-style-type: none">• Alarm severity. The state of the most recent alarm raised against the associated location: Warning ⚠, Critical 🔥, or Fatal ☠.
	<ul style="list-style-type: none">• All Monitor Locations. A parent node for the location object instances that appear in this view.
	<ul style="list-style-type: none">• Location. The name of the host on which the Net Monitor Agent is running.
Drill down on:	
Where to go next	<ul style="list-style-type: none">• All Monitor Locations. Shows the Summary - All Monitor Locations view in the Quick View.
	<ul style="list-style-type: none">• Location. Shows the Single Location Summary view in the Quick View.

Quick View

Purpose

The **Quick View** is a container view. It contains a combination of location or transaction views, depending on your selection in the [Net Monitor Environment view](#) and the panel on the left. Use it to understand the performance of the monitored network devices, and to investigate any issues that they may be experiencing.



How to get here

This view appears in the Performance Browser, just below the [Net Monitor Environment view](#).

Embedded views

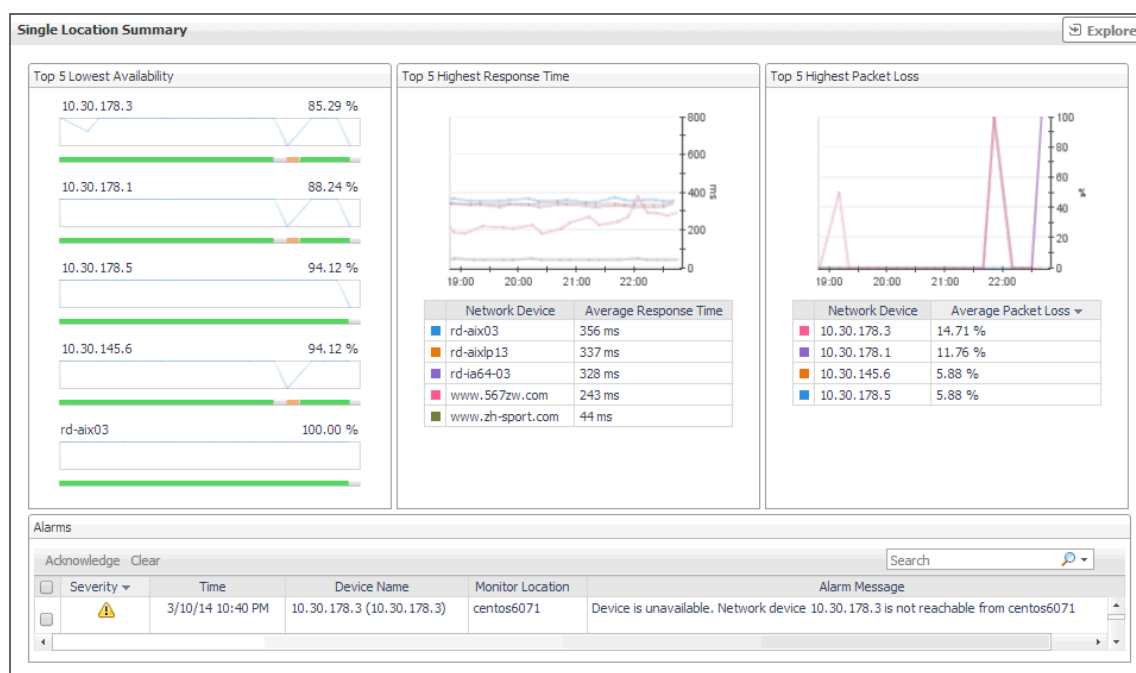
This view contains a combination of some of the following views, depending on your previous selections:

- [Alarms view](#)
- [FAQts view](#)
- [Monitor Locations view](#)
- [Network Devices view](#)
- [Single Location Summary view](#)
- [Summary - All Devices view](#)
- [Summary - All Monitor Locations view](#)
- [Summary - Single Device Summary view](#)

Single Location Summary view

Purpose

The **Single Location Summary** view displays overall response and availability information for the network devices monitored from the selected location. It identifies the network devices with the lowest availability, highest response time, and highest data packet loss, showing the top five transactions in each of these categories. Use this view to identify the network devices with performance disruptions, and to investigate them further.



How to get here

- 1 Navigate to the Performance Browser.
- 2 On the [Monitor tab](#), in the [Net Monitor Environment view](#), select the **Monitor Locations** tile.
- 3 In the [Quick View](#), in the [Monitor Locations view](#), select a monitoring location.

The **Single Location Summary** view appears on the right.

Description of embedded views

This view is made up of the following embedded views:

- [Alarms](#)
- [Top 5 Highest Packet Loss](#)
- [Top 5 Highest Response Time](#)
- [Top 5 Lowest Availability](#)

Alarms

For more information, see [Alarms view](#).

Top 5 Highest Packet Loss

Table 12. Top 5 Highest Packet Loss view

Description	Identifies the top five network devices that are monitored from the selected location and have the highest data packet loss.
Data displayed	<ul style="list-style-type: none"> • Average Packet Loss. The average percentage of time that the data packets sent to the monitored device from the selected location are not echoed back. By default, the monitoring agent sends five data packets to the monitored network device. The number of data packets the Net Monitor Agent sends to monitored devices is specified in the Net Monitor Agent properties. • Network Device. The IP address of the monitored network device.

Top 5 Highest Response Time

Table 13. Top 5 Highest Response Time view

Description	Identifies the top five network devices with the highest response time that are monitored from the selected location.
Data displayed	<ul style="list-style-type: none">• Avg Response Time. The average round-trip response time between the selected monitoring location and the network device.• Network Device. The IP address of the monitored network device.

Top 5 Lowest Availability

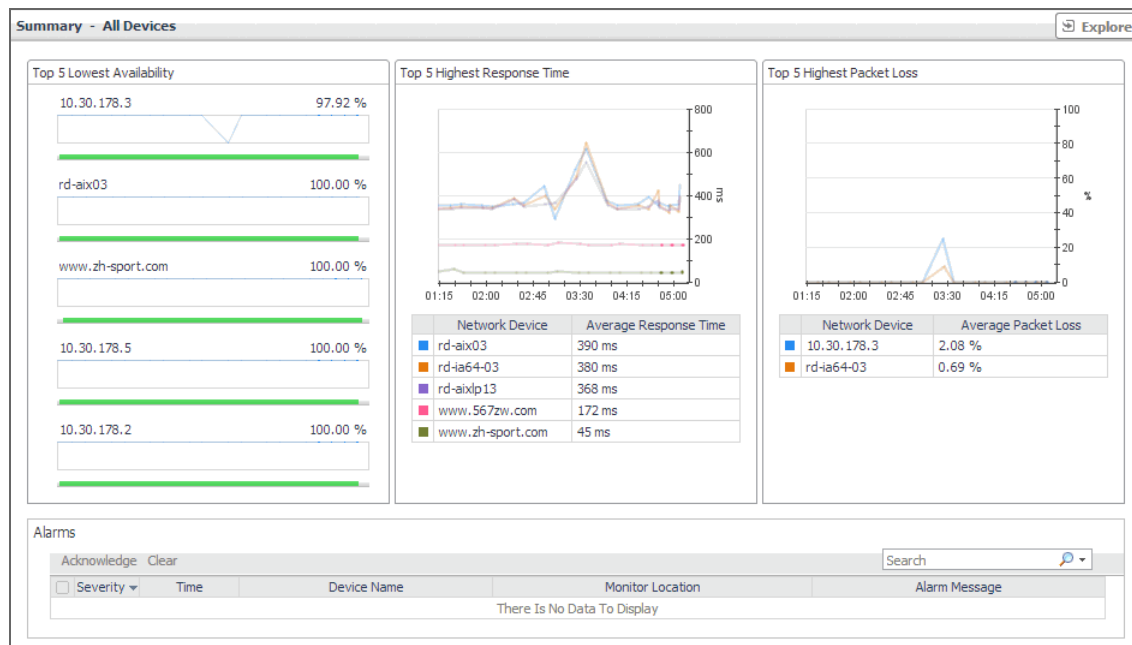
Table 14. Top 5 Lowest Availability view

Description	Identifies the top five network devices that are monitored from the selected location and have the lowest availability.
Data displayed	<ul style="list-style-type: none">• Availability. A sparkline and a color-coded bar, indicating the levels of availability of the network device over the selected time range.• Network Device. The IP address of the monitored network device, followed by the percentage of its average availability.

Summary - All Devices view

Purpose

The **Summary - All Devices** view displays overall response and availability information for all monitored network devices. It identifies the network devices with the lowest availability, highest response time, and highest data packet loss, showing the top five network devices in each of these categories. Use this view to identify the devices with performance degradation, and to investigate them further.



How to get here

- 1 Navigate to the Performance Browser.
- 2 On the **Monitor** tab, in the **Net Monitor Environment** view, select the **Network Devices** tile.

- 3 In the [Quick View](#), in the [Network Devices view](#), select **All Network Devices**.

The **Summary - All Devices** view appears on the right.

Description of embedded views

This view is made up of the following embedded views:

- [Alarms](#)
- [Top 5 Highest Packet Loss](#)
- [Top 5 Highest Response Time](#)
- [Top 5 Lowest Availability](#)

Alarms

For more information, see [Alarms view](#).

Top 5 Highest Packet Loss

Table 15. Top 5 Highest Packet Loss view

Description	Identifies the top five network devices with the highest data packet loss.
Data displayed	<ul style="list-style-type: none">• Average Packet Loss. The average percentage of time that the data packets sent to the monitored device are not echoed back. By default, the monitoring agent sends five data packets to the monitored network device. The number of data packets the Net Monitor Agent sends to monitored devices is specified in the Net Monitor Agent properties.• Network Device. The IP address of the monitored network device.

Top 5 Highest Response Time

Table 16. Top 5 Highest Response Time view

Description	Identifies the top five network devices with the highest response time.
Data displayed	<ul style="list-style-type: none">• Avg Response Time. The average round-trip response time between the network device and its monitoring locations.• Network Device. The IP address of the monitored network device.

Top 5 Lowest Availability

Table 17. Top 5 Lowest Availability view

Description	Identifies the top five network devices with the lowest availability.
Data displayed	<ul style="list-style-type: none">• Availability. A sparkline and a color-coded bar, indicating the levels of availability of the network device over the selected time range.• Network Device. The IP address of the monitored network device, followed by the percentage of its average availability.

Summary - All Monitor Locations view

Purpose

The **Summary - All Monitor Locations** view displays a list of existing monitoring locations, identifies the periods of time that each device was unavailable, and shows the counts of alarms generated for each location, if applicable.

Summary - All Monitor Locations

Explore

Location	Outage	Device Alarms
Host1	0	<div><div>0</div><div>0</div><div>0</div></div>
Host2	<div>1</div> <div>(0h : 9m : 22s)</div>	<div><div>0</div><div>0</div><div>0</div></div>

How to get here

- 1

Navigate to the Performance Browser.
- 2

On the [Monitor](#) tab, in the [Net Monitor Environment](#) view, select the **Monitor Locations** tile.
- 3





In the [Quick View](#), in the [Monitor Locations](#) view, select **All Monitor Locations**.

The **Summary - All Monitor Locations** view appears on the right.

Description of the view

Table 18. Summary - All Monitor Locations view

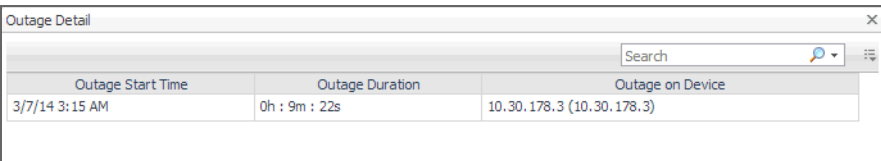
Data displayed

- **Location.** The name of the host from which network devices are monitored.
- **Outage.** The number of times any network devices was unresponsive to data collection requests, followed by the total outage duration.
- **Device Alarms.** The counts of alarms generated against the monitoring device in each alarm state: Normal , Warning , Critical , or Fatal .

Drill down on:

- **Outage.** Displays the **Outage Detail** dialog box.

Where to go next



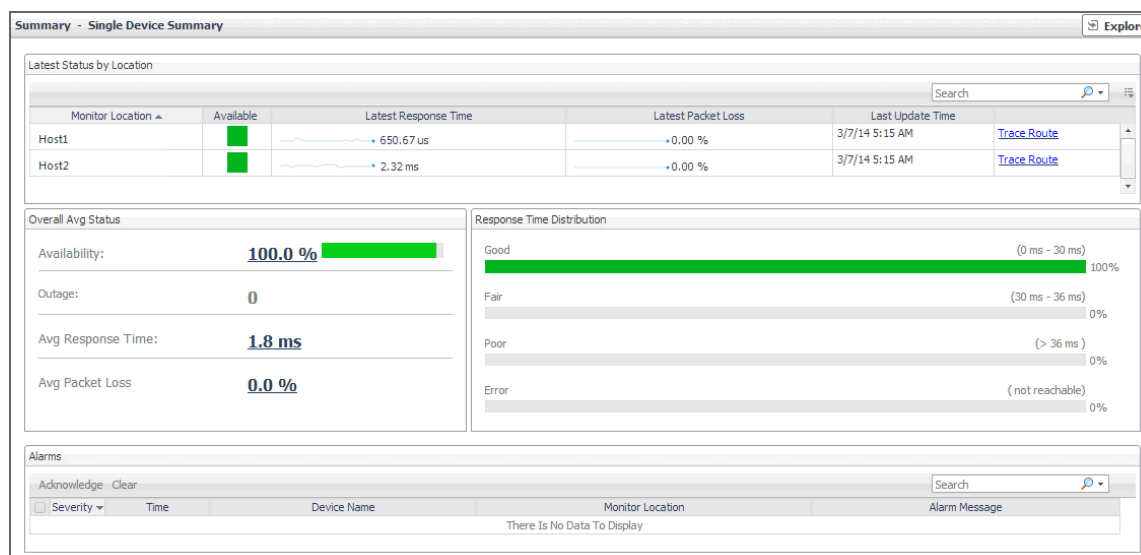
The screenshot shows a dialog box titled "Outage Detail" with a search bar and a table. The table has three columns: "Outage Start Time", "Outage Duration", and "Outage on Device". The first row of data shows the start time as "3/7/14 3:15 AM", the duration as "0h : 9m : 22s", and the device as "10.30.178.3 (10.30.178.3)".

Outage Start Time	Outage Duration	Outage on Device
3/7/14 3:15 AM	0h : 9m : 22s	10.30.178.3 (10.30.178.3)

Summary - Single Device Summary view

Purpose

The **Summary - Single Device Summary** view provides an overview of the selected network device. Use it to find out the latest data collection statistics from each monitoring location, and to review its overall health.



How to get here

1. Navigate to the Performance Browser.
2. On the **Monitor** tab, in the **Net Monitor Environment** view, select the **Network Devices** tile.
3. In the **Quick View**, in the **Network Devices** view, select a network device.

The **Summary - Single Device Summary** view appears on the right.

Description of embedded views

This view is made up of the following embedded views:

- [Alarms](#)
- [Latest Status by Locations](#)
- [Overall Avg Status](#)
- [Response Time Distribution](#)

Alarms

For more information, see [Alarms](#) view.

Latest Status by Locations

Table 19. Latest Status by Location view

Description	Lists the hosts from which the selected network device is monitored.
Data displayed	<ul style="list-style-type: none">• Available. A color-coded bar, representing the availability of the device over the selected time range. The color of the bar changes depending on the alarm state. Red indicates a Fatal state, orange indicates Critical, yellow means Warning, and green is the Normal state.• Latest Packet Loss. The percentage of data packets sent to the monitored device that are not echoed back in the most recent collection period. By default, the monitoring agent sends five data packets to the monitored network device. The number of data packets the Net Monitor Agent sends to monitored devices is specified in the Net Monitor Agent properties.• Latest Response Time. The round-trip response time between the monitoring agent and the network device in the most recent collection period.• Monitoring Location. The name of the host from which the selected network device is monitored.
Where to go next	Drill down on: <ul style="list-style-type: none">• Trace Route Now. For more information, see Trace Result view.

Overall Avg Status

Table 20. Overall Avg Status view

Description	Shows how well the selected network device is responding to the data collection requests from all of its monitoring locations.
Data displayed	<ul style="list-style-type: none">• Availability. The percentage of time the selected network device was available for monitoring, followed by a color-coded bar, representing the availability of the device over the selected time range. The color of the bar changes depending on the device availability. Orange indicates a device outage, green means a normal state, white means that no monitoring occurred.• Avg Packet Loss. The percentage of time that the data packets sent to the monitored device are not echoed back, over the selected time range. By default, the monitoring agent sends three data packets to the monitored network device. The number of data packets the Net Monitor Agent sends to monitored devices is specified in the Net Monitor Agent properties.• Avg Response Time. The round-trip response time between the monitoring agent and the network device, over the selected time range.• Outage. The number of times the selected network device was unresponsive to data collection requests, followed by the total outage duration.
Where to go next	Drill down on: Availability, Avg Packet Loss, or Outage. For more information, see Device Detail view .

Response Time Distribution

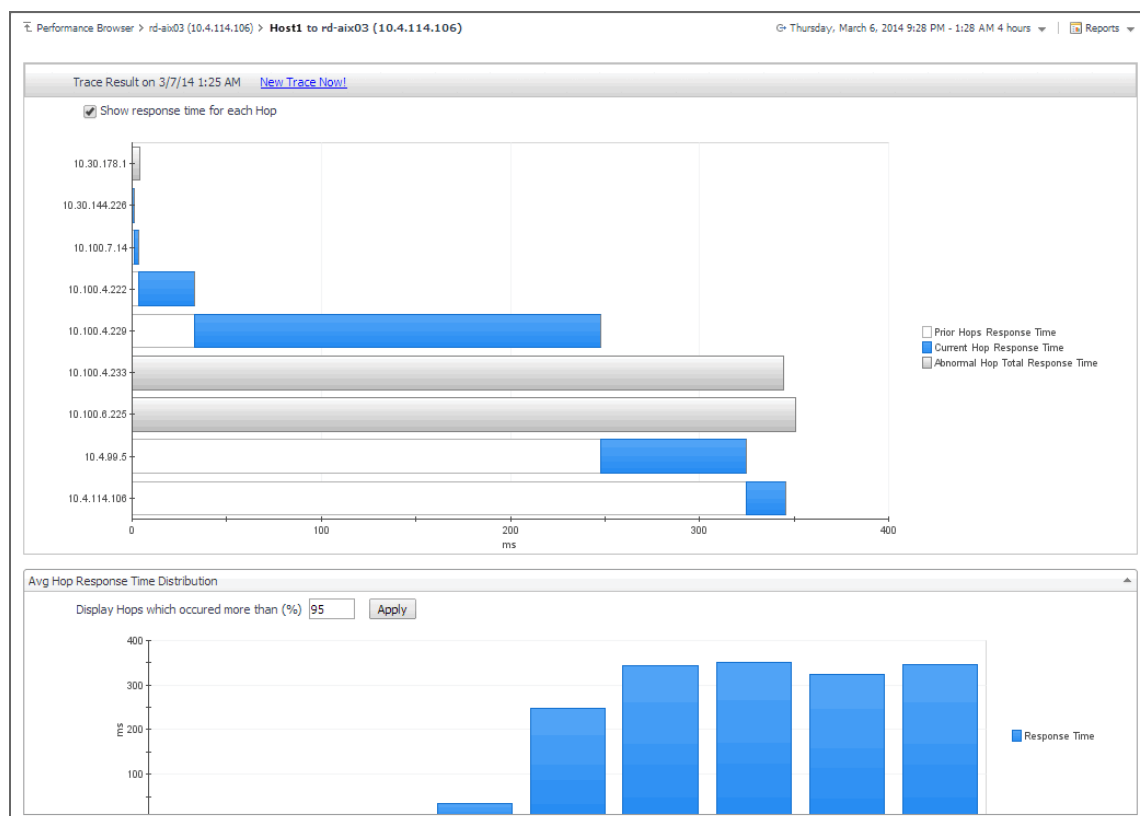
Table 21. Response Time Distribution view

Description	The distribution of the device response times in each of the available categories: Good , Fair , Poor , and Error .
Data displayed	<ul style="list-style-type: none">• Error: The percentage of times the network device was unresponsive.• Good: The percentage of times the network device takes between zero and the expected response time configured for the device.• Fair: The percentage of times the network device takes between the expected response time configured for the device and the expected response time, times the rate to respond to data collection requests.• Poor: The percentage of times the network device takes between higher than expected response time configured for the device, times the rate to respond to data collection requests.

Trace Result view

Purpose

The **Trace Result** view displays the length of the hops on a packet's route to its destination, and the distribution of average response times for each hop. Use this information to investigate a device with longer than expected response times and to identify the points in the route that may be the cause of the data packet delay.



How to get here

- 1 Navigate to the Performance Browser.
- 2 On the **Monitor** tab, in the **Net Monitor Environment** view, select the **Network Devices** tile.

- 3 In the [Quick View](#), in the [Network Devices view](#), select a network device.
- 4 In the [Summary - Single Device Summary view](#), in the embedded [Latest Status by Locations view](#), in the row containing a monitored location whose route to the selected network device you want to trace, click **Trace Route**.

The **Trace Result** view appears in the display area.

The trace route request runs in the background and takes several minutes to complete. Instead of waiting for it to complete, you can navigate to other dashboards, and then return to this page to review the trace route.

i | **IMPORTANT:** If the trace route option is disabled in the device settings (see [Viewing and editing individual network device details](#)), this page is not populated with data. You can quickly execute a trace route in real time on this page by clicking Trace Route Now.

Description of embedded views

This view is made up of the following embedded views:

- [Avg Hop Response Time Distribution](#)
- [Trace Result](#)

Avg Hop Response Time Distribution

Table 22. Avg Hop Response Time Distribution view

Description	Displays a chart showing the hop response times for the selected route. Each route consists of one or more hops. A hop is the route between one network device and the next on a packet's way to its destination. A hop destination is a device through which the packet passes on the route.
Data displayed	<ul style="list-style-type: none"> • Prior Hops Response Time. When Show response time for each Hop is selected, this area in the chart represents the length of time the data packets take to travel from the monitoring location to this device. • Current Hops Response Time. When Show response time for each Hop is selected, this area in the chart represents the length of time the data packets take to travel from the previous device to this device, on the way to its destination. • Abnormal Hops Response Time. When Show response time for each Hop is selected, this area in the chart represents the length of time the data packets take to travel from the monitoring location to this device, that result in an error. • Response Time. When Show response time for each Hop is cleared, this area in the chart represents the length of time the data packets take to travel from the monitoring location to this device, on the way to its destination.

Trace Result

Table 23. Trace Result view

Description	<p>The distribution of the device response times for each hop that occurred more than a selected percentage of times.</p> <p>NOTE: Use the Display Hops which occurred more than (%) box to specify a desired percentage.</p>
Data displayed	<ul style="list-style-type: none"> • Response Time. These areas in the chart represent the length of time the network device takes to send the data packet from the monitoring location to this device, on the way to its destination.

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 www.quest.com/contact.

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.