

Foglight Web Monitor 6.3.0

User and Reference Guide



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

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 Web Monitor User and Reference Guide
Updated - 2023
Foglight Version - 6.3.0
Foglight Web Monitor Version - 6.3.0
Foglight Net Monitor Version - 6.3.0

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

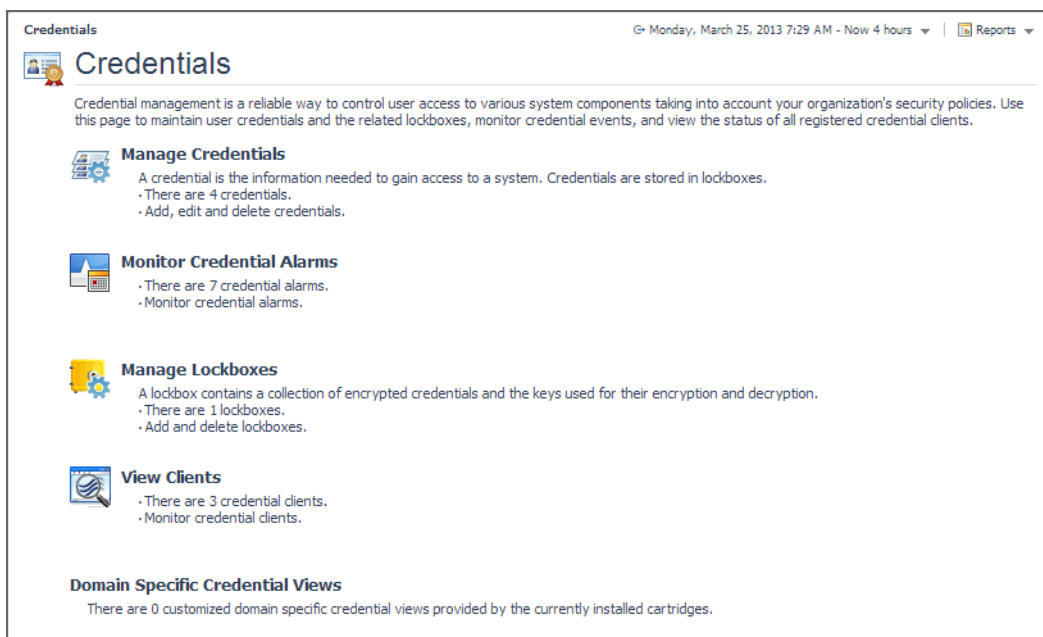
Monitoring Web sites that require user or proxy authentication requires some additional configuration. To successfully access these sites with the Web Monitoring Agent and collect response time metrics, you must provide the credentials these pages need to access them. A valid credential contains a user 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.

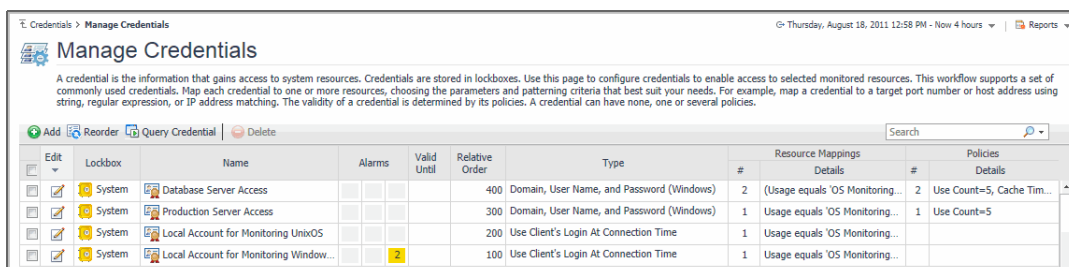
- Manage Credentials**
 - A credential is the information needed to gain access to a system. Credentials are stored in lockboxes.
 - There are 4 credentials.
 - Add, edit and delete credentials.
- Monitor Credential Alarms**
 - There are 7 credential alarms.
 - Monitor credential alarms.
- Manage Lockboxes**
 - 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:

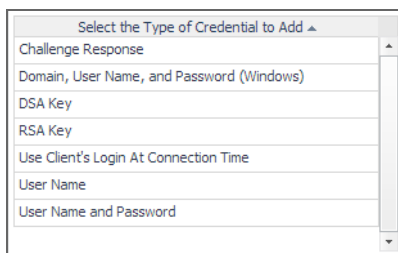
- Web site address
- User name
- Password

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.

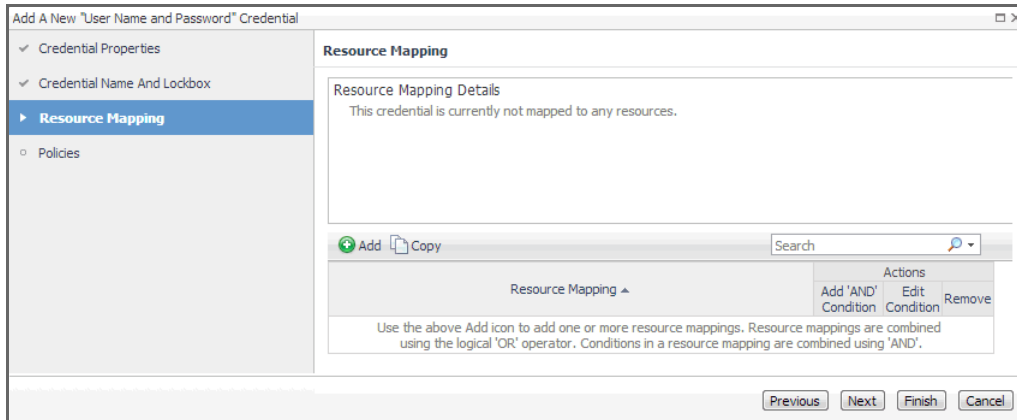
The **Credential Name and Lockbox** page appears.

- 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**.

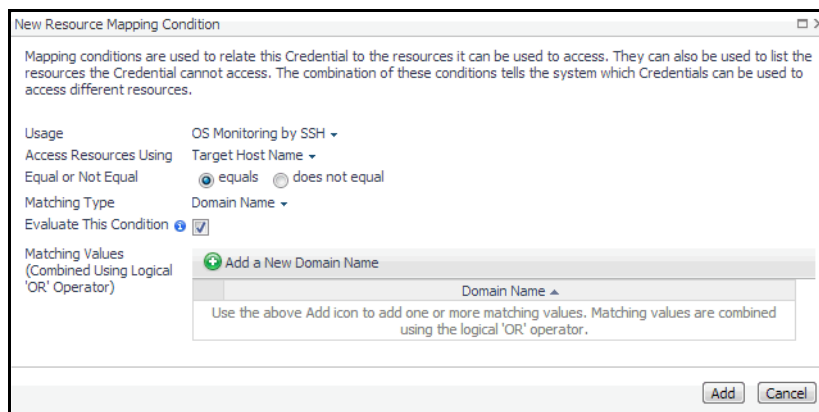
The **Resource Mapping** page appears.



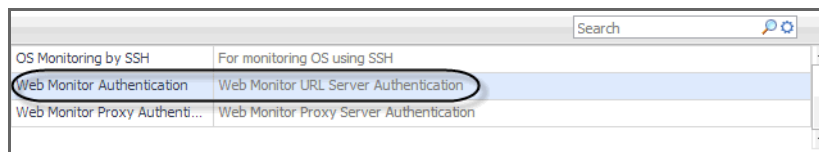
8 Provide the URL of the Web site that requires user authentication.

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.

Mapping conditions are used to relate this Credential to the resources it can be used to access. They can also be used to list the resources the Credential cannot access. The combination of these conditions tells the system which Credentials can be used to access different resources.

Usage: Web Monitor Authentication ▾
 Access Resources Using: Web Monitor URL ▾
 Equal or Not Equal: ☒ equals ☐ does not equal
 Matching Type: Exact Match (Case Sensitive) ▾
 Evaluate This Condition: ☒
 Matching Values (Combined Using Logical 'OR' Operator):
 Add a New String
 String ▾
 Use the above Add icon to add one or more matching values. Matching values are combined using the logical 'OR' operator.

Add Cancel

- 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.

Matching Values (Combined Using Logical 'OR' Operator):
 Add a New String
 String ▾

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.

Add A New "User Name and Password" Credential

✓ Credential Properties
 ✓ Credential Name And Lockbox
 ▶ Resource Mapping
 Policies

Resource Mapping

Resource Mapping Details
 Usage equals 'Web Monitor Authentication' AND Web Monitor URL equals 'www.example.com'

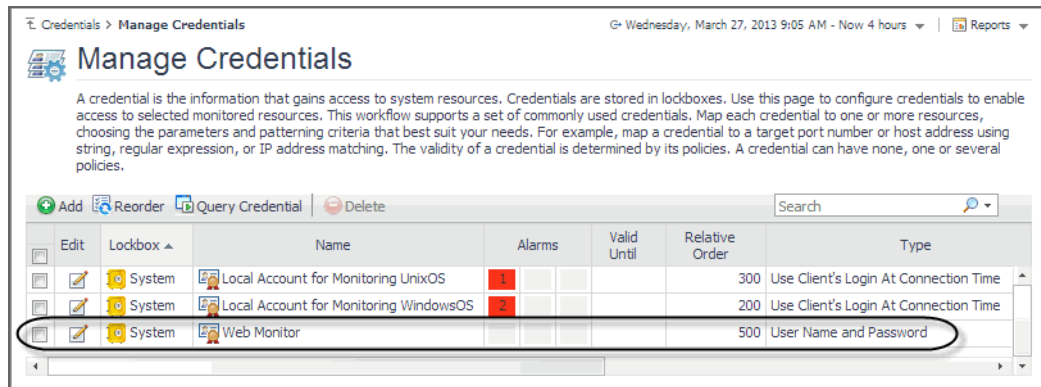
Add Copy Search

Resource Mapping ▾	Actions Add 'AND' Condition Edit Condition Remove
Usage equals 'Web Monitor Authentication' AND Web Monitor URL equals 'www.example.com'	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>

Previous Next Finish Cancel

- 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.

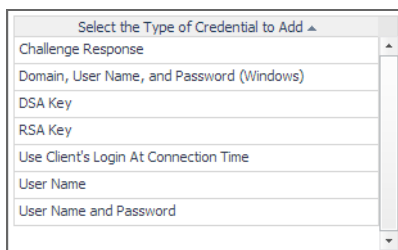
To get started, create a new credential of the *User Name and Password* type containing a resource mapping with the *Web Monitor Proxy Authentication* usage. Next, specify the host name or IP address of the proxy server and the port number, and save your changes.

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**.

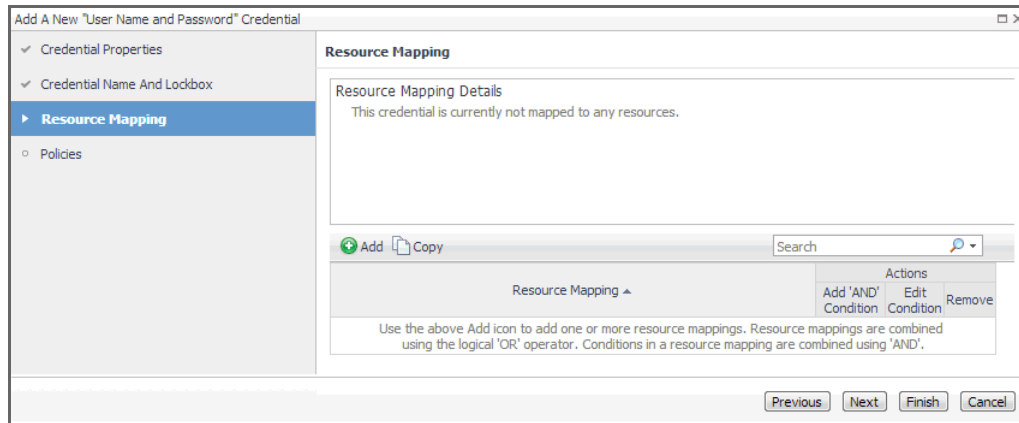
The **Credential Name and Lockbox** page appears.

- 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**.

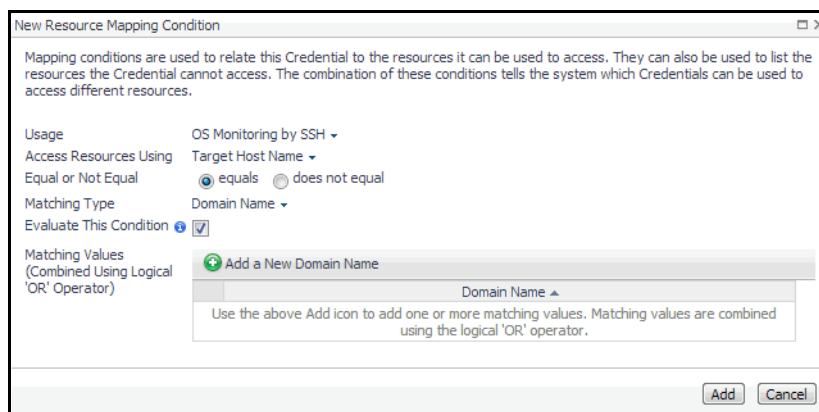
The **Resource Mapping** page appears.



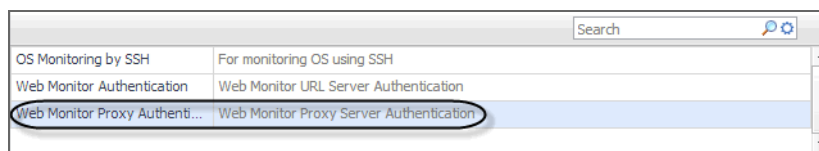
- 8 Specify the name or IP address of the proxy server that you want to use.

- 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.

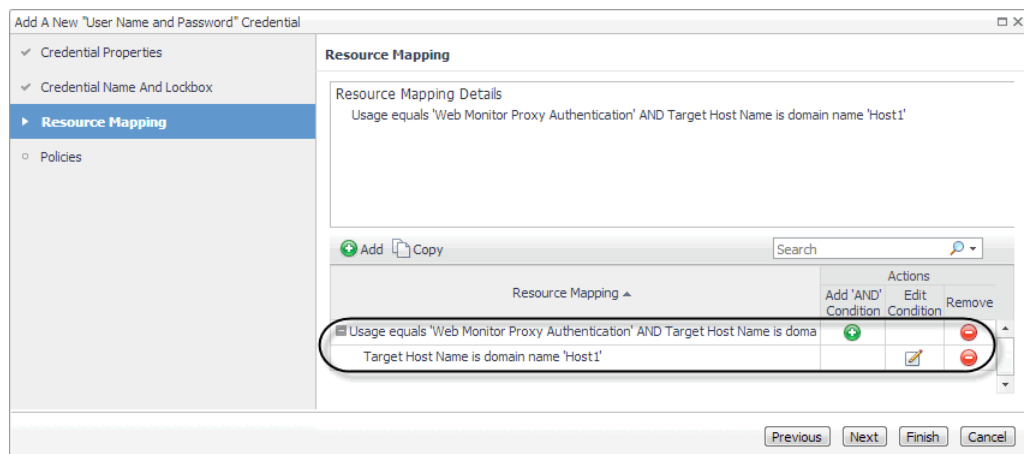
- e Indicate if you want to use a literal or regular expression to specify the host name or IP address. Using regular expressions in general gives you more flexibility in that you can specify multiple servers than using a single expression mapping.

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.

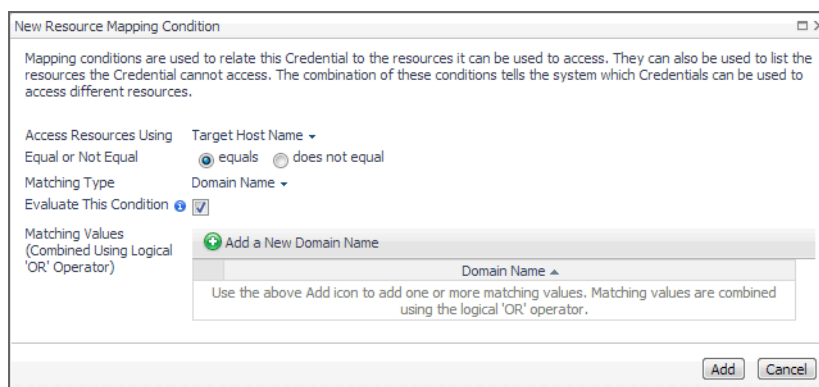
- g Click **Add**.
- h The **New Resource Mapping Condition** dialog box closes and the Resource Mapping page refreshes, showing the newly specified proxy server.



- 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.

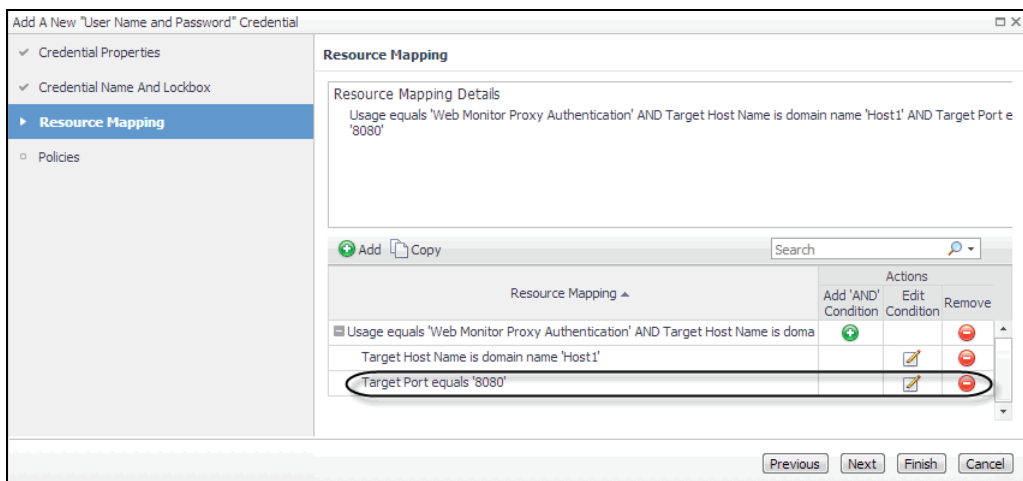
- c Ensure that **equals** and **Evaluate This Condition** are selected.
- d Indicate if you want to use a literal or regular expression to specify the port number. Using regular expressions in general gives you more flexibility in that you can specify multiple port numbers than using a single expression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

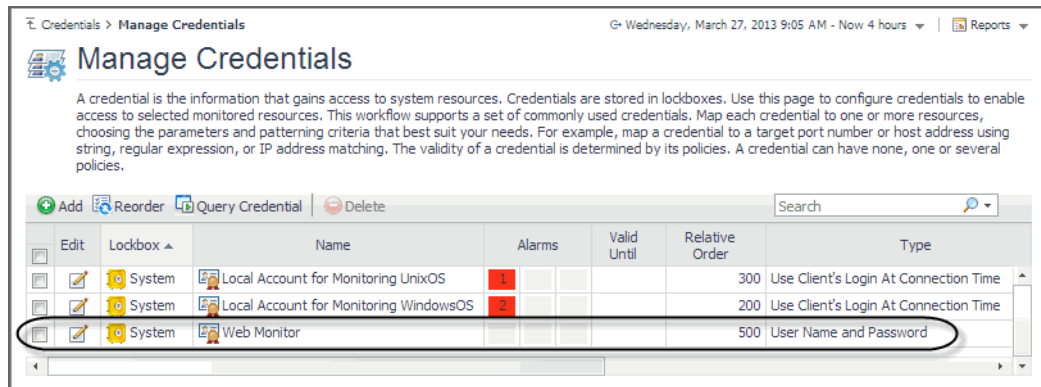
You can specify multiple servers, if required. During the evaluation, they are combined into an expression using the logical **OR** operator.

- 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.

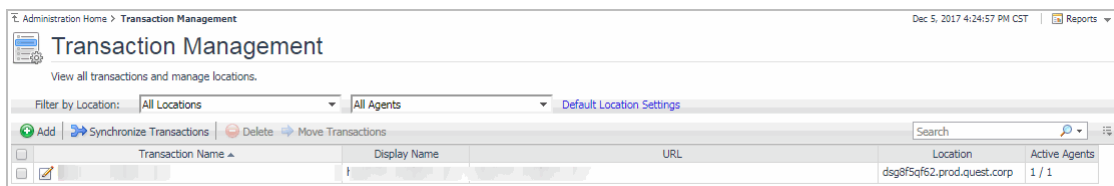
- **Workaround #2**

- 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

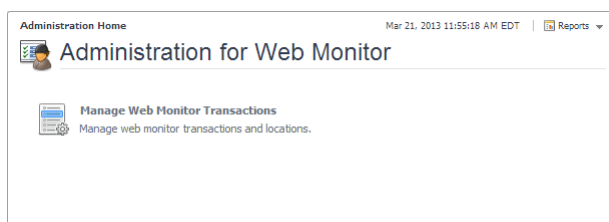


For complete details about the data appearing on this dashboard, see the [Transaction Management table](#).

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**.

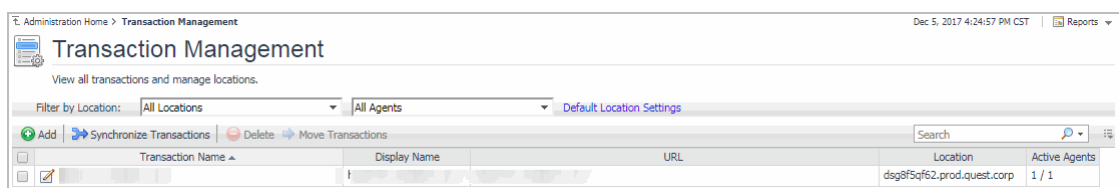
The Administration for Web Monitor page appears in the display area.



- 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
<input type="checkbox"/> dsg8f5qf62.prod.quest.corp	WebMonitorAgent@dsg8f5qf62.prod.quest.corp
<input type="checkbox"/> 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](#).

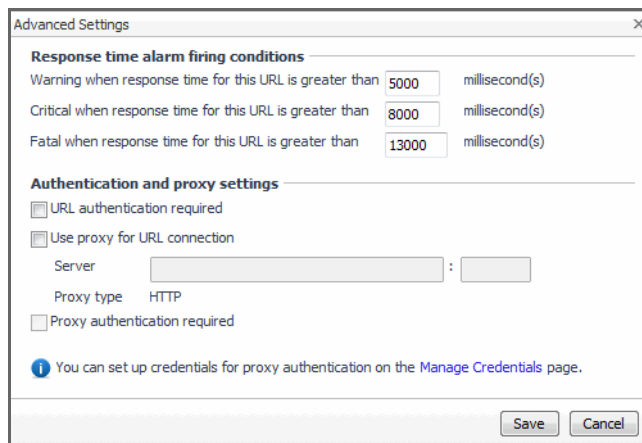
- 3 To add more URLs to the list, click **Add**, and populate the row that appears. To remove a row from the list, click .
- 4 In the **Deploy to Locations** area, select one or more Web Monitor Agent locations that you want to use to monitor the transactions with the newly specified Web sites.

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: 'Response time alarm firing conditions' and 'Authentication and proxy settings'. The first section has three rows for 'Warning', 'Critical', and 'Fatal' thresholds, each with a text input field and a unit dropdown set to 'millisecond(s)'. The values are 5000, 8000, and 13000 respectively. The second section has checkboxes for 'URL authentication required', 'Use proxy for URL connection', and 'Proxy authentication required'. Below the proxy checkbox is a 'Server' text field and 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.

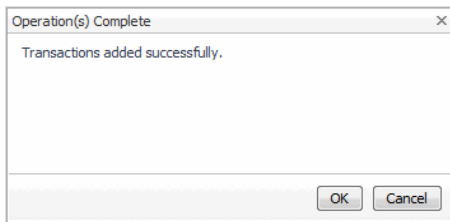
- **Use proxy for URL connection:** Select this check box only if the Web Monitor needs to use a proxy to access the specified URL. Click **Manage Credentials** to review the existing credentials, and create new ones, as required. For more information, see [Configuring credentials to access Web sites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

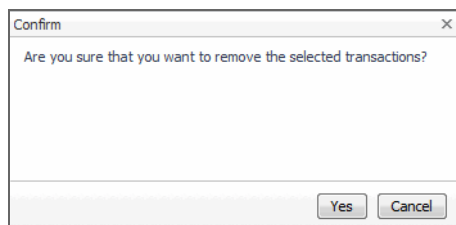
Removing Web sites from the existing collection

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:

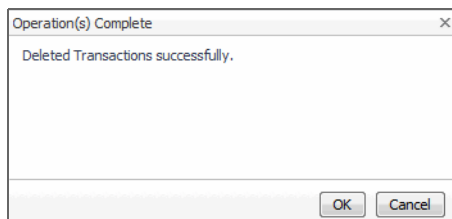
- 1 On the Transaction Management dashboard, select the Web site that you no longer want to monitor, and click **Delete**.

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.

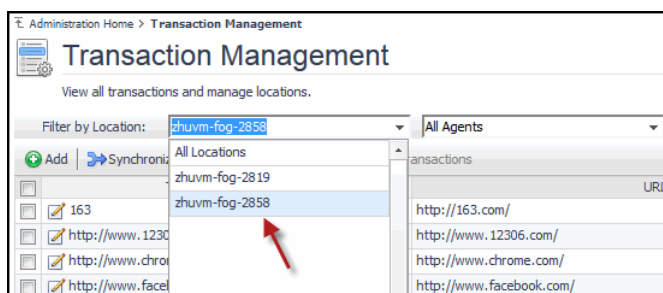
Moving multiple transactions as a group

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

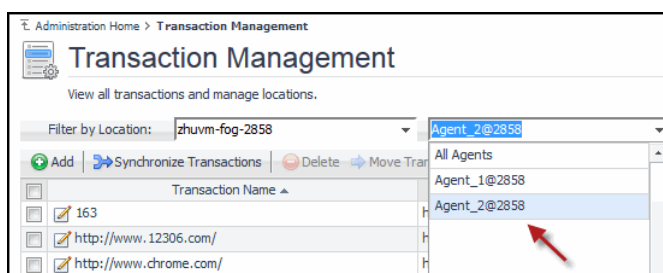
NOTE: You may not deploy the same transaction to multiple agents within the same location.

To move multiple transactions in a single operation:

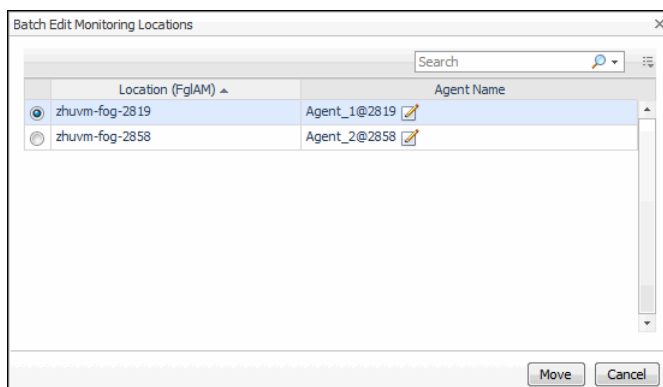
- 1 On the Transaction Management dashboard, filter the transactions by location.



- 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

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

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:

- 1 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

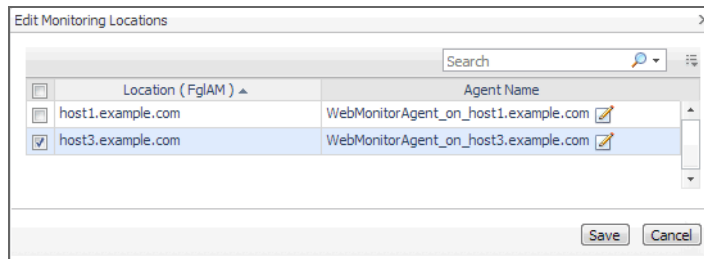
Transaction name: <http://www.baidu.com/>

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.

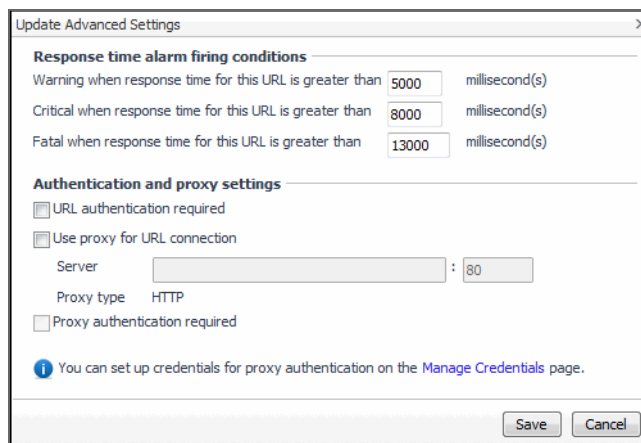
- To start monitoring this Web site with a new set of monitoring agents, in the **Monitoring Location** view, click **Edit**. The **Edit Monitoring Locations** dialog box appears.



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**.

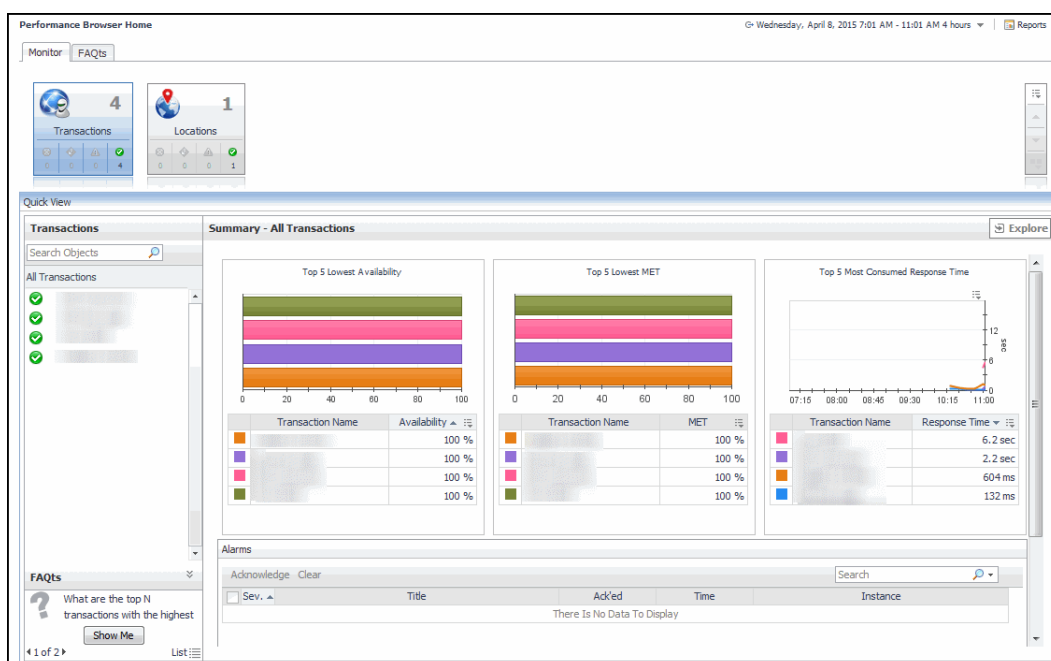
The dialog box closes.

- 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](#).

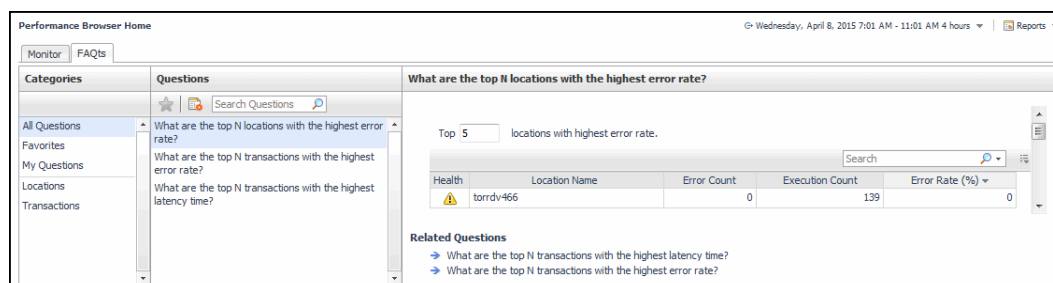
For more information, see the following topics:

- [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

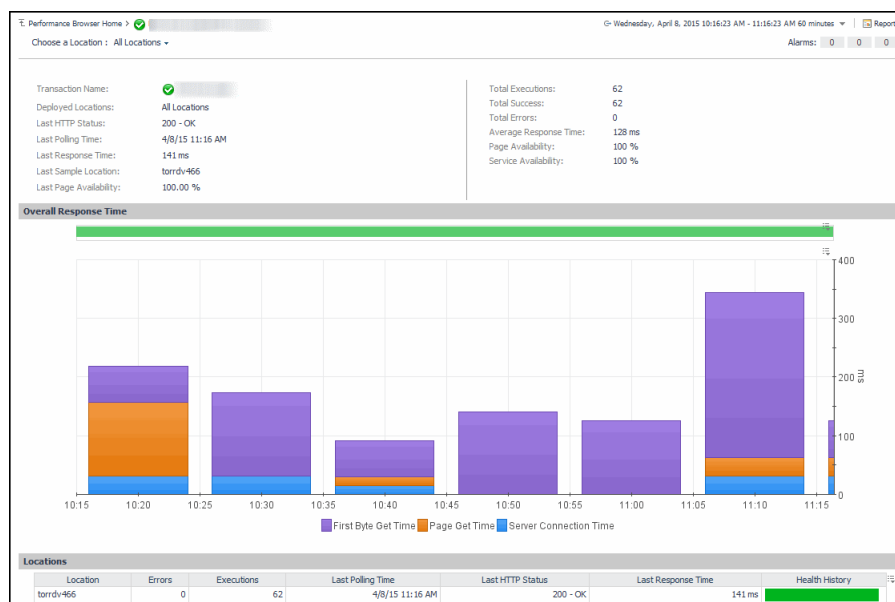


For complete information about the data appearing on this tab, see [FAQts tab](#).

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**.

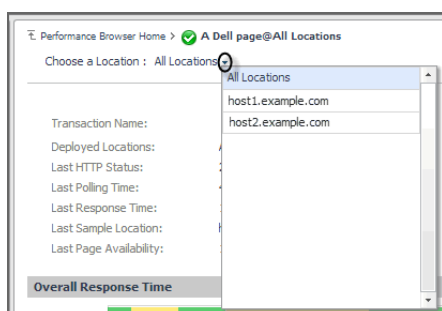
Figure 7. Transaction Additional Details



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](#).

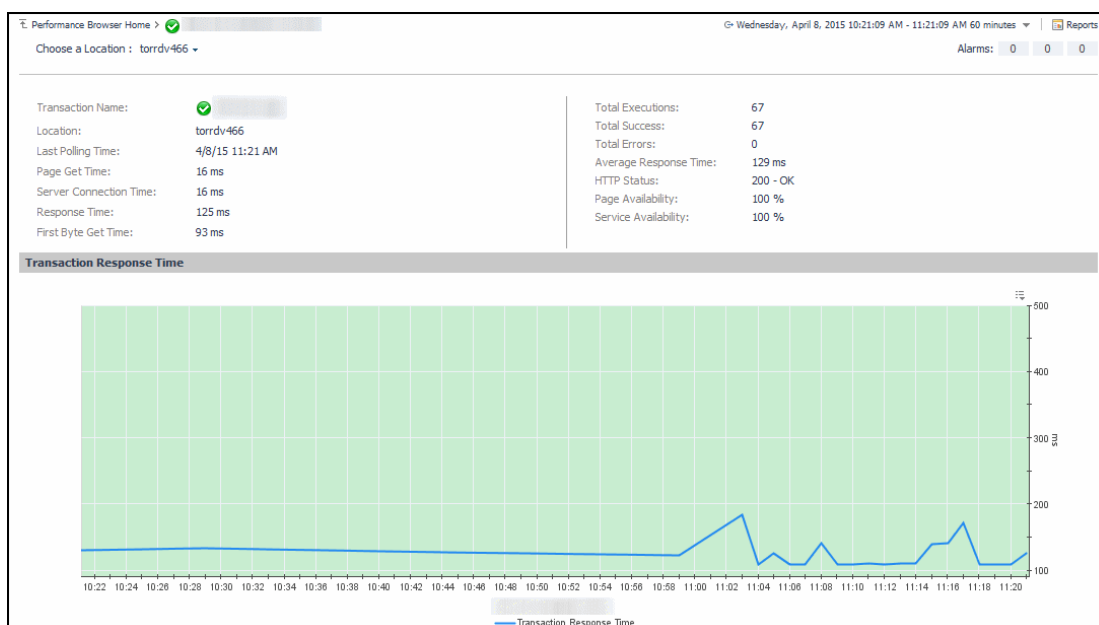
From here, you can drill down on a particular location and review its overall performance. To do that, click the down-facing arrow on the right of **Choose a Location**, and select a location from the list that appears.

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



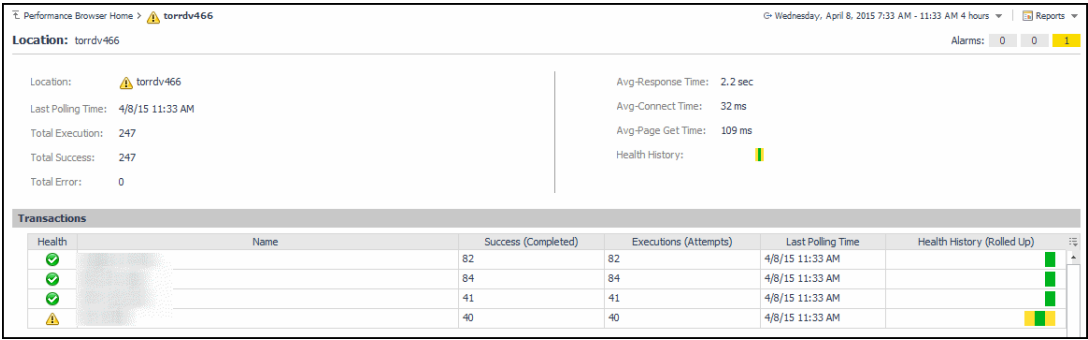
The top part of this view shows a number of metrics resulted from monitoring that transaction from the selected location. The bottom part of this view shows a graph indicating the total transaction response times over the selected time range. High peaks in the graph often suggest potential bottlenecks 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](#).

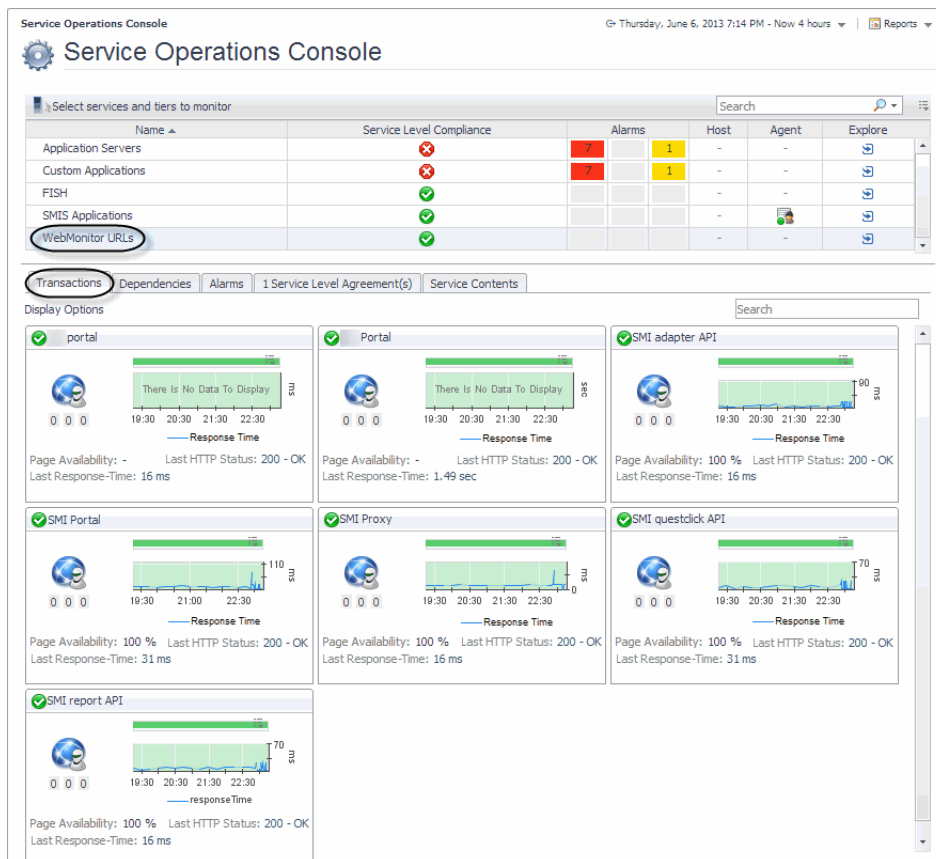
Exploring Web Monitor services

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*.

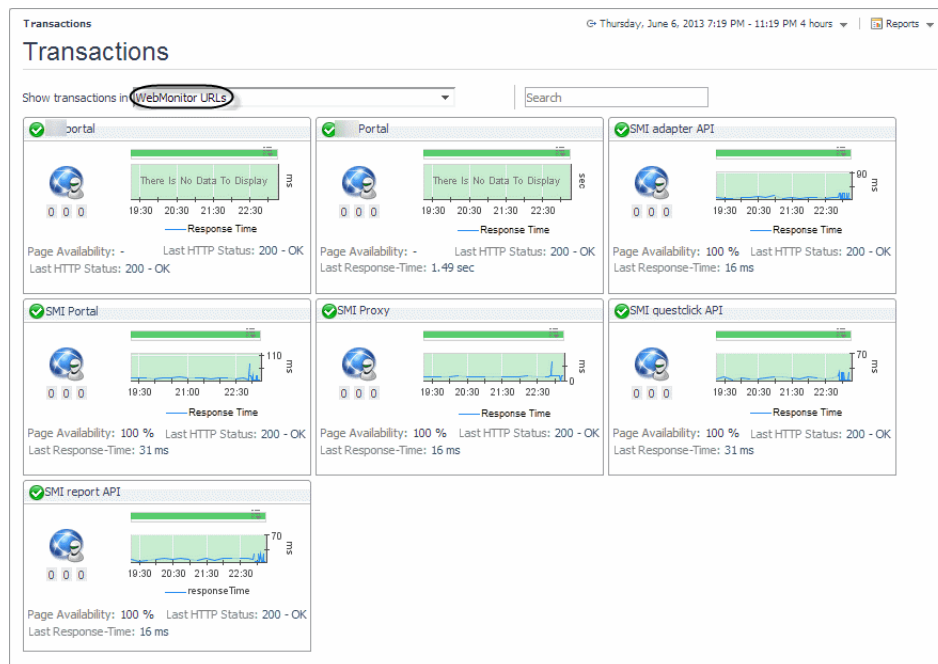
Start by navigating to the Service Operations Console dashboard and select a Web Monitor service. The Web Monitor tiles appear on the **Transactions** tab. The information displayed on these tiles helps you visualize how your Web transactions are performing, and to predict potential bottlenecks.

Figure 11. Service Operations Console



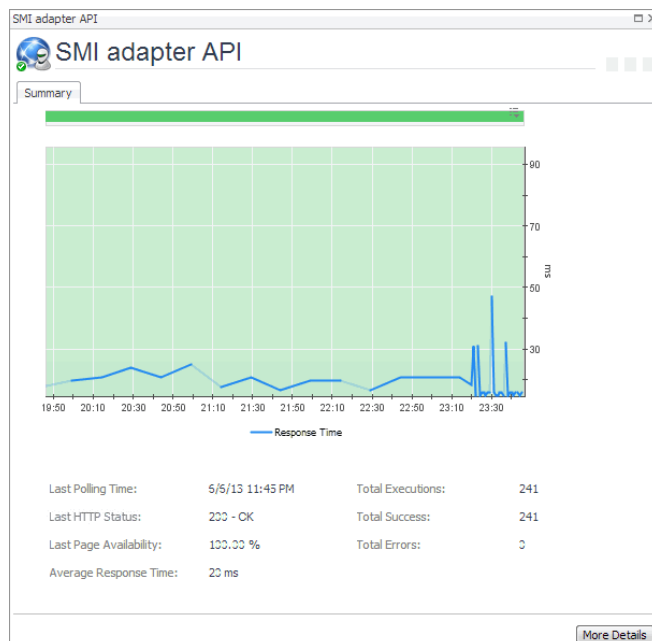
Another way to navigate to these tiles is using the Transactions dashboard included with Foglight for APM. When you select a Web Monitor service on this dashboard, the Web Monitor tiles are displayed.

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.

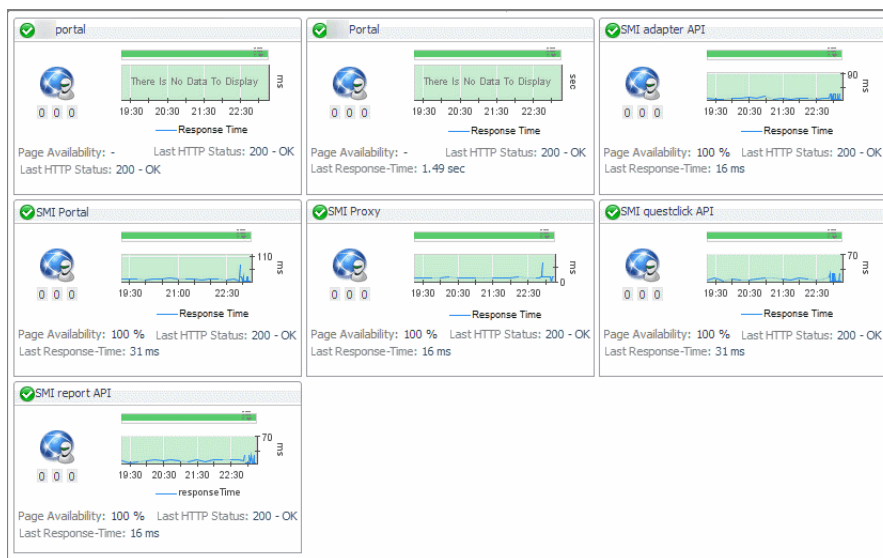
or

- 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.

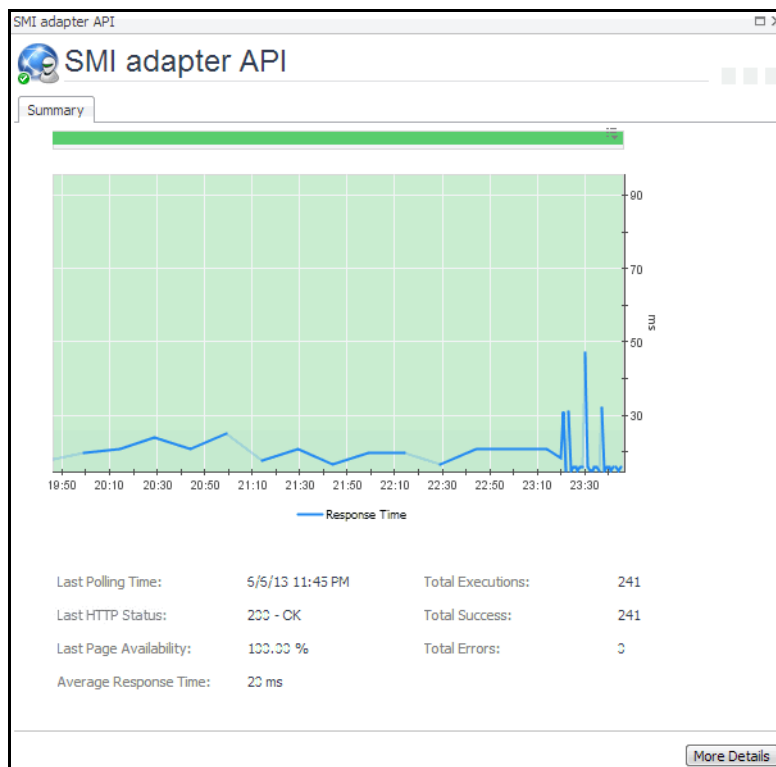
Figure 14. Transaction Tiles



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

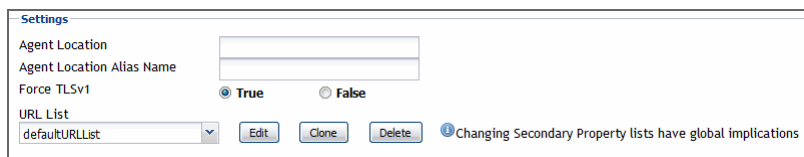
CAUTION: With the exception of “Force TLSv1” and “Data Collection Scheduler” agent properties, you must NOT change any properties through the Agent Status dashboard, unless instructed by Quest Customer Support. You should always go to Web Monitor > Administration Home > Transaction Management dashboard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

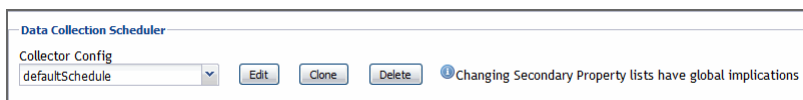
- **URL:** The URL of the monitored Web site.
- **Alias Name:** The name you want to associate with the transactions with this Web site.
- **Display Name:** The display name of the transaction.
- **Connection Time Out:** The maximum amount of time in milliseconds the agent instance can wait for establishing 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

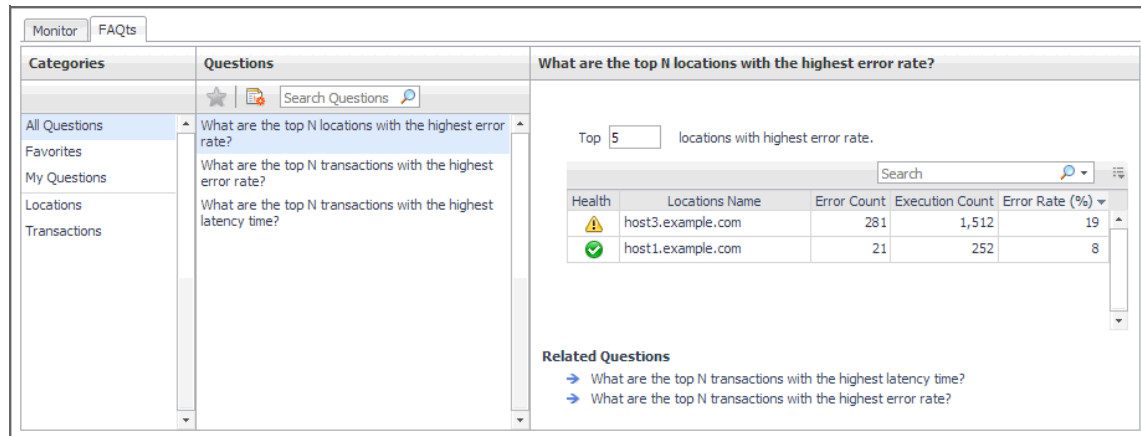
The Performance Browser contains the following views:

- [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.

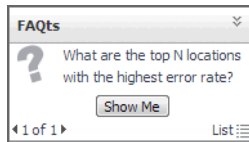
Click a question in the list to select it.

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.



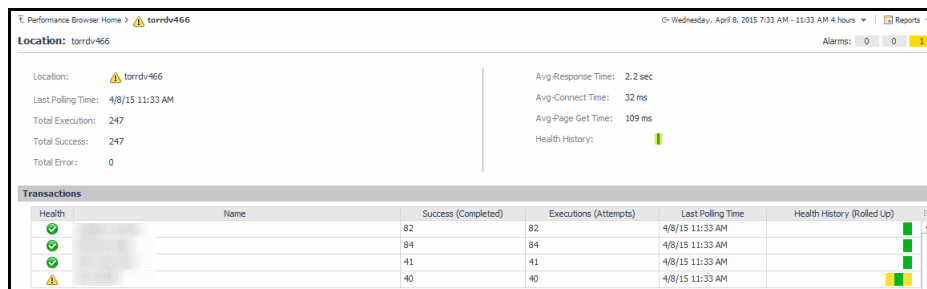
How to get here

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

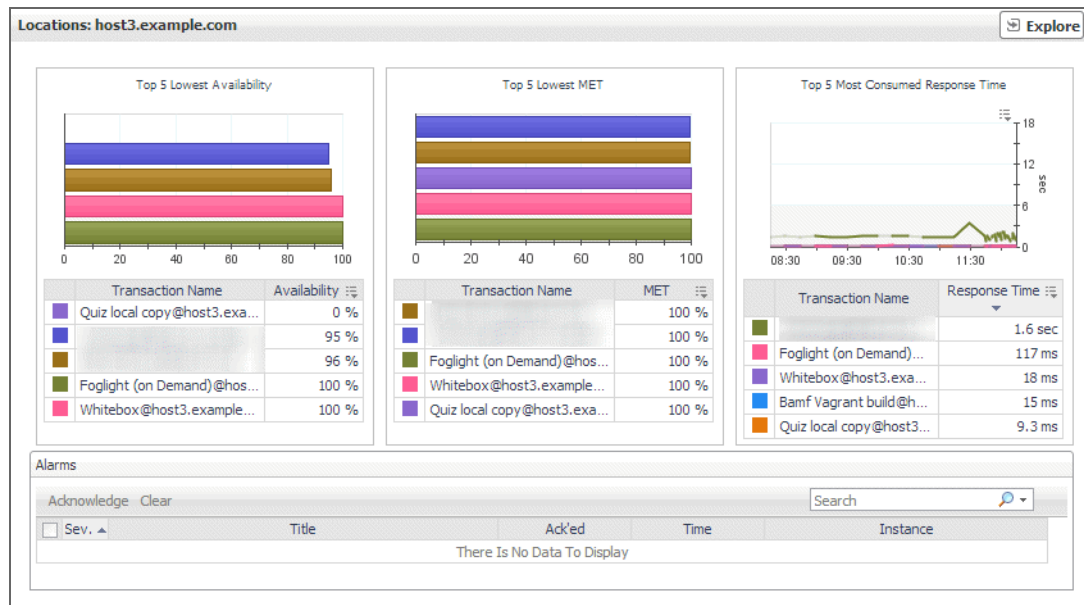
Table 4. Transactions view

	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

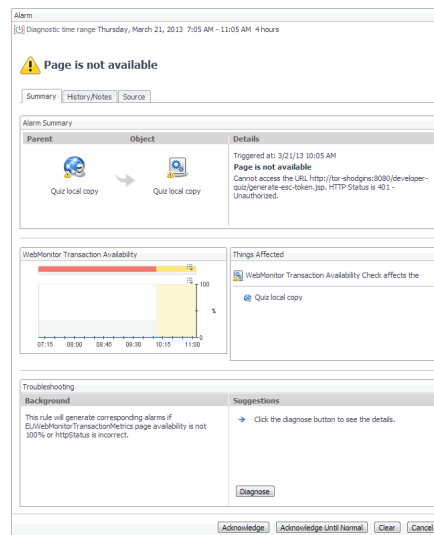
This view is made up of the following embedded views:

- [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](#).

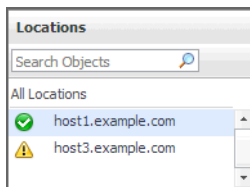
Top 5 Most Consumed Response Time

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

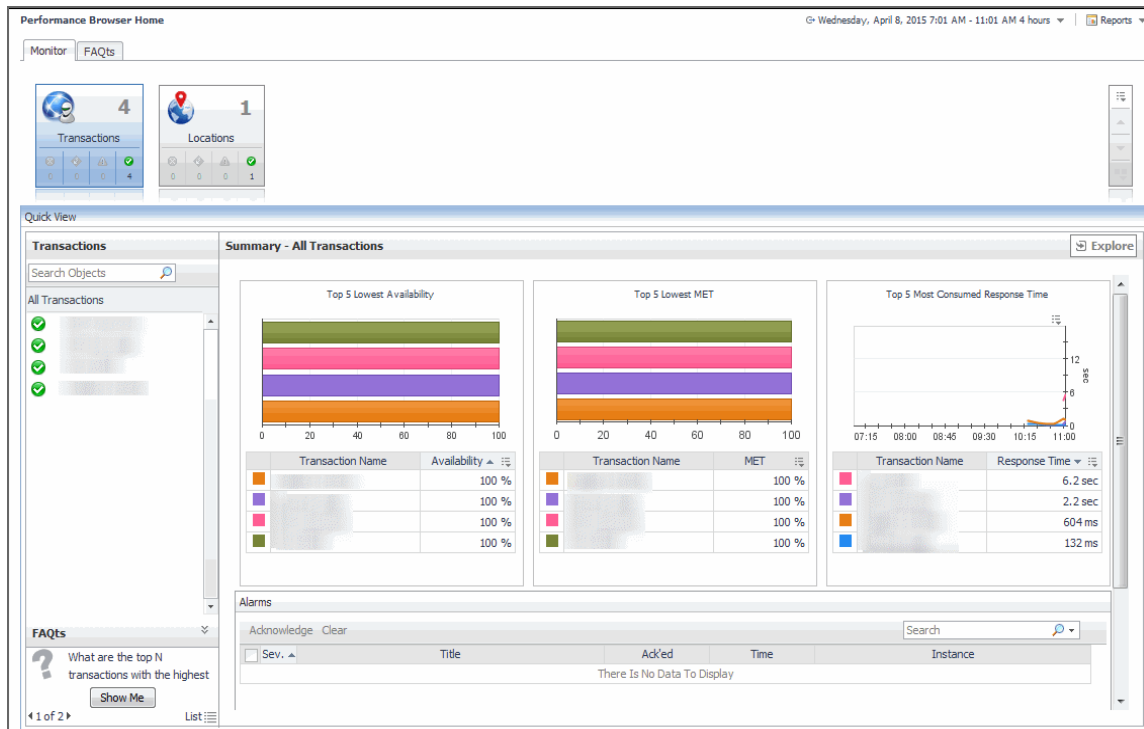
Table 9. Locations view

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

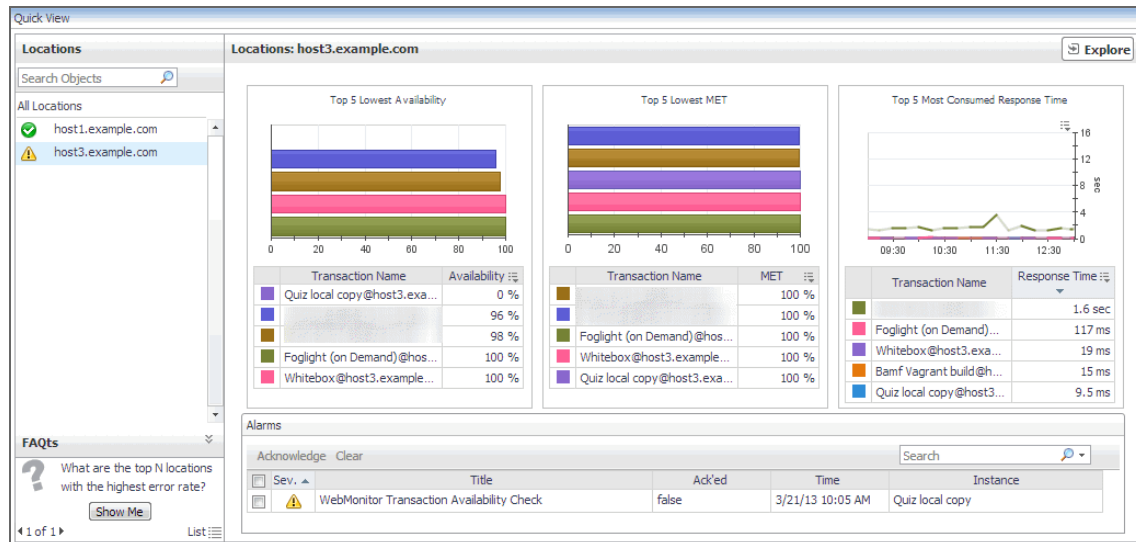
This view is made up of the following views:

- [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

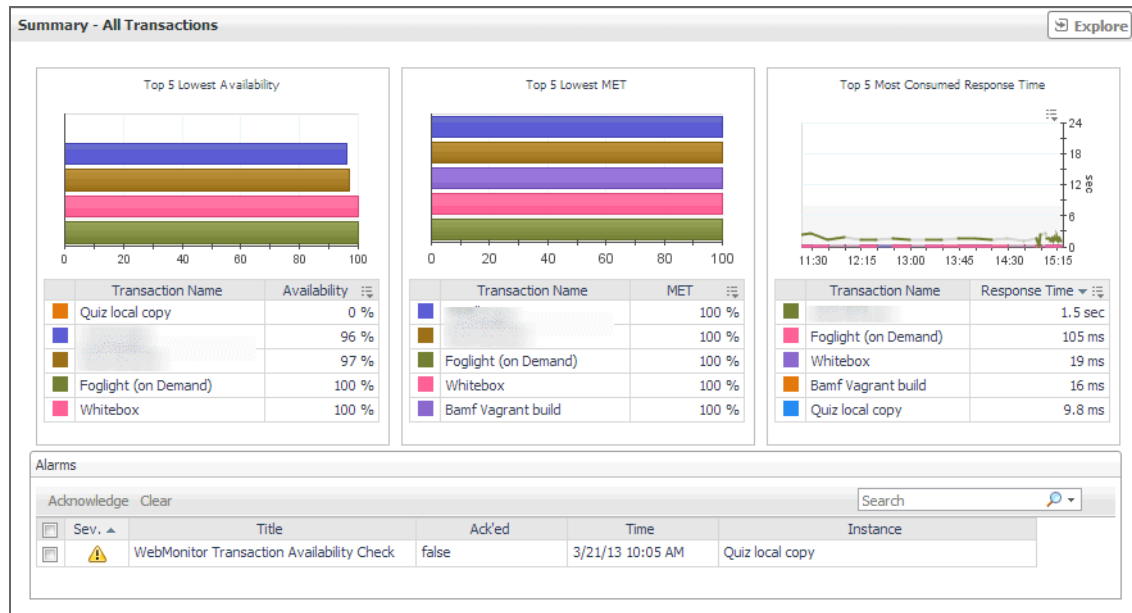
Table 11. All Locations view

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

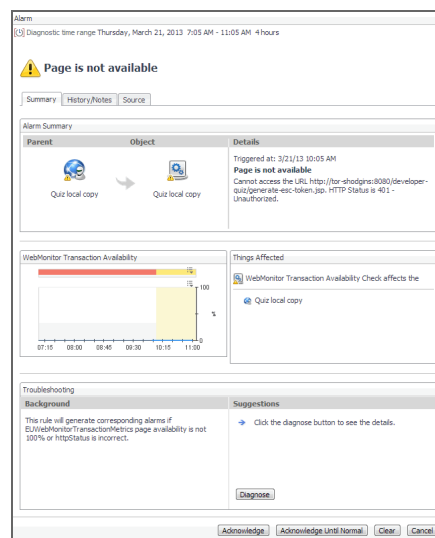
This view is made up of the following embedded views:

- **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

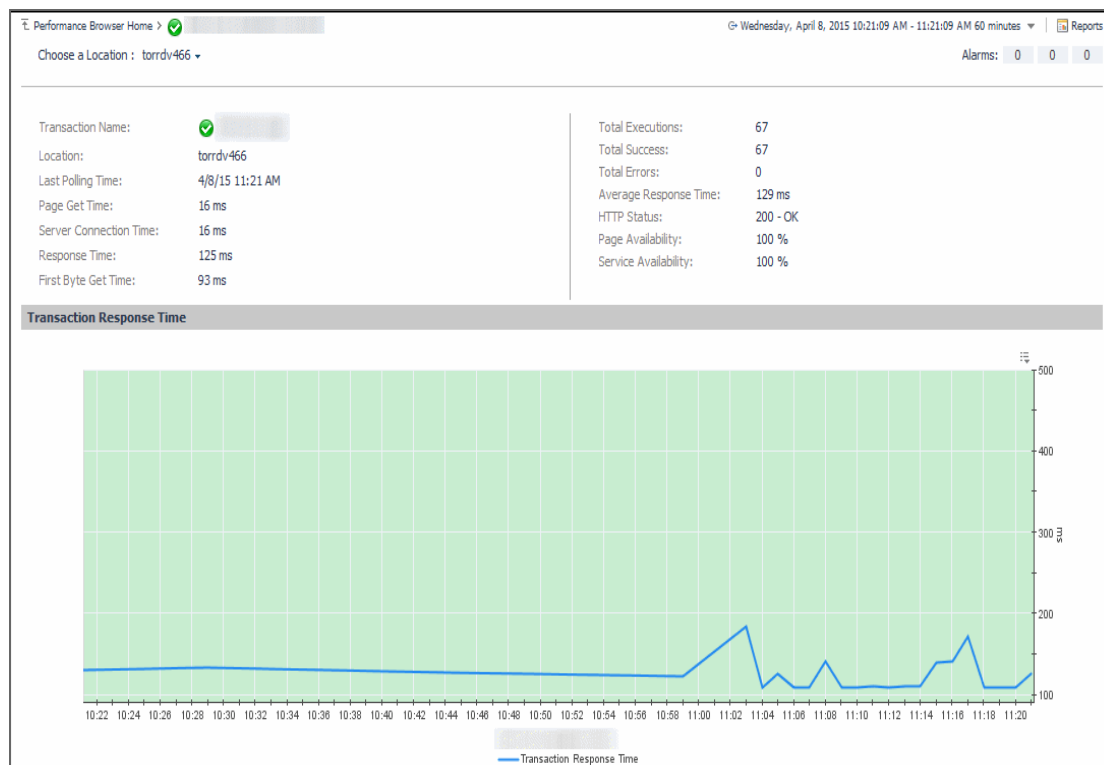
Table 15. Top 5 Most Consumed Response Time view

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

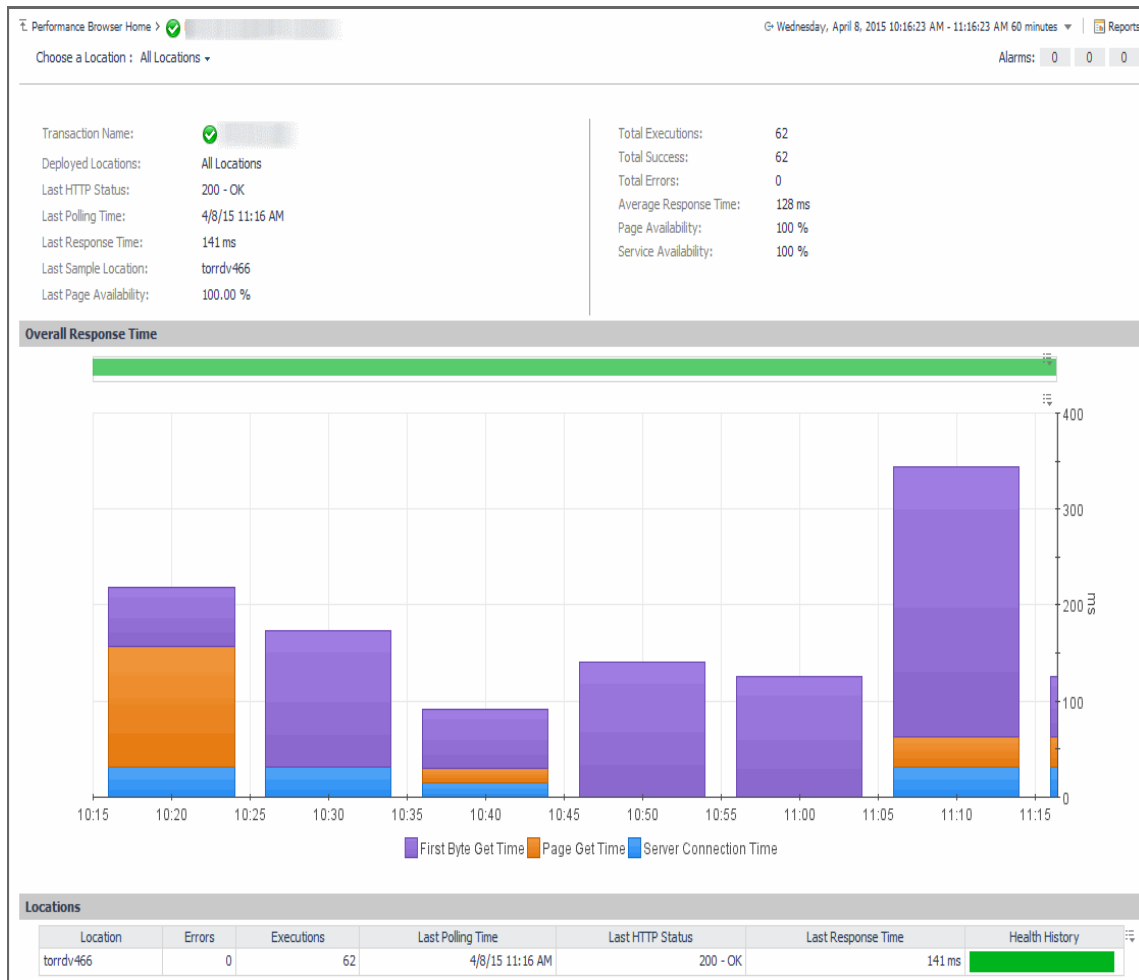
Table 18. Transaction Response Time view

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

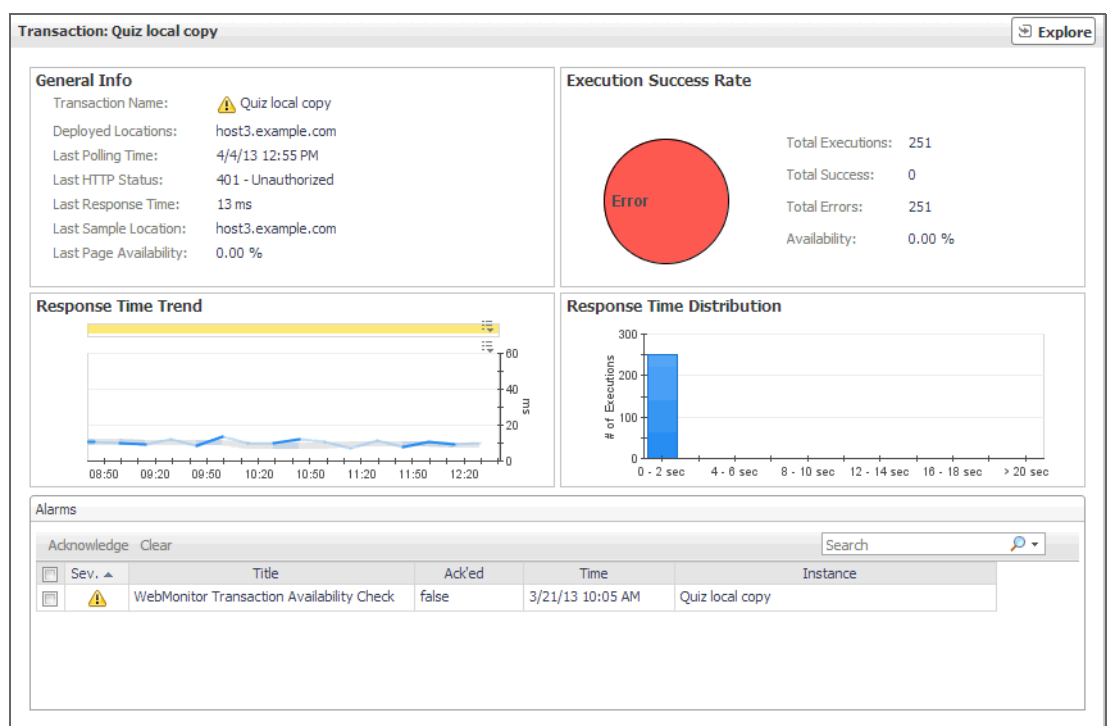
Table 22. Locations view

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

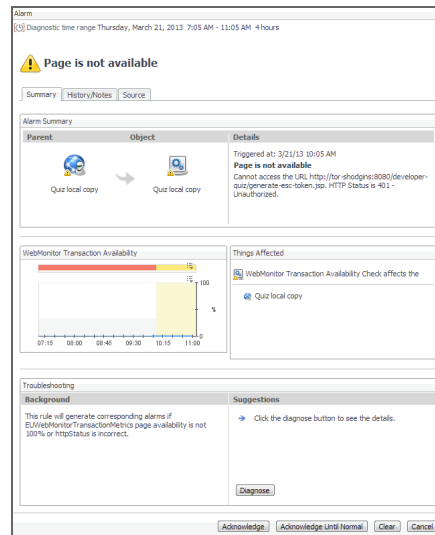
Table 23. Alarms view

	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.

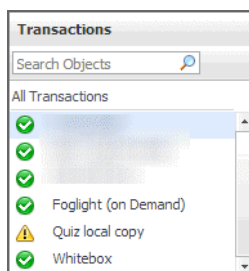
Response Time Distribution

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

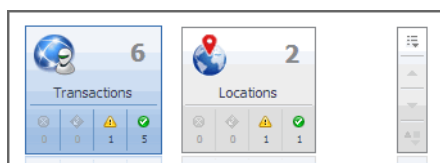
Table 28. Transactions view





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

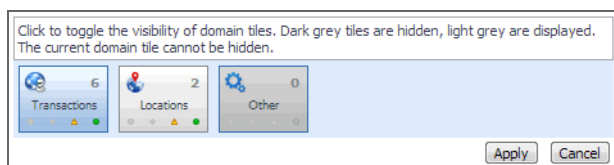
Purpose

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 8,000 milliseconds

Fatal when response time for this URL is greater than 13,000 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
			dsq8f5qf62.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

Data displayed	<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.
	<ul style="list-style-type: none">• Locations. The names of the hosts running the Web Monitor Agent instances that currently monitor this Web site.
	<ul style="list-style-type: none">• Transaction Name. The transaction name associated with the monitored Web site.
	<ul style="list-style-type: none">• Display Name. The display name of the transaction.
	<ul style="list-style-type: none">• 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

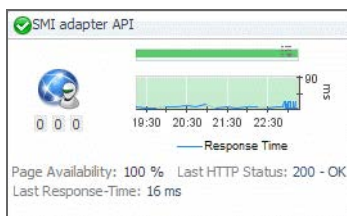
The Service Operations Console and Foglight for APM display the following Foglight Web Monitor views:

- [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

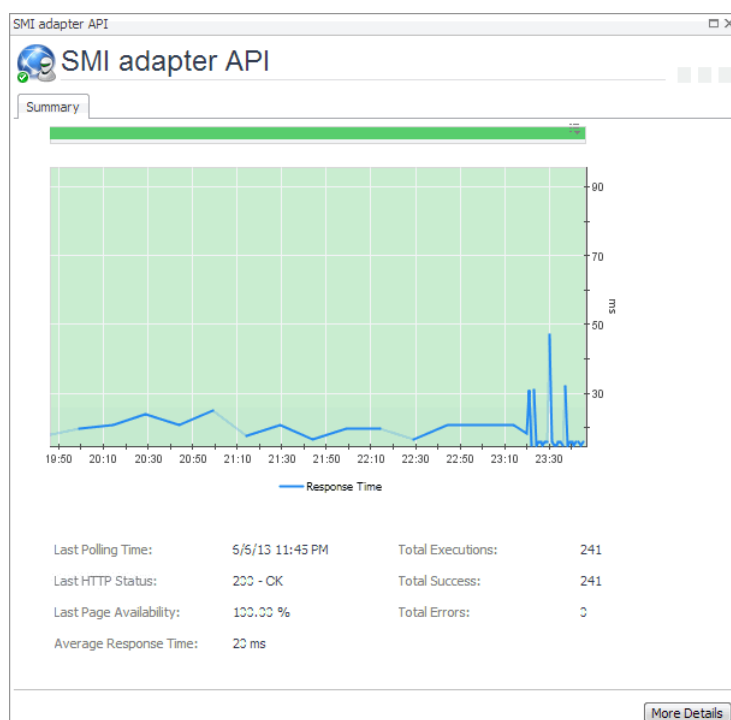
Table 35. Description of the view

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: <ul style="list-style-type: none"> • More Details. For more information, see Transaction at All Locations drilldown view.

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.