Product Guide

Real Time for ePolicy Orchestrator 1.0.0

TRADEMARK ATTRIBUTIONS

McAfee, the McAfee logo, McAfee Active Protection, McAfee AppPrism, McAfee Artemis, McAfee CleanBoot, McAfee DeepSAFE, ePolicy Orchestrator, McAfee ePO, McAfee EMM, McAfee Enterprise Mobility Management, Foundscore, Foundstone, McAfee NetPrism, McAfee Policy Enforcer, Policy Lab, McAfee QuickClean, Safe Eyes, McAfee SECURE, SecureOS, McAfee Shredder, SiteAdvisor, SmartFilter, McAfee Stinger, McAfee Total Protection, TrustedSource, VirusScan, WaveSecure, WormTraq are trademarks or registered trademarks of McAfee, Inc. or its subsidiaries in the United States and other countries. Other names and brands may be claimed as the property of others.

LICENSE INFORMATION

License Agreement

Contents

Contents

Preface

Contents

About this guide

This information describes the guide's target audience, the typographical conventions and icons used in this guide, and how the guide is organized.

Audience

McAfee documentation is carefully researched and written for the target audience.

The information in this guide is intended primarily for:

- **Administrators** — People who implement and enforce the company's security program.

- **Users** — People who use the computer where the software is running and can access some or all of its features.

- **Security officers** — People who determine sensitive and confidential data, and define the corporate policy that protects the company's intellectual property.

Conventions

This guide uses these typographical conventions and icons.

Book title, *term*, *emphasis*	Title of a book, chapter, or topic; a new term; emphasis.
Bold	Text that is strongly emphasized.
`User input, code, message`	Commands and other text that the user types; a code sample; a displayed message.
Interface text	Words from the product interface like options, menus, buttons, and dialog boxes.
Hypertext blue	A link to a topic or to an external website.
🛈	**Note:** Additional information, like an alternate method of accessing an option.
💡	**Tip:** Suggestions and recommendations.
⚠	**Important/Caution:** Valuable advice to protect your computer system, software installation, network, business, or data.
⚠	**Warning:** Critical advice to prevent bodily harm when using a hardware product.

Find product documentation

McAfee provides the information you need during each phase of product implementation, from installation to daily use and troubleshooting. After a product is released, information about the product is entered into the McAfee online KnowledgeBase.

Task

1 Go to the McAfee Technical Support ServicePortal at http://mysupport.mcafee.com.

2 Under **Self Service**, access the type of information you need:

To access...	Do this...
User documentation	**1** Click **Product Documentation**. **2** Select a product, then select a version. **3** Select a product document.
KnowledgeBase	• Click **Search the KnowledgeBase** for answers to your product questions. • Click **Browse the KnowledgeBase** for articles listed by product and version.

1 Introduction

Real Time for ePolicy Orchestrator® (Real Time for McAfee ePO™) gathers up-to-the-minute data about your managed systems so that you can take action based on the real-time condition of these systems.

With Real Time for McAfee ePO there is little to no delay in gathering system data, allowing for instant analysis of systems' health and quick response to events. Real Time for McAfee ePO collects data from all enterprise systems in seconds, even if your network has hundreds of thousands of systems, and even if they are geographically distributed over networks with slow connections.

This release supports ePolicy Orchestrator 5.0.

Contents

Components and what they do

To leverage Real Time for McAfee ePO technology, you must have a dedicated server and database. Deploying the Real Time for McAfee ePO client to managed systems is handled by your McAfee ePO™ server once the Real Time for McAfee ePO extension is installed. Real Time for McAfee ePO includes these components.

- **McAfee ePO server** — Communicates with the McAfee Agent, delivers security policies and tasks, controls updates, and processes events for all managed systems. ePolicy Orchestrator 5.0 is required.

- **McAfee ePO database** — The central storage component for all data created and used by ePolicy Orchestrator.

- **McAfee Agent** — Communicates with the McAfee ePO server. Retrieves updates, ensures task implementation, enforces policies, and forwards events for each managed system. McAfee Agent 4.6 and later is required.

- **Real Time for McAfee ePO extension** — Configures Real Time for McAfee ePO and deploys it to the Real Time for McAfee ePO client.

- **Real Time for McAfee ePO server** — Gathers information from the client and communicates it to ePolicy Orchestrator.

- **Real Time for McAfee ePO database** — The central storage component for Real Time for McAfee ePO configuration data.

- **Real Time for McAfee ePO client** — Responds to requests sent by the Real Time for McAfee ePO server and sends back the results. The client can also implement actions that are sent from the McAfee ePO server.

For information on the other products in the solution, download their documentation from the McAfee Technical Support ServicePortal at http://mysupport.mcafee.com/.

How Real Time for McAfee ePO provides current information

The McAfee ePO server prompts the Real Time for McAfee ePO server to run a script on all managed systems with a Real Time for McAfee ePO client.

Information is then communicated back to your McAfee ePO server using an optimized communication topology that delivers results from thousands of machines in just a few seconds. When your results are returned, you can use the management features to take action on any or all systems. Using Real Time for McAfee ePO is a three-step process:

1   Ask a question about a system or a group of systems.

2   Get results from the question.

3   Take action on the results. *(Optional)*
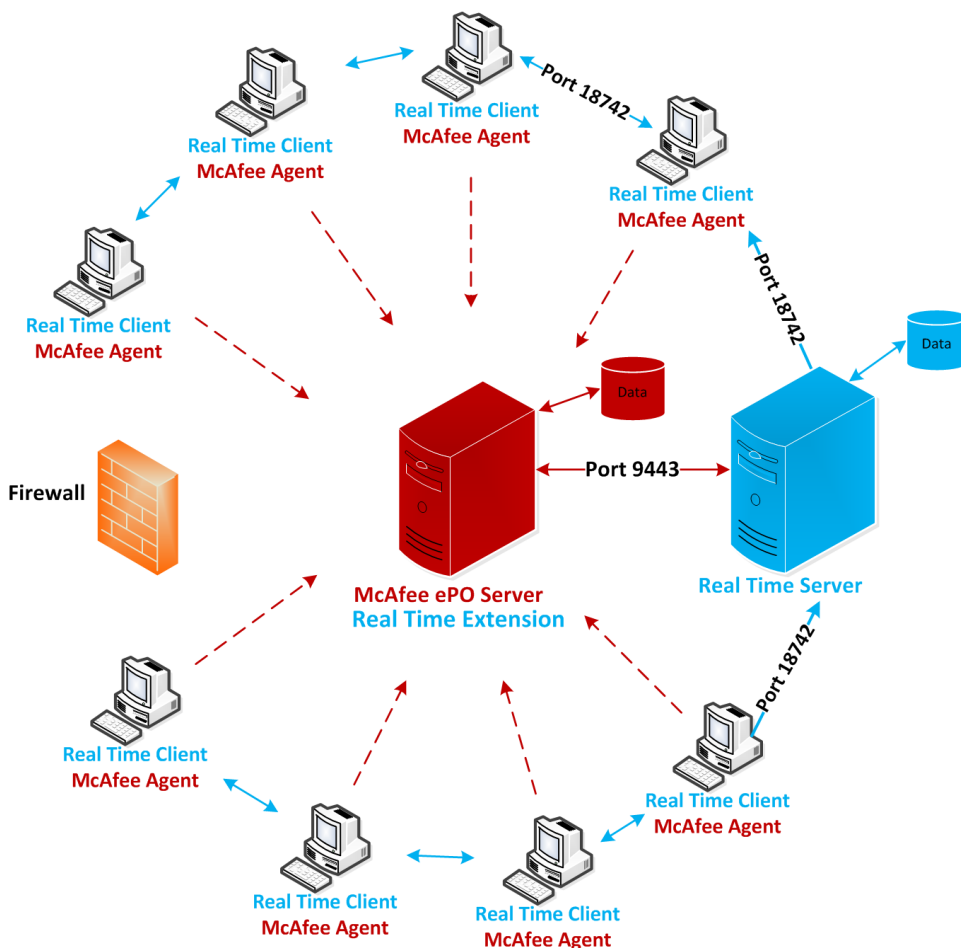
Real Time for McAfee ePO uses peer-to-peer architecture that relies on a point-to-point protocol. This functionality adds and removes clients as they come online without interaction from an administrator.

Each client uses a TCP port (by default, 18742) to communicate with the Real Time for McAfee ePO server. A single TCP port is used for communication between clients. This client-to-client communication channel makes the Real Time for McAfee ePO solution efficient and reduces the Wide Area Network (WAN) load.

> ⓘ To ensure optimal operations, clients must be able to communicate with their peers.

2 Installing and deploying

Making sure your environment has the correct hardware and software requirements is the first step to installing and deploying the Real Time for McAfee ePO components.

Contents

‣ *Hardware and software requirements*
‣ *Install and deploy components*
‣ *Deploy the client*

Hardware and software requirements

Your environment needs specific hardware and software before you can install and deploy Real Time for McAfee ePO. The Real Time for McAfee ePO server can be installed on a physical or virtual server.

Server hardware requirements

Number of managed systems						
Hardware	**Up to 3,000**	**Up to 10,000**	**Up to 35,000**	**Up to 75,000**	**Up to 150,000**	**Up to 400,000**
Processor Cores	2	4	8	16	32	48
Memory	4 GB	12 GB	16 GB	32 GB	48 GB	64 GB
Disk Space	40 GB	100 GB	200 GB	400 GB	1 TB	2 TB

Real Time for McAfee ePO software requirements

Component	Requirement
Real Time for McAfee ePO server	• Microsoft Windows Server 2003, 64-bit with latest service packs • Microsoft Windows Server 2003 R2, 64-bit with latest service packs • Microsoft Windows Server 2008, 64-bit with latest service packs • Microsoft Windows Server 2008 R2, 64-bit with latest service packs
Real Time for McAfee ePO client ⓘ A minimum of two clients are required. The question times out without returning an answer if you don't have a minimum of two clients.	• Microsoft Windows Server 2003, 2008 • Microsoft Windows XP, Vista, 7, 8 • Linux Red Hat (RHEL, CentOS, Fedora), SUSE, Debian/Ubuntu • Mac OS X 10.5 and later (Intel-only)

Other system requirements

Component	Requirement
ePolicy Orchestrator	5.0
McAfee Agent	4.6 or later

Real Time for McAfee ePO server database considerations

We recommend that you install the Real Time for McAfee ePO server on a dedicated system, but these scenarios are supported:

• Deployment with fewer than 100 clients: ePolicy Orchestrator, Real Time for McAfee ePO server, McAfee ePO database, and the Real Time for McAfee ePO database can exist on one server.

• Deployment for up to 1,000 users: Real Time for McAfee ePO server and Real Time for McAfee ePO database can be installed on the same server.

⚠ For installations with more clients, the Real Time for McAfee ePO server and the Real Time for McAfee ePO database must be installed on separate dedicated servers.

Table 2-1 Microsoft SQL server editions

Software	Edition	Maximum number of managed systems
SQL Server 2008	Workgroup	10,000
	Standard	75,000
	Enterprise	400,000
	R2 Data Center	400,000
SQL Server 2005	Workgroup	3,000
	Standard	75,000
	Enterprise	400,000

Install and deploy components

Follow this sequence to complete the Real Time for McAfee ePO installation.

> **Before you begin**
>
> These items must be in place before you begin the installation process:
>
> - ePolicy Orchestrator 5.0 is available on the network.
>
> - A supported SQL server is installed on the network.
>
> - The Real Time for McAfee ePO server .zip and Real Time for McAfee ePO client .zip files are available.

Task

1   Install the Real Time for McAfee ePO extension on your McAfee ePO server.

2   Check in the client and content packages in the Master Repository.

3   Install the Real Time for McAfee ePO server and database.

4   Verify that the content checked in successfully.

Tasks

- *Install the extension on your McAfee ePO server* on page 11
  The Real Time for McAfee ePO extension must be installed in ePolicy Orchestrator so that your McAfee ePO server can communicate with the Real Time for McAfee ePO server.

- *Check in the content package* on page 12
  The Real Time for McAfee ePO content package contains the questions and packages. The content package is checked into the master repository, and then imported by the Real Time for McAfee ePO server from the McAfee ePO server.

- *Check in the client package* on page 12
  The client package contains client installers that are deployed to client systems from ePolicy Orchestrator. This package must be checked in before you can deploy the client to your managed systems.

- *Install the Real Time for McAfee ePO server and database* on page 13
  The Real Time for McAfee ePO server setup installs the Real Time for McAfee ePO server application, a Real Time for McAfee ePO SQL database, and sets the options for communication with the McAfee ePO server.

- *Verify content check-in* on page 14
  Verify that the contents checked in to ePolicy Orchestrator successfully, and that the contents synchronized between ePolicy Orchestrator and the Real Time for McAfee ePO server.

Install the extension on your McAfee ePO server

The Real Time for McAfee ePO extension must be installed in ePolicy Orchestrator so that your McAfee ePO server can communicate with the Real Time for McAfee ePO server.

The Real Time for McAfee ePO extension is located in the Real Time for McAfee ePO server .zip file.

Task

For option definitions, click **?** in the interface.

1   Extract the Real Time for McAfee ePO extension, `MRTManagementExtension.zip`, from the Real Time for McAfee ePO server .zip file.

2   Click **Menu | Software | Extensions | Install Extension**.

3   In the **Install Extension** dialog box, browse to the extension file that you extracted, then click **OK**.

Check in the content package

The Real Time for McAfee ePO content package contains the questions and packages. The content package is checked into the master repository, and then imported by the Real Time for McAfee ePO server from the McAfee ePO server.

The Real Time for McAfee ePO content .zip package is included with the Real Time for McAfee ePO server .zip file.

Task

For option definitions, click **?** in the interface.

1   Extract the content package, `MRTContentPackage.zip`, from the Real Time for McAfee ePO server .zip file to a temporary location.

2   Click **Menu | Software | Master Repository | Check In Package** to open the wizard.

3   For the package type, select **Product or Update (.ZIP)**.

4   Click **Browse** and locate the **MRTContentPackage.zip**.

5   Click **OK**.

Check in the client package

The client package contains client installers that are deployed to client systems from ePolicy Orchestrator. This package must be checked in before you can deploy the client to your managed systems.

Task

For option definitions, click **?** in the interface.

1   Click **Menu | Software | Master Repository | Check In Package** to open the wizard.

2   For the package type, select **Product or Update (.ZIP)**.

3   Click **Browse** and locate the Real Time for McAfee ePO client .zip file.

4   Click **OK**.

Install the Real Time for McAfee ePO server and database

The Real Time for McAfee ePO server setup installs the Real Time for McAfee ePO server application, a Real Time for McAfee ePO SQL database, and sets the options for communication with the McAfee ePO server.

Task

1 Extract the Real Time for McAfee ePO server .zip file to any folder on the Real Time for McAfee ePO server system, then run **setup.exe**. Follow the instructions and type the required data when prompted.

For this setting...	Enter...
Real Time for McAfee ePO server location	• The network path where you want to install the server. The default path is `C:\Program Files (x86)\McAfee\Real Time Server\`. This location can be the same as the McAfee ePO server. ⓘ The server is installed under the 32-bit branch.
McAfee ePO server data ⓘ Global Administrator rights are required.	• **ePO Server** — IP address or host name of your McAfee ePO server. • **ePO Server Port** — The https port of the McAfee ePO server. 8443 is the default port. • **ePO Admin User** — User name of the McAfee ePO administrator. • **ePO Admin Password** — Password of the McAfee ePO administrator.
Windows Account and Password	The Real Time for McAfee ePO server account is the service account and is used to connect to the Real Time for McAfee ePO database. The account must belong to the local administrator group on the system where Real Time for McAfee ePO is installed, and must have permission to create and delete databases. • **Domain** — Domain name where the account exists. ⓘ You must be a member of the Local Administrator group. • **User name** — User's domain account name. • **Password** — User's domain account password.

For this setting...	Enter...
SQL Database Server	• **Database Server** — Browse to and select a location from the list. Default is the location of the McAfee ePO database. • **Database Port (optional)** — Alternative port used for database communication. (i) If the database port number is different than the default port number, edit the **Database Port** field to reflect the correct port number.
Server Configuration	This information is filled in automatically. • **Real Time Client-to-Server Communication Port** — The port number used by the Real Time for McAfee ePO server to communicate with the Real Time for McAfee ePO clients. 18742 is the default port. (i) The port number is determined by the extension. • **ePO Server-to-Real Time Server Secure Communication Port** — This port is used by the McAfee ePO server to communicate with the Real Time for McAfee ePO server. 9443 is the default port. • **Real Time Server SOAP Communication Port** — This port is used by the McAfee ePO server to communicate with the Real Time for McAfee ePO server for queries and responses. 9080 is the default port.

2   When you complete the settings, click **Install** to start the installation process.

3   When the install is complete, click **Finish**.

4   To verify the installation, go the ePolicy Orchestrator console, click **Menu | Configuration | Server Settings**, and select **Real Time Server**.

The right pane displays the configuration information provided during the installation.

Verify content check-in

Verify that the contents checked in to ePolicy Orchestrator successfully, and that the contents synchronized between ePolicy Orchestrator and the Real Time for McAfee ePO server.

Task

For option definitions, click **?** in the interface.

1   From the ePolicy Orchestrator console, click **Menu | System | System Tree**.

2   From the **Actions** drop-down list, select **Real Time | Ask Question**.

Deploy the client

After installing the Real Time for McAfee ePO server, you can deploy the client with ePolicy Orchestrator.

Tasks

• *Deploy clients with ePolicy Orchestrator*
  Use a deployment project to easily deploy and schedule the Real Time for McAfee ePO deployment.

Deploy clients with ePolicy Orchestrator

Use a deployment project to easily deploy and schedule the Real Time for McAfee ePO deployment.

Task

For option definitions, click **?** in the interface.

1   Click **Menu | Software | Product Deployment**.

2   Click **New Deployment** to start a new project.

3   Type a name and description for this deployment, which appears in the Deployment page after you save the deployment.

4   Choose the type of deployment:

   - **Continuous** — Uses your System Tree groups or tags to configure the systems receiving the deployment. This method these systems to change over time as they are added or removed from the groups or tags.

   - **Fixed** — Uses a fixed, or defined, set of systems to receive the deployment. System selection uses the System Tree or the table output from Managed Systems Queries.

5   To specify which software to deploy, select a product from the **Package** list. Click **+** or **-** to add or remove packages.

   > ⚠️ Your software must be checked in to the Master Repository before it can be deployed. The **Language** and **Branch** fields are populated automatically, from the location and language specified in the Master Repository.

6   In the **Command line** text field, specify any command-line installation options.

7   **Select the systems**, click **Select Systems**.

   The **System Selection** dialog box allows you to select groups in your System Tree, tags, or a subset of grouped or tagged systems. The selections you make in each tab are concatenated to filter the complete set of target systems for your deployment.

   > ⚠️ Fixed deployments have a limit of 500 systems that can receive the deployment.

   If needed, configure the following:

   - **Run at every policy enforcement (Windows only)**

   - **Allow end users to postpone this deployment (Windows only)**

   - **Maximum number of postponements allowed**

   - **Option to postpone expires after**

   - **Display this text**

8   Pick a start time or schedule your deployment:

   - **Run Immediately** — Starts the deployment task during the next ASCI.

   - **Once** — Opens the scheduler so you can configure the start date, time, and randomization.

9   Click **Save** at the top of the page. The **Product Deployment** page opens with your new project added to the list of deployments.

After you create a deployment project, a client task is automatically created with the deployment settings.

3 Using Real Time for McAfee ePO software

Real Time for McAfee ePO provides easy access to current information about the systems in your network.

Instead of querying a database, you can use this feature to quickly retrieve current, accurate information from thousands of systems. With this level of visibility you can collect and update systems across your network in seconds. Get live data for your managed network by running a query.

Contents
‣ *Configure permission sets*
‣ *Work with live data*

Configure permission sets

When you install the Real Time for McAfee ePO extension, it adds a section to the permission sets without applying any permissions, except for global administrators. To allow other users to see and use the Real Time for McAfee ePO features, you must configure the required permissions and create new permission sets.

Task

1 Select **Menu | User Management | Permission Sets**.

2 Under **Real Time Core**, click **Edit**.

3 Set these permissions:

For	Select
Sensor (Question) Permissions	• **No permissions** — Prevents the user from asking questions. The user can't see the **Real Time	Ask Question** menu item on the System Tree page, or the **Systems	Real Time Questions** page. • **All approved sensors** — Allows the user to ask questions.
Action Permissions	• **No permissions** — Prevents the user from taking actions. The user can't see the **Real Time	Take Action** menu item on the System Tree page or in the results returned from the question. • **All approved sensors** — Allows the user to take actions.

4   Click **Save**.

> ⚠️ The global administrator also needs to give permissions to handle other items that work with Real Time for McAfee ePO. These include:
>
> • **Queries and Reports**
>
> • **Dashboards**
>
> • **System Tree**
>
> • **System tree access**
>
> System Tree permissions, for example, govern which systems the user is able to ask questions of and take actions on; Queries and Dashboards permissions allow adding a Real Time for McAfee ePO dashboard. For more information on permission sets, see the ePolicy Orchestrator documentation.

Work with live data

Use Real Time for McAfee ePO to work with live data by submitting questions through a dashboard monitor, the System Tree view, or the Real Time Questions page. You can also perform an action based on the results of the questions.

Tasks

• *Ask questions using the System Tree* on page 18
Real Time for McAfee ePO lets you query your network by submitting a question.

• *Ask questions using the Systems page* on page 19
Real Time for McAfee ePO lets you ask questions from the Systems page in ePolicy Orchestrator.

• *Ask questions using dashboards* on page 19
Use ePolicy Orchestrator dashboards to create a Real Time for McAfee ePO monitor so you can ask questions about your managed network.

• *Use the Question (Sensor) Builder* on page 19
The Question Builder allows you to manage the list of questions that are available in Real Time for McAfee ePO. You can build your own custom questions from a list of available sensors and filters, and save them for later use, and you can delete questions that you no longer wish to use.

• *Take actions* on page 20
After you ask a question and receive the results, you can take multiple actions to refine the information.

Ask questions using the System Tree

Real Time for McAfee ePO lets you query your network by submitting a question.

Task

1   Click **Menu** | **Systems** | **System Tree**, then select a group or a single system.

2   From the **Actions** drop-down list, select **Real Time** | **Ask Question**.

3   In the **Ask Question** dialog box, select a question, then click **OK**.

The System Tree page displays the results.

Ask questions using the Systems page

Real Time for McAfee ePO lets you ask questions from the Systems page in ePolicy Orchestrator.

Task

1   Click **Menu | Systems | Real Time Questions**.

2   From the list of questions, select the question you want to ask, then click **Ask**.

3   Select a result, then from the **Actions** drop-down list select one of these options:

   •   **Drill Down**

   •   **Show Related Systems**

   •   **Take Action**

Ask questions using dashboards

Use ePolicy Orchestrator dashboards to create a Real Time for McAfee ePO monitor so you can ask questions about your managed network.

Task

1   From the ePolicy Orchestrator console, click **Dashboards**.

2   From the **Dashboard Actions** drop-down list, select **New**.

3   Type a **Dashboard Name**, select a **Dashboard Visibility** option, then click **OK**.

4   In the **Category** drop-down list, select **Real Time Questions**.

5   Drag the **Real Time Questions** monitor onto the dashboard. As you move the cursor around the dashboard, the nearest available drop location is highlighted.

   appears.

6   In the **New Monitor** dialog box, configure the settings as needed, select a question from the drop-down list, then click **OK**.

Use the Question (Sensor) Builder

The Question Builder allows you to manage the list of questions that are available in Real Time for McAfee ePO. You can build your own custom questions from a list of available sensors and filters, and save them for later use, and you can delete questions that you no longer wish to use.

To...	Do this...
Ask an existing question	**1** Select **Menu	Systems	Real Time Questions**. A list of the currently available questions appears. **2** Under **Actions**, click **Ask** to ask a question.
Delete a question	• Select the checkbox next to any question, and select **Actions	Delete**.

To...	Do this...
Create and ask question	**1** Select **Actions** | **New Question**. **2** Under the Sensors section, add one or more sensors to your question. If you know the name of the sensor, begin typing its name and a list of matching sensors is displayed. ⓘ If you do not know the name of the sensor, enter a space in the Sensor Name box, and a list of all sensors is displayed. **3** Add additional sensors by typing in the additional Sensor Name boxes. **4** Click **Submit Question**. ⓘ You can further tailor your question by adding filters in the Filters section. For example, if you wanted to list the versions of VirusScan Enterprise and the VirusScan Enterprise DAT files, but only for machines in the "mydomain.com" domain, then you could make the following selections: • In the first Sensor Name box, select "VirusScan Enterprise Version" • In the second Sensor Name box, select "VirusScan Enterprise DAT Version" • In the Filters section, select "Domain Name" in the Sensor Name box, select "matches" as the operator, and enter "mydomain.com" in the Filter Value box
Submit a new question	**1** Click **Save Question**. **2** In the Question Name and Description window, type a name and description for the question, and click **OK**. The question is saved to the list of available questions, and can be asked from the System Tree or the Real Time Questions page.

Take actions

After you ask a question and receive the results, you can take multiple actions to refine the information.

Task

1   Click **Menu** \| **Systems** \| **System Tree**.

2   Select a system where you want to submit an action.

3   From the **Actions** menu, select the action you want to take:

- **Drill Down** — Drill down to refine your results by asking another question based on the systems you select.

- **Show Related Systems** — View a list of related systems in the System Tree.

- **Take Action** — From the results, take an action on the selected systems. When the results to a question are returned, you can select one or more systems and take action on them.

4   Click **OK**.

Index