



IPSWITCH

# WhatsUp Gold

Application Performance Monitoring  
v16.4

## CHAPTER 1

### Introduction

Overview .....	1
APM Terminology.....	2
APM licensing and user rights.....	3
Getting started with APM.....	4
Application Profiles .....	5
Application Components .....	6
Action Policies.....	7
Discovering applications .....	7

### Dashboards and Reports

Viewing APM status.....	10
APM current status .....	10
APM historical status.....	11
Working with application states.....	18
APM dashboard reports .....	19
APM State Summary dashboard report.....	19
Application Event Log dashboard report.....	19

### Configuration and Settings

Application Profiles .....	21
Adding an application profile.....	21
Importing an application profile.....	22
Working with existing application profiles .....	23
Applying application attributes.....	76
Action policies .....	77
Working with action policies.....	78
Creating an action policy.....	78
Assigning an action policy to an instance or component.....	80
Managing action policies.....	81
Actions.....	81
Working with actions.....	81
Creating a new action .....	82
Blackout policies.....	92
Working with blackout policies .....	92

Creating a new blackout policy .....	92
Configuring APM application settings .....	92

# Introduction

## In This Chapter

Overview.....	1
APM Terminology.....	2
APM licensing and user rights.....	3
Getting started with APM.....	4
Discovering applications.....	7

## Overview

Application Performance Monitor monitors applications across multiple devices, servers, and systems, providing performance statistics and overall application health, while alerting on performance degradation and potential problems before they result in service outages. APM helps IT organizations measure and guarantee Service Level Agreements (SLAs) and assists in pinpointing application performance bottlenecks and points of failure. For more information, see *Getting Started with APM* and the Ipswitch Application Performance Monitor Getting Started Guide.



**Note:** APM is available with WhatsUp Gold Premium Edition only. To update your license, visit the *Customer Portal* (<http://www.whatsupgold.com/wugCustPortal>).

Each application monitored by APM is comprised of a collection of individual components as defined in the application profile. This application profile is then applied to a monitored device, creating an application instance. See *Learning about APM terminology* (on page 2).

The following are some examples of application types that APM supports:

- |  |  |
|--|--|
| § Cisco Unified Communications Manager | § Microsoft Windows Server                     |
| § Microsoft IIS                        | § Microsoft Active Directory/Domain Controller |
| § Ipswitch WhatsUp Gold                | § Microsoft SQL Server                         |
| § Ipswitch iMail                       | § Microsoft Lync Server                        |
| § Microsoft Exchange                   | § Microsoft SharePoint                         |
| § Microsoft Hyper-V Server             | § Oracle Database Server                       |

# APM Terminology

The following terms are used throughout APM:

- § **Application Type.** Groups application profiles, instances, and components by the type of application (e.g., Microsoft SQL Server, Microsoft IIS, Microsoft Windows). After profiles, instances, and components are configured for an application, you will begin monitoring information about application health.
- § **Application.** An application is made up of one or more programs running on one or more monitored systems. There are three distinct application types leveraged by APM:
  - § **Simple application.** A simple application is an application that is not dependent on another application to run. Example: Microsoft Server 2008 R2.
  - § **Complex application.** A complex application is an application configured to be dependent on one or more applications to run. Example: WhatsUp Gold (requires IIS and SQL Server).
  - § **Discrete application.** A discrete application is an application upon which a complex application has a dependency. For example, IIS and SQL Server are discrete applications on which the complex application WhatsUp Gold is dependent. A discrete application is used when you are monitoring a complex application.
- § **Application Profile.** An application profile is a blueprint for monitoring a given type of application within APM. It defines the collection of components and distinct applications that reflect the health and status of a specific type of application. An application instance is created from the application profile by associating it with the actual devices that host the components of the application as defined by the application profile. Changes to the application profile are inherited by all of the instances created from the profile. Changes in the profile are not inherited by overridden fields.
- § **Application Instance.** An application instance is a running copy of an application profile that monitors the defined collection of components, distinct applications, and thresholds necessary to define the health and performance of a given type of application. An application instance can *extend* the application profile by adding components, component groups, or discrete applications. The application profile is *not* changed when an application instance is extended.
- § **Component.** A component is a single data point collected as part of an application profile. Example: CPU Utilization
- § **Critical component.** A critical component is a component that impacts the status of an application instance. As a result, a critical component that goes into the down state, causes the application instance to go into the down state. However, if a non-critical component goes into a down state, the application instance goes into a warning state and only the component indicates being in the down state.
- § **Critical component group.** A critical component group is a grouping of components that contains specific logic to allow for complex evaluation of the up/down state of an application. For example, given four components A,B,C and D, the following logic can be applied, so that if A and B are down or C and D are down the application is placed

into the down state. ((A and B) or (C and D)). Critical component groups are always considered "critical", in that if a critical component group is evaluated to be in the down state, the entire application is in the down state.

## APM licensing and user rights

Application Performance Monitor is installed during the WhatsUp Gold installation. Your license determines whether the APM plug-in is available in WhatsUp Gold. To update your license for APM, visit the *WhatsUp Customer Portal* (<http://www.whatsupgold.com/wugCustPortal>).

An application instance is an application profile assigned to a specific device to monitor a running application. Each application instance consumes one license. End User Monitor components are used to monitor web site and application transactions. (For more information, see *Scripting (End User Monitor* (on page 57)) component). Each enabled End User Monitor component consumes one license.

The total count of APM licenses consumed is the number of application instances plus the number of enabled End User Monitor components. If an application instance has only End User Monitor components, the application instance does not consume a license.

### APM Licensing Examples

- § Monitoring 5 SQL Server implementations consumes 5 licenses.
- § Monitoring an application distributed across multiple servers requires a license for each member server.
- § Monitoring each server role of Microsoft Lync and Exchange requires a license, even if they are being run on the same server. APM includes multiple Ipswitch-certified application profiles for Microsoft Lync and Exchange, generally based on their server roles.
- § Monitoring 2 web application transactions from 2 locations requires 4 End User Monitor components and consumes 4 licenses.

To view current APM license information, click the Application Settings icon (⚙️) in the upper-right corner of the interface, then select **Application Settings** to launch the Application Settings interface. Select the **System** tab, then click **About WhatsUp Gold** to launch the About WhatsUp Gold dialog. APM license usage information is also available at the top of each page on the APM Configuration tab. You can see additional details about how licenses are being consumed by clicking Details.

### APM User Rights

In addition to having a license that includes APM, you must also have the proper user rights enabled for the user account logged in:

- § To view APM in the WhatsUp Gold interface, the Access APM user right must be enabled.
- § To create or modify application profiles, the Configure APM Application Profiles user right must be enabled.

- § To create or modify application instances, the Configure APM Application Instances user right must be enabled.

For more detailed information on user rights, see About user rights.

## Getting started with APM

Configuring APM to monitor an application is a simple process that starts with selecting a profile that captures the data points necessary to understand the performance, health, and status of a given type of application. The application profile groups the components, discrete applications, and associated thresholds necessary to capture the data points into a blueprint that can be used to create individual application instances. These instances actively monitor your applications.

Ipswitch provides a selection of profiles for use with APM which are available in the APM installation, or by download from the *WUGSpace Community* ([https://community.whatsupgold.com/library/apm\\_profiles](https://community.whatsupgold.com/library/apm_profiles)). You can also create your own application profiles which can be shared on the *WUGSpace Community* ([https://community.whatsupgold.com/library/apm\\_profiles](https://community.whatsupgold.com/library/apm_profiles)).

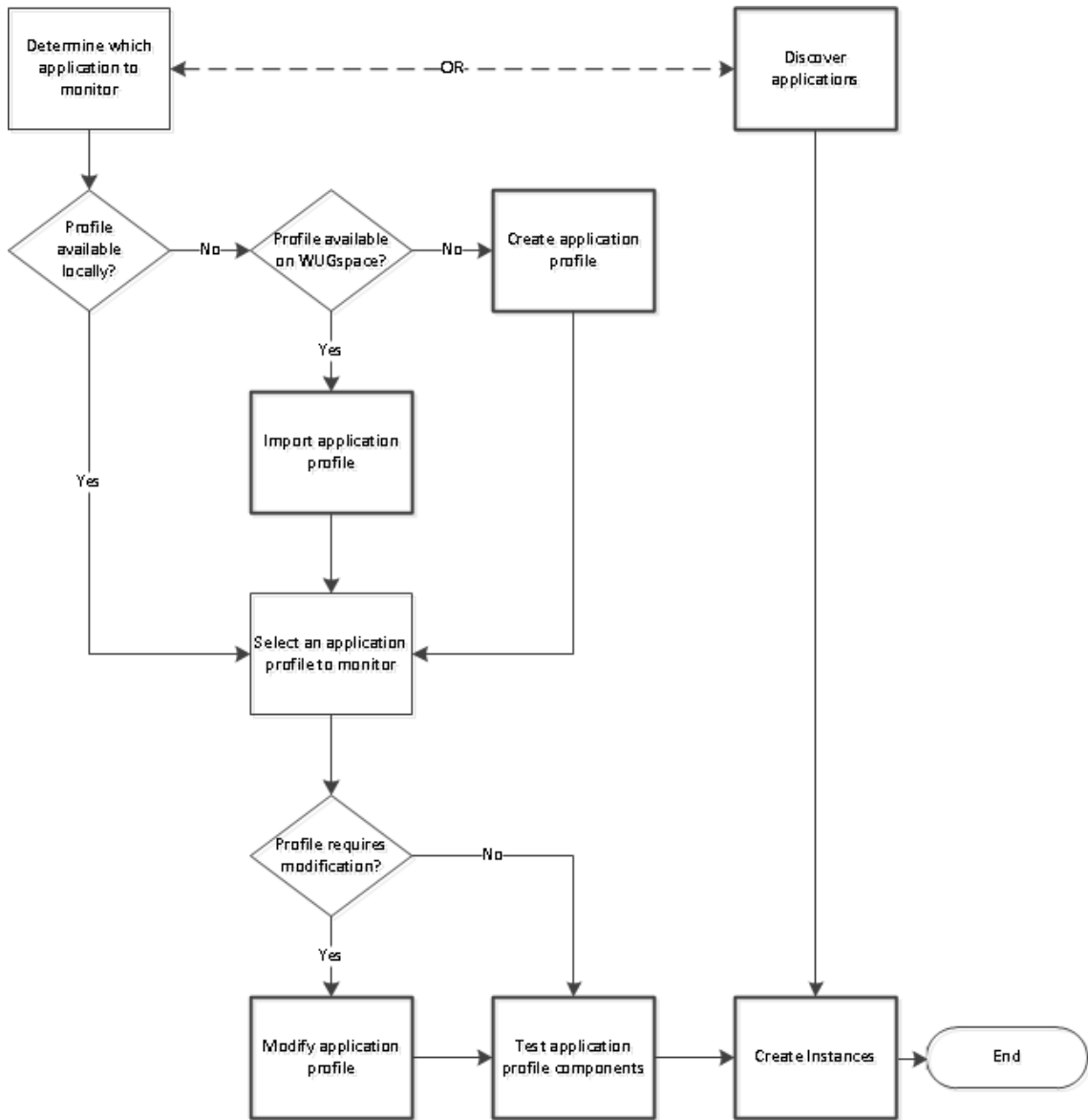
After you have the necessary profiles, you can use APM to automatically discover your applications and create instances for each discovered application, or you may choose to manually create and modify instances individually before you begin monitoring.

The following flowcharts represent the typical process of setting up an application to be monitored with APM:

- § *Application Profile Workflow* (on page 5)
- § *Application Component Workflow* (on page 6)
- § *Action Policy Workflow* (on page 7)

For more information, see the Ipswitch *Application Performance Monitor Getting Started Guide* ([http://www.whatsupgold.com/WUGAPM\\_164GSG](http://www.whatsupgold.com/WUGAPM_164GSG)).

## Application Profiles



Refer to the table below for step-by-step instructions for each configuration process in the flow chart.

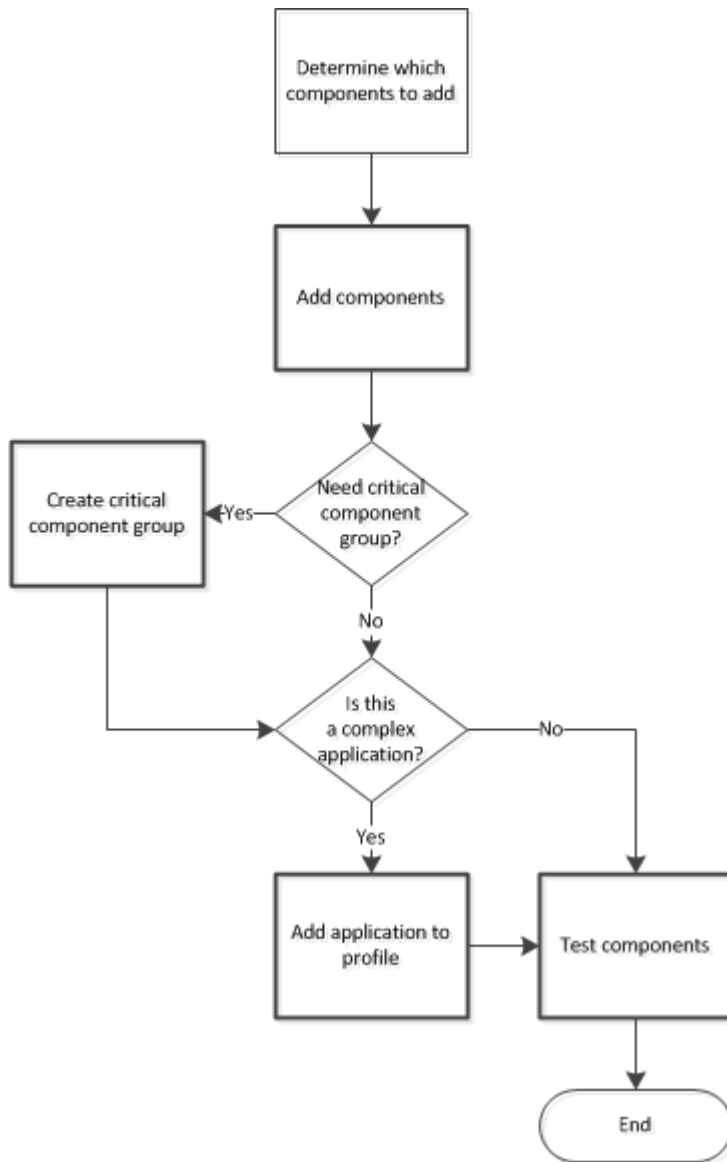
Create Application Profile	Creating a new application profile
Import Application Profile	Importing and downloading application profiles
Discover Applications	Discovering applications
Modify Application Profile	Adding components to an application profile Adding critical component groups to an application profile



	Adding discrete applications to an application profile
Test Application Profile	Testing components
Create Instance	Creating an application instance

## Application Components

Refer to the table below for step-by-step instructions for each configuration process in the flow chart.



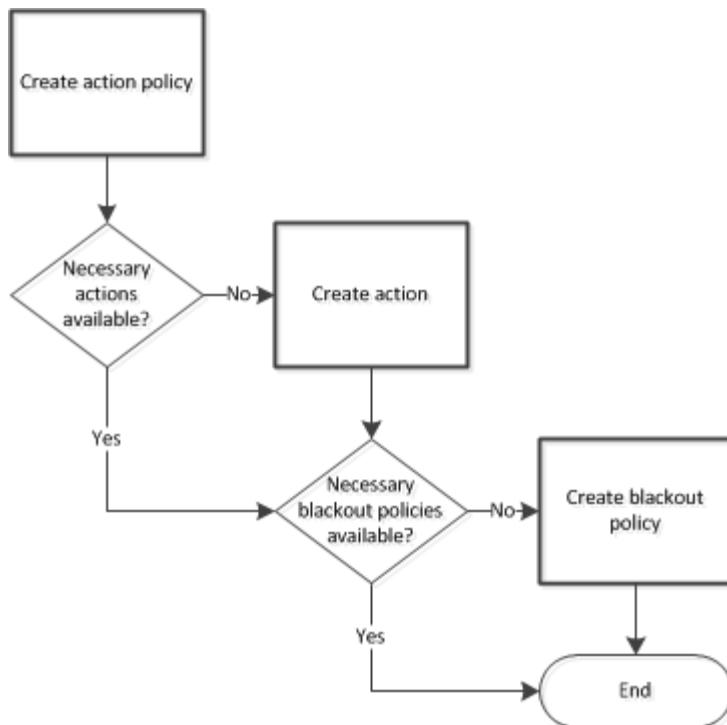
Add Components

Adding components

Create Critical Component Group	Adding critical component groups to an application profile Adding critical component groups to an application instance
Add Application	Adding discrete applications to an application profile
Test Components	Testing components

## Action Policies

Refer to the table below for step-by-step instructions for each configuration process in the flow chart.



Create Action Policy

Creating an action policy

Create Action

Creating an action

Create Blackout Policy

Creating a blackout policy

## Discovering applications

You can discover applications on and create application instances for devices previously added to Network Performance Monitor using APM. To be discoverable, an application must have at least one discoverable service or process component associated with its profile.



**Important:** Ensure the **Use in discovery** option is selected when adding or editing Windows service or process components within the application profile.

### To discover applications:

- 1 Click the **APM** tab, then select **Configuration**.
- 2 Initiate application discovery:
  - a) Select an application profile and click **Discover Applications**.
  - b) Select an application type, use the selection boxes at left to specify which applications you want to discover, and select **Discover applications** from the **For selected** menu.
  - c) Select an application type and then choose **Discover applications** from the **Options** menu at right.

A navigation tree appears mirroring your device list which displays dynamic groups and discovery scans.



**Note:** If a dialog appears indicating, "*Some of the Application Profiles you selected do not have discoverable components and will not be included in the search.*", click **OK**.

- 3 Select the groups and/or devices for which you want to discover applications by clicking the applicable check boxes in the navigation tree.
- 4 Click **Discover applications**. The Application Discovery: Discovery Results page appears.

After applications are discovered by APM, use the list of newly discovered applications to select which ones to monitor and subsequently create application instances.

### To monitor newly-discovered applications:

- 1 Identify an application on the list you want to begin monitoring and click **Start monitoring**. A Start Monitoring Application dialog appears and APM automatically begins testing the application profile components.
- 2 Use the Start Monitoring Application dialog to make any desired changes to the instance you are creating. The dialog contains the following information:
  - § **Name.** Use this box to modify the default name of the application instance.
  - § **Action Policy.** Use this list to select an action policy to be applied to the application instance.
  - § **TEST Timeout.** Use this box to indicate how long a component test should run prior to timeout.
  - § **Test Components.** Use this button to immediately initiate component testing.
  - § **Enabled.** Use these check boxes to enable or disable individual components for the Application instance.
  - § **Warning Threshold.** Use this box to indicate when APM reports the component is experiencing a problem.

- § **Down Threshold.** Use this box to indicate when APM reports the component as 'Down'.
- 3 Click **Finish** to save the application instance.
- 4 Close the dialog to return to the Application Discovery: Discovery Results page.
- 5 Repeat these procedures as needed to create additional application instances.

# Dashboards and Reports

## In This Chapter

Viewing APM status.....	10
Working with application states.....	18
APM dashboard reports.....	19

## Viewing APM status

The APM Status page allows you to view the performance status for the applications you are currently monitoring with APM. To view the APM Status page, click the **APM** tab, then select **Status**.

At left, the APM navigation tree displays a hierarchal view of the application data currently configured with a root view of "All Applications" at the top. From "All Applications", you have the ability to drill down through the following information:

- § **Application Type.** Groups application profiles, instances, and components by the type of application (e.g. SQL Server, IIS, Windows 2008 Server).
- § **Profile.** Groups the instances and components by the profile used to create the individual instance. Where the data points being monitored are different between two versions of the same application, there may be separate application profiles for each version.
- § **Instance.** Groups the components used to monitor the individual data points described in the profile.
- § **Component.** Details each component used to monitor the data points associated with the application instance.

The remainder of the page is divided into two sections, *Current Status* (on page 10) and *Historical Status* (on page 11).

### APM current status

The **Current Status** section of the status page provides information about the current state (Up, Down, Warning, Maintenance, or Unknown) of monitored applications and components as well as the running action policies. The information in this section is based on any information provided by APM during the latest poll of the components making up the instance or instances within the selected scope. The reports available in the Current Status section are listed below:

- § **Application State Summary.** Provides a pie-chart of the percentage of the instances of the selected application or application type that are in a particular state (Up, Down, Warning, Maintenance, or Unknown), and a grid with each instance in the selected application grouping, its current state, and amount of time the instance has been in that state.



**Tip:** Click a section of the pie chart representing an individual state to view only items in that state in the grid.

- § **Running Action Policies.** Provides a list of all of the action policies that have been configured and assigned to an instance or component.

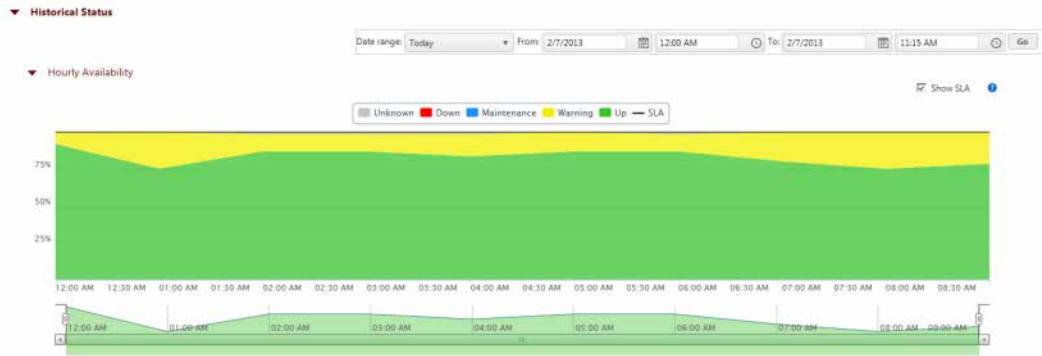
## APM historical status

The **Historical Status** section of the status page provides data about the availability, state change, actions, and resolved items during a defined time period. The reports available in the Historical Status section are listed below:

- § **Hourly Availability.** Displays the percentage of the application instances or components that were in each state (Up, Down, Warning, Maintenance, Disabled, or Unknown) over the defined time period.
- § **Instance Summary.** Displays availability information about the instances associated with all applications, a specific application type or profile for the defined time period.
- § **State Change Log.** Displays a chronological log of the changes in state for the instances in the selected application or profile, or the state of the components if a profile is selected, or the selected component.
- § **Action Log.** Displays a chronological log of all actions that were fired within the defined time period.
- § **Resolved Items Log.** Displays a chronological log of the Action Policies that were acknowledged in the Running Action Policies report during the defined time period for all instances or components in the selected application, or profile; or for the selected component, when a single component is selected.

## Hourly Availability

The Hourly Availability report displays the percentage of the application instances or components that were in each state (Up, Down, Warning, Maintenance, Disabled, or Unknown) over the defined time period. The scope of this report is defined by the scope you select. The following table describes the information that is displayed at each level in the Application Tree.



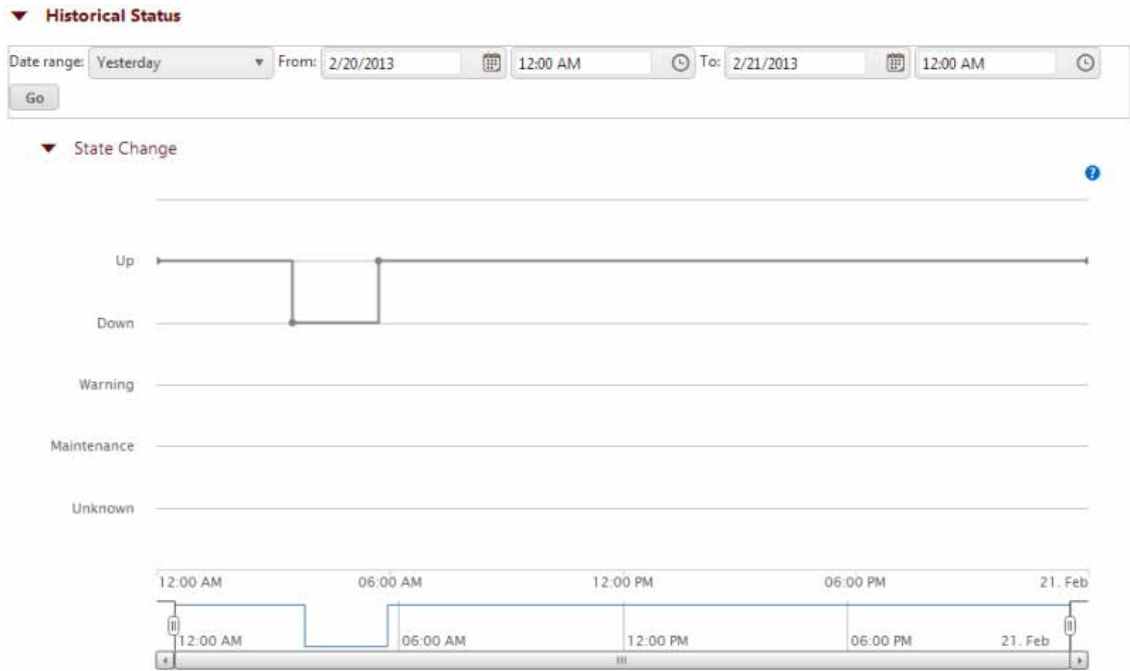
Scope	Displays:
<b>All Applications</b>	Percentage of all instances monitored by APM that are in each state over the defined time period.
<b>Application Type</b>	Percentage of instances of the selected application type that are in a given state
<b>Profile</b>	Percentage of all instances created from the selected profile that are in a given state.
<b>Instance</b>	Component State Summary report is visible when Instance is selected.
<b>Component</b>	Not available.

Use the sliders located below the graph to zoom in on a particular time in the defined range.

Click **Show SLA** to display the SLA percentage threshold set in the *APM Application Settings* (on page 92) as a single line within the graph.

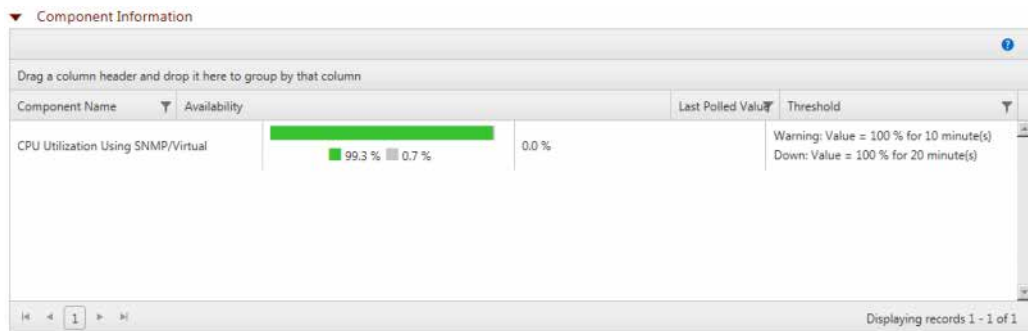
## State Change

The State Change report displays state changes that the selected component underwent during the defined time period. This report is used for components that directly return their state when polled. Use the sliders located below the graph to zoom in on a particular time in the defined range.



## Component Summary

The Component Information report displays current state, availability information for the defined time period, last polled value and threshold information used to determine the Warning and Down state for the selected component when APM manages the component's state based on values evaluated by thresholds defined in APM.



- § **Current State.** Displays the current state (Up, Down, Warning, Maintenance, Disabled, or Unknown) of the component.
- § **Component Name.** Displays the name of the component.
- § **Availability.** Displays percentage of time that the component was in each state (Up, Down, Warning, Maintenance and Unknown) during the defined time period.



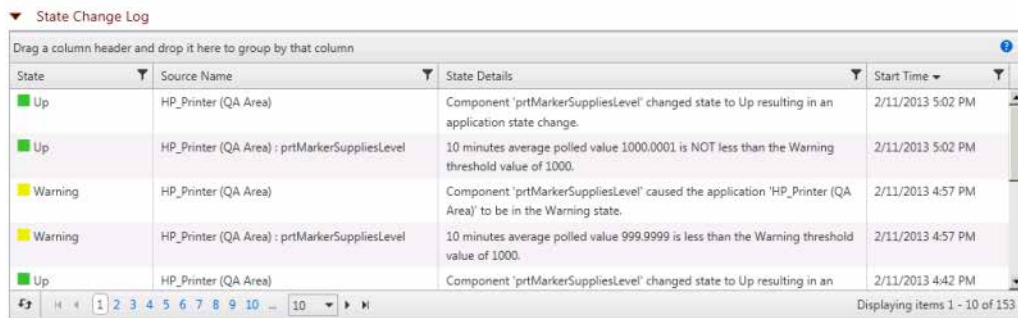
- § **Last Polled Value.** Displays the last polled value. This is the current state for components that return state, and a value for those that return a value.
- § **Threshold.** Displays the Down and Warning threshold settings for components for which APM performs state evaluations.

### Grouping and filtering data

You can group the Component Information grid report by any column. To group the output by a column, drag a column header to the grid header. You can group by more than one criteria by dragging more than one column header to the grid header. The grid is ordered by all of the groupings appearing in the grid header, from left to right. To remove a grouping, close the grouping you want to remove.

### State Change Log

The State Change Log, displays a chronological log of the changes in state for the instances in the selected application, or profile; or for the selected component, when a single component is selected.




State	Source Name	State Details	Start Time
Up	HP_Printer (QA Area)	Component 'prtMarkerSuppliesLevel' changed state to Up resulting in an application state change.	2/11/2013 5:02 PM
Up	HP_Printer (QA Area) : prtMarkerSuppliesLevel	10 minutes average polled value 1000.0001 is NOT less than the Warning threshold value of 1000.	2/11/2013 5:02 PM
Warning	HP_Printer (QA Area)	Component 'prtMarkerSuppliesLevel' caused the application 'HP_Printer (QA Area)' to be in the Warning state.	2/11/2013 4:57 PM
Warning	HP_Printer (QA Area) : prtMarkerSuppliesLevel	10 minutes average polled value 999.9999 is less than the Warning threshold value of 1000.	2/11/2013 4:57 PM
Up	HP_Printer (QA Area)	Component 'prtMarkerSuppliesLevel' changed state to Up resulting in an	2/11/2013 4:42 PM

- § **State.** Displays the state (Up, Down, Warning, Maintenance, Disabled, or Unknown) to which the instance or component entered at the start time.
- § **Source Name.** Displays the name of the instance or component.
- § **State Details.** Displays details gathered about the state change.
- § **Start Time.** Displays the time which the source entered the indicated state.


### Grouping and filtering data

You can group the State Change Log by any column. To group the output by a column, drag a column header to the grid header. You can group by more than one criteria by dragging more than one column header to the grid header. The grid is ordered by all of the groupings appearing in the grid header, from left to right. To remove a grouping, close the grouping you want to remove.

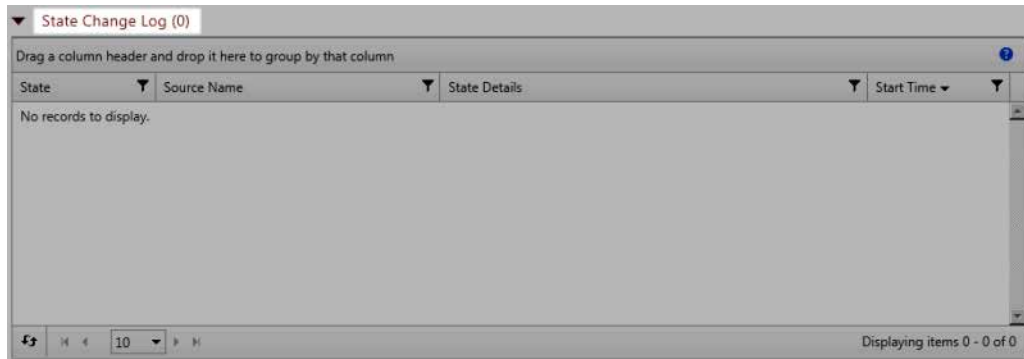
You can also filter the State Change Log based on criteria defined using the filter icon  in each column.

The Polled Values report is used to display data from components that return values when polled to which APM applies thresholds to determine the state.

### To filter the report:

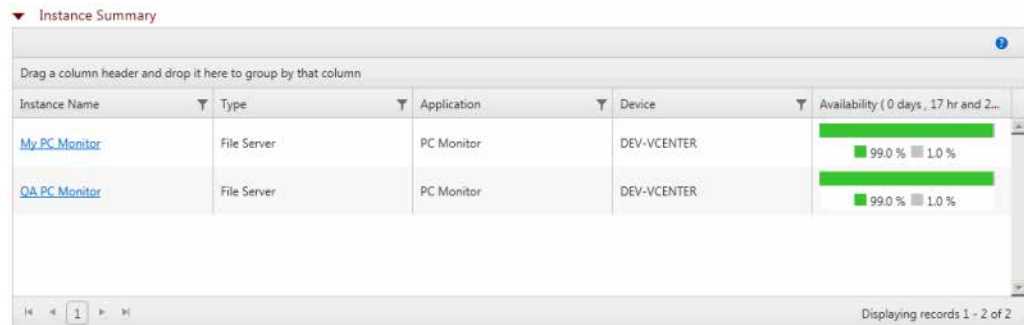
- 1 Click the filter icon  in the column containing the value on which you want to filter. The filter creation dialog appears.
- 2 Select the filter operation you want to use to create the filter criteria.
- 3 Enter the value you want the filter operation to use to create the filter criteria.
- 4 Click **Filter** to apply the filter to the entries in the report.

If no state changes have taken place, the number zero is displayed in parenthesis next to the report title.



## Instance Summary

The Instance Summary report displays availability information about the instances associated with all applications, a specific application type, or profile for the defined time period.



The screenshot shows a report titled "Instance Summary". The header includes columns for Instance Name, Type, Application, Device, and Availability (0 days, 17 hr and 2...). The main area contains two rows of data:

Instance Name	Type	Application	Device	Availability (0 days, 17 hr and 2...)
<a href="#">My_PC_Monitor</a>	File Server	PC Monitor	DEV-VCENTER	99.0 % 1.0 %
<a href="#">QA_PC_Monitor</a>	File Server	PC Monitor	DEV-VCENTER	99.0 % 1.0 %


The footer shows "Displaying records 1 - 2 of 2".

- § **Instance Name.** Displays the name of the instance.
- § **Type.** Displays the application type.
- § **Application.** Displays the application name.
- § **Device.** Displays the WhatsUp Gold device to which the instance is associated.
- § **Availability.** Displays percentage of time that the instance was in each state (Up, Down, Warning, Maintenance and Unknown) during the defined time period.
- § **Running Actions.** Displays the number of actions that were in a running state during the defined time period.

## Grouping and filtering data

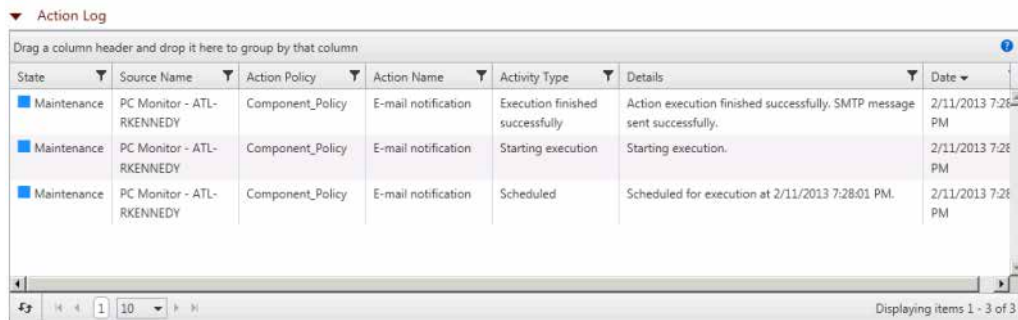
You can group the Instance Summary grid report by any column. To group the output by a column, drag a column header to the grid header. You can group by more than one criteria by dragging more than one column header to the grid header. The grid is ordered by all of

the groupings appearing in the grid header, from left to right. To remove a grouping, close the grouping you want to remove.

You can also filter the Instance Summary grid report based on criteria defined using the filter icon  in each column.

## Action Log

The Action Log displays a chronological log of the actions associated with all instances or components in the selected application, or profile; or for the selected component, when a single component is selected.




State	Source Name	Action Policy	Action Name	Activity Type	Details	Date
Maintenance	PC Monitor - ATL-RKENNEDY	Component_Policy	E-mail notification	Execution finished successfully	Action execution finished successfully. SMTP message sent successfully.	2/11/2013 7:28 PM
Maintenance	PC Monitor - ATL-RKENNEDY	Component_Policy	E-mail notification	Starting execution	Starting execution.	2/11/2013 7:28 PM
Maintenance	PC Monitor - ATL-RKENNEDY	Component_Policy	E-mail notification	Scheduled	Scheduled for execution at 2/11/2013 7:28:01 PM.	2/11/2013 7:28 PM


- § **State.** Displays the state (Up, Down, Warning, Maintenance, Disabled, or Unknown) which the instance or component was in when the Action was executed.
- § **Source Name.** Displays the name of the instance or component that triggered the action.
- § **Action Policy.** Displays the name of the action policy which contains the action.
- § **Action Name.** Displays the name of the action.
- § **Activity Type.** Displays the activity type that describes the state of the action policy at the time of the state change.
- § **Details.** Displays the details gathered by APM about the action.
- § **Date.** Displays the date and time that the action was executed.

## Grouping and filtering data

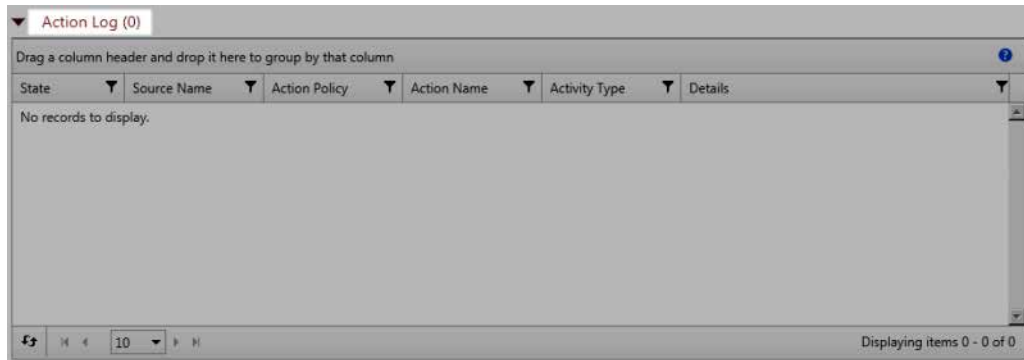
You can group the Action Log report by any column. To group the output by a column, drag a column header to the grid header. You can group by more than one criteria by dragging more than one column header to the grid header. The grid is ordered by all of the groupings appearing in the grid header, from left to right. To remove a grouping, close the grouping you want to remove.

You can also filter the Action Log report based on criteria defined using the filter icon  in each column.

### To filter the report:

- 1 Click the filter icon  in the column containing the value on which you want to filter. The filter creation dialog appears.
- 2 Select the filter operation you want to use to create the filter criteria.
- 3 Enter the value you want the filter operation to use to create the filter criteria.

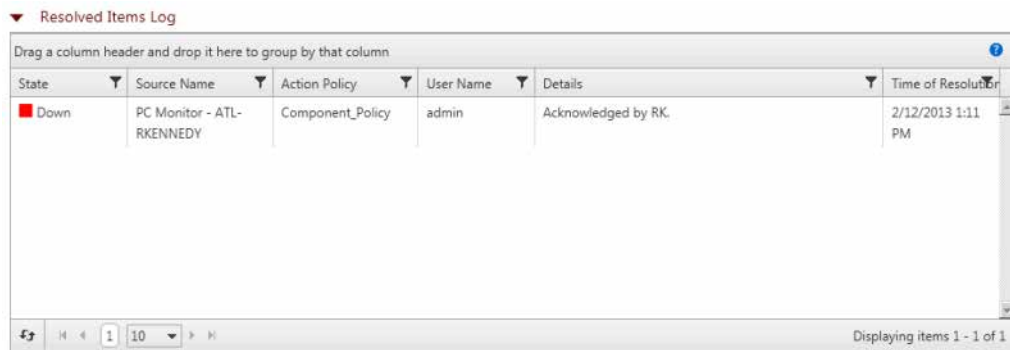
If no actions have been fired for policy, instance, or component, the number zero is displayed in parenthesis next to the report title.



- 4 Click **Filter** to apply the filter to the entries in the report.

## Resolved Actions Log

The Resolved Items Log displays a chronological log of the Action Policies that were acknowledged in the Running Action Policies report during the defined time period for all instances or components in the selected application, or profile; or for the selected component, when a single component is selected.



The screenshot shows a report titled "Resolved Items Log". The report header includes a search bar and a table with columns: State, Source Name, Action Policy, User Name, Details, and Time of Resolution. The table contains one record with the following data:

State	Source Name	Action Policy	User Name	Details	Time of Resolution
Down	PC Monitor - ATL-RKENNEDY	Component_Policy	admin	Acknowledged by RK.	2/12/2013 1:11 PM


The footer shows "Displaying items 1 - 1 of 1".

- § **State.** Displays the state (Up, Down, Warning, Maintenance, Disabled, or Unknown) which the instance or component was in when the Action Policy was Acknowledged.
- § **Source Name.** Displays the name of the instance or component that triggered the action.
- § **Action Policy.** Displays the name of the Action Policy which was Acknowledged in the Running Action Policies report.
- § **User Name.** Displays the name of the user who acknowledged the Action Policy in the Running Action Policies report.
- § **Details.** Displays the details entered by the user to describe the reason for Acknowledging the Action Policy.
- § **Time of Resolution.** Displays the date and time that the user acknowledged the Action Policy.


## Grouping and filtering data

You can group the Resolved Items Log report by any column. To group the output by a column, drag a column header to the grid header. You can group by more than one criteria

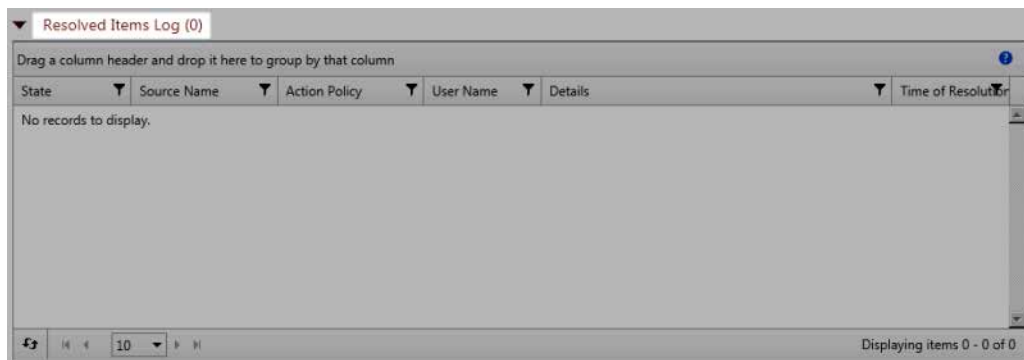
by dragging more than one column header to the grid header. The grid is ordered by all of the groupings appearing in the grid header, from left to right. To remove a grouping, close the grouping you want to remove.

You can also filter the Resolved Items log based on criteria defined using the filter icon  to in each column.

**To filter the report:**

- 1 Click the filter icon  in the column containing the value on which you want to filter. The filter creation dialog appears.
- 2 Select the filter operation you want to use to create the filter criteria.
- 3 Enter the value you want the filter operation to use to create the filter criteria.
- 4 Click **Filter** to apply the filter to the entries in the report.

If no policies that have run for the policy, instance, or component have been acknowledged, the number zero is displayed in parenthesis next to the report title.



## Working with application states

Applications can have the following states:

- § **Up** (Green). The Up state indicates that all of the monitored components, critical component groups and applications that are defined in the application instance are up.
- § **Down** (Red). The Down state indicates that one or more of an application's critical components, component groups or applications has exceeded its down threshold.
- § **Warning** (Yellow). The Warning state indicates that one or more non-critical component or application has entered the down state.
- § **Unknown** (Gray). The Unknown state indicates that the state of the component or application cannot be determined.
- § **Maintenance** (Blue). The Maintenance state indicates that one or more component or application has been placed into a Maintenance state.

Components marked as critical cause the application to go into a Down state if the component is out of threshold. Non-critical components cause the application to go into a Warning state, unless all components are down, in which case the application goes into the

Down state. Additionally, while groups are always evaluated as critical, Discreet applications within a complex application are not always critical.

# APM dashboard reports

In addition to the application monitoring data available under *Viewing APM status* (on page 10), you can also add individual APM dashboard reports custom dashboards you create in WhatsUp Gold. The *APM State Summary* (on page 19) and *Application Event Log* (on page 19) dashboard reports can be added to the WhatsUp Gold home page.

## APM State Summary dashboard report

The State Summary dashboard report displays a pie chart depicting the application state of a selected application profile type, application profile, or application instance.

**To configure the State Summary dashboard report:**

- 1 Add the dashboard report to a custom dashboard view. See Adding dashboard reports to a dashboard view for detailed procedures.
- 2 Click **Menu > Configure** to launch the Configure Report dialog.
- 3 Select an APM Source.



**Important:** The APM Source selection can be an application profile type, application profile, or application instance. Summary data for any profile type, application profile, or application instance selected includes data for all components and groups under your selection in the navigation tree.



**Note:** You can also modify the Report name displayed as well as the size of the dashboard report using this dialog.

- 4 Click **OK**.

## Application Event Log dashboard report

The Application Event Log dashboard report displays state change, action activity and action resolution information for a selected application profile type, application profile, or application instance.

**To configure the Application Event Log dashboard report:**

- 1 Add the dashboard report to a custom dashboard view. See Adding dashboard reports to a dashboard view for detailed procedures.
- 2 Click **Menu > Configure** to launch the Configure Report dialog.
- 3 Select an APM Source.



**Important:** The APM Source selection can be an application profile type, application profile, or application instance. Summary data for any profile type, application profile, or application instance selected includes data for all components and groups under your selection in the navigation tree.

#### 4 Click **OK**.

You can also modify the Report name displayed, the maximum number of items displayed, and the size of the dashboard report using this dialog. You can also disable specific event log types from displaying within the dashboard report by deselecting the applicable check box(es) in the configuration dialog. Applicable event log types are State Change, Action Activity, and Resolved Action. Additionally, enable **Show Source Type Column** to display the source of the state change or action for your selection within the dashboard report.

# Configuration and Settings

## In This Chapter

Application Profiles.....	21
Action policies.....	77
Actions.....	81
Blackout policies.....	92
Configuring APM application settings.....	92

## Application Profiles

The APM All Application Profiles page allows you to add new or configure existing application profiles. To view the APM All Application Profiles page, click the **APM** tab, then select **Configuration**. From this page, you can:

- § Create and add new application profiles.
- § Import shared application profiles from the WUGspace Community.

Additionally, for existing application profiles displayed, you can:

- § Add application instances.
- § Define application attributes.
- § Make configuration changes.
- § Export application profiles in.xml format.
- § Publish application profiles to the WUGSpace Community.
- § Copy application profiles.
- § Delete application profiles.



**Important:** In order to perform these functions, you must have the Configure APM Application Profiles user right enabled.

For additional information on these profile features, see *Working with existing application profiles* (on page 23).

## Adding an application profile

To add a new application profile to APM:

- 1 Click the **APM** tab, then select **Configuration**.



- 2 Select **All Application Profiles** or any application profile type displayed in the APM navigation tree and click **Add Application Profile**. The Configure New Application Profile page appears.
- 3 Configure the following:
  - § Enter a **Name**, **Version**, and **Description** for the application.
  - § Select the application type from the **Type** list.



**Note:** If you clicked **Add Application Profile** from a specific application profile type rather than from the All Application Profiles root, that application type is populated by default in the **Type** list.

- § Select any **Attributes (on page 76)** to apply to the profile if desired.
- § Select a configured action policy using the **Action Policy** list to apply to the profile, if desired.
- § Click the Browse button (...) and use the dialog displaying the device tree that appears to select a test device for the profile.
- § Specify the maximum duration in seconds before the test will time out in the **TEST Timeout** field.
- § Click **Save**.

In addition to these basic profile configuration elements, you can also use the controls on the Components grid on this page to:

- § Add components to or remove components from the profile.
- § Create critical component groups.
- § Create copies of components within the profile.
- § Test any or all components within the profile.
- § Modify the polling frequency for one or more components within the profile.

For more information, see Components.

## Importing an application profile

To import application profiles to APM from the WUGspace Community:

- 1 Click the **APM** tab, then select **Configuration**.
- 2 Select **All Application Profiles** or any application profile type displayed in the APM navigation tree.
- 3 Select **Import > From Community**. The WUGspace access dialog appears.



**Tip:** You can also select **Import > From Disk** to browse to and import an application profile stored on an accessible local or network location.

- 4 Enter your account credentials and click **Sign In** to access WUGspace.
- 5 Use the selection boxes at left to specify which application profile you want to import.

### 6 Click **Import Selected**.



**Tip:** You can also click **Download Selected** to save the application profile for later use.

### 7 When the profile import is complete, click **OK** to return to APM.



**Important:** When an *attribute* (on page 76) is applied to an application profile, it is automatically included when that profile is imported into or exported from APM by another end-user.

## Working with existing application profiles

### To edit an application profile:

- 1 Select the application profile you want to modify from the APM Application Tree.
- 2 Click **Edit Application Profile**.
- 3 Make the necessary changes to the profile and/or associated components.
- 4 Click **Save**.

### To export an application profile:

- 1 Select the application profile you want to export from APM.
- 2 Select **Export** from the Options menu for the applicable profile. An .xml file containing the application profile code downloads to your computer.



**Important:** When an attribute is applied to an application profile, it is automatically included when that profile is imported into or exported from APM by another end-user.

### To publish an application profile for use within the WUGspace Community:

- 1 Select the application profile you want to publish to WUGspace.
- 2 Select **Publish** from the Options menu for the applicable profile. The WUGspace access dialog appears.
- 3 Enter your account credentials and click **Sign In** to access WUGspace.
- 4 Enter a **Submission Title** and **Submission Description** for the profile.
- 5 Click **Publish to Community**.

### To copy an application profile:

- 1 Select the application profile you want to copy from the application profile tree at left.
- 2 If the application profile is Ipswitch-provided and/or read-only, click **Edit a copy** to the right of **View Application Profile**.  
OR  
Select **Copy** from the Options menu for the applicable profile. The Configure New Application Profile page appears with the attributes of the profile being copied prepopulated.
- 3 Configure the profile copy as if you were creating a new application profile.
- 4 Click **Save**.

### To delete an application profile:

- 1 Select the application profile you want to delete.
- 2 Select **Delete** from the Options menu for the applicable profile.

## Managing application instances

An application instance is a running copy of an application profile that monitors the defined collection of components, distinct applications, and thresholds necessary to define the health and performance of a given type of application. An application instance can *extend* the application profile by adding components, component groups, or discrete applications. The application profile is *not* changed when an application instance is extended.



**Important:** In order to perform these procedures, you must have the Configure APM Application Instances user right enabled.

### To create an instance for monitoring an application on a specific device:

- 1 Select an application type displayed on the APM All Application Profiles page and then select **New Instance** from the Options menu for the applicable profile.

OR

Select an application profile displayed on the APM All Application Profiles page and click **Add Application Instance**. The Configure New Application Instance page appears.

- 2 Configure the following:
  - § Enter a **Name** and **Description** for the application instance.
  - § Select any **Attributes (on page 76)** to apply to the instance if desired.
  - § Click the Browse button (...) and use the dialog displaying the device tree that appears to select a test device for the instance.
  - § Specify the maximum duration in seconds before the test will time out in the **TEST Timeout** field.
  - § Select a configured action policy using the **Action Policy** list to apply to the instance, if desired.
  - § Enable the **In Maintenance** option to place the instance in maintenance mode. While in maintenance mode, the application instance will not be monitored.

In addition to these basic instance configuration elements, you can also use the controls on the Components grid on this page to:

- § Add components to or remove components from the instance.
- § Create critical component groups.
- § Create copies of components within the instance.
- § Test any or all components within the instance.
- § Modify the polling frequency for one or more components within the instance

For more information, see Components.

## Managing application components

A component is a single data point collected as part of an application profile. Some application profiles can be edited, in which case individual components can be added to or removed from the profile. For editable application profiles, components can also be added to or removed from specific instances as opposed to the entire profile.

Adding components to an application profile helps create the foundation of the application profile. After adding components to an application profile, you must create an application instance to monitor an application on a device.

### To add components:

- 1 Select an application profile displayed on the APM All Application Profiles page, click **Edit Application Profile**, and then click **Add components**. If the application profile does not allow for the addition/removal of components, **View Application Profile** is seen in place of **Edit Application Profile**.

OR

Select a specific instance and then click **Add components**. Individual components can be added to specific instances even if the application profile overall is not editable. The Add Components dialog containing the Component Library appears.

- 2 Click the icon to the left of the component types you want to add to the application profile or instance. This expands the Component Library to display available component options.
- 3 Use the up and down arrows to specify the number of components of each type to add.
- 4 Click **Add Selected**. Configuration dialogs for each added component appear in the Component grid.
- 5 Use the **Test Device** browse button (...) to select a specific device on which to test a component if desired. If no test device is selected, the component is tested on the test device associated with the application profile. Test devices are not saved as part of the application profile.
- 6 Configure each component as needed. Component configuration fields will vary depending upon type. Refer to the following for individual component descriptions and their specific configuration fields:

- |                                       |   |
|---------------------------------------|---|
| § CPU Utilization (on page 26)        | § Database Query (on page 27)               |
| § Disk Utilization (on page 28)       | § Memory Utilization (on page 30)           |
| § Interface Statistics (on page 29)   | § Process Check (on page 55)                |
| § Network Port Check (on page 31)     | § Service Check (on page 66)                |
| § Scripting (PowerShell) (on page 56) | § Scripting (End User Monitor) (on page 57) |

- § SNMP (on page 67)
- § SSH (on page 68)
- § WMI (on page 70)
- § Windows Performance Counter (on page 71)

### 7 Click **Save**.

To remove a component from an application profile or instance, select **Delete** from the applicable **Options** menu.

### To test components:

- § Click the applicable **Test** button to test a single component.
- § Click **Test all** to test every component.
- § Use the selection boxes at left to select components and then select **For selected > Test** to test multiple components.

To copy components and critical component groups, select **Copy** from the Options menu of the individual component or critical component group you want to duplicate.

## CPU Utilization

The CPU Utilization component allows you to monitor the percentage of CPU being used on a particular device and alerts you if certain thresholds are exceeded. CPU Utilization components using either SNMP/Virtual or WMI credentials may be added to an application profile or an application instance.

Configure the following for the CPU Utilization component:

- § **Name.** Enter a unique name for the component.
- § **Description.** Enter additional information about the component.
- § **Critical.** Click to select this check box if the component is critical.



**Note:** Components specified as critical cause the application to go into a down state when the component is out of threshold. Non-critical components cause the application to go into a warning state. For more information on application states, see Working with application states.

- § **Polling frequency.** Select a time (in minutes or hours) you want APM to wait between polls.
- § **Polling timeout.** Enter the length of time APM attempts to connect to the selected device. When the time you enter is exceeded without connecting, a timeout occurs and APM stops trying to connect to the device. This is considered a failed connection.
- § **Poller retries.** (SNMP Only) Enter the number of times APM attempts to send the command before the device is considered down.
- § **Warning threshold.** Enter the component thresholds for the warning state. For example, if the component value is greater than 90 percent for 5 minutes, put the component in the warning state.
- § **Down threshold.** Enter the component thresholds for the down state. For example, if the component value is greater than 95 percent for 5 minutes, put the component in the down state.

### Database Query

There are two types of database components you can configure depending on your database server:

- § The *Oracle Query Check* (on page 27) component allows you to create a query to run on a specific device to assess the health of an Oracle database. You may add an Oracle Query component to either an application profile or an application instance.
- § The *Microsoft SQL Server Query Check* (on page 28) component provides you with real-time information about the state and health of a Microsoft® SQL Server application on a specific device. You may add a SQL Server Query component to either an application profile or an application instance.

### Database Query (Oracle)

The **Oracle Query Check** component allows you to create a query to run on a specific device to assess the health of an Oracle database. You may add an Oracle Query component to either an application profile or an application instance.

Configure the following for database components:

- § **Name.** Enter a unique name for the component.
- § **Description.** Enter additional information about the component.
- § **Critical.** Click to select this check box if the component is critical.



**Note:** Components specified as critical cause the application to go into a down state when the component is out of threshold. Non-critical components cause the application to go into a warning state. For more information on application states, see *Working with application states*.

- § **Polling frequency.** Select a time (in minutes or hours) you want APM to wait between polls.
- § **Port.** Enter the database server port number if other than the standard database port number.
- § **Connection timeout.** Enter the length of time APM attempts to connect to the selected device. When the time you enter is exceeded without connecting, a timeout occurs and APM stops trying to connect to the device. This is considered a failed connection.
- § **Query to Run.** Enter a query you want to run against a database to monitor and check for certain database conditions. Only SQL SELECT queries are allowed.



**Important:** Make sure that you include the full database name in your query.

- § **Warning threshold.** Enter the component thresholds for the warning state. For example, if the component value is greater than 90 for 5 minutes, put the component in the warning state.
- § **Down threshold.** Enter the component thresholds for the down state. For example, if the component value is greater than 95 for 5 minutes, put the component in the down state.

### Database Query (Microsoft SQL Server)

The **Microsoft SQL Server Query Check** component provides you with real-time information about the state and health of a Microsoft® SQL Server application on a specific device. You may add a SQL Server Query component to either an application profile or an application instance.

Configure the following for database components:

- § **Name.** Enter a unique name for the component.
- § **Description.** Enter additional information about the component.
- § **Critical.** Click to select this check box if the component is critical.



**Note:** Components specified as critical cause the application to go into a down state when the component is out of threshold. Non-critical components cause the application to go into a warning state. For more information on application states, see *Working with application states*.

- § **Polling frequency.** Select a time (in minutes or hours) you want APM to wait between polls.
- § **Port.** Enter the database server port number if other than the standard database port number.
- § **Connection timeout.** Enter the length of time APM attempts to connect to the selected device. When the time you enter is exceeded without connecting, a timeout occurs and APM stops trying to connect to the device. This is considered a failed connection.
- § **Query to Run.** Enter a query you want to run against a database to monitor and check for certain database conditions. Only SQL SELECT queries are allowed.



**Important:** Make sure that you include the full database name in your query.

- § **Warning threshold.** Enter the component thresholds for the warning state. For example, if the component value is greater than 90 for 5 minutes, put the component in the warning state.
- § **Down threshold.** Enter the component thresholds for the down state. For example, if the component value is greater than 95 for 5 minutes, put the component in the down state.

### Disk Utilization

The Disk Utilization component allows you to monitor the percentage of disk space being utilized on a specific device. Disk Utilization components using either SNMP/Virtual or WMI credentials may be added to an application profile or an application instance.

Configure the following for the Disk Utilization component:

- § **Name.** Enter a unique name for the component.
- § **Description.** Enter additional information about the component.
- § **Critical.** Click to select this check box if the component is critical.



**Note:** Components specified as critical cause the application to go into a down state when the component is out of threshold. Non-critical components cause the application to go into a warning state. For more information on application states, see *Working with application states*.

- § **Polling frequency.** Select a time (in minutes or hours) you want APM to wait between polls.
- § **Polling timeout.** (SNMP Only) Enter the length of time APM attempts to connect to the selected device. When the time you enter is exceeded without connecting, a timeout occurs and APM stops trying to connect to the device. This is considered a failed connection.
- § **Poller retries.** (SNMP Only) Enter the number of times APM attempts to send the command before the device is considered down.
- § **Warning threshold.** Enter the component thresholds for the warning state. For example, if the component value is greater than 90 percent for 5 minutes, put the component in the warning state.
- § **Down threshold.** Enter the component thresholds for the down state. For example, if the component value is greater than 95 percent for 5 minutes, put the component in the down state.

### Interface Statistics

There are three types of Interface components you can configure:

- § The **Interface Utilization In/Out** components allow you to monitor the percentage of in or out utilization on a specific device interface. You may add an Interface Utilization In/Out component to an application profile or an application instance.
- § The **Interface Errors In/Out** components allow you to monitor the number of in or out errors on a specific device interface. You may add an Interface Errors In/Out component to an application profile or an application instance.
- § The **Interface Discards In/Out** components allow you to monitor the number inbound or outbound packets which were chosen to be discarded on a specific device interface. You may add an Interface Discards In/Out component to an application profile or an application instance.

Configure the following for the Interface component:

- § **Name.** Enter a unique name for the component.
- § **Description.** Enter additional information about the component.
- § **Critical.** Click to select this check box if the component is critical.



**Note:** Components specified as critical cause the application to go into a down state when the component goes into a down state. When non-critical components go into a down state, they cause the application to go into a warning state. For more information on application states, see *Working with application states*.

- § **Polling frequency.** Select a time (in minutes or hours) you want APM to wait between polls.



- § **Polling timeout.** Enter the length of time APM attempts to connect to the selected device. When the time you enter is exceeded without connecting, a timeout occurs and APM stops trying to connect to the device. This is considered a failed connection.
- § **Poller retries.** Enter the number of times APM attempts to send the command before the device is considered down.
- § **Warning threshold.** Enter the component thresholds for the warning state. For example, if the component value is greater than 90 for 5 minutes, put the component in the warning state.
- § **Down threshold.** Enter the component thresholds for the down state. For example, if the component value is greater than 95 for 5 minutes, put the component in the down state.

### Memory Utilization

Memory Utilization components allows you to monitor the percentage or absolute amount of either *physical* (on page 30) or *virtual* (on page 30) memory being utilized on a specific device. In addition to specifying if the component monitors physical or virtual memory, you must also indicate if the component uses SNMP/Virtual or WMI credentials to access the test device.

### Memory Utilization

Configure the following for the Physical Memory component:

- § **Name.** Enter a unique name for the component.
- § **Description.** Enter additional information about the component.
- § **Critical.** Click to select this check box if the component is critical.



**Note:** Components specified as critical cause the application to go into a down state when the component is out of threshold. Non-critical components cause the application to go into a warning state. For more information on application states, see Working with application states.

- § **Polling frequency.** Select a time (in minutes or hours) you want APM to wait between polls.
- § **Polling timeout.** Enter the length of time APM attempts to connect to the selected device. When the time you enter is exceeded without connecting, a timeout occurs and APM stops trying to connect to the device. This is considered a failed connection.
- § **Poller retries.** Enter the number of times APM attempts to send the command before the device is considered down.
- § **Warning threshold.** Enter the component thresholds for the warning state. For example, if the component value is greater than 90 percent for 5 minutes, put the component in the warning state.
- § **Down threshold.** Enter the component thresholds for the down state. For example, if the component value is greater than 95 percent for 5 minutes, put the component in the down state.

### Memory Utilization (Virtual)

Configure the following for the Virtual Memory component:

- § **Name.** Enter a unique name for the component.

§ **Description.** Enter additional information about the component.

§ **Critical.** Click to select this check box if the component is critical.



**Note:** Components specified as critical cause the application to go into a down state when the component is out of threshold. Non-critical components cause the application to go into a warning state. For more information on application states, see *Working with application states*.

§ **Polling frequency.** Select a time (in minutes or hours) you want APM to wait between polls.

§ **Polling timeout.** Enter the length of time APM attempts to connect to the selected device. When the time you enter is exceeded without connecting, a timeout occurs and APM stops trying to connect to the device. This is considered a failed connection.

§ **Poller retries.** Enter the number of times APM attempts to send the command before the device is considered down.

§ **Warning threshold.** Enter the component thresholds for the warning state. For example, if the component value is greater than 90 percent for 5 minutes, put the component in the warning state.

§ **Down threshold.** Enter the component thresholds for the down state. For example, if the component value is greater than 95 percent for 5 minutes, put the component in the down state.

### Network Port Check

The Network Port Check component allows you to create a script to run on a specific device that monitors a designated TCP, UDP, or SSL network port. There are a number of options for this component type depending on the communication protocol you want to use to monitor the port:

- § Custom
- § Echo
- § FTP
- § HTTP
- § HTTPS
- § IMAP4
- § NNTP
- § POP3
- § Radius
- § SNMP
- § Time

Configure the following boxes for the Network Port Check component:

§ **Name.** Enter a unique name for the component.

§ **Description.** Enter additional information about the component.

§ **Critical.** Click to select this check box if the component is critical.



**Note:** Components specified as critical cause the application to go into a down state when the component is out of threshold. Non-critical components cause the application to go into a warning state. For more information on application states, see *Working with application states*.

- § **Polling frequency.** Select a time (in minutes or hours) you want APM to wait between polls.
- § **Protocol.** Select TCP, UDP, or SSL from the list. The network type for the FTP (File Transfer Protocol) service is TCP; the network type for the RADIUS (Remote Authentication and Dial-In User Service) service is UDP. The HTTPS monitor uses the SSL type.
- § **Port number.** Enter the port number that you want to monitor.
- § **Polling timeout.** Enter the length of time APM attempts to connect to the selected device. When the time you enter is exceeded without connecting, a timeout occurs and APM stops trying to connect to the device. This is considered a failed connection.
- § **Script to Run.** Write your script using as many `Send`, `Expect`, `SimpleExpect`, and `Flow Control` keywords as you want. For more information, see [Script Syntax](#).
- § **Expect.** (Optional) Click to open the Rules Expression Editor and test a string of text for particular patterns.

### Adding a Custom Port Check component

The Custom Port Check component allows you to create a script to run on a specific device that monitors a designated TCP, UDP, or SSL network port.



**Note:** Adding components to an application profile helps create the foundation of the application profile. After adding components to an application profile, you must create an application instance to monitor an application on a device. Learn more about APM terminology.

### To add a Custom Port Check component to an application profile:

- 1 From the WhatsUp Gold web interface, go to **APM > Configuration**. The All Application Profiles page appears.
- 2 Select the application profile for which you want to add a component, then click **Edit/View Application Profile**. The Components list appears.
- 3 Click **Add Components**. The Component Library appears.
- 4 Click the arrow next to **Network Port Check** to expand the dialog controls used to add the component(s).
- 5 Specify the number of components you want to add by clicking the up and down arrows next to **Custom**.
- 6 Click **Add Selected**.
- 7 Click browse (...) next to the TEST Device box to launch the Select a Device dialog.



- 8 Select a device from the navigation tree on which to test the individual component and click **OK**.
- 9 Click **Test** to test the component on the selected device (optional). To remove the device override and revert to the device associated with the application component, click **X**.



**Note:** If no test device is selected, the component is tested on the test device associated with the application profile.



Test devices are not saved as part of the application profile.

**10** Enter or select the appropriate information:

**11** Click **Save** to save your changes or click **Save and Close** to complete your changes.

**To add a Custom Port Check component to an application instance:**

**1** From the WhatsUp Gold web interface, go to **APM > Configuration**. The All Application Profiles page appears.

**2** Select the application instance for which you want to add a component.

**3** Click **Add Components**. The Component Library appears.

**4** Click the arrow next to **Network Port Check**, then specify the number of components you want to add by clicking the up and down arrows next to **Custom**.

**5** Click **Add Selected**.

**6** Enter or select the appropriate information:

§ **Enabled**. Select this option to enable or disable the component.

§ **Action Policy**. Select an action policy from the list for the component.

§ **Device Override**. (Optional) Override the device associated with the instance and designate a specific device to assign to the component.


§ Click browse (...) next to the Device Override box to launch the Select a Device dialog.



**Important:** If the device you want to use is configured with a WhatsUp Gold down dependency, make sure that you use a cloned device for this device selection in the APM plug-in. For more information, see the Dependencies overview.

§ Select a device from the navigation tree on which to test the individual component and click **OK**.

§ Click **Test** to test the component on the selected device.

§ **Note:** Click  to remove the device override and revert to the device associated with the application instance.

**7** Enter or select the appropriate information in the *Custom Port Check component boxes* (on page 33).

**8** Click **Save** to save your changes or click **Save and Close** to complete your changes.

### Custom Port Check component boxes

You may configure the following boxes for the Custom Port Check component:

§ **Name**. Enter a unique name for the component.

§ **Description**. (Optional) Enter additional information about the component.

§ **Critical**. Click to select this check box if the component is critical.



**Note:** Components specified as critical cause the application to go into a down state when the component is out of threshold. Non-critical components cause the application to go into a warning state. For more information on application states, see *Working with application states*.

- § **Polling frequency.** Select a time (in minutes or hours) you want APM to wait between polls.
- § **Protocol.** Select TCP, UDP, or SSL from the list. The network type for the FTP (File Transfer Protocol) service is TCP; the network type for the RADIUS (Remote Authentication and Dial-In User Service) service is UDP. The HTTPS monitor uses the SSL type.
- § **Port number.** Enter the port number that you want to monitor.
- § **Polling timeout.** Enter the length of time APM attempts to connect to the selected device. When the time you enter is exceeded without connecting, a *timeout* occurs and APM stops trying to connect to the device. This is considered a failed connection.
- § **Script to Run.** Write your script using as many `Send`, `Expect`, `SimpleExpect`, and `Flow Control` keywords as you want. For more information, see *Script Syntax*.
- § **Expect.** (Optional) Click to open the Rules Expression Editor and test a string of text for particular patterns.

### Adding an Echo Port Check component

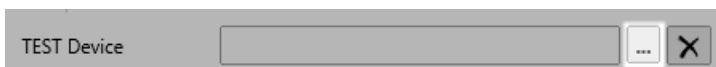
The Echo Port Check component allows you to create a script to run on a specific device that monitors a designated TCP, UDP, SSL network port using the Echo protocol. You may add an Echo Port Check component to an application profile or an application instance.




**Note:** Adding components to an application profile helps create the foundation of the application profile. After adding components to an application profile, you must create an application instance to monitor an application on a device. Learn more about APM terminology.

### To add an Echo Port Check component to an application profile:

- 1 From the WhatsUp Gold web interface, go to **APM > Configuration**. The All Application Profiles page appears.
- 2 Select the application profile for which you want to add a component, then click **Edit/View Application Profile**. The Components list appears.
- 3 Click **Add Components**. The Component Library appears.
- 4 Click the arrow next to **Network Port Check**, then specify the number of components you want to add by clicking the up and down arrows next to **Echo**.
- 5 Click **Add Selected**.
- 6 Click browse (...) next to the TEST Device box to launch the Select a Device dialog.



- 7 Select a device from the navigation tree on which to test the individual component and click **OK**.

- 8 Click **Test** to test the component on the selected device (optional). To remove the device override and revert to the device associated with the application component, click .



**Note:** If no test device is selected, the component is tested on the test device associated with the application profile.



Test devices are not saved as part of the application profile.


- 9 Enter or select the appropriate information in the *Echo Port Check component boxes* (on page 35).
- 10 Click **Save** to save your changes or click **Save and Close** to complete your changes.

### To add an Echo Port Check component to an application instance:

- 1 From the WhatsUp Gold web interface, go to **APM > Configuration**. The All Application Profiles page appears.
- 2 Select the application instance for which you want to add a component.
- 3 Click **Add Components**. The Component Library appears.
- 4 Click the arrow next to **Network Port Check**, then specify the number of components you want to add by clicking the up and down arrows next to **Echo**.
- 5 Click **Add Selected**.
- 6 Enter or select the appropriate information:
  - § **Enabled**. Select this option to enable or disable the component.
  - § **Action Policy**. Select an action policy from the list for the component.
  - § **Device Override**. (Optional) Override the device associated with the instance and designate a specific device to assign to the component.
    - § Click browse (...) next to the Device Override box to launch the Select a Device dialog.



**Important:** If the device you want to use is configured with a WhatsUp Gold down dependency, make sure that you use a cloned device for this device selection in the APM plug-in. For more information, see the Dependencies overview.

- § Select a device from the navigation tree on which to test the individual component and click **OK**.
  - § Click **Test** to test the component on the selected device.
  - § **Note:** Click  to remove the device override and revert to the device associated with the application instance.
- 7 Enter or select the appropriate information in the *Echo Port Check component boxes* (on page 35).
  - 8 Click **Save** to save your changes or click **Save and Close** to complete your changes.

### Echo Port Check component boxes

You may configure the following boxes for the Echo Port Check component:

- § **Name.** Enter a unique name for the component.
- § **Description.** (Optional) Enter additional information about the component.
- § **Critical.** Click to select this check box if the component is critical.



**Note:** Components specified as critical cause the application to go into a down state when the component is out of threshold. Non-critical components cause the application to go into a warning state. For more information on application states, see *Working with application states*.

- § **Polling frequency.** Select a time (in minutes or hours) you want APM to wait between polls.
- § **Protocol.** Select TCP, UDP, or SSL from the list. The network type for the FTP (File Transfer Protocol) service is TCP; the network type for the RADIUS (Remote Authentication and Dial-In User Service) service is UDP. The HTTPS monitor uses the SSL type.
- § **Port number.** Enter the port number that you want to monitor.
- § **Polling timeout.** Enter the length of time APM attempts to connect to the selected device. When the time you enter is exceeded without connecting, a *timeout* occurs and APM stops trying to connect to the device. This is considered a failed connection.
- § **Script to Run.** Enter your script using as many *Send*, *Expect*, *SimpleExpect*, and *Flow Control* keywords as you want. For more information, see *Script Syntax*.
- § **Expect.** (Optional) Click to open the Rules Expression Editor and test a string of text for particular patterns.

### Adding an FTP Port Check component

The FTP Port Check component allows you to create a script to run on a specific device that monitors a designated TCP, UDP, SSL network port using the File Transfer Protocol (FTP). You may add an FTP Port Check component to an application profile or an application instance.



**Note:** Adding components to an application profile helps create the foundation of the application profile. After adding components to an application profile, you must create an application instance to monitor an application on a device. Learn more about APM terminology.

### To add an FTP port Check component to an application profile:

- 1 From the WhatsUp Gold web interface, go to **APM > Configuration**. The All Application Profiles page appears.
- 2 Select the application profile for which you want to add a component, then click **Edit/View Application Profile**. The Components list appears.
- 3 Click **Add Components**. The Component Library appears.
- 4 Click the arrow next to **Network Port Check** to expand the dialog controls used to add the component(s).
- 5 Specify the number of components you want to add by clicking the up and down arrows next to **FTP**.
- 6 Click **Add Selected**.



- 7 Click browse (...) next to the TEST Device box to launch the Select a Device dialog.



- 8 Select a device from the navigation tree on which to test the individual component and click **OK**.
- 9 Click **Test** to test the component on the selected device (optional). To remove the device override and revert to the device associated with the application component, click **X**.



**Note:** If no test device is selected, the component is tested on the test device associated with the application profile.



Test devices are not saved as part of the application profile.

- 10 Enter or select the appropriate information in the *FTP Port Check component boxes* (on page 38).
- 11 Click **Save** to save your changes or click **Save and Close** to complete your changes.

### To add an Echo Port Check component to an application instance:

- 1 From the WhatsUp Gold web interface, go to **APM > Configuration**. The All Application Profiles page appears.
- 2 Select the application profile for which you want to add a component, then click **Edit/View Application Profile**. The Components list appears.
- 3 Click **Add Components**. The Component Library appears.
- 4 Click the arrow next to **Network Port Check**, then specify the number of components you want to add by clicking the up and down arrows next to **FTP**.
- 5 Click **Add Selected**.
- 6 Enter or select the appropriate information:
  - § **Enabled**. Select this option to enable or disable the component.
  - § **Action Policy**. Select an action policy from the list for the component.
  - § **Device Override**. (Optional) Override the device associated with the instance and designate a specific device to assign to the component.
    - § Click browse (...) next to the Device Override box to launch the Select a Device dialog.



**Important:** If the device you want to use is configured with a WhatsUp Gold down dependency, make sure that you use a cloned device for this device selection in the APM plug-in. For more information, see the Dependencies overview.

- § Select a device from the navigation tree on which to test the individual component and click **OK**.
- § Click **Test** to test the component on the selected device.
- § **Note:** Click **X** to remove the device override and revert to the device associated with the application instance.



- 7 Enter or select the appropriate information in the *FTP Port Check component boxes* (on page 38).
- 8 Click **Save** to save your changes or click **Save and Close** to complete your changes.

### FTP Port Check component boxes

You may configure the following boxes for the FTP Port Check component:

- § **Name.** Enter a unique name for the component.
- § **Description.** (Optional) Enter additional information about the component.
- § **Critical.** Click to select this check box if the component is critical.



**Note:** Components specified as critical cause the application to go into a down state when the component is out of threshold. Non-critical components cause the application to go into a warning state. For more information on application states, see *Working with application states*.

- § **Polling frequency.** Select a time (in minutes or hours) you want APM to wait between polls.
- § **Protocol.** Select TCP, UDP, or SSL from the list. The network type for the FTP (File Transfer Protocol) service is TCP; the network type for the RADIUS (Remote Authentication and Dial-In User Service) service is UDP. The HTTPS monitor uses the SSL type.
- § **Port number.** Enter the port number that you want to monitor.
- § **Polling timeout.** Enter the length of time APM attempts to connect to the selected device. When the time you enter is exceeded without connecting, a *timeout* occurs and APM stops trying to connect to the device. This is considered a failed connection.
- § **Script to Run.** Enter your script using as many *Send*, *Expect*, *SimpleExpect*, and *Flow Control* keywords as you want. For more information, see *Script Syntax*.
- § **Expect.** (Optional) Click to open the Rules Expression Editor and test a string of text for particular patterns.

### Adding an HTTP Port Check component

The HTTP Port Check component allows you to create a script to run on a specific device that monitors a designated TCP, UDP, SSL network port using the Hypertext Transfer Protocol (HTTP). You may add an HTTP Port Check component to an application profile or an application instance.

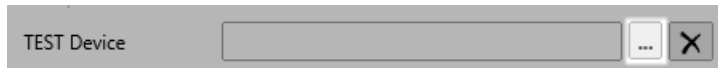


**Note:** Adding components to an application profile helps create the foundation of the application profile. After adding components to an application profile, you must create an application instance to monitor an application on a device. Learn more about APM terminology.

#### To add an HTTP Port Check component to an application profile:

- 1 From the WhatsUp Gold web interface, go to **APM > Configuration**. The All Application Profiles page appears.
- 2 Select the application profile for which you want to add a component, then click **Edit/View Application Profile**. The Components list appears.

- 3 Click **Add Components**. The Component Library appears.
- 4 Click the arrow next to **Network Port Check** to expand the dialog controls used to add the component(s).
- 5 Specify the number of components you want to add by clicking the up and down arrows next to **HTTP**.
- 6 Click **Add Selected**.
- 7 Click browse (...) next to the TEST Device box to launch the Select a Device dialog.



- 8 Select a device from the navigation tree on which to test the individual component and click **OK**.
- 9 Click **Test** to test the component on the selected device (optional). To remove the device override and revert to the device associated with the application component, click **X**.



**Note:** If no test device is selected, the component is tested on the test device associated with the application profile.



Test devices are not saved as part of the application profile.


- 10 Enter or select the appropriate information in the *HTTP Port Check component boxes* (on page 40).
- 11 Click **Save** to save your changes or click **Save and Close** to complete your changes.

### To add an HTTP Port Check component to an application instance:

- 1 From the WhatsUp Gold web interface, go to **APM > Configuration**. The All Application Profiles page appears.
- 2 Select the application instance for which you want to add a component.
- 3 Click **Add Components**. The Component Library appears.
- 4 Click the arrow next to **Network Port Check**, then specify the number of components you want to add by clicking the up and down arrows next to **HTTP**.
- 5 Click **Add Selected**.
- 6 Enter or select the appropriate information:
  - § **Enabled**. Select this option to enable or disable the component.
  - § **Action Policy**. Select an action policy from the list for the component.
  - § **Device Override**. (Optional) Override the device associated with the instance and designate a specific device to assign to the component.
    - § Click browse (...) next to the Device Override box to launch the Select a Device dialog.



**Important:** If the device you want to use is configured with a WhatsUp Gold down dependency, make sure that you use a cloned device for this device selection in the APM plug-in. For more information, see the Dependencies overview.

- § Select a device from the navigation tree on which to test the individual component and click **OK**.
  - § Click **Test** to test the component on the selected device.
  - § **Note:** Click  to remove the device override and revert to the device associated with the application instance.
- 7 Enter or select the appropriate information in the *HTTP Port Check component boxes* (on page 40).
  - 8 Click **Save** to save your changes or click **Save and Close** to complete your changes.

### HTTP Port Check component boxes

You may configure the following boxes for the HTTP Port Check component:

- § **Name.** Enter a unique name for the component.
- § **Description.** (Optional) Enter additional information about the component.
- § **Critical.** Click to select this check box if the component is critical.



**Note:** Components specified as critical cause the application to go into a down state when the component is out of threshold. Non-critical components cause the application to go into a warning state. For more information on application states, see *Working with application states*.

- § **Polling frequency.** Select a time (in minutes or hours) you want APM to wait between polls.
- § **Protocol.** Select TCP, UDP, or SSL from the list. The network type for the FTP (File Transfer Protocol) service is TCP; the network type for the RADIUS (Remote Authentication and Dial-In User Service) service is UDP. The HTTPS monitor uses the SSL type.
- § **Port number.** Enter the port number that you want to monitor.
- § **Polling timeout.** Enter the length of time APM attempts to connect to the selected device. When the time you enter is exceeded without connecting, a *timeout* occurs and APM stops trying to connect to the device. This is considered a failed connection.
- § **Script to Run.** Enter your script using as many *Send*, *Expect*, *SimpleExpect*, and *Flow Control* keywords as you want. For more information, see *Script Syntax*.
- § **Expect.** (Optional) Click to open the Rules Expression Editor and test a string of text for particular patterns.

### Adding an HTTPS Port Check component

The HTTPS Port Check component allows you to create a script to run on a specific device that monitors a designated TCP, UDP, SSL network port using Hypertext Transfer Protocol Secure (HTTPS). You may add an HTTPS Port Check component to an application profile or an application instance.



**Note:** Adding components to an application profile helps create the foundation of the application profile. After adding components to an application profile, you must create an application instance to monitor an application on a device. Learn more about APM terminology.

### To add an HTTPS Port Check component to an application profile:

- 1 From the WhatsUp Gold web interface, go to **APM > Configuration**. The All Application Profiles page appears.
- 2 Select the application profile for which you want to add a component, then click **Edit/View Application Profile**. The Components list appears.
- 3 Click **Add Components**. The Component Library appears.
- 4 Click the arrow next to **Network Port Check** to expand the dialog controls used to add the component(s).
- 5 Specify the number of components you want to add by clicking the up and down arrows next to **HTTPS**.
- 6 Click **Add Selected**.
- 7 Click browse (...) next to the TEST Device box to launch the Select a Device dialog.



- 8 Select a device from the navigation tree on which to test the individual component and click **OK**.
- 9 Click **Test** to test the component on the selected device (optional). To remove the device override and revert to the device associated with the application component, click **X**.



**Note:** If no test device is selected, the component is tested on the test device associated with the application profile.



Test devices are not saved as part of the application profile.

- 10 Enter or select the appropriate information in the *HTTPS Port Check component boxes* (on page 42).
- 11 Click **Save** to save your changes or click **Save and Close** to complete your changes.

### To add an HTTPS Port Check component to an application instance:


- 1 From the WhatsUp Gold web interface, go to **APM > Configuration**. The All Application Profiles page appears.
- 2 Select the application instance for which you want to add a component.
- 3 Click **Add Components**. The Component Library appears.
- 4 Click the arrow next to **Network Port Check**, then specify the number of components you want to add by clicking the up and down arrows next to **HTTPS**.
- 5 Click **Add Selected**.
- 6 Enter or select the appropriate information:
  - § **Enabled**. Select this option to enable or disable the component.
  - § **Action Policy**. Select an action policy from the list for the component.
  - § **Device Override**. (Optional) Override the device associated with the instance and designate a specific device to assign to the component.
    - § Click browse (...) next to the Device Override box to launch the Select a Device dialog.



**Important:** If the device you want to use is configured with a WhatsUp Gold down dependency, make sure that you use a cloned device for this device selection in the APM plug-in. For more information, see the Dependencies overview.

- § Select a device from the navigation tree on which to test the individual component and click **OK**.
- § Click **Test** to test the component on the selected device.



**Note:** Click  to remove the device override and revert to the device associated with the application instance.

- 7 Enter or select the appropriate information in the *HTTPS Port Check component boxes* (on page 42).
- 8 Click **Save** to save your changes or click **Save and Close** to complete your changes.

### HTTPS Port Check component boxes

You may configure the following boxes for the HTTPS Port Check component:

- § **Name.** Enter a unique name for the component.
- § **Description.** (Optional) Enter additional information about the component.
- § **Critical.** Click to select this check box if the component is critical.



**Note:** Components specified as critical cause the application to go into a down state when the component is out of threshold. Non-critical components cause the application to go into a warning state. For more information on application states, see Working with application states.

- § **Polling frequency.** Select a time (in minutes or hours) you want APM to wait between polls.
- § **Protocol.** Select TCP, UDP, or SSL from the list. The network type for the FTP (File Transfer Protocol) service is TCP; the network type for the RADIUS (Remote Authentication and Dial-In User Service) service is UDP. The HTTPS monitor uses the SSL type.
- § **Port number.** Enter the port number that you want to monitor.
- § **Polling timeout.** Enter the length of time APM attempts to connect to the selected device. When the time you enter is exceeded without connecting, a *timeout* occurs and APM stops trying to connect to the device. This is considered a failed connection.
- § **Script to Run.** Enter your script using as many `Send`, `Expect`, `SimpleExpect`, and `Flow Control` keywords as you want. For more information, see Script Syntax.
- § **Expect.** (Optional) Click to open the Rules Expression Editor and test a string of text for particular patterns.

### Adding an IMAP4 Port Check component

The IMAP4 Port Check component allows you to create a script to run on a specific device that monitors a designated TCP, UDP, SSL network port using the Internet Message Access

Protocol (IMAP4). You may add an IMAP4 Port Check component to an application profile or an application instance.



**Note:** Adding components to an application profile helps create the foundation of the application profile. After adding components to an application profile, you must create an application instance to monitor an application on a device. Learn more about APM terminology.

### To add an IMAP4 Port Check component to an application profile:

- 1 From the WhatsUp Gold web interface, go to **APM > Configuration**. The All Application Profiles page appears.
- 2 Select the application profile for which you want to add a component, then click **Edit/View Application Profile**. The Components list appears.
- 3 Click **Add Components**. The Component Library appears.
- 4 Click the arrow next to **Network Port Check**, to expand the dialog controls used to add the component(s).
- 5 Specify the number of components you want to add by clicking the up and down arrows next to **IMAP4**.
- 6 Click **Add Selected**.
- 7 Click browse (...) next to the TEST Device box to launch the Select a Device dialog.



- 8 Select a device from the navigation tree on which to test the individual component and click **OK**.
- 9 Click **Test** to test the component on the selected device (optional). To remove the device override and revert to the device associated with the application component, click **X**.



**Note:** If no test device is selected, the component is tested on the test device associated with the application profile.



Test devices are not saved as part of the application profile.

- 10 Enter or select the appropriate information in the *IMAP4 Port Check component boxes* (on page 42).
- 11 Click **Save** to save your changes or click **Save and Close** to complete your changes.

### To add an IMAP4 Port Check component to an application instance:

- 1 From the WhatsUp Gold web interface, go to **APM > Configuration**. The All Application Profiles page appears.
- 2 Select the application instance for which you want to add a component.
- 3 Click **Add Components**. The Component Library appears.
- 4 Click the arrow next to **Network Port Check**, then specify the number of components you want to add by clicking the up and down arrows next to **IMAP4**.
- 5 Click **Add Selected**.
- 6 Enter or select the appropriate information:


- § **Enabled.** Select this option to enable or disable the component.
- § **Action Policy.** Select an action policy from the list for the component.
- § **Device Override.** (Optional) Override the device associated with the instance and designate a specific device to assign to the component.
  - § Click browse (...) next to the Device Override box to launch the Select a Device dialog.



**Important:** If the device you want to use is configured with a WhatsUp Gold down dependency, make sure that you use a cloned device for this device selection in the APM plug-in. For more information, see the Dependencies overview.

- § Select a device from the navigation tree on which to test the individual component and click **OK**.
- § Click **Test** to test the component on the selected device.



**Note:** Click  to remove the device override and revert to the device associated with the application instance.

- 7 Enter or select the appropriate information in the *IMAP4 Port Check component boxes* (on page 42).
- 8 Click **Save** to save your changes or click **Save and Close** to complete your changes.

### IMAP4 Port Check component boxes

You may configure the following boxes for the IMAP4 Port Check component:

- § **Name.** Enter a unique name for the component.
- § **Description.** (Optional) Enter additional information about the component.
- § **Critical.** Click to select this check box if the component is critical.



**Note:** Components specified as critical cause the application to go into a down state when the component is out of threshold. Non-critical components cause the application to go into a warning state. For more information on application states, see Working with application states.

- § **Polling frequency.** Select a time (in minutes or hours) you want APM to wait between polls.
- § **Protocol.** Select TCP, UDP, or SSL from the list. The network type for the FTP (File Transfer Protocol) service is TCP; the network type for the RADIUS (Remote Authentication and Dial-In User Service) service is UDP. The HTTPS monitor uses the SSL type.
- § **Port number.** Enter the port number that you want to monitor.
- § **Polling timeout.** Enter the length of time APM attempts to connect to the selected device. When the time you enter is exceeded without connecting, a *timeout* occurs and APM stops trying to connect to the device. This is considered a failed connection.
- § **Script to Run.** Enter your script using as many *Send*, *Expect*, *SimpleExpect*, and *Flow Control* keywords as you want. For more information, see Script Syntax.



- § **Expect.** (Optional) Click to open the Rules Expression Editor and test a string of text for particular patterns.

### Adding an NNTP Port Check component

The NNTP Port Check component allows you to create a script to run on a specific device that monitors a designated TCP, UDP, SSL network port using the Network News Transfer Protocol (NNTP). You may add an NNTP Port Check component to an application profile or an application instance.



**Note:** Adding components to an application profile helps create the foundation of the application profile. After adding components to an application profile, you must create an application instance to monitor an application on a device. Learn more about APM terminology.

#### To add an NNTP Port Check component to an application profile:

- 1 From the WhatsUp Gold web interface, go to **APM > Configuration**. The All Application Profiles page appears.
- 2 Select the application profile for which you want to add a component, then click **Edit/View Application Profile**. The Components list appears.
- 3 Click **Add Components**. The Component Library appears.
- 4 Click the arrow next to **Network Port Check** to expand the dialog controls used to add the component(s).
- 5 Specify the number of components you want to add by clicking the up and down arrows next to **NNTP**.
- 6 Click **Add Selected**.
- 7 Click browse (...) next to the TEST Device box to launch the Select a Device dialog.



- 8 Select a device from the navigation tree on which to test the individual component and click **OK**.
- 9 Click **Test** to test the component on the selected device (optional). To remove the device override and revert to the device associated with the application component, click **X**.



**Note:** If no test device is selected, the component is tested on the test device associated with the application profile.



Test devices are not saved as part of the application profile.

- 10 Enter or select the appropriate information in the *NNTP Port Check component fields* (on page 46).
- 11 Click **Save** to save your changes or click **Save and Close** to complete your changes.

#### To add an NNTP Port Check component to an application instance:

- 1 From the WhatsUp Gold web interface, go to **APM > Configuration**. The All Application Profiles page appears.
- 2 Select the application instance for which you want to add a component.




- 3 Click **Add Components**. The Component Library appears.
- 4 Click the arrow next to **Network Port Check**, then specify the number of components you want to add by clicking the up and down arrows next to **NNTP**.
- 5 Click **Add Selected**.
- 6 Enter or select the appropriate information:
  - § **Enabled**. Select this option to enable or disable the component.
  - § **Action Policy**. Select an action policy from the list for the component.
  - § **Device Override**. (Optional) Override the device associated with the instance and designate a specific device to assign to the component.
    - § Click browse (...) next to the Device Override box to launch the Select a Device dialog.



**Important:** If the device you want to use is configured with a WhatsUp Gold down dependency, make sure that you use a cloned device for this device selection in the APM plug-in. For more information, see the Dependencies overview.

- § Select a device from the navigation tree on which to test the individual component and click **OK**.
- § Click **Test** to test the component on the selected device.



**Note:** Click  to remove the device override and revert to the device associated with the application instance.

- 7 Enter or select the appropriate information in the *NNTP Port Check component boxes* (on page 46).
- 8 Click **Save** to save your changes or click **Save and Close** to complete your changes.

### **NNTP Port Check component boxes**

You may configure the following boxes for the NNTP Port Check component:

- § **Name**. Enter a unique name for the component.
- § **Description**. (Optional) Enter additional information about the component.
- § **Critical**. Click to select this check box if the component is critical.



**Note:** Components specified as critical cause the application to go into a down state when the component is out of threshold. Non-critical components cause the application to go into a warning state. For more information on application states, see *Working with application states*.

- § **Polling frequency**. Select a time (in minutes or hours) you want APM to wait between polls.
- § **Protocol**. Select TCP, UDP, or SSL from the list. The network type for the FTP (File Transfer Protocol) service is TCP; the network type for the RADIUS (Remote Authentication and Dial-In User Service) service is UDP. The HTTPS monitor uses the SSL type.

- § **Port number.** Enter the port number that you want to monitor.
- § **Polling timeout.** Enter the length of time APM attempts to connect to the selected device. When the time you enter is exceeded without connecting, a *timeout* occurs and APM stops trying to connect to the device. This is considered a failed connection.
- § **Script to Run.** Enter your script using as many *Send*, *Expect*, *SimpleExpect*, and *Flow Control* keywords as you want. For more information, see *Script Syntax*.
- § **Expect.** (Optional) Click to open the Rules Expression Editor and test a string of text for particular patterns.

### Adding a POP3 Port Check component

The POP3 Port Check component allows you to create a script to run on a specific device that monitors a designated TCP, UDP, SSL network port using the Post Office Protocol (POP3). You may add a POP3 Port Check component to an application profile or an application instance.



**Note:** Adding components to an application profile helps create the foundation of the application profile. After adding components to an application profile, you must create an application instance to monitor an application on a device. Learn more about APM terminology.

#### To add a POP3 Port Check component to an application profile:

- 1 From the WhatsUp Gold web interface, go to **APM > Configuration**. The All Application Profiles page appears.
- 2 Select the application profile for which you want to add a component, then click **Edit/View Application Profile**. The Components list appears.
- 3 Click **Add Components**. The Component Library appears.
- 4 Click the arrow next to **Network Port Check** to expand the dialog controls used to add the component(s).
- 5 Specify the number of components you want to add by clicking the up and down arrows next to **POP3**.
- 6 Click **Add Selected**.
- 7 Click browse (...) next to the TEST Device box to launch the Select a Device dialog.



- 8 Select a device from the navigation tree on which to test the individual component and click **OK**.
- 9 Click **Test** to test the component on the selected device (optional). To remove the device override and revert to the device associated with the application component, click **X**.



**Note:** If no test device is selected, the component is tested on the test device associated with the application profile.



Test devices are not saved as part of the application profile.

- 10 Enter or select the appropriate information in the *POP3 Port Check component boxes* (on page 48).

11 Click **Save** to save your changes or click **Save and Close** to complete your changes.

To add a POP3 Port Check component to an application instance:


- 1 From the WhatsUp Gold web interface, go to **APM > Configuration**. The All Application Profiles page appears.
- 2 Select the application instance for which you want to add a component.
- 3 Click **Add Components**. The Component Library appears.
- 4 Click the arrow next to **Network Port Check**, then specify the number of components you want to add by clicking the up and down arrows next to **POP3**.
- 5 Click **Add Selected**.
- 6 Enter or select the appropriate information:
  - § **Enabled**. Select this option to enable or disable the component.
  - § **Action Policy**. Select an action policy from the list for the component.
  - § **Device Override**. (Optional) Override the device associated with the instance and designate a specific device to assign to the component.
    - § Click browse (...) next to the Device Override box to launch the Select a Device dialog.



**Important:** If the device you want to use is configured with a WhatsUp Gold down dependency, make sure that you use a cloned device for this device selection in the APM plug-in. For more information, see the Dependencies overview.

- § Select a device from the navigation tree on which to test the individual component and click **OK**.
- § Click **Test** to test the component on the selected device.



**Note:** Click  to remove the device override and revert to the device associated with the application instance.

- 7 Enter or select the appropriate information in the *POP3 Port Check component boxes* (on page 48).
- 8 Click **Save** to save your changes or click **Save and Close** to complete your changes.

### POP3 Port Check component boxes

You may configure the following boxes for the POP3 Port Check component:

- § **Name**. Enter a unique name for the component.
- § **Description**. (Optional) Enter additional information about the component.
- § **Critical**. Click to select this check box if the component is critical.



**Note:** Components specified as critical cause the application to go into a down state when the component is out of threshold. Non-critical components cause the application to go into a warning state. For more information on application states, see *Working with application states*.

- § **Polling frequency.** Select a time (in minutes or hours) you want APM to wait between polls.
- § **Protocol.** Select TCP, UDP, or SSL from the list. The network type for the FTP (File Transfer Protocol) service is TCP; the network type for the RADIUS (Remote Authentication and Dial-In User Service) service is UDP. The HTTPS monitor uses the SSL type.
- § **Port number.** Enter the port number that you want to monitor.
- § **Polling timeout.** Enter the length of time APM attempts to connect to the selected device. When the time you enter is exceeded without connecting, a *timeout* occurs and APM stops trying to connect to the device. This is considered a failed connection.
- § **Script to Run.** Enter your script using as many *Send*, *Expect*, *SimpleExpect*, and *Flow Control* keywords as you want. For more information, see *Script Syntax*.
- § **Expect.** (Optional) Click to open the Rules Expression Editor and test a string of text for particular patterns.

### Adding a Radius Port Check component to an application profile

The Radius Port Check component allows you to create a script to run on a specific device that monitors a designated TCP, UDP, SSL network port using the Radius protocol. You may add a Radius Port Check component to an application profile or an application instance.



**Note:** Adding components to an application profile helps create the foundation of the application profile. After adding components to an application profile, you must create an application instance to monitor an application on a device. Learn more about APM terminology.

### To add a Radius Port Check component to an application profile:

- 1 From the WhatsUp Gold web interface, go to **APM > Configuration**. The All Application Profiles page appears.
- 2 Select the application profile for which you want to add a component, then click **Edit/View Application Profile**. The Components list appears.
- 3 Click **Add Components**. The Component Library appears.
- 4 Click the arrow next to **Network Port Check** to expand the dialog controls used to add the component(s).
- 5 Specify the number of components you want to add by clicking the up and down arrows next to **Radius**.
- 6 Click **Add Selected**.
- 7 Click browse (...) next to the TEST Device box to launch the Select a Device dialog.



- 8 Select a device from the navigation tree on which to test the individual component and click **OK**.
- 9 Click **Test** to test the component on the selected device (optional). To remove the device override and revert to the device associated with the application component, click



**Note:** If no test device is selected, the component is tested on the test device associated with the application profile.



Test devices are not saved as part of the application profile.

**10** Enter or select the appropriate information in the *Radius Port Check component boxes* (on page 50).

**11** Click **Save** to save your changes or click **Save and Close** to complete your changes.

### To add a Radius Port Check component to an application instance:

**1** From the WhatsUp Gold web interface, go to **APM > Configuration**. The All Application Profiles page appears.

**2** Select the application instance for which you want to add a component.

**3** Click **Add Components**. The Component Library appears.

**4** Click the arrow next to **Network Port Check**, then specify the number of components you want to add by clicking the up and down arrows next to **Radius**.

**5** Click **Add Selected**.

**6** Enter or select the appropriate information:

§ **Enabled**. Select this option to enable or disable the component.

§ **Action Policy**. Select an action policy from the list for the component.

§ **Device Override**. (Optional) Override the device associated with the instance and designate a specific device to assign to the component.

§ Click browse (...) next to the Device Override box to launch the Select a Device dialog.




**Important:** If the device you want to use is configured with a WhatsUp Gold down dependency, make sure that you use a cloned device for this device selection in the APM plug-in. For more information, see the Dependencies overview.

§ Select a device from the navigation tree on which to test the individual component and click **OK**.

§ Click **Test** to test the component on the selected device.



**Note:** Click  to remove the device override and revert to the device associated with the application instance.

**7** Enter or select the appropriate information in the *Radius Port Check component boxes* (on page 50).

**8** Click **Save** to save your changes or click **Save and Close** to complete your changes.

### Radius Port Check component boxes

You may configure the following boxes for the Radius Port Check component:

§ **Name**. Enter a unique name for the component.

§ **Description**. (Optional) Enter additional information about the component.

§ **Critical.** Click to select this check box if the component is critical.



**Note:** Components specified as critical cause the application to go into a down state when the component is out of threshold. Non-critical components cause the application to go into a warning state. For more information on application states, see *Working with application states*.

- § **Polling frequency.** Select a time (in minutes or hours) you want APM to wait between polls.
- § **Protocol.** Select TCP, UDP, or SSL from the list. The network type for the FTP (File Transfer Protocol) service is TCP; the network type for the RADIUS (Remote Authentication and Dial-In User Service) service is UDP. The HTTPS monitor uses the SSL type.
- § **Port number.** Enter the port number that you want to monitor.
- § **Polling timeout.** Enter the length of time APM attempts to connect to the selected device. When the time you enter is exceeded without connecting, a *timeout* occurs and APM stops trying to connect to the device. This is considered a failed connection.
- § **Script to Run.** Enter your script using as many *Send*, *Expect*, *SimpleExpect*, and *Flow Control* keywords as you want. For more information, see *Script Syntax*.
- § **Expect.** (Optional) Click to open the Rules Expression Editor and test a string of text for particular patterns.

### Adding an SMTP Port Check component

The SMTP Port Check component allows you to create a script to run on a specific device that monitors a designated TCP, UDP, SSL network port using the Simple Mail Transfer Protocol (SMTP). You may add an SMTP Port Check component to an application profile or an application instance.



**Note:** Adding components to an application profile helps create the foundation of the application profile. After adding components to an application profile, you must create an application instance to monitor an application on a device. Learn more about APM terminology.

### To add an SMTP Port Check component to an application profile:

- 1 From the WhatsUp Gold web interface, go to **APM > Configuration**. The All Application Profiles page appears.
- 2 Select the application profile for which you want to add a component, then click **Edit/View Application Profile**. The Components list appears.
- 3 Click **Add Components**. The Component Library appears.
- 4 Click the arrow next to **Network Port Check** to expand the dialog controls used to add the component(s).
- 5 Specify the number of components you want to add by clicking the up and down arrows next to **SMTP**.
- 6 Click **Add Selected**.

- 7 Click browse (...) next to the TEST Device box to launch the Select a Device dialog.



- 8 Select a device from the navigation tree on which to test the individual component and click **OK**.
- 9 Click **Test** to test the component on the selected device (optional). To remove the device override and revert to the device associated with the application component, click **X**.



**Note:** If no test device is selected, the component is tested on the test device associated with the application profile.



Test devices are not saved as part of the application profile.

- 10 Enter or select the appropriate information in the *SMTP Port Check component fields* (on page 53).
- 11 Click **Save** to save your changes or click **Save and Close** to complete your changes.

### To add an SMTP Port Check component to an application instance:

- 1 From the WhatsUp Gold web interface, go to **APM > Configuration**. The All Application Profiles page appears.
- 2 Select the application instance for which you want to add a component.
- 3 Click **Add Components**. The Component Library appears.
- 4 Click the arrow next to **Network Port Check**, then specify the number of components you want to add by clicking the up and down arrows next to **SMTP**.
- 5 Click **Add Selected**.
- 6 Enter or select the appropriate information:
  - § **Enabled**. Select this option to enable or disable the component.
  - § **Action Policy**. Select an action policy from the list for the component.
  - § **Device Override**. (Optional) Override the device associated with the instance and designate a specific device to assign to the component.
    - § Click browse (...) next to the Device Override box to launch the Select a Device dialog.



**Important:** If the device you want to use is configured with a WhatsUp Gold down dependency, make sure that you use a cloned device for this device selection in the APM plug-in. For more information, see the Dependencies overview.

- § Select a device from the navigation tree on which to test the individual component and click **OK**.
- § Click **Test** to test the component on the selected device.



**Note:** Click **X** to remove the device override and revert to the device associated with the application instance.



- 7 Enter or select the appropriate information in the *SMTP Port Check component fields* (on page 53).
- 8 Click **Save** to save your changes or click **Save and Close** to complete your changes.

### SMTP Port Check component boxes

You may configure the following boxes for the SMTP Port Check component:

- § **Name.** Enter a unique name for the component.
- § **Description.** (Optional) Enter additional information about the component.
- § **Critical.** Click to select this check box if the component is critical.



**Note:** Components specified as critical cause the application to go into a down state when the component is out of threshold. Non-critical components cause the application to go into a warning state. For more information on application states, see *Working with application states*.

- § **Polling frequency.** Select a time (in minutes or hours) you want APM to wait between polls.
- § **Protocol.** Select TCP, UDP, or SSL from the list. The network type for the FTP (File Transfer Protocol) service is TCP; the network type for the RADIUS (Remote Authentication and Dial-In User Service) service is UDP. The HTTPS monitor uses the SSL type.
- § **Port number.** Enter the port number that you want to monitor.
- § **Polling timeout.** Enter the length of time APM attempts to connect to the selected device. When the time you enter is exceeded without connecting, a *timeout* occurs and APM stops trying to connect to the device. This is considered a failed connection.
- § **Script to Run.** Enter your script using as many *Send*, *Expect*, *SimpleExpect*, and *Flow Control* keywords as you want. For more information, see *Script Syntax*.
- § **Expect.** (Optional) Click to open the Rules Expression Editor and test a string of text for particular patterns.

### Adding a Time Port Check component

The Time Port Check component allows you to create a script to run on a specific device that monitors a designated TCP, UDP, SSL network port using the Time protocol. You may add a Time Port Check component to an application profile or an application instance.



**Note:** Adding components to an application profile helps create the foundation of the application profile. After adding components to an application profile, you must create an application instance to monitor an application on a device. Learn more about APM terminology.


#### To add a Time Port Check component to an application profile:

- 1 From the WhatsUp Gold web interface, go to **APM > Configuration**. The All Application Profiles page appears.
- 2 Select the application profile for which you want to add a component, then click **Edit/View Application Profile**. The Components list appears.
- 3 Click **Add Components**. The Component Library appears.



- 4 Click the arrow next to **Network Port Check** to expand the dialog controls used to add the component(s).
- 5 Specify the number of components you want to add by clicking the up and down arrows next to **Time**.
- 6 Click **Add Selected**.
- 7 Click browse (...) next to the TEST Device box to launch the Select a Device dialog.



- 8 Select a device from the navigation tree on which to test the individual component and click **OK**.
- 9 Click **Test** to test the component on the selected device (optional). To remove the device override and revert to the device associated with the application component, click .



**Note:** If no test device is selected, the component is tested on the test device associated with the application profile.



Test devices are not saved as part of the application profile.

- 10 Enter or select the appropriate information in the *Time Port Check component boxes* (on page 55).
- 11 Click **Save** to save your changes or click **Save and Close** to complete your changes.

### To add a Time Port Check component to an application instance:

- 1 From the WhatsUp Gold web interface, go to **APM > Configuration**. The All Application Profiles page appears.
- 2 Select the application instance for which you want to add a component.
- 3 Click **Add Components**. The Component Library appears.
- 4 Click the arrow next to **Network Port Check**, then specify the number of components you want to add by clicking the up and down arrows next to **Time**.
- 5 Click **Add Selected**.
- 6 Enter or select the appropriate information:
  - § **Enabled**. Select this option to enable or disable the component.
  - § **Action Policy**. Select an action policy from the list for the component.
  - § **Device Override**. (Optional) Override the device associated with the instance and designate a specific device to assign to the component.
    - § Click browse (...) next to the Device Override box to launch the Select a Device dialog.




**Important:** If the device you want to use is configured with a WhatsUp Gold down dependency, make sure that you use a cloned device for this device selection in the APM plug-in. For more information, see the Dependencies overview.

- § Select a device from the navigation tree on which to test the individual component and click **OK**.

§ Click **Test** to test the component on the selected device.



**Note:** Click  to remove the device override and revert to the device associated with the application instance.

7 Enter or select the appropriate information in the *Time Port Check component boxes* (on page 55).

8 Click **Save** to save your changes or click **Save and Close** to complete your changes.

### Time Port Check component boxes

You may configure the following boxes for the Time Port Check component:

- § **Name.** Enter a unique name for the component.
- § **Description.** (Optional) Enter additional information about the component.
- § **Critical.** Click to select this check box if the component is critical.



**Note:** Components specified as critical cause the application to go into a down state when the component is out of threshold. Non-critical components cause the application to go into a warning state. For more information on application states, see *Working with application states*.

- § **Polling frequency.** Select a time (in minutes or hours) you want APM to wait between polls.
- § **Protocol.** Select TCP, UDP, or SSL from the list. The network type for the FTP (File Transfer Protocol) service is TCP; the network type for the RADIUS (Remote Authentication and Dial-In User Service) service is UDP. The HTTPS monitor uses the SSL type.
- § **Port number.** Enter the port number that you want to monitor.
- § **Polling timeout.** Enter the length of time APM attempts to connect to the selected device. When the time you enter is exceeded without connecting, a *timeout* occurs and APM stops trying to connect to the device. This is considered a failed connection.
- § **Script to Run.** Enter your script using as many *Send*, *Expect*, *SimpleExpect*, and *Flow Control* keywords as you want. For more information, see *Script Syntax*.
- § **Expect.** (Optional) Click to open the Rules Expression Editor and test a string of text for particular patterns.

### Process Check

The Process Check component allows you to monitor a process on a specific device using either *SNMP* (on page 55) or *WMI* (on page 56). You may add a Process Check component to an application profile or an application instance.

#### Process Check (SNMP)

Configure the following for the SNMP Process Check component:

- § **Name.** Enter a unique name for the component.
- § **Description.** Enter additional information about the component.
- § **Critical.** Click to select this check box if the component is critical.



**Note:** Components specified as critical cause the application to go into a down state when the component is out of threshold. Non-critical components cause the application to go into a warning state. For more information on application states, see *Working with application states*.

- § **Polling frequency.** Select a time (in minutes or hours) you want APM to wait between polls.
- § **Process Name.** Enter the name of the process you would like to monitor. You can type the process name or click browse (...) to open the device browser and select the specific device and process.
- § **Down if not running.** Select this option to put the application in a down state if the process is not running.
- § **Polling timeout.** Enter the length of time APM attempts to connect to the selected device. When the time you enter is exceeded without connecting, a timeout occurs and APM stops trying to connect to the device. This is considered a failed connection.
- § **Poller retries.** Enter the number of times APM attempts to send the command before the device is considered down.

### Process Check (WMI)

Configure the following for the WMI Process Check component:

- § **Name.** Enter a unique name for the component.
- § **Description.** Enter additional information about the component.
- § **Critical.** Click to select this check box if the component is critical.



**Note:** Components specified as critical cause the application to go into a down state when the component is out of threshold. Non-critical components cause the application to go into a warning state. For more information on application states, see *Working with application states*.

- § **Polling frequency.** Select a time (in minutes or hours) you want APM to wait between polls.
- § **Process Name.** Enter the name of the process you would like to monitor. You can type the process name or click browse (...) to open the device browser and select the specific device and process.
- § **Down if not running.** Select this option to put the application in a down state if the process is not running.

### Scripting (PowerShell)

This component allows you to run a PowerShell script and analyze the output. You may add a PowerShell Execution component to an application profile or an application instance.

Windows PowerShell is a scripting language and command-line shell that system administrators can use to manage Windows operating systems. For more information on PowerShell, please visit the Microsoft web site.



**Important:** Network Performance Monitor uses a 32-bit (i.e. x86) PowerShell engine. Therefore, only 32-bit PowerShell snap-ins are supported and 64-bit only snap-ins will not function properly. Snap-ins usable in both 32-bit and 64-bit operating systems are configured for 64-bit systems by default and must be manually configured for 32-bit PowerShell engine to function properly with Network Performance Monitor.



If you are using additional pollers with Network Performance Monitor, PowerShell must be installed and any desired snap-ins must be registered identically on all poller machines for any PowerShell performance monitors, active monitors, and actions to function properly.

Configure the following:

- § **Name.** Enter a unique name for the component.
- § **Description.** Enter additional information about the component.
- § **Critical.** Click to select this check box if the component is critical.



**Note:** Components specified as critical cause the application to go into a down state when the component is out of threshold. Non-critical components cause the application to go into a warning state. For more information on application states, see [Working with application states](#).

- § **Polling frequency.** Select a time (in minutes or hours) you want APM to wait between polls.
- § **Script timeout.** Enter the length of time APM attempts to connect to the selected device. When the time you enter is exceeded without connecting, a timeout occurs and APM stops trying to connect to the device. This is considered a failed connection.
- § **Add a Reference Variable.** Click to open the Reference Variable dialog and add a reference variable to the component.
- § **Run under device credentials.** Select this check box to execute the script using the Windows credentials for the affected device. For additional information, see [Using the Credentials Library](#).
- § **Script to Run.** Enter your script to return a single, numeric value.
- § **Warning threshold.** Enter the component thresholds for the warning state. For example, if the component value is greater than 90 for 5 minutes, put the component in the warning state.
- § **Down threshold.** Enter the component thresholds for the down state. For example, if the component value is greater than 95 for 5 minutes, put the component in the down state.

### Scripting (End User Monitor)

This component enables you to monitor the experience of end users for specific web transactions – a series of steps through a web site or application. By continuously replaying your recorded web transactions from anywhere in your network, End User Monitor (EUM) components let you know when your web sites or applications are down, broken or slow before your end users complain. Before configuring an End User Monitor component in APM, you must:

- § Deploy an iDrone (EUM Poller) which will execute the web transaction from anywhere on your network, see *Configuring iDrone (EUM Poller)*, and
- § Use Ipswitch's iMacros web recording engine to record the web transaction to be monitored, see *Using iMacros with End User Monitor components*.

End User Monitor components require an iDrone (EUM Poller) registered with APM. iDrone software installed on a VM is an iDrone virtual appliance, which you can locate anywhere in your network. They replay your recorded web site and application transactions, just as an end user, measuring response times and testing functionality. iDrones are not licensed. You may deploy as many as you like, such as one at headquarters and one at a branch office, to give you multiple perspectives of an application's performance. For information on installing and configuring iDrone, see *Configuring iDrone (EUM Poller)*.

Ipswitch's iMacros web recording engine is used to record the web transactions to be monitored by End User Monitor components. Simply perform the web transaction you want to monitor while in recording mode. iMacros will generate an editable iMacros script that defines your transaction. The contents of the iMacros scripts are included in End User Monitor components' configuration. APM passes the scripts' text to iDrones, which replay the macros, just as if an end user was performing the transactions. See *Using iMacros with End User Monitor components*.

Configure the following:

- § **iDrone Name.** Select the iDrone (EUM Poller) from which you want your web transaction monitored.



**Important:** An End User Monitor component cannot be configured without a registered iDrone. See *Configuring iDrone (EUM Poller)* (on page 60).

- § **Name.** Enter a unique name for the component.
- § **Description.** Enter additional information about the component.
- § **Critical.** Click to select this check box if the component is critical.



**Note:** Components specified as critical cause the application to go into a down state when the component is out of threshold. Non-critical components cause the application to go into a warning state. For more information on application states, see *Working with application states* (on page 18).

- § **Polling frequency.** Select a time (in minutes or hours) you want APM to wait between polls.
- § **Browser type.** Select the web browser in which to replay the monitored web transaction.



**Note:** Web sites and applications can perform and function differently in different browsers. iMacros supports recording and replaying in real browsers, Internet Explorer and Firefox. See *Using iMacros with End User Monitor (EUM) components* (on page 65).



**Note:** If the performance or functionality of your web transactions in specific browsers is important to you, record the transaction using the iMacros browser add-on for that browser and select that browser type here. Otherwise, Ipswitch recommends using the iMacros Browser for recording and playback.



**Important:** End User Monitor components currently do not support the iMacros browser add-on for Chrome.

- § **Polling timeout.** Enter the length of time APM attempts to connect to the selected device. When the time you enter is exceeded without connecting, a timeout occurs and APM stops trying to connect to the device. This is considered a failed connection.
- § **Poller retries.** Enter the number of times the iDrone should attempt to execute its script in the event of an initial failure.
- § **Script text.** Paste the iMacros script text for the web transaction to be monitored.



**Note:** End User Monitor components require an iMacros script defining the web transaction to be monitored. See *Using iMacros with End User Monitor (EUM) components* (on page 65).



**Note:** Application Attribute percent variables may be used in the script text. They are resolved before the script is executed by iMacros on the iDrone.

- § **Warning threshold.** Enter the component thresholds for the warning state. For example, if the component value is greater than 9000 milliseconds for 5 minutes, put the component in the warning state.
- § **Down threshold.** Enter the component thresholds for the down state. For example, if the component value is greater than 10000 milliseconds for 5 minutes, put the component in the down state.



**Note:** End User Monitor components return transaction response time values in milliseconds.

### About iDrone (EUM Poller) and using EUM Components

End User Monitor (EUM) components enable you to monitor the experience of end users for specific web transactions – a series of steps through a web site or application. By continuously replaying your recorded web transactions from anywhere in your network, End User Monitor components let you know when your web sites or applications are down, broken or slow before your end users complain.

There are three pieces to APM's End User Monitoring architecture:

- 1 iDrones (EUM Pollers) which execute the web transaction from anywhere on your network, see *Configuring iDrone (EUM Poller)*.
- 2 Ipswitch's iMacros web recording engine to record the web transaction to be monitored, See *Using iMacros with End User Monitor components*.
- 3 APM's End User Monitor component configuration to define the polling parameters for monitoring the web transaction, see *Scripting (End User Monitor)* (on page 57) components.

End User Monitor components require an iDrone (EUM Poller) registered with APM. iDrone software installed on a VM is an iDrone virtual appliance, which you can locate anywhere in your network. They replay your recorded web site and application transactions, just as an end user, measuring response times and testing functionality. iDrones are not licensed. You may deploy as many as you like, such as one at headquarters and one at a branch office, to give you multiple perspectives of an application's performance. For information on configuring iDrone, see *Configuring iDrone (EUM Poller)* (on page 60).

Ipswitch's iMacros web recording engine is used to record the web transactions to be monitored by End User Monitor components. Simply perform the web transaction you want to monitor while in recording mode. iMacros will generate an editable iMacros script that defines your transaction. The contents of the iMacros scripts are included in End User Monitor components' configuration. APM passes the scripts' text to iDrones, which replay the macros, just as if an end user was performing the transactions. See *Using iMacros with End User Monitor components*.

Once you have deployed iDrones as monitoring locations throughout your network and recorded the web transactions you want to monitor with iMacros, you can configure End User Monitor components. Each End User Monitor component monitors one web transaction (iMacros script) from one location (iDrone). Just choose the iDrone to monitor from, paste in the iMacros script content for your recorded transaction and set the rest of the polling parameters as you like, see *Scripting (End User Monitor)* (on page 57) components.



**Note:** Each enabled End User Monitor component consumes one APM license.

### Configuring iDrone (EUM Poller)

Installing the iDrone software converts an empty virtual machine into an iDrone (EUM Poller) virtual appliance. Once configured and registered with APM, iDrones enable APM's End User Monitor (EUM) components to monitor the performance of your most important web transactions from locations throughout your network. The iDrone software is not licensed. You can deploy multiple iDrone virtual appliances to monitor your end users' experience from where they are located. Each End User Monitor component can only use one iDrone. To monitor the same web transaction from multiple iDrones, you must configure an End User Monitor component for each iDrone.



**Note:** You can give multiple iDrones the same iDrone Name. End User Monitor components configured with that iDrone Name use any of the iDrones sharing the name randomly. This configuration can help to scale iDrone's monitoring or give you transaction monitoring from multiple locations with a single End User Monitor component. You will not be able to know which measurement came from which iDrone.

To prepare for the installation, create a new virtual machine using VMWare or VirtualBox and one of the following Guest Operating Systems:

- § Windows 7
- § Windows Server 2008 R2 or Windows Server 2012 R2 with the latest updates and all service packs installed (for Win 2008 R2 and Win 2012 R2, you need to enable .NET Framework 3.5)



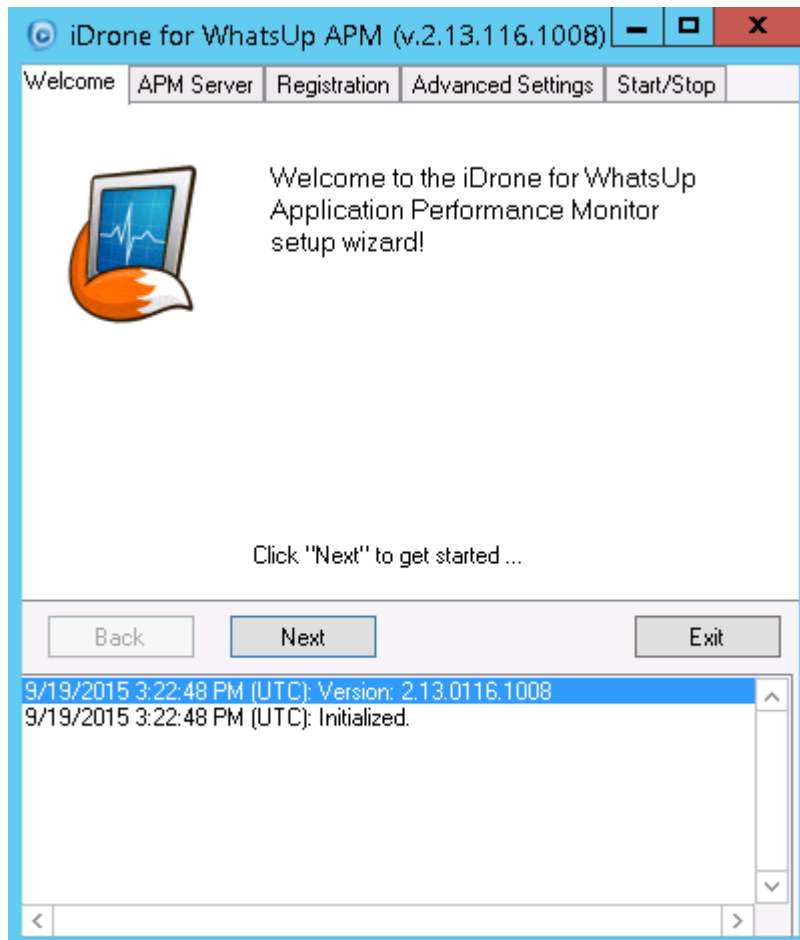
## WhatsUp Gold Application Performance Monitoring Guide

- 1 Take a snapshot of your virtual machine configuration.
- 2 Download the iDrone installer from [WhatsUpGold.com/iDrone](http://WhatsUpGold.com/iDrone) onto your new virtual machine.



**Important:** Ipswitch recommends installing the iDrone on a dedicated VM that is not used for any other purposes.

- 3 Run the installer and complete the installation process. If prompted, reboot the virtual machine after installation. Once the installation is complete, the iDrone Configuration dialog launches automatically.
- 4 At the initial iDrone for WhatsUp APM Welcome tab, click **Next**.



- 5 Enter the IP address or host name of the server running WhatsUp Gold, then click **Check** to ensure the iDrone can communicate with APM.



## WhatsUp Gold Application Performance Monitoring Guide



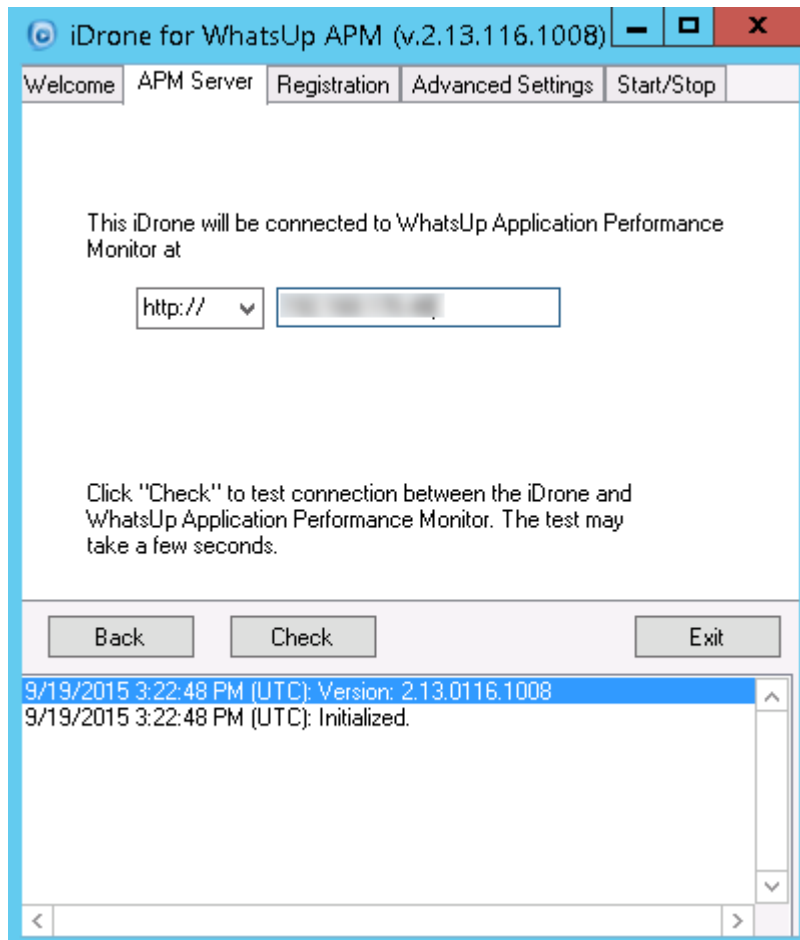
**Important:** If your WhatsUp Gold IIS instance is using a non-standard port, in *APM Application Settings* (on page 92) click **Auto Detect** to update the iDrone Service Manager's URL.

If your WhatsUp Gold server is configured to use SSL only:

a. Choose `https://` from the list.

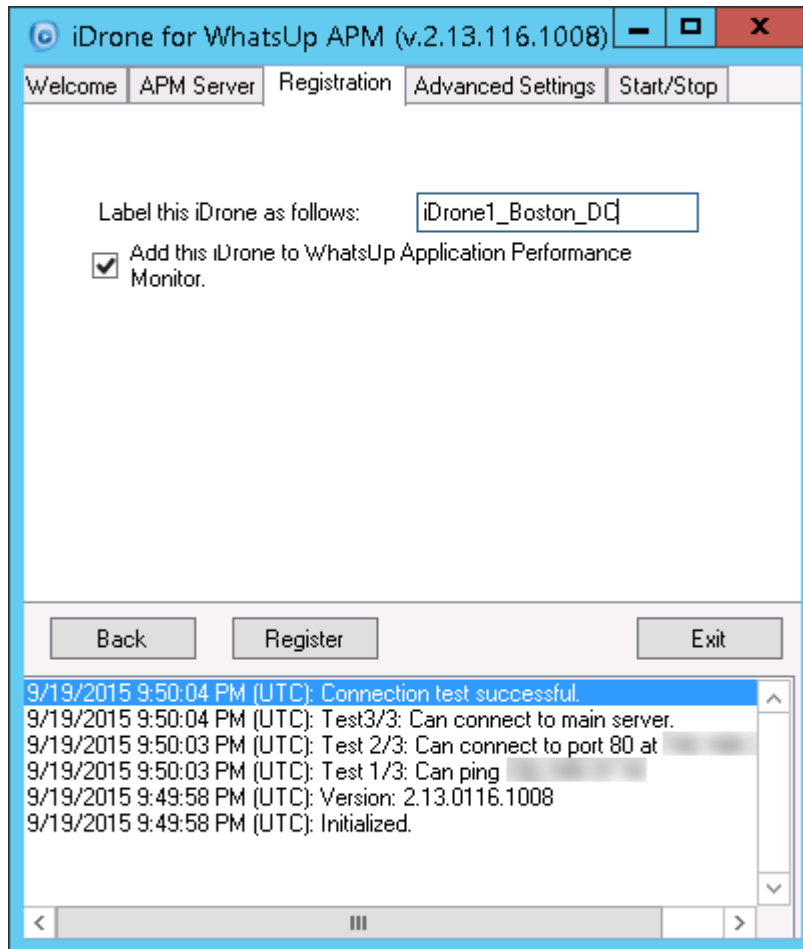
b. Enter the host name of the machine where WhatsUp Gold is installed. The host name of the WhatsUp Gold server must match the common name (Subject) on the certificate configured on the WhatsUp Gold server. The certificate also needs to be imported into the Trusted Root Certification Authorities store for the local machine where the iDrone is installed.

c. In APM Application Settings, click Auto Detect to update the iDrone Service Manager's URL. Verify the URL starts with `https` and the host name is exactly the same as the host name you used in the iDrone configuration.

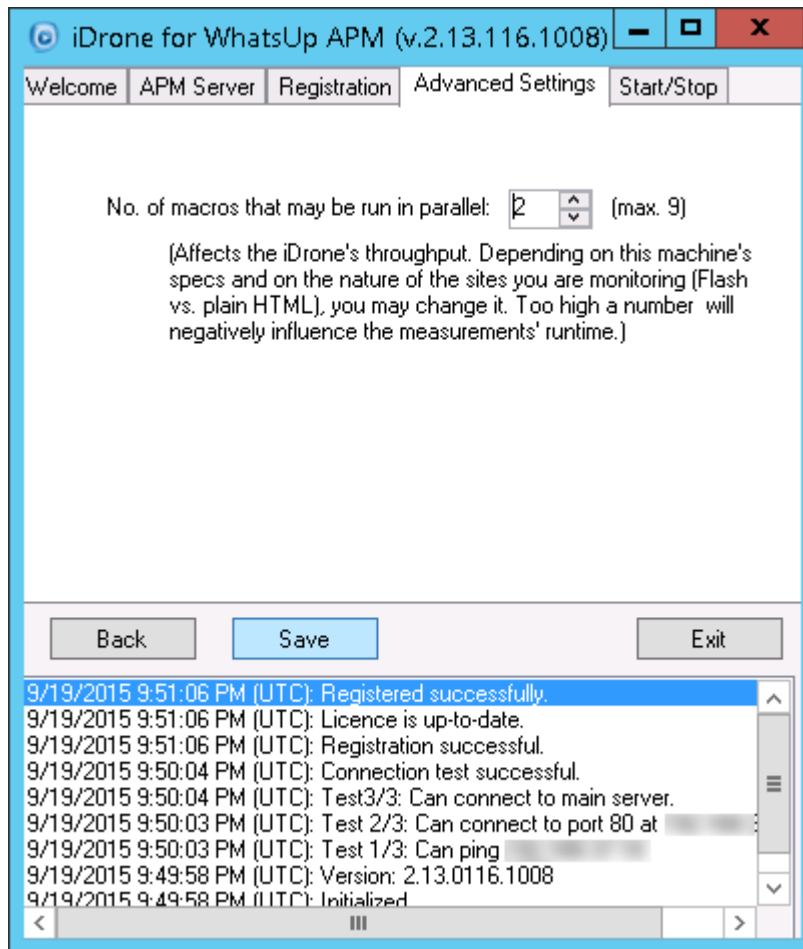


## WhatsUp Gold Application Performance Monitoring Guide

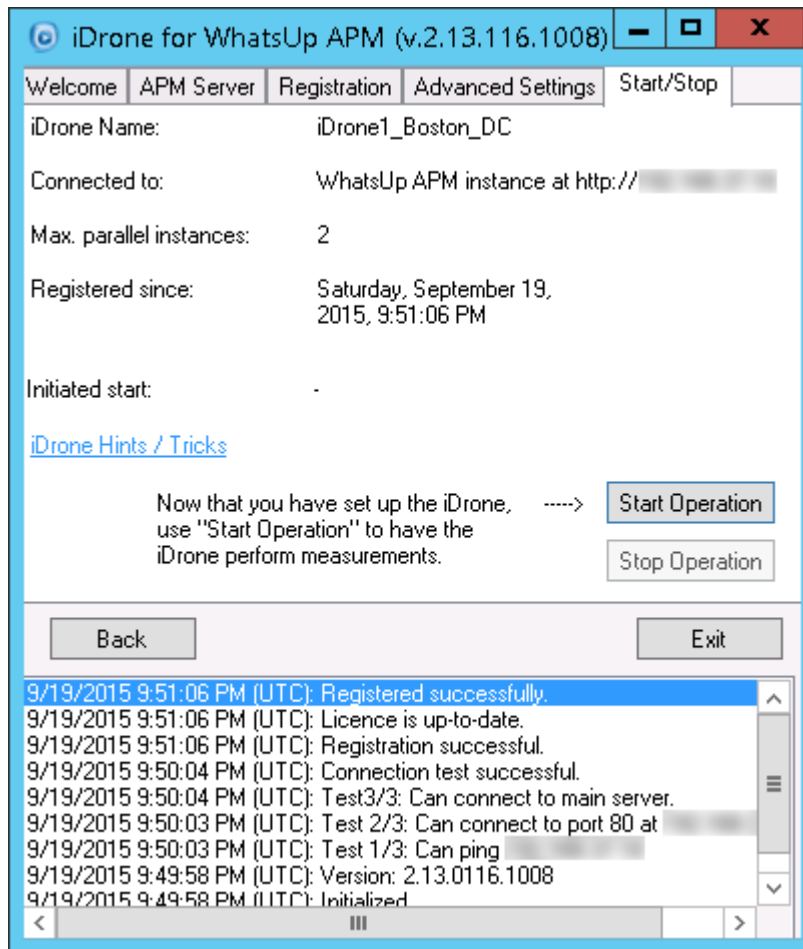
- 6 Enter a name for your iDrone and ensure **Add this iDrone to WhatsUp APM** is enabled, then click **Register**.



- 7 Select the number of macros that can be run in parallel if desired, then click **Save**.



8 To begin monitoring using the iDrone, click **Start Operation**.



### Using iMacros with End User Monitor (EUM) Components

Ipswitch's iMacros web recording engine is used to record the web transactions to be monitored by End User Monitor (EUM) components. It supports WYSIWYG recording of web site and application transactions. Simply perform the web transaction you want to monitor while in recording mode. iMacros generates an editable iMacros script that defines your transaction. iMacros uses these scripts to playback the web transaction. In APM, iMacros plays back the script on iDrones throughout your network to monitor the performance and verify the functionality of your web sites and applications.

You can record and play back web transactions in the iMacros Browser which is an emulated browser based on Internet Explorer. Or, you can use Internet Explorer and Firefox browsers using the iMacros browser addons. The browser addons are useful if you are concerned about the performance and function of your web transactions in a specific browser. If you don't have a need to monitor your transactions in a specific browser, use the iMacros browser. The iMacros real browser addons are freely distributed. The iMacros Browser is licensed as either the Enterprise or Standard edition. To compare features between the free and licensed edition, see <http://www.iMacros.net/compare-versions>. To download any of the versions, go to <http://www.iMacros.net/download>.


The iMacros Browser Enterprise Edition and Internet Explorer and Firefox browser addons are already installed on the iDrone for you to get started. Once your iDrone is operational,

Ipswitch recommends you install iMacros on your desktop for recording or editing iMacros scripts. If you would prefer not to install iMacros or license the iMacros browser, you can register another iDrone with WhatsUp Gold just to use for script recording and editing.



**Note:** End User Monitor components do not currently support the iMacros addon for Chrome.

### To create a macro for use with APM End User Monitor components:

- 1 Log in to a registered iDrone or install a version of iMacros on your desktop.
- 2 Launch the Internet Explorer, Firefox or iMacros Browser. If you are using Internet Explorer or Firefox, click the iMacros icon (  ) found in the browser's Command Bar or to the left of the address window, respectively. You should see the iMacros sidebar once iMacros has been started.
- 3 Navigate to the URL of the site or application where your web transaction begins.
- 4 Select the **Rec** or **Recording** tab in the iMacros sidebar, then click **Record**.
- 5 Perform your transaction. Whenever possible, use mouse clicks instead of keystrokes. When your transaction is complete, click **Stop**. iMacros saves the most recently recorded macro in `#Current.iim`. The macro is now highlighted in the navigation tree in the iMacros sidebar.
- 6 Navigation to the **Play** tab, then click **Play** to view the transaction and confirm it was recorded as intended.
- 7 Save your macro to another filename so it will not be overwritten with the next recording:

Select `#Current.iim` in the navigation tree.

- a) Navigate to the **Rec** or **Record** tab.
  - b) Click **Save Macro As**.
  - c) Enter a new filename and location as desired.
- 1 To see the script text of the macro, make sure the correct file is highlighted in the navigation tree.
  - 2 Navigate to the **Manage** tab, then click **Edit Macro** to launch the iMacros Editor.
  - 3 Edit your scripts as needed.
  - 4 Copy the script content to your clipboard.
  - 5 Return to the End User Monitor component you are configuring in APM, then paste the script content into the Script Text field.

### Service Check

The Service Check component allows you to monitor a service on a specific device using either *SNMP* (on page 66) or *WMI* (on page 67) credentials. You may add a Service Check component to an application profile or an application instance.

#### Service Check (SNMP)

Configure the following for the SNMP Service Check component:

- § **Name.** Enter a unique name for the component.
- § **Description.** Enter additional information about the component.

§ **Critical.** Click to select this check box if the component is critical.



**Note:** Components specified as critical cause the application to go into a down state when the component is out of threshold. Non-critical components cause the application to go into a warning state. For more information on application states, see *Working with application states*.

§ **Polling frequency.** Select a time (in minutes or hours) you want APM to wait between polls.

§ **Service Name.** Type the name of the service you want to monitor or click browse (...) to bring up the device browser to select the specific device and service. The name of the service must be entered exactly as it appears in the list of available services.

§ **Restart on failure.** Select this option to have the monitor attempt to restart the service when it enters a down state.

§ **Polling timeout.** (SNMP Only) Enter the length of time APM attempts to connect to the selected device. When the time you enter is exceeded without connecting, a timeout occurs and APM stops trying to connect to the device. This is considered a failed connection.

§ **Poller retries.** (SNMP Only) Enter the number of times APM attempts to send the command before the device is considered down.

### Service Check (WMI)

Configure the following for the WMI Service Check component:

§ **Name.** Enter a unique name for the component.

§ **Description.** Enter additional information about the component.

§ **Critical.** Click to select this check box if the component is critical.



**Note:** Components specified as critical cause the application to go into a down state when the component is out of threshold. Non-critical components cause the application to go into a warning state. For more information on application states, see *Working with application states*.

§ **Polling frequency.** Select a time (in minutes or hours) you want APM to wait between polls.

§ **Service Name.** Type the name of the service you want to monitor or click browse (...) to bring up the device browser to select the specific device and service. The name of the service must be entered exactly as it appears in the list of available services.

§ **Restart on failure.** Select this option to have the monitor attempt to restart the service when it enters a down state.

### SNMP

The SNMP Check component allows you to use SNMP credentials to monitor a specific application instance running on a device. You may add an SNMP Check component to an application profile or an application instance.

§ **Name.** Enter a unique name for the component.

§ **Description.** Enter additional information about the component.

§ **Critical.** Click to select this check box if the component is critical.



**Note:** Components specified as critical cause the application to go into a down state when the component is out of threshold. Non-critical components cause the application to go into a warning state. For more information on application states, see *Working with application states*.

§ **Polling frequency.** Select a time (in minutes or hours) you want APM to wait between polls.

§ **Performance Counter.** The performance counter you would like to monitor. You may type the performance counter or click browse (...) next to Instance to select the counter.

§ **Instance.** The instance you would like to monitor. You may type the instance or click browse (...) to access the SNMP MIB browser and select the specific device, performance counter, and application instance you want to monitor.

§ **Use raw value.** Select this check box to gauge the current polled value instead of tracking the rate of change over time.

§ **Polling timeout.** Enter the length of time APM attempts to connect to the selected device. When the time you enter is exceeded without connecting, a timeout occurs and APM stops trying to connect to the device. This is considered a failed connection.

§ **Poller retries.** Enter the number of times APM attempts to send the command before the device is considered down.

§ **Warning threshold.** Enter the component thresholds for the warning state. For example, if the component value is greater than 90 for 5 minutes, put the component in the warning state.

§ **Down threshold.** Enter the component thresholds for the down state. For example, if the component value is greater than 95 for 5 minutes, put the component in the down state.

### SSH

The SSH component allows you to run a command on a specific device and analyze the output. You can configure the SSH component as either an *active* (on page 68) monitor check or a *performance* (on page 69) monitor check.

#### SSH (Active)

Configure the following boxes for the SSH Active Monitor Check component:

§ **Name.** Enter a unique name for the component.

§ **Description.** Enter additional information about the component.

§ **Critical.** Click to select this check box if the component is critical.



**Note:** Components specified as critical cause the application to go into a down state when the component is out of threshold. Non-critical components cause the application to go into a warning state. For more information on application states, see *Working with application states*.

- § **Polling frequency.** Select a time (in minutes or hours) you want APM to wait between polls.
- § **Command to run.** Enter the command to execute on the device. This command can be anything that a device can interpret and run; for example, a basic UNIX command or Perl script. The command or script must return a single numeric value. For example:  
Single-line Unix-style: `free -m | awk 'NR==2{print $3}'`
- § **Line end characters.** Select the appropriate character type; either None, Linefeed, Carriage return, or Carriage return linefeed. Multiline scripts are entered and persisted on a Windows operating system, and include line-ending characters that may not be recognized on the target device. This configuration feature instructs the application to replace the line-ending characters with the selected characters prior to connection and command execution.
- § **Output to match.** Enter the output that should match the command result.
- § **Up if matches.** Select this option to put the application in the up state if the output matches.
- § **Use regex.** Select to use a regular expression to evaluate the match.

### SSH (Performance)

Configure the following boxes for the SSH Performance Monitor Check component:

- § **Name.** Enter a unique name for the component.
- § **Description.** Enter additional information about the component.
- § **Critical.** Click to select this check box if the component is critical.



**Note:** Components specified as critical cause the application to go into a down state when the component is out of threshold. Non-critical components cause the application to go into a warning state. For more information on application states, see *Working with application states*.

- § **Polling frequency.** Select a time (in minutes or hours) you want APM to wait between polls.
- § **Command to run.** Enter the command to execute on the device. This command can be anything that a device can interpret and run; for example, a basic UNIX command or Perl script. The command or script must return a single numeric value. For example:  
Single-line Unix-style: `free -m | awk 'NR==2{print $3}'`
- § **Line end characters.** Select the appropriate character type; either None, Linefeed, Carriage return, or Carriage return linefeed. Multiline scripts are entered and persisted on a Windows operating system, and include line-ending characters that may not be recognized on the target device. This configuration feature instructs the application to replace the line-ending characters with the selected characters prior to connection and command execution.
- § **Warning threshold.** Enter the component thresholds for the warning state. For example, if the component value is greater than 90 for 5 minutes, put the component in the warning state.



- § **Down threshold.** Enter the component thresholds for the down state. For example, if the component value is greater than 95 for 5 minutes, put the component in the down state.

### WMI

The WMI component allows you to use Windows credentials to monitor either *formatted* (on page 70) or *raw* (on page 70) data for a specific application instance.

#### WMI (Formatted)

Configure the following for the WMI Formatted counter check component:

- § **Name.** Enter a unique name for the component.
- § **Description.** Enter additional information about the component.
- § **Critical.** Click to select this check box if the component is critical.



**Note:** Components specified as critical cause the application to go into a down state when the component is out of threshold. Non-critical components cause the application to go into a warning state. For more information on application states, see *Working with application states*.

- § **Polling frequency.** Select a time (in minutes or hours) you want APM to wait between polls.
- § **Performance Counter.** The performance counter you would like to monitor.
- § **Instance.** Type the instance name or click browse (...) to access the WMI Performance Counter dialog and select the specific device, performance counter, and application instance you want to monitor.
- § **Polling timeout.** Enter the length of time APM attempts to connect to the selected device. When the time you enter is exceeded without connecting, a timeout occurs and APM stops trying to connect to the device. This is considered a failed connection.
- § **Warning threshold.** Enter the component thresholds for the warning state. For example, if the component value is greater than 90 for 5 minutes, put the component in the warning state.
- § **Down threshold.** Enter the component thresholds for the down state. For example, if the component value is greater than 95 for 5 minutes, put the component in the down state.

#### WMI (Raw)

Configure the following for the WMI raw counter check component:

- § **Name.** Enter a unique name for the component.
- § **Description.** Enter additional information about the component.
- § **Critical.** Click to select this check box if the component is critical.



**Note:** Components specified as critical cause the application to go into a down state when the component is out of threshold. Non-critical components cause the application to go into a warning state. For more information on application states, see *Working with application states*.

- § **Polling frequency.** Select a time (in minutes or hours) you want APM to wait between polls.
- § **Performance Counter.** The performance counter you would like to monitor.
- § **Instance.** Type the instance name or click browse (...) to access the WMI Performance Counter dialog and select the specific device, performance counter, and application instance you want to monitor.
- § **Polling timeout.** Enter the length of time APM attempts to connect to the selected device. When the time you enter is exceeded without connecting, a timeout occurs and APM stops trying to connect to the device. This is considered a failed connection.
- § **Warning threshold.** Enter the component thresholds for the warning state. For example, if the component value is greater than 90 for 5 minutes, put the component in the warning state.
- § **Down threshold.** Enter the component thresholds for the down state. For example, if the component value is greater than 95 for 5 minutes, put the component in the down state.

### Windows Performance Counter

The Windows Performance Counter component enables data collection from performance counters exposed by various Windows applications. This monitor requires Windows credentials on the device for which you want to monitor Windows applications. Additionally, devices for which you want to monitor Windows applications must have the *Remote Procedure Call* and *Remote Registry* services enabled and running.

You can utilize the Windows Performance Monitor tool available from the Windows Start menu. Click **Start**, type `perfmon.exe`, and then press **Enter** to view available Windows performance counters on Windows devices.

Configure the following for the Windows Performance Counter component:

- § **Name.** Enter a unique name for the component.
- § **Description.** Enter additional information about the component.
- § **Critical.** Click to select this check box if the component is critical.



**Note:** Components specified as critical cause the application to go into a down state when the component is out of threshold. Non-critical components cause the application to go into a warning state. For more information on application states, see *Working with application states*.

- § **Polling frequency.** Select a length in time (in minutes or hours) you want APM to wait between polls.
- § **Category.** Enter the category to which the Windows performance counter you want to monitor belongs, such as *Processor*.
- § **Counter.** Enter the specific performance counter in the category specified above for which you want to monitor, such as *% Processor Time*.
- § **Instance.** (Optional) If applicable, enter the specific instance of the performance counter specified above for which you want to monitor, such as *\_Total*. Not all counters have specific instances, so this box may be left blank.

- § **Sample interval.** For continuous counters, enter the length of time (in milliseconds) that should elapse between collecting samples. You can enter a value between 10 and 60,000 milliseconds.
- § **Warning threshold.** The Warning threshold signifies that the performance counter has reached the threshold criteria specified and is in a warning state. First, specify the threshold; select either Value equal to, Value less than, or Value equal to, and then enter a numerical value. Second, specify the threshold Duration; enter a numerical value, and then select either Minutes, Hours, Days, or Polls.
- § **Down threshold.** The Down threshold signifies that the performance counter has reached the threshold criteria specified and is in a down state. First, specify the threshold; select either Value equal to, Value less than, or Value equal to, and then enter a numerical value. Second, specify the threshold Duration; enter a numerical value, and then select either Minutes, Hours, Days, or Polls.

### Managing critical component groups

A critical component group is a grouping of components that contains specific logic to allow for complex evaluation of the up/down state of an application. For example, given four components A,B,C and D, the following logic can be applied, so that if A and B are down or C and D are down the application is placed into the down state. ((A and B) or (C and D)). Critical component groups are always considered "critical", in that if a critical component group is evaluated to be in the down state, the entire application is in the down state.

Components can be added to or removed from entire application profiles or specific instances.

For example, you create a critical component group called *Device Utilization* and assign the following components to the group:

- § CPU Utilization
- § Disk Utilization
- § Physical Memory Utilization
- § Virtual Memory Utilization

You then assign the following state logic to the critical component group: If CPU Utilization and Virtual Memory Utilization equal Down and Disk Utilization equal Warning, then the component group is Down. Since this component group is considered "critical", the application instance that contains this critical component group would also be Down.



**Note:** After an instance has been created, each component uses *one license each* since they are individual components of an application instance.

*Learn more about APM terminology (on page 2).*

### Adding critical component groups to an application profile

There must be at least two components included in a critical component group. For more information, see *Working with critical component groups*.

To add a critical component group to an application profile:

- 1 Click the **APM** tab, then select **Configuration**.
- 2 Select the application profile for which you want to add a critical component group, then click **Edit/View Application Profile**. The Components list appears.
- 3 In the Components section, click **Add critical component group**. The Critical Component Group information appears.
- 4 Enter or select the appropriate information:
  - § **Name**. Enter a unique name for the critical component group.
  - § **Description**. (Optional) Enter additional information about the critical component group.
  - § **State Configuration**. Select a configuration for the critical component group. For example, if CPU Utilization component is down and the Disk Utilization component is down, then the component group is down.
- 5 Click **Save**.

Learn more about APM terminology

### Adding critical component groups to an application instance

To add a critical component group to an application instance:

- 1 Create an application instance.
- 2 In the Components section, click **Add critical component group**. The Critical Component Group information appears.  
Enter or select the appropriate information:
  - § **Enabled**. Select this option to enable or disable the critical component group.
  - § **Action Policy**. Select an action policy for the critical component group.
  - § **Name**. Enter a unique name for the critical component group.
  - § **Description**. (Optional) Enter additional information about the critical component group.
  - § **State Configuration**. Select a configuration for the critical component group. For example, if CPU Utilization component is *down* and the Disk Utilization component is *down*, then the component group is *down*.



**Note:** When a critical component group is added to an application instance, not inherited from the profile, you must add additional unique components for the critical component group to evaluate for application states.

- 3 Click **Save**.

### Managing discrete applications

A discrete application is an application upon which a complex application has a dependency. For example, IIS and SQL Server are discrete applications on which the complex application WhatsUp Gold is dependent. A discrete application is used when you are monitoring a complex application. You may *add a discrete application to an application profile* (on page 74) or *add a discrete application to an application instance* (on page 75) as a component. *Learn more about APM terminology* (on page 2).



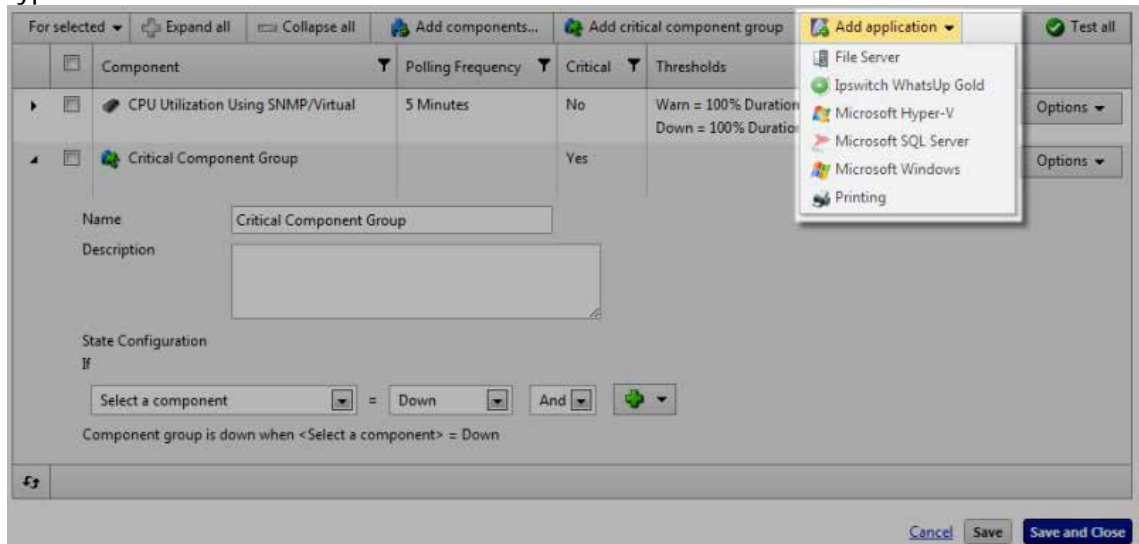
**Note:** Adding a discrete application to an application profile helps build the foundation of the profile, but does not add the discrete application to an application instance.

### Adding discrete applications to an application profile

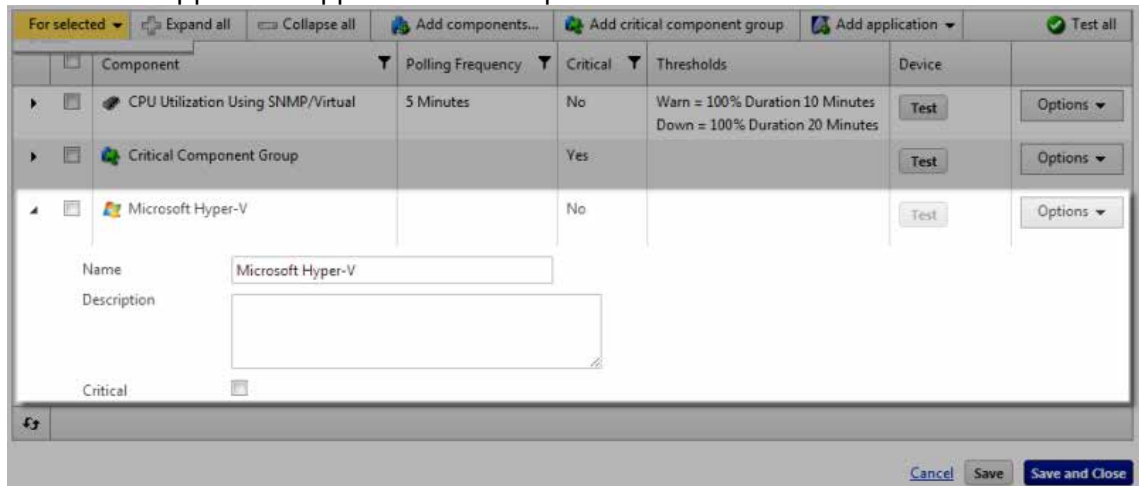
A discrete application is an application upon which a complex application has a dependency. For example, IIS and SQL Server are discrete applications on which the complex application WhatsUp Gold is dependent. A discrete application is used when you are monitoring a complex application. Learn more about APM terminology.

To add a discrete application to an application profile:

- 1 From the WhatsUp Gold web interface, go to **APM > Configuration**. The All Application Profiles page appears.
- 2 Select the application profile for which you want to add a critical component group, then click **Edit/View Application Profile**. The Components list appears.
- 3 In the Components section, click **Add application**, then select an application profile type from the list.



The discrete application appears in the Components section.



## WhatsUp Gold Application Performance Monitoring Guide

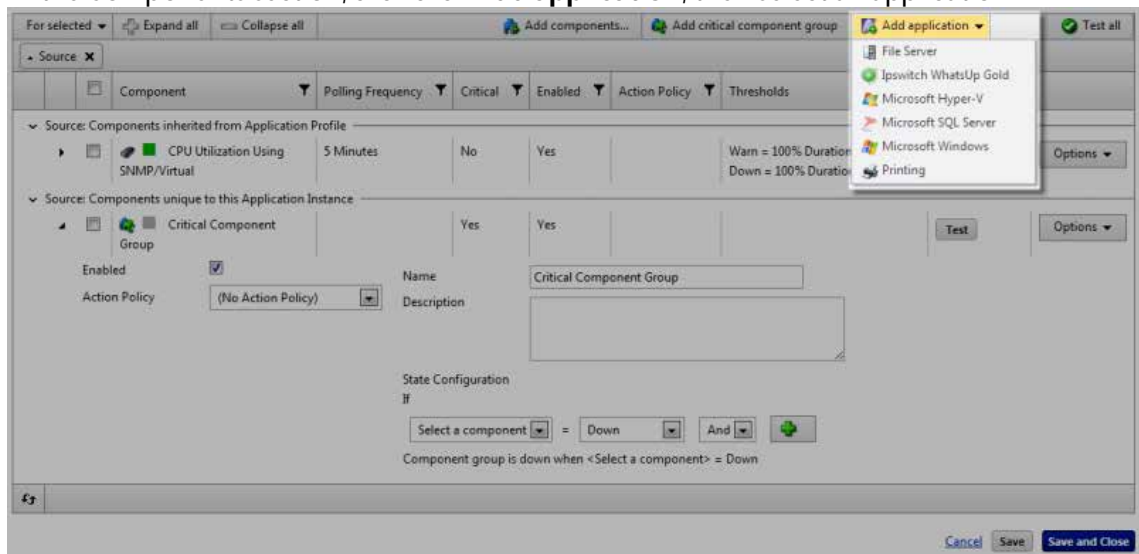
- 4 Enter or select the appropriate information:
  - § **Name.** Enter a unique name for the discrete application.
  - § **Description.** (Optional) Enter additional information about the discrete application.
  - § **Critical.** Select this option if the discrete application is critical.
- 5 Click **Save** to save your changes or click **Save and Close** to complete your changes.

### Adding discrete applications to an application instance

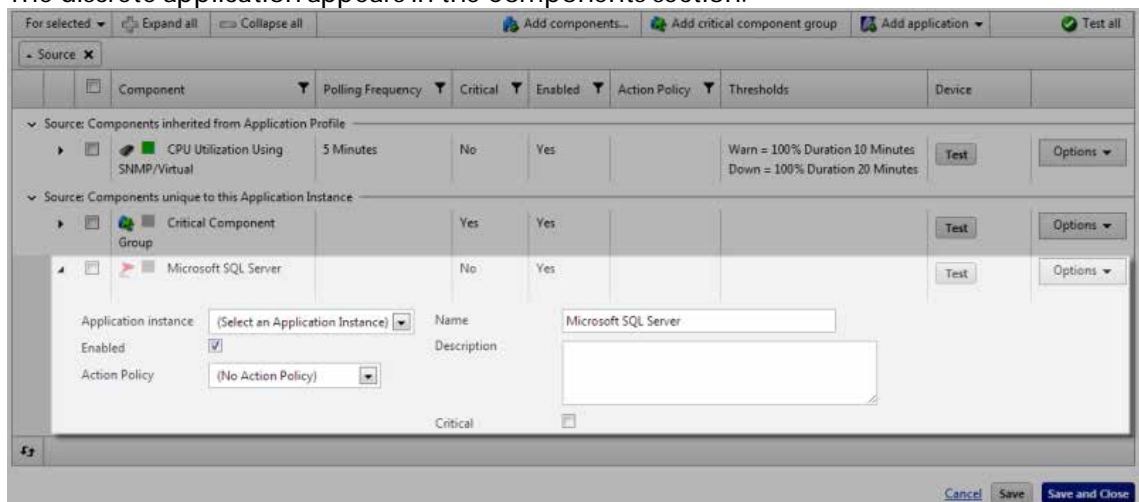
A discrete application is an application upon which a complex application has a dependency. For example, IIS and SQL Server are discrete applications on which the complex application WhatsUp Gold is dependent. A discrete application is used when you are monitoring a complex application. Learn more about APM terminology.

To add a discrete application to an application instance:

- 1 Create an application instance from a preconfigured application profile.
- 2 In the Components section, click **Add application**, then select an application.



The discrete application appears in the Components section.



- 3 Enter or select the appropriate information:

- § **Application instance.** Select the application instance to be monitored for the component.
  - § **Enabled.** Select this option to enable or disable the discrete application.
  - § **Action Policy.** Select an action policy for the discrete application.
  - § **Name.** Enter a unique name for the discrete application.
  - § **Description.** (Optional) Enter additional information about the discrete application.
  - § **Critical.** Select this option if the discrete application is critical.
- 4 Click **Save** to save your changes or click **Save and Close** to complete your changes.

## Applying application attributes

Attributes are used to specify identifying information about an application. Just as attributes can be created for and applied to devices in WhatsUp Gold, they can also be created for and applied to application profiles in APM. Application attributes can be used when configuring components and actions.

Attributes created in APM can also be applied to individual application instances without changing the parent application profile. When instances are created from an application profile, any attributes applied to that profile are inherited by the instance. However, inherited attributes can be overridden if desired.

**To create a new attribute:**

- 1 Click the **APM** tab, then select **Configuration**.
- 2 Select **All Application Profiles** or any application profile type displayed in the APM navigation tree and click **Add Application Profile**. Or, select an existing editable application profile, then click **Edit Application Profile**.



**Tip:** You can also create a new application profile using an existing application profile as a template by clicking **Edit a Copy**.

- 3 Expand the Details configuration table to the right of **Attributes**.



- Click **Add attribute**, then select an attribute from the list.

■ WhatsUp Gold v16.3.x on JCB12Win7x64

Name

Description

Attributes ▼ Details

Name	Value	
Location	<input type="text" value="Atlanta"/>	<input type="button" value="Clear"/>

▼

Device

TEST Timeout  seconds

Action Policy  ▼

In Maintenance

22 active components, 2 disabled components

Licensing (APM total: 69 active components of 10,000 available) [Details](#)

- Enter a Value for the new attribute. If you selected **Create new attribute** from the list, enter a Name for the attribute as well.
- Click **Save**.



**Important:** When an attribute is applied to an application profile, it is automatically included when that profile is imported into or exported from APM by another end-user.

After an attribute has been created and has an assigned value, it is available for use and can easily be applied when configuring APM actions or components using percent variables. When added to actions, attributes automatically populate their assigned values in message content. When added to component definitions, attributes are used to poll components and test functionality.

Please note, when using application attributes when configuring components:

- § Application attribute values are resolved when you initiate the Test feature so the correct component settings are sent.
- § Application attribute values are resolved when polling components that use them.
- § If an inherited application attribute value is overridden at instance level, that value is used during polling.

## Action policies

APM allows you to configure action policies that can be applied to application instances and components you are monitoring with APM.



An action policy determines actions to take when an application instance or component transitions from one state to another. The transition to states are up, down, warning, and maintenance. You must create one or more actions before creating an action policy. You may also apply a blackout policy to the action policy. The blackout policy determines when to apply the action policy and when it should be ignored due to routine activities, such as maintenance periods.



**Important:** All applications and systems monitored with APM must have their system clocks synchronized so that Action Policies and Actions work correctly according to the settings and scheduled actions.

## Working with action policies

To access the action policies feature, click the **APM** tab, then select **Actions**. Use the Action Policies page to configure new or existing policies.

- § Click **Add Action Policy** to configure a new action policy.
- § Select an action policy, then click **Edit** in Options to modify its configuration.
- § Select an action policy, then click **Delete** to remove it from the library.

## Creating an action policy

Action policies enable you to determine the actions you would like the system to perform when an instance or component transitions from one state to another. The state transition rules evaluate whether to permit the associated action to fire based on the amount of time the source was in a previous state. The action rules determine which action to fire, how long to wait in the target state before firing the action, and which blackout policy to apply. The blackout policy prohibits an action from firing during defined periods of time when activities such as server maintenance generate large numbers of actions that are not of interest.

### Sources

The Sources area displays the application instances to which the application policy is applied.

### State Transition Rules

State transition rules use the time in the previous state (state transition criteria) to evaluate whether to perform an associated action for each state transition type (Up to Down, Maintenance to Down, Warning to Down, Up to Unknown, etc.). If the source was in the previous state for the amount of time stated in the rule prior to transitioning to the current state, the action defined in the Action Rules section is performed. Using state transition criteria can help reduce the number of state transitions that cause an action to fire by ignoring state transitions that are short lived or intermittent.

For example, you can create a state transition rule that performs an email action when the source goes to the Down state (target current state) from the Up state (previous state) and had been in the Up state for at least 5 minutes prior to entering the Down state (state

transition criteria). This state transition rule does not cause the action to fire for state transitions where the source was in the Down state for less than 5 minutes.

The state transition rules may be defined for the following current states, each represented by a separate tab:

- § **Up.** Designate the state transition rules for each event going to the Up state from Down, Maintenance, Warning, or Unknown.
- § **Down.** Designate the state transition rules for each event going to the Down state from Maintenance, Up, Warning, or Unknown.
- § **Warning.** Designate the state transition rules for each event going to the Warning state from Down, Maintenance, Up, or Unknown.
- § **Maintenance.** Designate the state transition rules for each event going to the Maintenance state from Down, Up, Warning, or Unknown.

### Action Rules

The Action Rules section allows you to designate the actions that occur when a State Transition Rule for the target current state is met. For example, you may assign the email action to occur when the source goes into the Up state from the Down state and remains in the up state for 5 minutes, after meeting the state transition rule of having been in the Down state for at least 10 minutes before transitioning to the Up state.

#### To create a new action policy:

- 1 Click the **APM** tab, then select **Actions**. The Action Policies page appears.
- 2 Click **Add Action Policy**. The Edit Action Policy page appears.
- 3 Enter a unique **Name** for the Action Policy.
- 4 Select the **Up** tab and create the state transition and action rules for the Up state.
- 5 Select the **Down** tab and create the state transition and action rules for the Down state.
- 6 Select the **Warning** tab and create the state transition and action rules for the Warning state.
- 7 Select the **Maintenance** tab and create the state transition and action rules for the Maintenance state.
- 8 Click **Save** or **Save and Close**. The Action Policy is added to the Action Policies list on the Action Policies screen.

#### To create the state transition and action rules for transitions to the Up state:

- 1 If the associated actions are to be triggered from the Down to Up transition, select **Down** and enter the minimum amount of time the source must have been in the Down state prior to the transition.
- 2 If the associated actions are to be triggered from the Maintenance to Up transition, select **Maintenance** and enter the minimum amount of time the source must have been in the Maintenance state prior to the transition.
- 3 If the action is to be triggered by a transition from the Warning to Up transition, select **Warning** and enter the minimum amount of time the source must have been in the Warning state prior to the transition.
- 4 If the action is to be triggered by a transition from the Unknown to Up transition, select **Unknown** and enter the minimum amount of time the source must have been in the Unknown state prior to the transition.

- 5 Create the action rules to be associated with transitions to the Up state.
  - a) Click **Add action rule**. The Action rule dialog controls appear.
  - b) Select an **Action** from the list of currently configure actions. If the list is empty, click **Create new action** to configure a new action for the policy.
  - c) Enter the number of minutes to wait after entering the Up state before firing the action in the **Fire after (minutes)** box.
  - d) Select the **Blackout policy** you want to apply to the action. If the list is empty, click **Create new blackout policy** to configure a new blackout policy for the action policy.
  - e) Click **Save**. The action is added to the Actions list.
- 6 When you have completed configuring the policy, click **Save and Close**.

### Assigning an action policy to an instance or component

Once created, you can assign action policies to application instances or selected components within an instance.

#### To assign an action policy to a single application instance or component:

- 1 In the Application Profiles navigation tree, select the application profile for which you want to add an action policy.
- 2 Select the component within the profile or the specific application instance for which you want to add an action policy, then click **Edit Application Profile**.
- 3 Select the action policy you want to apply. If you select from the Action Policy list for the instance, the action policy is applied to every component within the instance. If you select from the Action Policy list for an individual expanded component in the Components section below, the action policy is only applied to that component.
- 4 Click **Save**.

#### To assign an action policy to multiple application instances or components:

- 1 Select an application profile from the Application Profiles navigation tree if you want to apply an action policy to multiple instances of an application.  
OR  
Select an application instance from the Application Profiles navigation tree if you want to apply an action policy to specific components within an individual instance.
- 2 Use the selection boxes at left to choose specific application instances or components. Whether you select instances or components depends upon your selection from the Application Profile navigation tree in the previous step.
- 3 Select **For selected > Assign Action Policy** and then choose the action policy you want to apply.
- 4 Click **Save**.



**Note:** If you select All Application Profiles from the top level of the Application Profiles navigation tree, you also have the ability to apply action policies to multiple application profiles as once using the same methods described here. However, assigning action policies to application profiles only serves to modify the profiles' settings in the event an instance is created using that profile in the future.

## Managing action policies

Action Policies are managed from the Running Action Policies screen, accessible from the APM Status page, in the Current Status section. Here you can see all of the Action Policies that are active in your APM environment. Information about the source being monitored by the policy, the current state, any actions taken, as well as the next action to be taken is visible in a table that can be filtered and sorted for quick access to the data about your action policies. You can also acknowledge any action policies with outstanding actions from this screen. The following fields are available for filtering and sorting:

- § **Source.** The application or component to which the Action Policy is being applied.
- § **State.** The state of the application or component to which the Action Policy is being applied.
- § **Action Policy.** The name of the Action Policy being applied to the application or component.
- § **Most Recent Action.** The most recent action that has fired in response to a condition of the Action Policy.
- § **Next Action.** The next action that will fire in response to a condition of the Action Policy.
- § **Start Time.** The time at which the first condition was met that caused an action to fire in response to the Action Policy.

To acknowledge an action policy:

- 1 Select the action policy you want to acknowledge from the Running Action Policies list.
- 2 Click **Acknowledge Selected**.

## Actions

APM allows you to designate specific actions to execute when an application instance or component is outside of its action policy thresholds. For example, you may designate that an email is sent to your company email address each time an event occurs.

### Working with actions

To access the Actions page, first click the **APM** tab. Select **Actions** from the top of the APM interface, then **Actions** under Actions Management at left. Use the APM Actions page to configure new or existing actions.

- § Click **Add Action** to *configure a new action* (on page 82).
- § Select **Edit** from the Options menu associated with an action to modify an action's configuration.
- § Select **Delete** from the Options menu associated with an action to remove an action from the library.

## Creating a new action

To create a new action in APM:

- 1 Click the **APM** tab, then select **Actions**.
- 2 Click **Add Action**. The Edit Action page appears.
- 3 Select an action from the **Action Type** list.
- 4 Enter the appropriate information:
  - § **Name**. Enter a unique name for the action.
  - § **Description**. (Optional) Enter additional information about the action.
- 5 Enter or select the appropriate information into each of the action boxes applicable to the selected action type.
- 6 Click **Save**.

## Adding an Active Script action

This action allows you to write either VBScript or JScript code to perform a customized action. If the script returns an error code, the action failed.



**Note:** This script action has a context object you can use to get specific information about the context of the action.



**Note:** We have provided several code samples for you to create useful script actions for your devices.



**Note:** All script features in WhatsUp Gold utilize the SNMP API.

To add a new Active Script action:

- 1 From the WhatsUp Gold web interface, go to **APM > Actions**, then click **Actions** in the Actions Management tree. The Actions page appears.
- 2 Click **Add Action**. The Edit Action page appears.
- 3 Select **Active Script** from the **Action type** list. The boxes for the Active Script action appear.
- 4 Enter or select the appropriate information:
  - § **Name**. Enter a unique name for the action. This name displays in the Action Library.
  - § **Description**. (Optional) Enter additional information about the action. This description displays next to the action in the Action Library.
  - § **Timeout (seconds)**. Enter the length of time WhatsUp Gold attempts to connect to the selected device. When the time you enter is exceeded without connecting, a *timeout* occurs and WhatsUp Gold stops trying to connect to the SMTP server. This is considered a failed connection.



**Note:** Though the maximum timeout is 60 seconds, you are discouraged from using a timeout longer than the default of 10 seconds. You are encouraged to use the shortest timeout possible.

- § **Script type.** Select the scripting language that you want to use to write this active script (either VBScript or JScript).
- § **Script text.** Enter your action code here.



**Note:** We do not recommend that you use percent variables in script text, because they may resolve to text containing special characters ( ' ' (quotes), " " (double-quotes), % (percent), new line characters, and the like) that may break your script.

- 5 Click **Save**. The action is added to the Actions list.

### Adding an E-mail action

The E-mail action sends an SMTP mail message to a specific e-mail account. An E-mail action can also be used as an e-mail notification in the WhatsUp Gold Alert Center. While you can configure this action on both the console and web interface, you can only configure the Alert Center notification message on the web.

#### To add an E-mail action:

- 1 From the WhatsUp Gold web interface, go to **APM > Actions**, then click **Actions** in the Actions Management tree. The Actions page appears.
- 2 Click **Add Action**. The Edit Action page appears.
- 3 Select **E-mail** from the **Action type** list. The boxes for the E-mail action appear.
- 4 Enter or select the appropriate information:
  - § **Name.** Enter a unique name for the action. This name displays in the Action Library.
  - § **Description.** (Optional) Enter additional information about the action. This description displays next to the action in the Action Library.
- 5 Complete the information on the **Configuration** tab. This tab contains options pertaining to the action e-mail destination.
  - § **SMTP Server.** Enter the IP address or Host (DNS) name of your e-mail server (SMTP mail host).
  - § **Port.** Enter the port number on which the SMTP server is listening.
  - § **Timeout (sec).** Enter the length of time WhatsUp Gold attempts to connect to the selected device. When the time you enter is exceeded without connecting, a *timeout* occurs and WhatsUp Gold stops trying to connect to the SMTP server. This is considered a failed connection.
  - § **Mail To.** Enter the email addresses to which you want to send the alert. Email addresses must be fully qualified. You can enter multiple addresses, separated by a semi-colon (;), comma (,), or the [SPACE] character. The address should not contain brackets, braces, quotes, or parentheses.
  - § **Mail From.** Enter the email address you want to appear in the From field of the e-mail that is sent by the Email action.
  - § **SMTP server requires authentication.** Check this option if your SMTP server uses authentication. This enables the Username and Password boxes.

The Email action supports three authentication types:

- § CRAM-MD5

§ login

§ plain

The authentication type is not configurable. It is negotiated with the SMTP server automatically.

§ **Username.** Enter the username for SMTP authentication.

§ **Password.** Enter the password of the username for authentication.

§ **Use an encrypted connection (SSL/TLS).** Check this option if your SMTP server requires the data to be encrypted over a TLS connection (formerly known as SSL).

6 Complete the information on the **Mail Content** tab. This tab contains options pertaining to the action email message content.

§ **Subject.** Enter a text message or edit the default message. You can use percent variables to display specific information in the subject.

§ **Message body.** Enter a text message or edit the default message. You can use percent variables to display specific information in the message body.

7 Click **Save**. The E-mail action is added to the Actions list.

### Adding a Log-to-Text File action

The Log to Text action logs custom messages to specified text files.

To add a new Log to Text File action:

1 From the WhatsUp Gold web interface, go to **APM > Actions**, then click **Actions** in the Actions Management tree. The Actions page appears.

2 Click **Add Action**. The Edit Action page appears.

3 Select **Log to Text File** from the **Action type** list. The boxes for the Log To Text File action appear.

4 Enter or select the appropriate information:

§ **Name.** Enter a unique name for the action. This name displays in the Action Library.

§ **Description.** (Optional) Enter additional information about the action. This description displays next to the action in the Action Library.

§ **Log file.** Enter the full path to the location where the log file will be written.

§ **Log file write mode.** Select **Append** to have log messages appended to the Log file. Select **Overwrite** to have log messages overwrite existing log messages.

§ **Log Message.** Enter the message that will be written to the log file. This message supports percent variables. The default log message is:

```
%Application.ApplicationInstance.ApplicationName is  
%Application.ApplicationInstance.CurrentState.
```

Details:

```
Application is hosted on
```

```
%Application.ApplicationInstance.MasterDeviceDisplayName
```

```
Triggering component: %Application.TriggeringComponent.Name
```

```
Triggering component's current state:
```

```
%Application.TriggeringComponent.CurrentState
```

```
Triggering component's previous state:
%Application.TriggeringComponent.PreviousState
-----
```

```
This message was logged on %System.Date at %System.Time
Ipswitch WhatsUp Gold
```

- 5 Click **Save**. The Log to Text File action is added to the actions list.

### Adding a Windows Event Log action

The Windows Event Log action allows you to configure log messages to post to the Windows Event Viewer.

#### To add a Windows Event Log action:

- 1 From the WhatsUp Gold web interface, go to **APM > Actions**, then click **Actions** in the Actions Management tree. The Actions page appears.
- 2 Click **Add Action**. The Edit Action page appears.
- 3 Select **Windows Event Log** from the **Action type** list. The boxes for the Windows Event Log action appear.
- 4 Enter or select the appropriate information:

§ **Name**. Enter a unique name for the action. This name displays in the Action Library.

§ **Description**. (Optional) Enter additional information about the action. This description displays next to the action in the Action Library.

§ **Source**. The origin of messages logged to the Windows Event Viewer. The default source is the Ipswitch WhatsUp Log Action.

§ **Event ID**. Enter an event ID for the messages that are logged to the Windows Event Viewer. The default event ID is 1000, the WhatsUp engine event ID.

§ **Level**. Select a level for messages logged to the Windows Event Viewer. You can select Error, Warning, or Information. The default level is Error.

§ **Log Message**. Enter a log message that displays in the Windows Event Viewer. This message supports percent variables. The default log message is:

```
%Application.ApplicationInstance.ApplicationName is
%Application.ApplicationInstance.CurrentState.
```

Details:

```
Application is hosted on
```

```
%Application.ApplicationInstance.MasterDeviceDisplayName
```

```
Triggering component: %Application.TriggeringComponent.Name
```

```
Triggering component's current state:
```

```
%Application.TriggeringComponent.CurrentState
```

```
Triggering component's previous state:
```

```
%Application.TriggeringComponent.PreviousState
-----
```

```
This message was logged on %System.Date at %System.Time
```



Ipswitch WhatsUp Gold

- 5 Click **Save**. The Windows Event Log action is added to the Actions list.

### Adding a PowerShell Script action

The PowerShell action delivers a robust and flexible environment to the experienced user for developing custom actions through direct access to script component libraries, including the .NET Framework. For more information, see PowerShell action script examples.



**Important:** WhatsUp Gold uses a 32-bit (i.e. x86) PowerShell engine. Therefore, only 32-bit PowerShell snap-ins are supported and 64-bit only snap-ins will not function properly. Snap-ins usable in both 32-bit and 64-bit operating systems are configured for 64-bit systems by default and must be manually configured for 32-bit PowerShell engine to function properly with WhatsUp Gold.



If you are using additional pollers with WhatsUp Gold, PowerShell must be installed and any desired snap-ins must be registered identically on all poller machines for any PowerShell performance monitors, active monitors, and actions to function properly. Associated errors resulting from failed monitors will appear in the WhatsUp Gold Status Center. Errors resulting from failed actions will appear in the WhatsUp Gold Event Viewer.

#### To add a new PowerShell script action:

- 1 From the WhatsUp Gold web interface, go to **APM > Actions**, then click **Actions** in the Actions Management tree. The Actions page appears.
- 2 Click **Add Action**. The Edit Action page appears.
- 3 Select **PowerShell Script** from the **Action type** list. The boxes for the PowerShell Script action appear.
- 4 Enter or select the appropriate information:
  - § **Name.** Enter a unique name for the action. This name displays in the Action Library.
  - § **Description.** (Optional) Enter additional information about the action. This description displays next to the action in the Action Library.
  - § **Timeout (seconds).** Enter the length of time WhatsUp Gold attempts to connect to the selected device. When the time you enter is exceeded without connecting, a timeout occurs and WhatsUp Gold stops trying to connect to the device. This is considered a failed connection.



**Note:** You are highly discouraged from using a timeout longer than 10 seconds. Please use the shortest timeout possible.

- § **Use device credentials.** Select this check box to execute the script using the Windows credentials for the affected device. For additional information, see Using the Credentials Library.
  - § **Script Text.** Enter your action code.
- 5 Click **Save**. The PowerShell Script action is added to the actions list.

### Adding a Program action

Program actions can be defined to launch an external application when a state change occurs.

To add a new Program action:

- 1 From the WhatsUp Gold web interface, go to **APM > Actions**, then click **Actions** in the Actions Management tree. The Actions page appears.
- 2 Click **Add Action**. The Edit Action page appears.
- 3 Select **Program** from the **Action type** list. The boxes for the Program action appear.
- 4 Enter or select the appropriate information:
  - § **Name**. Enter a unique name for the action. This name displays in the Action Library.
  - § **Description**. (Optional) Enter additional information about the action. This description displays next to the action in the Action Library.
  - § **Program file name**. Enter the file path where the working files for the application are stored.
  - § **Working path**. Enter the file path where the working files for the application are stored. The working path is located on the server where WhatsUp Gold is running.
  - § **Program arguments**. Enter any percent variables you want to pass to the specified program.
- 5 Click **Save**. The Program action is added to the actions list.

### Adding a Service Restart action

To add a Service Restart action:

- 1 From the WhatsUp Gold web interface, go to **APM > Actions**, then click **Actions** in the Actions Management tree. The Actions page appears.
- 2 Click **Add Action**. The Edit Action page appears.
- 3 Select **Service Restart** from the **Action type** list. The boxes for the Service Restart action appear.
- 4 Enter or select the appropriate information:
  - § **Name**. Enter a unique name for the action. This name displays in the Action Library.
  - § **Description**. (Optional) Enter additional information about the action. This description displays next to the action in the Action Library.
  - § **Service**. Click browse (...) to select the desired service associated with your host.
  - § **Command**. Select either *Start* or *Stop*, depending on whether you want the associated alert to start or stop the service you have selected.
- 5 Click **Save** or **Save and Close**. The Service Restart action is added to the actions list.

### Adding an SMS action

The SMS Action sends a Short Message Service (SMS) notification to a pager or cell phone using an email gateway or dial-up modem. An SMS Action can also be used as an SMS notification in the WhatsUp Gold Alert Center.

### To add a new SMS action:

- 1 From the WhatsUp Gold web interface, go to **APM > Actions**, then click **Actions** in the Actions Management tree. The Actions page appears.
- 2 Click **Add Action**. The Edit Action page appears.
- 3 Select **SMS** from the **Action type** list. The boxes for the SMS action appear.
- 4 Enter or select the appropriate information:
  - § **Name**. Enter a unique name for the action. This name displays in the Action Library.
  - § **Description**. (Optional) Enter additional information about the action. This description displays next to the action in the Action Library.
  - § **Country**. Select the country for the SMS provider.
  - § **Provider**. Select the desired provider. If the provider list is incomplete and/or incorrect, you can click browse (...) to add, edit, or delete providers in this list.
  - § **Mode**. Either *Email* or *Dialup*, depending on how the provider was created in the system.
  - § **Email to**. If the connection setting is *Email*, enter the email address of the SMS device.
  - § **Phone Number**. If the connection setting is *Dialup*, enter the phone number to call with the message. You can enter multiple phone numbers, separated by a comma. There is a 2,000 character limit in this field. Also, non-numeric characters such as "-" and "." are ignored.
  - § **Message**. Enter a text message plus any desired Percent variables for APM actions. Keep in mind that if you use percent variables, this will greatly increase the character count. This message supports percent variables. The default log message is:  
%Application.ApplicationInstance.ApplicationName is  
%Application.ApplicationInstance.CurrentState.  
Message sent on %System.Date at %System.Time
- 5 Click **Save**. The SMS action appears in the Actions list.



**Note:** If the message exceeds 140 characters, the message will be broken into up to 3 parts and will be sent as separate messages ("1 of 3", "1 of 2", etc.).



**Tip:** Click **Mobile Device Status** to insert a link to the device status in the message.

## Adding an SMS Direct action

SMS Direct messages are similar to SMS messages, except a phone line is not required. Instead, messages are sent directly to a cell phone, or other texting capable device, via a GSM modem. If the receiving phone is not active or is out of range when a SMS message is sent, messages are received when the phone is turned on. SMS messages are listed in the WhatsUp Gold Action log.

You need the following items to use the SMS Direct Action:

- § GSM modem to connect to the WhatsUp machine
- § SIM card for the GSM modem

- § Cell service/signal in the room in which the WhatsUp machine and GSM modem reside

### To add a new SMS Direct action:

- 1 From the WhatsUp Gold web interface, go to **APM > Actions**, then click **Actions** in the Actions Management tree. The Actions page appears.
- 2 Click **Add Action**. The Edit Action page appears.
- 3 Select **SMS Direct** from the **Action type** list. The boxes for the SMS Direct action appear.
- 4 Enter or select the appropriate information:

- § **Name**. Enter a unique name for the action. This name displays in the Action Library.

- § **Description**. (Optional) Enter additional information about the action. This description displays next to the action in the Action Library.

- § **Phone number**. Enter the cell phone number(s) of the intended SMS message recipients.



**Note:** All non-numeric characters such as "-" and ".", are ignored.



**Note:** There is a 2,000 character limit in this box.

- § **COM Port**. Select the COM port you want to use with this notification.



**Note:** The list displays all ports associated with the GSM modem, including virtual and hard-wired, serial ports. You must select the port that is assigned to the modem in the Windows Device Manager.

- § **Message**. Enter a text message, plus any desired percent variable codes. Using percent variables greatly increases character count.



**Note:** If the message exceeds 140 characters, the message may be broken into up to three parts and is sent as separate messages ("1 of 3", "1 of 2", etc.), each message containing up to 140 characters, for a total of up to 420 characters. Spaces are included in the character count.

- 5 Click **Save**. The SMS Direct action appears in the Actions list.

## Adding an SSH action

The SSH action connects to remote devices via SSH to execute commands or scripts.

### To add a new SSH action:

- 1 From the WhatsUp Gold web interface, go to **APM > Actions**, then click **Actions** in the Actions Management tree. The Actions page appears.
- 2 Click **Add Action**. The Edit Action page appears.
- 3 Select **SSH** from the **Action type** list. The boxes for the SSH action appear.
- 4 Enter or select the appropriate information:

- § **Name**. Enter a unique name for the action. This name displays in the Action Library.

- § **Description.** (Optional) Enter additional information about the action. This description displays next to the action in the Action Library.
- § **IP address.** Enter the IP address of the device to which you want to connect using SSH.



**Note:** You can enter `%Device.Address` into the **IP Address** field; however, an SSH action that does not specify a specific IP address in this field is not available in the Recurring Actions wizard.

- § **Command to run.** Enter the command to be run and executed on the remote device. This command can be anything that the device can interpret and run; for example, a Unix shell command or a perl script.



**Note:** If you create a script to run on the remote device, the script must be developed, tested, and/or debugged on the remote machine. WhatsUp Gold does not support manipulation of the remote script.

- § **Line end character.** Select the appropriate character type; either *None*, *Linefeed*, *Carriage return*, or *Carriage return linefeed*.
  - § **SSH credential.** Select the appropriate SSH credential that WhatsUp Gold uses to connect to the remote device. If you select Use the device SSH credential, WhatsUp Gold uses the SSH credential assigned to the device for which the IP address is listed above. If the appropriate SSH credential is not listed, or the device has no SSH credentials assigned, browse (...) to the WhatsUp Gold Credentials Library to configure a set of credentials.
- 5 Click **Save**. The SSH action is added to the Actions list.

## Adding a Syslog action

When a device does not respond to polling, you can send a Syslog message to a host that is running a Syslog server.

### To add a new Syslog action:

- 1 From the WhatsUp Gold web interface, go to **APM > Actions**, then click **Actions** in the Actions Management tree. The Actions page appears.
- 2 Click **Add Action**. The Edit Action page appears.
- 3 Select **Syslog** from the **Action type** list. The boxes for the Syslog action appear.
- 4 Enter or select the appropriate information:
  - § **Name.** Enter a unique name for the action. This name displays in the Action Library.
  - § **Description.** (Optional) Enter additional information about the action. This description displays next to the action in the Action Library.
  - § **Syslog Server.** Enter the IP address or hostname of the machine that is running the Syslog server.
  - § **Port.** Enter the UDP port that the Syslog listener is listening on. The default port is 514.
  - § **Message.** Enter a text message to send to the Syslog server. This message may include notification variables. The Syslog message box limits input to 511 characters.

If notification variables are used, then the message that actually gets sent is limited to 1023 bytes, in order to comply with the Syslog protocol. Non-visible ASCII characters such as tabs and line feeds are replaced by space characters.

- 5 Click **Save**. The Syslog action is added to the Actions list.

### Adding a VMware action

VMware actions perform operations such as starting, stopping, or taking a snapshot of virtual machines running on a VMware host or being managed by a VMware vCenter server.

To add a new VMware action:

- 1 From the WhatsUp Gold web interface, go to **APM > Actions**, then click **Actions** in the Actions Management tree. The Actions page appears.
- 2 Click **Add Action**. The Edit Action page appears.
- 3 Select **VMware** from the **Action type** list. The boxes for the VMware action appear.
- 4 Enter or select the appropriate information:
  - § **Name**. Enter a unique name for the action. This name displays in the Action Library.
  - § **Description**. (Optional) Enter additional information about the action. This description displays next to the action in the Action Library.
  - § **VMware server IP address**. Enter the IP address of the VMware host or vCenter server managing the virtual machine.
  - § **VMware credentials**. Select the VMware credentials from the Credentials Library for the VMware host or vCenter server managing the virtual machine. Click browse (...) to manage credentials in the credentials library.
  - § **VMware name**. Select the Virtual machine VMware name for the virtual machine on which you want the action performed. You can enter the VMware name, or select from the list of virtual machines associated with the VMware host or vCenter server. Click browse (...) to access the list of virtual machines associated with the VMware host.
  - § **Operation**. Select the operation you want the action to perform from the list.

The following operations can be performed on a virtual machine:

    - § **Power On**. Powers up the virtual machine and boots the guest operating system if the guest operating system is installed.
    - § **Power Off**. Powers down the virtual machine. The virtual machine does not attempt to gracefully shut down the guest operating system.
    - § **Reset**. Powers down the virtual machine and restarts it.
    - § **Shutdown**. Shuts down the guest operating system. If the guest operating system automatically powers off its host, then the virtual machine also powers off.
    - § **Suspend**. Pauses the virtual machine activity; all transactions are frozen.
    - § **Restart**. Shuts down and restarts the guest operating system; does not power off the virtual machine.
    - § **Take snapshot**. Saves the current state of the virtual machine to the virtual disk of the guest system.
- 5 Click **Save**. The VMware action is added to the Actions list.

## Blackout policies

APM blackout policies allow you to designate specific days of the week and times that APM does not alert you on the health of the components monitored with APM. For example, you may not want to receive alerts on the weekend. To do this, create a blackout policy that includes blackout times from 12:00AM Saturday to 12:00AM Monday.

### Working with blackout policies

To access APM blackout policies, first click the **APM** tab. Select **Actions** from the top of the page, then **Blackout Policies** under Actions Management at left. Use the APM Blackout Policies page to configure new or existing policies.

- § Click **Add Blackout Policy** to *configure a new blackout policy* (on page 92).
- § Select a blackout policy, then click **Edit** to modify its configuration.
- § Select a blackout policy, then click **Delete** to remove it from the library.

### Creating a new blackout policy

To schedule a new blackout policy in APM:

- 1 Click the **APM** tab.
- 2 Select **Actions** from the top of the page, then **Blackout Policies** under Actions Management at left.
- 3 Click **Add Blackout Policy**. The Edit Blackout Policy page appears.
- 4 Enter the appropriate information:
  - § **Name**. Enter a unique name for the blackout policy.
  - § **Description**. Enter additional information about the blackout policy.
- 5 Click and drag to select the blackout periods you want to create.
- 6 Click **Save**. The blackout policy is added to the Blackout Policies list.

## Configuring APM application settings

The APM Application Settings page allows you to configure application states and set APM-specific data retention schedules.

To access APM Application Settings:

- 1 Click the Application Settings icon  in the upper-right corner of the page and click **Application Settings**. The Application Settings interface appears.
- 2 Click **Application Performance Management** under Application Settings.

You can configure APM to report certain application states as either Up or Down. These states are:

- § Warning
- § Maintenance

§ Unknown

The default setting for all three is Up.

**To modify how SLA-related reports are displayed:**

- 1 Determine one or more reporting states you want to change.
- 2 Select **Up** or **Down** from the list to the right of each state.
- 3 Click **Save**. Applications in the applicable state are now reported as either Up or Down depending on your selection.

You can also configure APM to retain multiple data types for a specific duration. These data types are:

- § Hourly
- § Raw
- § Action log
- § Resolved Items log
- § State change log

The default setting for all three is 90 days.

**To modify data retention schedules:**

- 1 Determine one or more data types for which you want to change the duration of retention.
- 2 Enter the number of days in the data entry boxes to the right of each applicable data type.
- 3 Click **Save**.



**Important:** If the APM Application Settings **Component and group data** check box is selected, reporting and log activity for any application profile or profile type selected on the APM Status tab includes data for all components and groups under your selection in the navigation tree. Deselecting this check box increases performance of the APM Status page.

**To use End User Monitor components when the WhatsUp Gold IIS instance is using a non-standard port, such as for SSL:**

Click **Auto Detect** to update the iDrone Manager Service's URL automatically.



**Important:** If your WhatsUp Gold server is configured to use SSL, verify the resulting URL starts with `https` and the host name is exactly the same host name you are using to access the Application Settings interface. In addition, the host name must match the common name (Subject) in the certificate configured on the WhatsUp Gold IIS instance exactly.