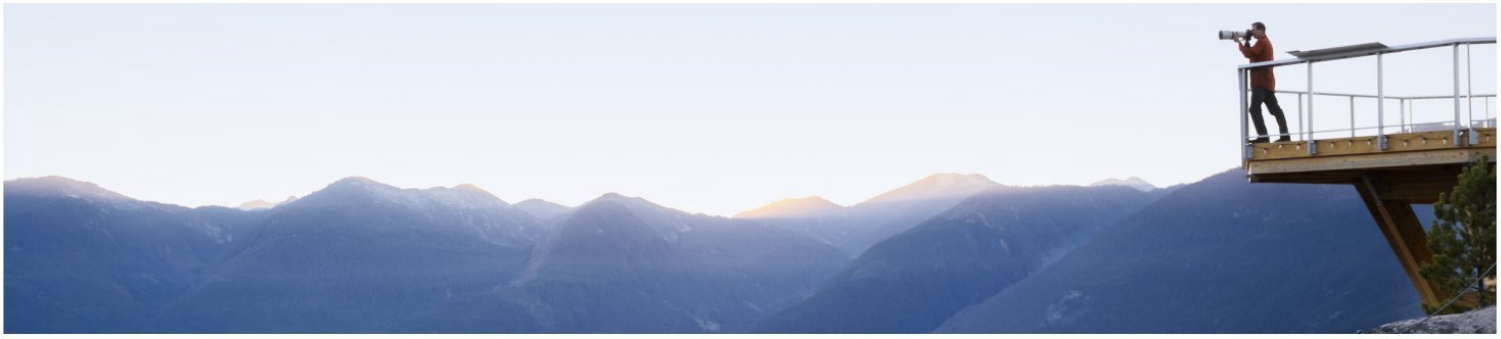
Hewlett Packard Enterprise

Application Performance Management

Version 9.31, Released June 2017

APM Platform Administration Guide

Published June 2017



Legal Notices

Warranty

The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HPE shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Valid license from HPE required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notice

Trademark Notices

Adobe® and Acrobat® are trademarks of Adobe Systems Incorporated.

AMD and the AMD Arrow symbol are trademarks of Advanced Micro Devices, Inc.

Google™ and Google Maps™ are trademarks of Google Inc.

Intel®, Itanium®, Pentium®, and Intel® Xeon® are trademarks of Intel Corporation in the U.S. and other countries.

iPod is a trademark of Apple Computer, Inc.

Java is a registered trademark of Oracle and/or its affiliates.

Microsoft®, Windows®, Windows NT®, Windows Server® and Windows Vista™ are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Oracle is a registered trademark of Oracle Corporation and/or its affiliates.

UNIX® is a registered trademark of The Open Group.

Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number, which indicates the software version.
- Document Release Date, which changes each time the document is updated.
- Software Release Date, which indicates the release date of this version of the software.

To check for recent updates or to verify that you are using the most recent edition of a document, go to: https://softwaresupport.hpe.com/group/softwaresupport/search-result?keyword=.

This site requires an HPE Passport account. If you do not have one, click the **Create an account** button on the HPE Passport Sign in page.

PDF Version of Online Help

This document is a PDF version of the online help. This PDF file is provided so you can easily print multiple topics from the help information or read the online help in PDF format.

Support

Visit the HPE Software Support website at: **https://softwaresupport.hpe.com**

This website provides contact information and details about the products, services, and support that HPE Software offers.

HPE Software Support provides customer self-solve capabilities. It provides a fast and efficient way to access interactive technical support tools needed to manage your business. As a valued support customer, you can benefit by using the support website to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Download software patches
- Manage support contracts
- Look up HPE support contacts

- Review information about available services
- Enter into discussions with other software customers
- Research and register for software training

Most of the support areas require that you register as an HPE Passport user and sign in. Many also require a support contract. To register for an HPE Passport ID, go to **https://softwaresupport.hpe.com** and click **Register**.

To find more information about access levels, go to:
https://softwaresupport.hpe.com/web/softwaresupport/access-levels

HPE Software Integrations and Solutions

Visit the Integrations and Solutions Catalog at **https://softwaresupport.hpe.com/km/KM01702731** to explore how the products in the HPE Software catalog work together, exchange information, and solve business needs.

Contents

Platform Administration Overview

This guide provides instructions on how to open, configure, and administer HPE Application Performance Management (APM).

The guide is divided into the following parts:

- **Accessing and Navigating APM**. Describes how to start APM, how to log into the application, and a general overview of the user interface.
- **Setup and Maintenance.** Describes basic setup options such as infrastructure settings, time zones, languages, logs, and backups.
- **Data Enrichment.** Describes how to work with multiple geographic locations.
- **Users, Permissions, and Recipients.** Describes how to control user access to APM.
- **Reports and Alerts Administration.** Describes how to schedule reports and set up alerts.
- **Downtime Management.** Describes how to control system downtime.
- **Troubleshooting.** Discusses common system issues or limitations.

Part 1: Accessing and Navigating APM

Chapter 1: Starting, Stopping, or Restarting APM

This section provides instructions for starting, stopping, or restarting APM.

Note: If you are working in a distributed environment, first enable the Data Processing Server, and then enable the Gateway Server.

Tasks

How to Start, Stop, or Restart APM

To start or stop APM in Windows:

Select **Start > Programs > HPE Application Performance Management > Administration > Enable | Disable HPE Application Performance Management**.

To start, stop, or restart APM in Linux:

```
/opt/HP/BSM/scripts/run_hpbsm <start | stop | restart>
```

To start, stop, or restart APM using a Daemon Script: (in Linux)

```
/etc/init.d/hpbsmd <start | stop | restart>
```

Note: When you stop APM in Windows, the HPE Application Performance Management service is not removed from Microsoft's Services window. The APM service is removed from the Services window only after you uninstall APM.

UI Description

Windows Start Menu

In a Windows environment, the installation process adds an HPE Application Performance Management menu to the Windows Start Menu.

This menu includes the following options:

Option	Description
Open HPE Application Performance Management	Opens the APM application Login page in a web browser.
Administration > Configure HPE Application Performance Management	Runs the Setup and Database Configuration utility. This enables you to create and connect to management and RTSM, databases on Microsoft SQL Server or Oracle Server. For details, see Server Deployment and Setting Database Parameters in the APM Installation Guide.

Option	Description
Administration > Disable HPE Application Performance Management	Stops APM on the specific machine, and disables it from running automatically when the machine is started.
Administration > Enable HPE Application Performance Management	Starts APM on the specific machine, and sets it to run automatically when the machine is started.
Administration > HPE Application Performance Management Status	Opens the APM Status page in a web browser. This page displays the status of the services run by the APM Service and High Availability Controller.
Documentation > HPE Application Performance Management Help	Opens the APM Help in a web browser.

Chapter 2: Viewing Status of Processes and Services

This section discusses how to view the status of processes and services run by the APM service and High Availability Controller.

Tasks

How to View the Status of Processes and Services

In Windows:

Select **Start > Programs > HPE Application Performance Management > Administration > HPE Application Performance Management Status**.

In Linux:

Enter the following command: `opt/HP/BSM/tools/bsmstatus/bsmstatus.sh`

Troubleshooting and Limitations

Remote Viewing Limitations

- The JBoss application server must be running to enable viewing the status of the processes and services from a remote computer.
- If JMX-RMI with basic authentication over SSL was set up using the SYSTEM user in Window or Linux, the processes and services status page does not display any data. For details on configuring JMX-RMI with basic authentication over SSL, see Securing JMX-RMI Channel Used for Internal APM Communications in the APM Hardening Guide.

Chapter 3: Logging into APM

This section provides instructions for logging into APM.

Learn About

Accessing APM

You can access APM using a supported web browser, from any computer with a network connection (intranet or Internet) to the APM servers.

Note: You can only open one APM session per browser.

The level of access granted to a user depends on the user's permissions. For more information, see "Permissions" on page 130.

By default, APM is configured with Lightweight Single Sign-On (LW-SSO). For more information, see "Logging into APM with LW-SSO" on page 19.

The following table provides information on how to access APM based on APM's LDAP configuration.

	User login	APIs/REST
No LDAP – only internal users	No LDAP field. The domain name is not required. You can enter your user name or internal/user name.	The domain name is not required. Optional: You can enter internal/user name.
Only one LDAP	No LDAP field. The domain name is not mandatory. You can enter your user name or domain/user name.	The domain name is not required. Optional: You can enter your domain/user name.
Several LDAPs	LDAP field drop down list appears.	—
Mixed mode with one LDAP	No LDAP field. The domain name is not mandatory. You can enter your user name or domain/user name or internal/user name.	The domain name is not required. Optional: You can enter your internal/user name or domain/user name.
Several LDAPs with mixed mode	LDAP field drop down list appears and contains internal name	—

Requirements

For details on browser requirements, as well as minimum requirements to view APM, see the APM System Requirements and Support Matrixes guide.

Tasks

This section includes:

How to Log into APM

1. In a browser, enter the following URL:
   http://<server_name>.<domain_name>/bsm

   where

   <server_name> and **<domain_name>** represent the Fully Qualified Domain Name (FQDN) of the APM server (for example, http://server1.domain1.ext/bsm). If there are multiple servers, or if APM is deployed in a distributed architecture, specify the load balancer or Gateway Server URL, as required.
2. Enter your login name and password. Initial access can be gained using the administrator user name ("admin") and password. If there are multiple LDAP configurations, select the relevant LDAP domain to access APM.

   Note: The password is configured in the final step of the Setup and Database Configuration utility or in the Config server utility which can be run separately from the installation.

   Caution: We recommend that the system superuser change this password upon first login to prevent unauthorized entry. For details on changing the user password, see "Personal Settings" on page 195. The login name cannot be changed.

After you log in, your login name appears at the top right of the page, under the top menu bar.

Note: If Lightweight Single Sign-On (LW-SSO) is disabled, you do not need to add the **.<domain_name>** syntax in the login URL. For information on LW-SSO, see "Logging into APM with LW-SSO" on page 19.

How to Enable Automatic Login

If you enable automatic login, when you open APM, the Login page does not appear and you do not have to enter your user name or password to access APM.

Caution: This could be considered a security risk and should be used with caution.

1. On the APM Login page, select **Remember my login name and password for 14 days**.
2. When completing your session, close the browser window. Do not click **Logout** at the top of the page. Clicking **Logout** disables the automatic login option and requires the login name and password to be entered when accessing APM.

How to Modify Automatic Login Settings

1. Navigate to **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings**.
2. Click **Foundations** and select **Security**. In this context, you can modify the following options:

Option	Does the following
Days to remember login	Sets the number of days that users can log in automatically without entering a user name and password. The default value is **14**.
Enable automatic login	If this option is set to **true**, the **Remember my login name and password** check box appears in the Login page. Selecting this check box in the Login page enables the user to log in without opening the Login page when next accessing APM. For details see "How to Enable Automatic Login" on the previous page. If this option is set to **false**, users cannot bypass the Login page and will always need to enter a user name and password when opening APM. The default value is **true**.
Maximum machines per login name	Sets the number of machines that can simultaneously access APM using the same login name. The default value is **0** which means that the number of logins is unlimited. It is highly recommended to set the maximum number of sessions to **1**.

How to Log In Using a URL

You can log into APM using a URL that contains several parameters (including your login name and password). This is a convenient way to create a bookmark to APM or to send a direct link to other users.

Caution: Though convenient, this method is not secure since the password is not encrypted in the URL.

In a browser, enter the following URL:
http://<server_name>.<domain_name>/<APM_root_directory>/TopazSiteServlet?autologin=yes&strategyName=Topaz&requestType=login&userlogin=<loginname>&userpassword=<password>&createSession=true

where:

- **<server_name>** represents the name of the APM server.
- **<domain_name>** represents the name of the user's domain according to the user's network configuration.
- **<loginname>** and **<password>** represent the login name and password of a user defined in APM.

You can also create a URL to access APM using the Link to This Page window. For further information, see "Creating a Link to an APM Page" on page 23.

How to Log Out of APM

When you complete your session, it is recommended that you log out to prevent unauthorized entry.

Click **Logout** at the top of the page.

Note: Clicking **Logout** cancels the Automatic Login option. If a user logs out, the next time the user logs in, the Login page will open and the user will need to enter a login name and password. This can be useful if another user needs to log in on the same machine using a different user name and password.

UI Description

APM Login Page

User interface elements are described below:

UI Element (A-Z)	Description
LDAP domain	If there are multiple LDAP Configurations or if **Mixed mode authentication** is enabled, select the relevant domain to access APM.
Login Name	Enter the relevant login name to access APM.
Password	Enter the relevant password to access APM.
Remember my login name and password for 14 days	Select this option to bypass the Login page the next time you open APM. For further information, see "How to Enable Automatic Login" on page 14.

Tips/Troubleshooting

Login Troubleshooting

To resolve login issues, reference the possible login failure causes in the following table using the error number shown in the error alert dialog box. For additional troubleshooting information, refer to the HPE Software Support.

Error No.	Problem/Possible Cause(s)	Solution(s)
LI001	APM failed to connect to the JBoss application server running on the Gateway Server. This may be due to: • The JBoss server being down. • Problems with the APM service. • The port required by the application server being used by another application.	**Solution 1:** Close all applications on the Gateway Server machine and restart the machine. **Solution 2:** Ensure that there are no other running applications on the Gateway Server machine that use this port (for example, applications that run from the Startup directory, another instance of JBoss, an MSDE or Microsoft SQL Server, or any other process).
LI002	The JBoss application server running on the Gateway Server is not responding or is not installed correctly.	Restart APM.
LI003	The management database is corrupted (for example, if a user record was accidentally deleted from the database).	Try logging in as a different user, or ask the APM administrator to create a new user for you.

Error No.	Problem/Possible Cause(s)	Solution(s)
LI004	The connection between the Tomcat servlet engine and the JBoss application server failed due to a Remote Method Invocation (RMI) exception. This may be due to problems in RMI calls to JBoss.	Ensure that none of the JBoss ports are in use by another process. Also, ensure that the RMI ports are bound. For details on ports, see "Port Usage" on page 93.
LI005	The APM login fails or hangs. This may be due to: • An incorrect login name/password combination. • An inability to connect to the management database. • The current user does not have access rights to a profile. • Authentication strategy has not been set/configured correctly.	**Solution 1:** Ensure that you enter a correct login name/password combination. **Solution 2:** Ensure that the connection to the management database is healthy: 1. In the web browser, type **http://<Gateway or Data Processing Server name>:29000** to connect to the JMX management console. 2. Click the link **System > JMX MBeans > Topaz > Topaz:service=Connection Pool Information**. 3. Locate **java.lang.String showConfigurationSummary()** and click **Invoke**. 4. In **Active configurations in the Connection Factory**, find the appropriate row for the management database. 5. Verify that columns **Active Connection** and/or **Idle Connection** have a value greater than **0** for the management database. 6. If there is a problem with the connection to the database, verify that the database machine is up and running. If required, rerun the Setup and Database Configuration utility. **Solution 3:** Ensure that the user has appropriate permissions to access APM. For details on user permissions, see "Permissions" on page 130. **Solution 4:** Verify that an authentication strategy has been configured correctly. For details on authentication strategies, see "Authentication Strategies" on page 201.

Error No.	Problem/Possible Cause(s)	Solution(s)
LI006	The APM login fails. This may be due to: • Incorrect cookie settings in the web browser. • An unsupported character in the names of the machines running the APM servers.	**Solution 1:** Ensure that the client web browser is set to accept cookies from APM servers. **Solution 2:** Ensure that there are no underscore characters (_) in the names of the machines running the APM servers. If there are, either rename the server or use the server's IP address when accessing the machine. For example, to access APM, use `http://111.222.33.44/<APM root directory>` instead of `http://my_server/<APM root directory>`
LI007	The APM login fails. This is because the maximum number has been reached of concurrent logins from different machines that access HPE Application Performance Management using the same login name.	**Solution 1:** Log out of the instances of APM that have logged in using the same login name from different machines. You can then retry logging in, if the maximum number has not been reached. **Solution 2:** Log in using a different login name, if available. **Solution 3:** The administrator can edit the Infrastructure Settings to remove the limitation or increase the maximum number of concurrent logins using the same login name from different machines. For details, see "How to Modify Automatic Login Settings" on page 15.

Forgot Password

To reset your password, contact your system administrator.

For information about assigning passwords, see "Configure APM Users" on page 126 and "Define a Superuser" on page 126.

Chapter 4: Logging into APM with LW-SSO

Lightweight Single Sign-On (LW-SSO) Authentication Support enables users to log into APM automatically and securely without needing to enter a user name and password.

Learn About

Working with LW-SSO

By default, APM is configured with Lightweight Single Sign-On (LW-SSO). With LW-SSO, once you log in to APM you automatically have access to other configured applications, without needing to log into those applications.

When LW-SSO Authentication Support is enabled, you must ensure that the other applications in the Single Sign-On environment have LW-SSO enabled and are working with the same initString. If the applications are in different domains, the domains must be trusted domains.

Disabling LW-SSO

If you do not require Single Sign-On for APM, it is recommended that you disable LW-SSO. You can disable LW-SSO using the SSO Configuration Wizard. For information on how to disable LW-SSO using the SSO Configuration Wizard, see "How to Disable LW-SSO" on the next page.

Using Client-Side Authentication Certificates for Secure User Access to APM

You can provide user access to APM using client-side authentication certificates. This provides a secure alternative to entering a user name and password to log in.

From the SSO Configuration Wizard, you can configure LW-SSO to accept such certificates. When a certificate is accepted, users are automatically logged into APM if the client certificate card is inserted in the machine. If LW-SSO is configured to accept certificate, users are not able to login to APM without the client certificate card. For information about the SSO Configuration Wizard, see "SSO Configuration Wizard" on page 214.

For configuration instructions, see "Smart Card Authentication on APM Servers" in the Smart Card Authentication Configuration Guide.

Using an External Authentication Point for Secure User Access to APM

LW-SSO 2.4 enables you to use an external authentication point. This allows you to use your own credential validation method, for example LDAP, a proprietary user/password database, or a custom SSO solution.

The external authentication point is an external URL that performs the actual user authentication. It obtains the user credentials (usually the user name and password, but it could be something else, such as the user's class-B certificate, or a proprietary SSO token), validates these credentials, and then creates an "authentication assertion", a token that states who the authenticated user is. The authentication assertion usually also provides information about how the user was authenticated.

For information about configuring an external authentication point for secure access to APM, see "LDAP General Configuration Page" on page 209.

Tasks

How to Disable LW-SSO

1. Select **Admin > Platform > Users and Permissions > Authentication Management**, and click **Configure**.
2. Select **Disable** to disable SSO.

How to Secure User Access to APM Using an External Authentication Point

1. If you are using LDAP, ensure that the same user repository is used by APM and the authentication point server.

   If you are not using LDAP, create the users manually in APM.
2. Set the LW-SSO configuration file on the authentication point server side to use the same **initString** as in APM.
   a. In a browser on the APM Gateway server, enter the URL of the JMX console: **http://<Gateway or Data Processing Server name>:29000/**
   b. Enter your JMX console authentication credentials. The JMX Agent View appears.
   c. Under the domain name **Topaz**, click **service=LW-SSO Configuration**.
   d. Locate the **AuthenticationPointServer** attribute and enter the Authentication Point Server URL.
   e. Locate the **ValidationPointEnabled** attribute and set it to **true**.
   f. If you do not want particular URLs to use this feature, locate **addNonsecureURL()** and add the URLs to the list.
   g. Click **Apply Changes**.
3. Restart the APM Gateway server.
4. Make sure that you can log into APM through the external authentication point. If you are unable to log in, see "Unable to Log into APM when Using an External Authentication Point" on page 222.

Tips/Troubleshooting

APM Login Page Appears after Entering Valid Client Certificate

If the APM Login page appears after entering a valid client certificate, test the following:

- Try to log in using the User Identifier (often email address).
  If you can log in, make sure that the LDAP user filter was configured to use the same user identifier.
- If the Login page still appears and you are using the Apache web server, add the following to **<APM Gateway installation directory>/Webserver/conf/extra/httpd-ssl.conf** under **#SSLOptions**: **SSLOptions +ExportCertData**.

  For details on how to configure Apache to require a client certificate, see "Configuring Apache to Require a Client Certificate" in the APM Hardening Guide. A link to the Hardening Guide can be found on the Planning and Deployment Documentation page.

Resetting LDAP/SSO Settings Using the JMX Console

If your LDAP or SSO settings have not been configured properly, you may not be able to access APM. If this happens, reset your LDAP or SSO settings remotely using the JMX console.

1. In the JMX Agent View, under the domain name **Topaz**, click **service=SSO**.
2. Locate the **void setSingleSignOnMode()** attribute and set it to **Disabled**.

Unable to Login

If LDAP is configured and you are unable to login:

1. In the JMX Agent View, under the domain name **Foundations**, click **service=users-remote-repository**.
2. Locate **void disabledLDAPConfiguration()** and invoke it to disable all LDAP configurations.

Chapter 5: Tracking Login Attempts and Logged In Users

This section provides instructions for tracking who attempted to log into APM, and for displaying a list of users currently logged in.

How To Track Who Attempted to Log into APM

Open the following file:
<APM GW root directory>\log\Jboss\UserActions.servlets.log.

How To Display a List of Users Currently Logged into APM

1. Open the JMX console on the machine that is running APM. (For detailed instructions, see "JMX Console" on page 78.)
2. Under the **Topaz** section, select **service=Active Topaz Sessions**.
3. Invoke the **java.lang.String showActiveSessions()** operation.

Chapter 6: Creating a Link to an APM Page

This section provides instructions for sending a user to a target page in APM.

To access

Select **Admin > Link to this page**.

Learn About

Overview

Depending on which **Link to this page** option you select, the receiver can access an APM page using one of the following:

- Their own user name and password.
- A URL encrypted with your user name and password.
- A URL encrypted with another user's user name and password.

Note: By default, only administrators have permission to access this feature.

Using an Encrypted URL

When using an encrypted URL, the receiver bypasses the APM Login page because the URL supplies the user name and password information.

To use an encrypted URL, you must activate this option in the Infrastructure Settings. For instructions about activating this option, see "How to Activate the Encrypted URL Option" on the next page.

The user name in the URL must be an account with sufficient privileges to access the target page. If the account does not have sufficient privileges, a higher level page for which the receiver has permissions appears.

Example:

You want to direct the receiver to the Infrastructure Settings page, but you select the **Use credentials** option for a regular user (who is not authorized to view Infrastructure Settings). When a receiver enters this URL, the receiver is sent to the Setup and Maintenance page and is unable to access Infrastructure Settings.

Verifying User Names and Passwords

The **Link to this page** option does not verify the user name and password sent in the URL. Verification is done only when the receiver tries to access the target page. If the user name and password are not correct, or the user account has been deleted, the receiver is sent to the APM Login page to log in normally. Once logged in, the receiver does not proceed to the target page and there is no message displaying the reason for the login failure.

Third-party Portals

To view Service Health or MyBSM pages in a third-party portal, select the **Embedded link** check box in the

Link to this page window. When the user accesses the generated URL, only the specific page is displayed, and not the entire APM application with menus.

Note: In a third-party portal, only one Service Health or MyBSM page can be embedded in each portal page. If you need to see more information, create a page that uses multiple or tabbed components. For details, see "How to Set Up the MyBSM Workspace" in the APM User Guide.

Creating a Direct Link to RTSM

You can create a link to a specific target page in Run-time Service Model (RTSM) using the Direct Links feature. For details on Direct Links, see "Generate a Direct Link - Overview" in the Modeling Guide.

Security Notes and Precautions

When using APM direct login, the user name and password in the URL are encrypted so that no login information is ever revealed.

Sending encrypted information by email entails a security risk, since the mail system can be breached. If the email is intercepted, access to APM is given to an unknown party.

Do not use the URL from Direct Login as a link in any web page.

Receivers have all privileges of the user name they were given in the URL.

Tasks

How to Create and Send a Link to a User

1. Access the APM page whose link you want to send to a user.
2. Click **Admin > Link to this page**.
3. Select one of the following:
   - To create a link with no user name or password, click **No credentials**. Users will need to enter their own user name and password.
   - To create a link with your user name and password, click **My credentials**.
   - To create a link with another user's user name and password, click **User credentials** and in the login name and password fields, enter a user name and password of an APM user.
4. Click **Create a link**.
5. Click **Copy to clipboard**.
6. Send the link to the user.

How to Activate the Encrypted URL Option

1. Select **Admin > Platform > Setup and Maintenance > Infrastructure Settings**.
2. Select **Foundations**.
3. Select **Security**.
4. In the Security - Login table, locate **Disable credentials usage in the direct link to BSM pages** and set the value to **False**

UI Description

Link to This Page Window

User interface elements are described below:

UI Element (A-Z)	Description
Cancel	Cancels the Link to This Page operation.
Create link	Creates the URL of the current APM page. The user enters this URL in their browser and the specified APM page is displayed. **Note:** If you select this option after selecting **No credentials** or **Use credentials** (to use credentials other than your own) and you want to invoke the login URL on the same local machine you created it on, you must first log out of APM.
Confirm password	Re-enter the password entered in the **Password** field.
Copy to clipboard	Copies the content of the **Link** field to the clipboard. This button is only available after you click **Create Link**. **Note:** If you use the Firefox browser, you must change your security settings for this option to work. Enter `about:config` in the browser's search window, locate the **signed.applets.codebase_principal_support** option, and set it to **true**.
Embedded link	Displayed in Service Health and MyBSM only. Select this check box to create a URL which can be used in a third-party portal, so that only the specific page is displayed, and not the entire APM application with menus.
Generate HTML	Generates an HTML page for the specified APM page. **Note:** If you select this option after selecting **No credentials** or **Use credentials** (to use credentials other than your own) and you want to log in using the generated HTML page on the same local machine you created it on, you must first log out of APM.
Link	Displays the URL that the receiver uses to access the specified APM page. **Note:** This field only appears after clicking **Create link**.
Login name	The login user name to be encrypted in the URL the receiver uses to access the specified page. This must be the user name of an actual user.
My credentials	Select to encrypt the link with your user name and password.
No credentials	Select if receivers need to use their own user name and password to access the page specified in the link.

UI Element (A-Z)	Description
Password	The password to be encrypted in the URL that the receiver uses to access the specified page. This must be the password of an actual user.
Use credentials	Select to encrypt the link with the login user name and password of another user.

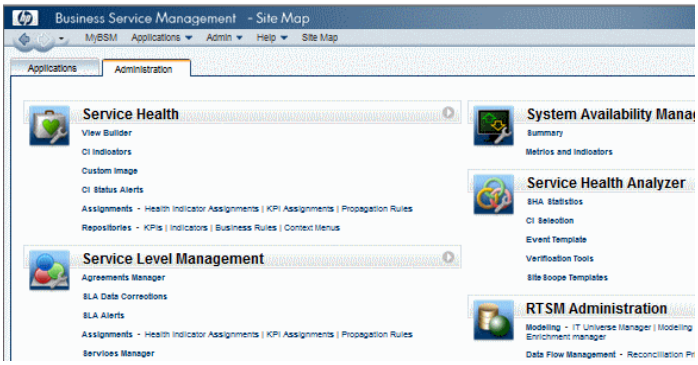
Chapter 7: Navigating and Using APM

APM runs in a web browser. This section describes APM navigational functions and the APM user interface.

Learn About

Site Map

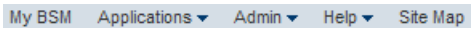
The Site Map enables quick access to all top- and second-level contexts in the Applications or Administration menu. By default, the Site Map is the first page that opens after logging into APM.You can also access the Site Map by clicking the **Site Map** link on the menu bar.



Title and Menu Bars

The title bar displays a logo, the name of the active APM application, and the current user. It also displays the **Full Screen View** link and a Logout button Logout.

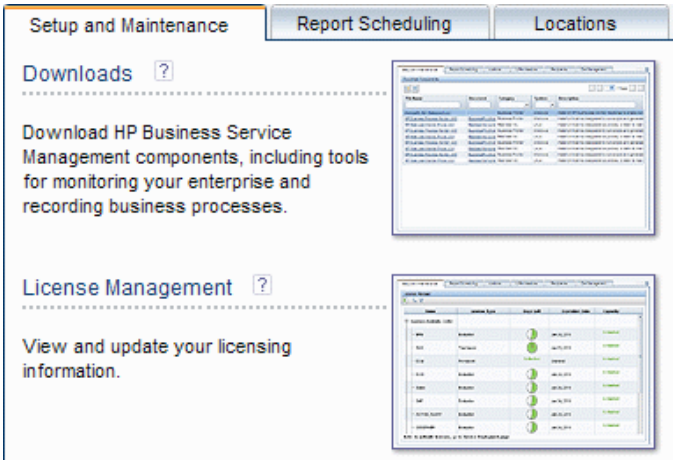
The menu bar enables navigation to the applications, Administration Console pages, help resources, and a link to the Site Map. For more information, see "UI Description" on page 29.



Tabs

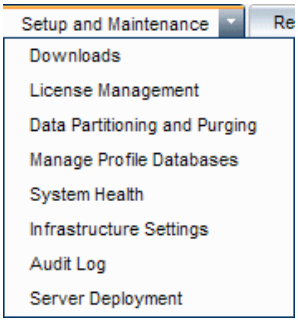
Tabs enable navigation to various contexts within a particular area of APM, such as to different types of reports within an application, views within a report, or administrative functions within the Administration Console. In certain contexts, tabs are used to distinguish between functions; in other contexts, tabs are used to group logically similar functions or features together.

The tab main menus enable navigation from a tab front page to various contexts related to the tab. Tab main menus appear when selecting a tab that represents a category containing several contexts, such as report types or administrative settings. Tab main menus include a description and thumbnail image of each tab context.



Tab controls enable you to navigate from any context related to a tab to any other of the tab's contexts. To open the tab main menu, click the tab name.

To quickly jump to another context related to the tab, click the down arrow to open the tab drop-down menu and click a tab menu option to move to that context.



Navigation Buttons

The forward and back buttons,  , positioned in the upper left corner of the window, enable you to navigate between viewed pages. You can go back to your most recently viewed page or forward to the page you viewed before you clicked the back button.

Clicking the down arrow adjacent to the forward and back buttons, displays a list of the last 20 pages that you viewed during the current session. You can click any one of these links to display the desired page.

The pages are stored in the APM server. For all reports, if you return to a previously viewed page, the page opens exactly as you left it with the filters and conditions selected as previously.

There are several pages whose contexts and selections are not saved as previously viewed and when you return to that page, you may have to make your selections again. For example, if you were working in a specific context in Infrastructure Settings and return to the Infrastructure Settings page using the history option, your context has not been saved and you are returned to the default Infrastructure Settings page.

Tip: You can change the number of pages stored in history (default is 20) by accessing the file **<APM GW root directory>\conf\settings\website.xml** and changing the value of the **history.max.saved.pages** field. You must restart APM for the change to take affect. This change is on the server and, therefore, affects all users.

Breadcrumbs

Breadcrumbs enable you to keep track of your location within the active application. They provide links back to each page you navigated through to get to the current page.

You can view previous pages within a multi-level context by clicking one of the links in the breadcrumb. For example, in the following breadcrumb trail, you would click **Breakdown Summary** to return to the Breakdown Summary report:

If the breadcrumb is longer than the width of the screen, only the tail of the breadcrumb is displayed. Click the **View**  icon to the left of the breadcrumb to display the hidden portion of the breadcrumb in the current tab.

Tip: The web browser **Back** function is not supported in APM. Using the **Back** function does not always revert the current context to the previous context. To navigate to a previous context, use the navigation buttons within APM or the breadcrumb function.

Tasks

How to Access Full Screen View

Note: When selecting **Full Screen View**, Menu Bar, Breadcrumbs, and Tabs are hidden.

- Click the **Full Screen View** link to display the current page over the full screen.
- To return to the standard view of the page, click **Standard View** or press `Esc` on your keyboard.

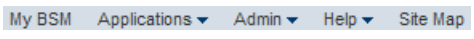
How to Change the Default Entry Page

The Site Map is the default page displayed when you log into APM. You can select a different APM page to display when you log in.

1. From the upper right corner of the Site Map, click **Change the default page**.
2. On the Personal Settings page, click the **Customization Menu** tab.
3. In the left pane, highlight the page you want to display when you log into APM.
4. Click **Set at Default Entry Context**.

UI Description

The Menu Bar enables navigation to the following applications and resources:



- "MyBSM " on the next page
- "Applications Menu" on the next page
- "Admin Menu" on page 31
- "Help Menu" on page 32

MyBSM

Opens the MyBSM application, a portal that individual users can customize to display key content relevant to them. For details, see "Monitoring Your Environment With MyBSM" in the APM User Guide.

Applications Menu

APM features the business user applications listed below. You access all applications from the **Applications** menu, except for the MyBSM application which is accessed from the Menu Bar.

Note: Only applications for which you have a valid license will appear in the Applications menu.

Menu Option	Description
Service Health	Opens the Service Health application, a real-time dashboard for viewing performance and availability metrics from a business perspective. For details, see "Introduction to Service Health" in the APM User Guide.
Application Health	Opens the Application Health interface which is a set of apps that provides key functions of APM's most commonly used apps: Dashboard, App Overview, Service Level Manager (SLM), Business Process Monitor (BPM), Real User Monitoring (RUM), App Settings, and Administration.
CI Status	Opens the CI Status Reports interface. CI Status reports enable you to view and analyze performance data collected by APM data collectors and stored in the APM database. For details, see "CI Status Reports User Interface" in the APM User Guide.
Service Level Management	Opens the Service Level Management application to proactively manage service levels from a business perspective. Service Level Management provides IT Operations teams and service providers with a tool to manage service levels and provide service level agreement (SLA) compliance reporting for complex business applications in distributed environments. For details, see"Working with the Service Level Management Application" in the APM User Guide.
End User Management	Opens the End User Management application, used to monitor applications from the end user perspective and analyze the most probable cause of performance issues. For details, see "End User Management Reports Overview" in the APM User Guide.
System Availability Management	Opens the System Availability Management application, used for complete system and infrastructure monitoring as well as event management. For details, see "System Availability Management Overview" in the APM User Guide.
Service Health Analyzer	Opens the Service Health Analyzer application, used to view CIs with anomalies. For further information, see "Service Health Analyzer Overview" on page 1
User Reports	Opens the Report Manager, used for creating and saving user reports—customized reports containing user-defined data and formatting that can help you focus on specific aspects of your organization's application and infrastructure resource performance. For details on the Report Manager, see "User Reports Overview" in the APM User Guide.

Admin Menu

Administrators use the **Admin** menu to administer the APM platform and applications. The Admin menu consists of several sections, organized by function.

Note: The options available to you depend on your deployment package.

Menu Option	Description
Service Health	Opens the Service Health Administration pages, where you attach health indicators and Key Performance Indicators (KPIs) to CIs, define the custom and geographical maps, and customize the repositories. For details, see "View-Specific and Cross-View Administration" on page 1 in the APM Application Administration Guide.
Service Level Management	Opens the Service Level Management Administration pages, where you create service agreements (SLAs, OLAs, UCs) and build services that link to the data that Service Level Management collects. For details, see "Introduction to SLM Administration" on page 1 in the APM Application Administration Guide.
End User Management	Opens the End User Management Administration pages, where you configure and administer Business Process Monitor and Real User Monitor data collectors, as well as configure transaction order, color settings, and report filters. For details, see "End User Management Administration" on page 1 in the APM Application Administration Guide.
System Availability Management	Opens the System Availability Management Administration pages, where you configure and administer the SiteScope data collector. For details, see "System Availability Management Administration Overview" on page 1 in the APM Application Administration Guide.
Service Health Analyzer	Opens the Service Health Analyzer application, used to view CIs with anomalies. For further information, see "Service Health Analyzer Overview" on page 1
RTSM Administration	Opens the RTSM Administration pages, where you build and manage a model of your IT universe in the Run-time Service Model (RTSM). From RTSM Administration, you use Data Flow Management and the adapter sources that are used to populate the IT Universe model with configuration items (CIs), the templates for creating CIs, and the viewing system for viewing the CIs in APM applications. You can also manually create CIs to add to the model. For details, see the Modeling Guide.
Platform	Opens the Platform Administration pages, which provide complete platform administration and configuration functionality.

Menu Option	Description
Integrations	Opens the APM Integrations administration area, where you can administer the following: • APM Connector integrations to capture and forward data from third-party systems to APM. • Mappings between CIs and Operations Orchestration runbooks. • Application Lifecycle Management integrations to export related data and monitoring tools configurations. • Deprecated integration methods - Integrations Adapter and EMS Integrations. For details, see "Integrating with Other Applications - Overview" on page 1
Link to this page	Select to access the Link to this page feature, where you can create a URL that enables direct access to a specific page in APM. For details, see "Creating a Link to an APM Page" on page 23. By default only administrators have security rights to access this feature.
Personal Settings	Select to access the Personal Settings tab, which enables personalization of various aspects of APM, including menus and passwords. Note that Personal Settings are available to all users. For details, see "Personal Settings" on page 195.

Help Menu

You access the following online resources from the APM Help menu:

Menu Option	Description
Help on this page	Opens the APM Help file to the topic that describes the current page or context.
APM Help	Opens the APM Help home page. The home page provides quick links to the main help topics.
Planning and Deployment Guides	Opens a page with links to planning guides, installation and upgrade guides (including release notes), data collector installation guides, and other resources.
Product News and Updates	Opens the Product News page on the HPE Software Support website (requires HPE Passport login). The URL for this web site is http://support.openview.hp.com/product_news.jsp.
APM Videos	Opens the Quick Links to APM Videos page (requires HPE Passport login). The URL for this web site is https://community.hpe.com/t5/Application-Perf-Mgmt-BAC-BSM/Quick-Links-to-BSM-Videos/m-p/6422810.
Troubleshooting & Knowledge Base	Opens the Enterprise Support page on the HPE Software Support (requires HPE Passport login). The URL for this web site is https://www.hpe.com/us/en/support.html.

Menu Option	Description
HPE Live Network	Opens the Business Service Management page in the HPE Live Network website (requires HPE Passport login). The URL for this web site is https://hpln.hpe.com/product/business-service-management/content.
HPE Software Support	Opens the HPE Software Support website. This site enables you to browse the knowledge base and add your own articles, post to and search user discussion forums, submit support requests, download patches and updated documentation, and more. The URL for this web site is https://softwaresupport.hpe.com/.
HPE Software Web Site	Opens the HPE Software Support website, which contains information and resources about HPE Software products and services.The URL for this web site is https://softwaresupport.hpe.com/.
Site Map	Opens the site map, with links to all top-level contexts in the Applications menu or the Administration Console. **Note:** The Site Map is the default entry page when you log into APM. To change the default entry page, see "How to Change the Default Entry Page" on page 29.
What's New?	Opens the What's New document, which describes the new features and enhancements in this version.
HPE BPM Anywhere	Opens HPE BPM Anywhere.
About HPE Application Performance Management	Opens the About HPE Application Performance Management dialog box, which provides version, license, patch, and third-party notice information.

Chapter 8: Customizing APM

This section describes how to customize APM.

Learn About

Section 508 Compliance

APM is compliant with the accessibility and usability standards for people with disabilities set by the US Federal Electronic and Information Technology Accessibility and Compliance Act ("Section 508"), and supports the JAWS® screen reader. For more information, see "How to Enable Section 508 Compliance" below.

Personalization

APM remembers from one session to the next adjustments you made to tables (such as column width and column visibility) in a variety of applications and features, such as recipient management, reports management, reports, and report scheduling.

Note: If two or more users are logged in simultaneously with the same credentials, your settings may not be saved.

Customization of the Title Bar

You can customize the header text of the application title and the logo (HP logo by default) displayed in the upper left-hand corner of the APM window. This change is made on the server side and affects all users accessing APM.

For details, see "How to Customize the Title Bar" on the next page.

Automatic Session Expiration

By default, a ping-to-server mechanism, called **Session Keepalive**, prevents your APM session from timing out when not in active use. You can enable automatic session expiration by disabling Session Keepalive. If you disable Session Keepalive, your session expires after 5 minutes.

For details, see "How to Enable Automatic Session Expiration" on the next page.

Tasks

How to Enable Section 508 Compliance

JAWS users should change the **User Accessibility** setting to true to comply with the Section 508.

1. Select **Admin > Platform > Setup and Maintenance > Infrastructure Settings**.
2. Select **Foundations**.
3. Select **Application Performance Management Interface**.
4. In the **Application Performance Management Interface - Display** area, locate **User Accessibility** and select **true**.

How to Customize the Title Bar

1. Select **Admin > Platform > Setup and Maintenance > Infrastructure Settings**.
2. Select the **Foundations** context.
3. Select **Application Performance Management Interface** from the list.
4. In the **Application Performance Management Interface - Customized Masthead** table, change the following:
   - In the **Customized Masthead Application Title,** enter the text to use as the title for the application. Application Performance Management appears by default if there is no value defined for this field. You can use html coding to enter the text but do not include any scripts. If you using html, verify its validity before saving.
   - In the **Customized Masthead Logo URL**, enter the URL of the file containing the logo you want to appear at the top of the window. The HPE logo appears by default if there is no value defined for this field. It is recommended to use an image with a height of 19 pixels. If the image is larger, it does not appear correctly in the title bar.

   When you modify these settings, the changes appear as soon as the browser is refreshed.

How to Enable Automatic Session Expiration

By default, a ping-to-server mechanism prevents your APM session from timing out when not in active use. You can enable automatic session expiration.

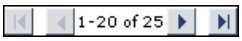
1. Select **Admin > Platform > Setup and Maintenance > Infrastructure Settings**.
2. Select **Foundations**.
3. Select **Application Performance Management Interface**.
4. In the **Application Performance Management Interface - Timing** area, locate **Enable Session Keepalive** and select **false**.

Chapter 9: Working with APM Tables

You can manipulate tables in APM in a number of ways.

Note: Not all tables support all table functionality.

The following is describes a variety of APM table controls:

- **Filtering.** APM tables include various filtering options. For advanced editing of filters, click  .
- **Sorting.** Click a column heading to sort the table by that column. The sort order toggles between ascending and descending order each time you click the column heading.
- **Selecting columns.** Click  to select which columns to display.
- **Changing column width.** Drag a column heading border to the left or right to modify the column width. Click  to reset the column width to its original state.
- **Changing column order.** Drag a column heading to the left or right to change the order in which the columns appear.
- **Paging.** Click the page control buttons 

to move to a table's first, previous, next, or last page.
- **Exporting.** Click the appropriate button to export a table to another format, such as Excel  , PDF  , or CSV  .

For details about table functionality in reports, see Common Report and Page Elements in the APM User Guide.

Part 2: Setup and Maintenance

Chapter 10: Downloads

After the servers for APM are installed, there are several components that can be downloaded. These components include tools for monitoring your enterprise and recording business processes.

These components are located separately in the Web delivery package download area. You can upload them to the APM Downloads page. These files can then be downloaded from APM and used when required.

You can also upload files to the Downloads page for internal web distribution to your users.

To access

Click **Admin> Platform > Setup and Maintenance > Downloads**

Tasks

How to Upload Files to the Downloads Page

Copy the files that you want available in the Downloads page to the **<APM root directory>\AppServer\webapps\site.war\admin\install** directory on the APM Gateway Server. If required, create the **admin\install** directory structure.

How to Download Files from the Downloads Page

1. Click **Admin> Platform > Setup and Maintenance > Downloads**.
2. Right-click the file you want to download and select **Save Target As**.

   Note: Since some files run immediately when you click to download them, right-click the file you want to download, select **Save Target As**, and select the location in which you want to save the file.

3. Select the location in which you want to save the file and click **Save**.
4. Run the component's setup file to install the component.

UI Components

Download Components Page

This page lists the APM components available for download, including tools for monitoring your enterprise and recording business processes.

User interface elements are described below:

UI Element (A-Z)	Description
	Resets the table columns' width to its default setting. You can adjust the width of the table's columns by dragging the borders of the column to the right or the left.

UI Element (A-Z)	Description
	Opens the Select Columns dialog box enabling you to select the columns you want to be displayed on the table.
	Divides the table of data into pages. You move from page to page by clicking the relevant button: • To view more reports, click **Next page** or **Last page**. • To view previous reports in the list, click **Previous page** or **First page**.
Category	The downloadable component's category. Available categories are: • **Business Process Monitor.** Downloadable files that enable you to install and run Business Process Monitor components on APM. • **Data Flow Probe.** The Data Flow Probe downloadable file that enables you to install and run the Data Flow Probe component on APM. • **Diagnostics.** Downloadable files that enable you to install and run Diagnostics components. • **Other**. Used for other applications for download. If you see no applications listed for this category, there are none available. • **Real User Monitor.** Downloadable files that enable you to install and run Real User Monitor components. • **SiteScope.** The SiteScope downloadable file that enables you to install and run SiteScope components. **Note:** Ensure that you have selected the file that corresponds to your operating system. • **Diagnostics.** Downloadable files that enable you to install and run the HPE Diagnostics Agent for Java file.
Description	An explanation of the specific downloadable file.
Document	A link to the PDF describing the component. **Note:** Not all components have a corresponding PDF document available.
File Name	The name of the specific file available for download.
System	The operating system on which APM components are to run.

Chapter 11: License Management

The License Management page enables you to update your APM deployment with a new APM license and to view the status of your current license.

To access

To open the License Management Page, select **Admin > Platform > Setup and Maintenance > License Management**.

Learn About

About Managing APM Licenses

You must have a valid APM license to run monitors and transactions, and to use various integral applications in APM.

The APM license enables you to simultaneously run a predetermined number of monitors and transactions for a specified period of time. The number of monitors and transactions that you can run simultaneously, the specific applications that you can run, and the license expiration date, depend on the license your organization purchased from HPE.

You install the initial license in the configuration wizard, during the installation process.

APM posts a license expiration reminder after the Login page of the web site (for administrators only) 15 days before license expiration.

Several APM applications require additional licensing. To use these applications, you must obtain a license from HPE and then upload the license file in APM.

Tasks

How to add a new license to your APM deployment

1. Select **Admin** > **Platform** > **Setup and Maintenance** > **License Management**.
2. Click **Add license from file** to open the Add License dialog box where you can search for the relevant .dat file. The file is uploaded from the client machine to the APM server.
3. At the bottom of the License Management page, click the **Server Deployment** link.

UI Description

License Management Page

UI Element	Description
	**Add license from file.** Opens the Add License dialog box. From the dialog box browse to and select the license file to upload. The license file is a data file with a **.DAT** extension.

UI Element	Description
Name	The name of the licensed feature. It includes an association to the product resource with which it was bundled.
License Type	There are three types of licenses: • **Evaluation:** A license with a fixed trial period of up to 60 days. This type of license is available only until a Time Based or Permanent license is purchased. Once purchased, the trial period immediately terminates. **Note:** An Evaluation license cannot be renewed. • **Time Based:** A license which has a time-based expiration date. • **Permanent:** A license which does not expire.
Days Left	Displays the number of remaining days for which the license is valid. When green, the expiry time is pending; when red, the license is expired.
Expiration Date	Displays the license's fixed expiration date. This date is displayed only for time-based licenses.
Capacity	If the license is capacity-based, the amount of capacity available and the amount of capacity used is displayed as a status bar. **Note:** This feature is available when the license is capacity-based. If the license is not capacity-based, the words Not Applicable appear in the capacity column.
Capacity Details	If the license is capacity-based, the amount of capacity available and the amount of capacity used is displayed as a ratio. **Note:** This feature is available when the license is capacity-based. If the license is not capacity-based, the words Not Applicable appear in the capacity column.
Server Deployment Link	When you add a license to APM, you must enable the application in the Server Deployment page. This includes a check to see whether the physical resources of your deployment can handle the added application. For details, see "Customizing APM Server Deployment" on page 43.

Tips/Troubleshooting

Manual License Activation

Some licenses are not automatically activated upon installation. These licenses must be activated for specific use and do not run at all times. To activate such a license, click the **Server Deployment** link at the bottom of the License Manager pane.

Installed Licenses and Server Deployment

Although a particular license is installed, you may find that not all features offered by the license are available to you. This can be a result of how these features are configured in APM. You can configure these on the Server Deployment page, available by clicking the **Server Deployment** link at the bottom of the License Management pane, or by running the APM Setup and Database Configuration Utility. For details, see "Server

Deployment and Setting Database Parameters" in the APM Installation Guide.

Make sure that the enabled application matches the installed licenses.

Chapter 12: Customizing APM Server Deployment

This section provides information about how to determine and configure the optimal APM server deployment.

To access

Select **Admin > Platform > Setup and Maintenance > Server Deployment**

Learn About

Server Deployment Overview

APM is composed of many applications and subsystems that consume hardware and software resources. The available applications answer a variety of use cases, not all of which are required by every user. You can align the deployment of the APM servers with your company's business requirements by enabling or disabling APM applications according to your business needs..

APM's Server Deployment page provides a mechanism to deploy only the applications required by your company. You can determine the required hardware according to the required capacity for your specific deployment. The Server Deployment feature displays exactly how much hardware capacity you need for your deployment and enables you to free up unused resources.

The Server Deployment page is available both in the Setup and Database Configuration utility that is run once APM servers are installed, and in the Platform Admin area of the APM interface. This enables you to update your deployment, enable or disable applications as needed, and adjust your deployment's capacities even after installation is complete and any time you have adjustments to make to your APM deployment. You can enable or disable applications, as needed, so as not to use any unnecessary resources in your deployment.

Capacity Calculator

You can use the capacity calculator Excel sheet to determine the scope and size of your APM deployment. You input the information regarding the scope of your deployment in terms of numbers of applications running, users, and expected data. The capacity calculator then calculates the required memory, CPU cores, and determines the size of your deployment. If you are making any change to your deployment, for example adding a license for an application, you use the information in the capacity calculator to determine your hardware requirements and deployment configuration.

You can upload a file that has been saved with your data directly into the Server Deployment page. This enables you to automatically populate the fields in the page with the data as you entered it into the Excel sheet.

If you used the file when you first installed APM, use your saved version whenever you need to make any changes to your deployment. If you do not have your own version, you can download the latest version from the HPE Software Support site (https://softwaresupport.hpe.com).

You enter the information regarding your deployment in the **Deployment Calculator** sheet of the file. In the **Capacity Questionnaire** columns, include information such as applications and size and the **Output** tables automatically calculate the hardware and software requirements. Make sure to save the file in a location from which you can upload it to the Server Deployment page. It is recommended that you make a copy of the file each time before updating it.

When you update the capacity calculator, you are not making any changes to your deployment. You use the capacity calculator to update the values in the Server Deployment page. Only changing values and clicking **Save** in the Server Deployment page actually updates your deployment.

Tasks

How to Update Your APM Licenses, Applications, or Deployment Scope

This task describes how to make changes to your server deployment.

1. ### *Use the capacity calculator to determine the required capacity of your deployment change*

   Before you make any changes to your APM deployment, such as adding a license for an application, it is recommended that you use the capacity calculator Excel file to determine if your current servers meet the required capacity.

   It is recommended that you modify the saved version of the capacity calculator that was used prior to installing APM. If you did not save your own version of the capacity calculator before installation or thereafter, you can download the latest version from the HPE Software Support site (https://softwaresupport.hpe.com/).

   Make sure to save the file with your current requirements in a location from which you can upload it to the Server Deployment page.

2. ### *Add a new license — optional*

   Perform this step if you are updating your deployment with a new license.

   a. Select **Admin > Platform > Setup and Maintenance > License Management**.

   b. Click **Add license from file** to open the Add License dialog box where you can search for the relevant .dat file. The file is uploaded from the client machine to the APM server.

   c. At the bottom of the License Management page, click the **Server Deployment** link.

3. ### *Update the deployment in the Server Deployment page*

   Select **Admin** > **Platform** > **Setup and Maintenance** > **Server Deployment**.

   - **Input table**. Click the **Browse** button to upload the saved version of your capacity calculator Excel file. When you select a file to upload, the values entered in the capacity calculator file automatically populate the Server Deployment page with the correct information for your deployment.

     Alternatively, you can enter the required information in the upper table manually, but it is recommended to use the capacity calculator so that it calculates the capacity for you and determines the scope of your deployment based on the values you input.

   - **Server status table**. In the lower table indicating the status of the servers, ensure that the required memory does not exceed the detected memory on the servers. If it does, you must either remove selected applications, change the capacity level, or increase the memory on the servers.

4. ### *Restart APM*

   After you click **Save** in the Server Deployment page, you need to restart APM. For details, see "Starting, Stopping, or Restarting APM" on page 10.

5. ***Verify results***

   Verify that any applications you added to your deployment now appear in the APM menus. For example, if you enabled the System Availability Management application, you can now find the menu option under both the **Admin** and **Applications** menu.

   Conversely, if you removed any applications from your deployment, they are no longer available in the applicable menus.

UI Description

Server Deployment Page

This page enables you to update your deployment and determine if your hardware meets the memory requirements of any change you make. After you save the changes to this page, APM must be restarted for the changes to take effect.

User interface elements are described below (unlabeled elements are shown in angle brackets):

UI Element	Description
<Capacity Calculator file name>	Use the **Browse** button to locate and upload your saved capacity calculator Excel file. If you have not yet entered your values into a capacity calculator, it is recommended that you do so prior to making any changes to this page. You can download the latest version of the capacity calculator from the HPE Software Support site (https://softwaresupport.hpe.com/).
<Capacity table>	The upper table in the page displays the current information regarding deployment and applications. If you upload a capacity calculator file, this table is automatically updated with the information in the capacity calculator. You can change capacity level of your deployment for: • **Users.** Number of logged in users. • **Model.** The number of configuration items in your model determines whether your model is small, medium, large, or extra-large. • **Metric Data.** The number of monitored applications, transactions, locations, and hosts determines whether your metric data load is small, medium, or large. You can also enable/disable applications and features, and change their capacity levels. After you click **Save** and restart APM: • If you selected an application that was previously not selected, the application is available in APM and applicable menus. • If you cleared an application that was previously selected, the application is no longer accessible.

UI Element	Description
<Server status table>	The lower table lists all the servers running APM including: • **Status**. Whether the machine is up and running. • **Aligned**. Whether this machine is aligned with the current deployment configuration. It would be aligned only if APM was restarted on this machine after any changes were made. If APM was not yet restarted on this machine since any configuration changes were made in this page, the machine is not aligned. • **Machine**. The name of the server. • **Installed**. Which type of APM server is installed on the machine, Gateway or Processing or both (Typical installation when Gateway and Data Processing are on the same machine). • **Activated**. Which type of APM server is currently activated on the machine, Gateway or DPS (data processing server). • **Detected**. The free memory detected on the machine. • **Required**. The required memory for each type of server based on the applications and capacity levels listed in the upper table. If the Required memory is higher than the memory in the Detected column, you must either: • Change capacity levels for your deployment, for example: clear applications from the list of available applications. • Add memory to the physical machines and try to update your deployment again.
To disable machine	Link to page on which you can disable server machines whose installed APM components are no longer relevant to the ongoing operation of the system. Before disabling a machine, verify that it is no longer an operational part of the APM server architecture. To re-enable a machine after disabling it here, you need to run the Setup and Database Configuration Utility on that machine.

Troubleshooting and Limitations

Troubleshooting

- If an application is missing from the APM interface, activate it using the Server Deployment page.
- If an application was activated but does not appear in the APM interface, restart all APM servers.
- If an application was selected in the capacity calculator but was not imported to the Server Deployment page, ensure that you have a valid license for this application.

Chapter 13: Managing Databases

Database Overview

From the Setup and Maintenance tab of the Platform Administration, you can create the databases APM uses to store monitoring data.

A profile database stores data for different types of data sources (Business Process Monitor, SiteScope). You can either create one database for all data or create dedicated databases (for example, for each data type).

A profile database can collect the following types of data:

- Service Level Management data
- SOA data
- Data from Real User Monitor and Business Process Monitor
- Data used in Service Health
- Diagnostics data

An analytics database stores data for the Service Health Analyzer application.

Supported Database Types

APM supports two database types:

- **Microsoft SQL server.** This database runs on Windows operating systems only.
- **Oracle server.** This database runs on any APM supported operating system. An Oracle server database is referred to as a user schema.

Database Management Tasks

The Manage Profile/Analytics Databases page page enables you to perform the following database management tasks:

- **Create a new database.** APM creates a new database and populates it with profile tables.
- **Assign a default profile database.** You must assign a default profile database, to enable APM to collect the required data. The first database added on the Database Management page is designated as the default profile database.
- **Connect to an existing database populated with tables.** APM connects to a database that was either manually created and populated with tables, or previously defined in Platform Administration.

For details on creating databases, assigning a default profile database, and connecting to an existing database, see "Creating Databases" on the next page.

Deploying Databases

To deploy databases on Microsoft SQL server or Oracle server for your organization's particular environment, follow the instructions in "Introduction to Preparing the Database Environment" in the APM Database Guide. We recommend that you review the relevant portions of the APM Database Guide before performing profile and analytics database management tasks.

Additional Database Tasks

APM aggregates non-obsolete data when generating future reports.To mark data as obsolete, see "Marking

Data as Obsolete for Reports" on page 54

The purging manager configures data partitioning for performance enhancement and automatic removal of historical data from profile databases. For details, see "Partitioning Databases and Purging Historical Data from Databases" on page 59

By default, the Data Marking utility always runs the data marking process, followed by the re-aggregation process. To run re-aggregation only, see "Running Re-aggregation Only" on page 64

Database Loader

The database loader persister is responsible for storing incoming data samples until the data is processed by the loader in order to prevent data loss in case of system failure. To learn more, see "Database Loader Persistence Folders" on page 65.

Creating Databases

This section provides information and instructions for creating profile and analytics databases.

Note: It is possible to create multiple profile database. However, HPE recommends that you do not create more than 10 profile databases. Creating more than 10 profile databases can adversely affect the performance of the metric load in the database and the performance of the Partition Manager. Note that historical data will be lost (for example, SLM data, Alerts, SiS data, and KPI Over Time) if you change the default profile schema..

To access

- To create a profile database, select **Admin > Platform > Setup and Maintenance > Manage Profile Databases**.
- To create an analytics database, select **Admin > Platform > Setup and Maintenance > Manage Analytics Databases**.

Tasks

This section includes:

- "How to Create a Profile Database on a Microsoft SQL Server" below
- "How to Create a Profile User Schema on an Oracle Server" on the next page
- "How to Create an Analytics Database on a Microsoft SQL Server" on the next page
- "How to Create an Analytics Database on an Oracle Server" on page 50

How to Create a Profile Database on a Microsoft SQL Server

Tip: We recommend that you configure Microsoft SQL server databases manually, and then connect to them in the Database Management page. For details on manually configuring Microsoft SQL server databases, see "Microsoft SQL Server Deployment Overview" in the APM Database Guide.

Before beginning this procedure, make sure you have the following database server connection information: server name, database user name and password, and server port.

1. Access the Database Management page, located at **Admin> Platform > Setup and Maintenance > Manage Profile Databases**.

2. Select **MS SQL** from the drop-down list, and click **Add**.
3. Enter the parameters of your database on the **Profile Database Properties - MS SQL Server** page. For information about the profile database parameters, see "Profile Database Properties — MS SQL Server Page" on page 51 .

How to Create a Profile User Schema on an Oracle Server

Tip: We recommend that you configure Oracle server user schemas manually, and then connect to them in the Database Management page. For details on manually configuring Oracle server user schemas, see "Oracle Server Deployment Overview" in the APM Database Guide

Prerequisites

- Create a dedicated default tablespace for profile user schemas (and a dedicated temporary tablespace, if required).
- Use a secure network connection if you do not want to submit database administrator connection parameters over a non-secure connection. If you do not want to submit database administrator connection parameters using your web browser at all, you can manually create profile user schemas and then connect to them from the Database Management page.
- Make sure you have the following database server connection information: host name, SID, port, database administrator user name and password, default tablespace, and temporary tablespace.

To add a profile user schema:

1. Access the Database Management page, located at **Admin > Platform > Setup and Maintenance > Manage Profile Databases**.
2. Select **Oracle** from the drop-down list, and click **Add**.
3. Enter the parameters of your user schema on the **Profile Database Properties - Oracle Server** page. For information about the profile database parameters, see "Profile User Schema Properties — Oracle Server Page" on page 52.

Note: If your profile database is part of Oracle Real Application Cluster (RAC), see "Support for Oracle Real Application Cluster" in the APM Database Guide.

How to Create an Analytics Database on a Microsoft SQL Server

Tip: We recommend that you configure Microsoft SQL server databases manually, and then connect to them in the Database Management page. For details on manually configuring Microsoft SQL server databases, see "Microsoft SQL Server Deployment Overview" in the APM Database Guide.

Before beginning this procedure, make sure you have the following database server connection information: server name, database user name and password, and server port.

1. Access the Database Management page, located at **Admin> Platform > Setup and Maintenance > Manage Analytics Databases**.
2. Select **MS SQL** from the drop-down list, and click **Add**.
3. Enter the parameters of your database on the **Analytics Database Properties - MS SQL Server** page. For information about the profile database parameters, see "Profile Database Properties — MS SQL Server Page" on page 51.

How to Create an Analytics Database on an Oracle Server

Prerequisites

- Create a dedicated default tablespace for SHA user schemas (and a dedicated temporary tablespace, if required).
- Use a secure network connection if you do not want to submit database administrator connection parameters over a non-secure connection. If you do not want to submit database administrator connection parameters using your web browser at all, you can manually create SHA user schemas and then connect to them from the Database Management page.
- Make sure you have the following database server connection information: host name, SID, port, database administrator user name and password, default tablespace, and temporary tablespace.

To add an analytics user schema:

1. Access the Database Management page, located at **Admin > Platform > Setup and Maintenance > Manage Analytics Databases**.
2. Select **Oracle** from the drop-down list, and click **Add**.
3. Enter the parameters of your user schema on the **Analytics Database Properties - Oracle Server** page. For information about the analytics database parameters, see "Profile User Schema Properties — Oracle Server Page" on page 52.

Note: If your analytics database is part of Oracle Real Application Cluster (RAC), see "Support for Oracle Real Application Cluster" in the APM Database Guide.

UI Description

This section includes:

Database Management Page

User interface elements are described below:

UI Element (A-Z)	Description
	Click to edit the properties of the Microsoft SQL server database or Oracle server user schema.
	Disconnects the database or user schema. This button only appears if you have more than one connected databases or user schema. **Note:** You cannot delete the default profile database or a database that is in use.
Add	Adds a Microsoft SQL server database or Oracle server user schema, as specified in the drop-down database list.

UI Element (A-Z)	Description
Database Name	The name of the database.
Database Type	The type of database, either Microsoft SQL or Oracle.
Server Name	The name of the server on which the database is running.

Profile Database Properties — MS SQL Server Page

User interface elements are described below:

UI Element (A-Z)	Description
Create database and/or tables	• To create a new database, or connect to an existing, empty database and populate it with profile tables, select the check box. • To connect to an existing database already populated with profile tables, clear the check box.
Database name	• If you are configuring a new database, type a descriptive name for the database. • If you are connecting to a database that was previously created, type the name of the existing database.
Disconnect	Disconnects the database from APM. **Note:** This button appears only after you have clicked the **Disconnect Database**  button on the Database Management page. This option is not available for analytics databases.
Make this my default profile database	Select this check box to make this database the default profile database. **Note:** • This setting is required if you are collecting Service Health, Real User Monitor, HPE Diagnostics (if installed), Service Level Management, SOA. • Selecting this check box overwrites the existing default profile database. • This option is available only for profile databases.
Port	Enter the port number if: • The Microsoft SQL server's TCP/IP port is configured to work on a port different from the default (1433). • You use a non-default port in static mode. • You use a non-default port in dynamic mode. In this case, enter port **1434**.

UI Element (A-Z)	Description
Server name	Enter the name of the machine on which the Microsoft SQL server is installed. If you are using a non-default instance in dynamic mode, enter the server name in the following format: `<my_server\my_instance>`
SQL server authentication	Select if the Microsoft SQL server is using SQL server authentication.
Time Zone	If you select the **Make this my default profile database** option, select the time zone of the data in this database from the drop-down list. This option is only available for profile databases.
User name	• If you are using Windows authentication, this field should remain empty. • If you are using SQL server authentication, enter the user name of a user with administrative rights on Microsoft SQL server.
User Password	• If you are using Windows authentication, this field should remain empty. Make sure that the APM service is run by a Windows user configured in the database server as an authorized Windows login. • If you are using SQL server authentication, enter the password of a user with administrative rights on Microsoft SQL server.
Windows authentication	Select if the Microsoft SQL server is using Windows authentication.

Profile User Schema Properties — Oracle Server Page

User interface elements are described below:

UI Element (A-Z)	Description
Create database and/or tables	• To create a new user schema, or connect to an existing, empty user schema and populate it with profile tables, select the check box. • To connect to an existing user schema already populated with profile tables, clear the check box. **Note:** Clearing this check box disables the database administrator connection parameter and tablespace fields on the page, and instructs the platform to ignore the information in these fields when connecting to the Oracle server machine.
Database administrator password	Enter the password of a user with administrative permissions on the Oracle server. This parameter is used to create the user, and is not stored in the system. **Note:** This field is enabled only if you selected the **Create database and/or tables** check box.

UI Element (A-Z)	Description
Database administrator user name	Enter the user name of a user with administrative permissions on the Oracle server. This parameter is used to create the user, and is not stored in the system. **Note:** This field is enabled only if you selected the **Create database and/or tables** check box.
Default tablespace	Enter the name of the default tablespace designated for use with user schemas. For details on creating a dedicated tablespace, see "Oracle Server Deployment Overview" in the APM Database Guide. If you did not create, and do not require, a dedicated default tablespace, specify an alternate tablespace. The default Oracle tablespace is called users.
Disconnect	Disconnects the user schema from APM. **Note:** This button appears only after you have clicked the **Disconnect Database**  button on the Database Management page.
Host name	Enter the name of the machine on which the Oracle server is installed.
Make this my default profile database	Select or clear as required. **Note:** • This setting is required if you are collecting Service Health, Real User Monitor, HPE Diagnostics (if installed), Service Level Management, SOA. • Selecting this check box overwrites the existing default profile database. • This option is only available for profile databases.
Port	Enter the Oracle listener port, if different from the default value, **1521**.
Retype password	Retype the user schema password.
SID	Enter the Oracle instance name that uniquely identifies the instance of the Oracle database being used, if different from the default value, **orcl**.
Temporary tablespace	Enter the name of the dedicated temporary tablespace designated for use with user schemas. If you did not create, and do not require, a dedicated temporary tablespace, specify an alternate tablespace, if different from the default Oracle temporary tablespace, **temp**.
Time Zone	If you select the **Make this my default profile database** option,select the time zone of the data in this database from the drop-down list. This option is only available for profile databases.
User schema name	• If you are configuring a new user schema, enter a descriptive name for the user schema. • If you are connecting to a user schema that was previously created, enter the name of the existing user schema.

UI Element (A-Z)	Description
User schema password	• If you are configuring a new user schema, enter a password that enables access to the user schema. • If you are connecting to a user schema that was previously created, enter the password of the existing user schema. **Note:** You must specify a unique user schema name for each user schema you create for APM on the Oracle server.

Tips/Troubleshooting

Timeouts

Database creation can take several minutes. The browser might time out before the creation process is completed. However, the creation process continues on the server side.

If a timeout occurs before you a confirmation message appears, verify that the database name appears in the database list on the Database Management page to ensure that the database was successfully created.

Syntax Rules

- The database name cannot contain: /, \\, :, *, ?, \",<, >, |, or spaces, and cannot begin with a digit.
- The host name cannot contain: /, :, *, ?, \",<, >, |, or spaces.

Marking Data as Obsolete for Reports

Using the Data Marking utility, you can mark Business Process Monitor and SiteScope data as obsolete. APM aggregates only non-obsolete data when generating future reports.

To access

On the Gateway Server, run the following file:

- For Windows: **<APM Gateway Server root directory>\tools\dataMarking\dataMarking.bat**
- For Linux: **<APM Gateway Server root directory>/HP/BSM/tools/dataMarking/datamarking.sh**

Learn About

Data Marking Utility Overview

The Data Marking utility enables APM users with superuser security privileges to mark specific sets of data in profile databases as obsolete so that the marked data is not included when generating reports.

While the utility does not physically remove marked data from the database, it renders the marked data unusable in reports and applications by assigning the marked data a status of **unavailable** in the database.

In this way, the Data Marking utility enables you to filter out obsolete data and enables APM to display only the most relevant data for the specified time period. After you mark a specific set of data from a given time period as obsolete, APM reruns the aggregation process on the remaining raw data for the relevant time period.

Additional Data Marking Utility Features

If necessary, you can re-aggregate a defined set of data without marking it as obsolete. This might be necessary if data marking passed successfully but re-aggregation failed. For details, see "Running Re-aggregation Only" on page 64.

Since the Data Marking utility supports partitions, users running the Purging Manager can also use the Data Marking utility. For details, see "Partitioning Databases and Purging Historical Data from Databases" on page 59.

Tasks

This section includes:

How to Mark Data as Obsolete

1. On the Gateway Server, double-click the **<APM Gateway Server root directory>\tools\dataMarking\dataMarking.bat** file. A Command Prompt window opens, followed by the Data Marking Utility Login dialog box.
2. Enter the user name and password of an APM user with superuser privileges.
3. From the **View by** drop-down list, select the type of data to appear in the Data Marking Utility page, for example, data from **Applications** or **SiteScope**.
4. Click **Mark data as obsolete**.
5. Select the appropriate critera to mark as obsolete (Applications, Business Transaction Flows, Transactions, Locations, or SiteScope Targets).
6. Select the **Start Time** and **Duration** for the Data Marking and Re-aggregation process. For example, if you select a **Start Time** of May 22, 2013 8:20 am, and a **Duration** of 3 hours, the Data Marking utility marks all data in the selected criteria that is dated May 22, 2013 with a time stamp of 8:20 am through 11:20 am.
7. Before the Data Marking utility marks the data as obsolete, you can view the SLAs affected by the marked data by clicking **Get Info**. For details, see "Data Marking Information Window" on page 57.
8. Click **Start**. The progress bars display the progress of the Data Marking and Re-aggregation process.

Note: There is no indication in the user interface of which data is to be marked as obsolete.

How to Mark Obsolete Data as Valid

You can select obsolete data and mark it as valid.

Note: There is no indication in the user interface of which data was marked obsolete.

1. On the Gateway Server, double-click the **<APM Gateway Server root directory>\tools\dataMarking\dataMarking.bat** file. A Command Prompt window opens, followed by the Data Marking Utility Login dialog box.
2. Enter the user name and password of an APM user with superuser privileges.

3. From the **View by** drop-down list, select the type of view to appear in the Data Marking Utility pagee, for example, data from **Applications** or **SiteScope**
4. Click **Mark data as valid**.
5. Select the appropriate critera to mark as valid (Applications, Business Transaction Flows, Transactions, Locations, or SiteScope Targets).
6. Select the **Start Time** and **Duration** for the Data Marking and Re-aggregation process. For example, if you select a **Start Time** of May 22, 2013 8:20 am, and a **Duration** of 3 hours, the Data Marking utility marks all data in the selected criteria that is dated May 22, 2013 with a time stamp of 8:20 am through 11:20 am.
7. Before the Data Marking utility marks the data as valid, you can view the SLAs affected by the marked data by clicking **Get Info**. For details, see "Data Marking Information Window" on the next page.
8. Click **Start**. The progress bars display the progress of the Data Marking and Re-aggregation process.

How to Configure Data Marking Maximum Time Duration

You can configure the maximum duration for which the marked data is obsolete. For example, you can set the maximum duration to be 15 hours. This means that you cannot mark data as obsolete (or valid) for more than 14 hours and 59 minutes.

The default maximum duration is 6 hours and 59 minutes.

To configure the maximum duration:

1. Open the **<Gateway Server root directory>\tools\dataMarking\dataMarking.bat** file in a text editor.
2. Add the **DmaximumDuration** property, with a value of the maximum duration in hours, to the **SET SERVICE_MANAGER_OPTS** line.

   For example, to change the maximum duration to 23 hours and 59 minutes:

   ```
   SET SERVICE_MANAGER_OPTS=
   -DhacProcessName=%PROCESS_NAME%
   -Dlog.folder.path.output=%PROCESS_NAME% -DmaximumDuration=24
   ```
3. Save and close the file.

UI Description

Data Marking Utility Page

This page enables you to select sets of data as obsolete by application or by location for Business Process Monitor data, and by the SiteScope target machine for SiteScope data.

User interface elements are described below:

UI Element (A-Z)	Description
Advanced Button	This button appears if the re-aggregation only feature has been enabled. It enables you to run re-aggregation without the data marking process. For more information see "Running Re-aggregation Only" on page 64.
Applications	List of applications you can mark as obsolete.

UI Element (A-Z)	Description
BTF	List of business transaction flows you can mark as obsolete. **Note:** This field is visible only in the Applications view (**View by** > **Applications**).
Duration	Select the period of time, starting from the specified start time, for the utility to mark data as obsolete. The default value is 6 hours and 59 minutes. For details on customizing this value, see "How to Configure Data Marking Maximum Time Duration" on the previous page.
Get Info	Click before running the Data Marking utility to view the SLAs affected by the marked data. For details, see "Data Marking Information Window" below.
Locations	List of locations you can mark as obsolete.
Mark data as obsolete	Marks the filtered criteria (Applications, Business Transaction Flows, Transactions, Locations, or SiteScope Targets) as obsolete.
Mark data as valid (undo mark as obsolete)	Makes selected data valid after having been marked as obsolete.
Progress	Displays the progress of the data marking process and re-aggregation process.
SiteScope Targets	List of SiteScope target machines (machines being monitored by SiteScope) that you can mark as obsolete. **Note:** This field is visible only in the SiteScope view (**View by** > **SiteScope View**).
Start	Activates the Data Marking utility and marks data as obsolete.
Start Time	Select a starting date and time for data to be marked as obsolete.
Transactions	List of transactions you can mark as obsolete. **Note:** This field is visible only in the Applications view (**View by** > **Applications**).
View by	Select the type of view to be visible in the Data Marking utility: • Applications • Locations • SiteScope Targets

Data Marking Information Window

The Data Marking Information window displays the data to be marked as obsolete by the Data Marking utility.

The lower portion of the Data Marking Information window displays the SLAs affected by the marked data. You can recalculate the affected SLAs on the Agreements Manager tab under **Admin > Service Level Management**. For details, see Recalculation for SLAs in the APM Application Administration Guide.

User interface elements are described below:

UI Element (A-Z)	Description
Application Name	The name of the application to be marked as obsolete.
Number of Rows to Update	The number of data rows per selected criteria to be marked as obsolete. A row appears for each criterion selected in the Data Marking Utility window.
Total Rows to Update	The sum of all the number of rows to be marked as obsolete. This number can differ from the value of the **Number of Rows to Update** field.

Tips/Troubleshooting

Tips

- Do not run more than one instance of the Data Marking utility at a time, as this can affect the re-aggregation process.
- Do not mark data sets for time periods that include purged data (data that has been removed using the Partition and Purging Manager) as this can affect the re-aggregation process.

Limitations

- The Data Marking utility does not mark late arriving data.

  For example, if a set of data for a specific time period is marked as obsolete and APM later receives data from that time period (which arrived late due to a Business Process Monitor temporarily being unable to connect to the Gateway Server), the late arriving data is not marked as obsolete and is available for use in reports. Use the **Get Info** button to check for late arriving data. If any value other than zero rows are displayed, run the utility again, if required, to mark the data that arrived late as obsolete.
- The Data Marking utility does not mark data as obsolete if it arrives while the utility is running.

  For example, if a set of data for a specific time period is marked as obsolete, and during that same time period (while the utility is running), data arrives and enters the profile database, the rows of newly arrived data are not marked as obsolete, and are therefore included in the report. In this case, after the utility finishes running, click the **Get Info** button to determine whether all rows of data were marked as obsolete for the selected time period. If rows are displayed, run the utility again, if required, to mark the data that arrived during the run as obsolete. This is a rare scenario, as you typically mark data for a previous time period and not for a time period that ends in the future.
- While the Data Marking utility is running and removing data, reports that are generated for that time period may not show accurate results. Therefore, it is recommended to run the utility during off-peak APM usage times.

Troubleshooting

Generally, when an error occurs, the Data Marking utility displays the following error message:

```
The Data Marking utility must shut down due to an internal error. For details see:
<HPEAPMGateway Server root directory>\log\datamarking.log
```

Reasons for which the utility might display this error include:

- Failure to connect to the database server or profile database.
- Failure to complete the data marking process, for example, due to a communication error between the aggregation server and database.
- Failure of APM to successfully re-aggregate raw data for the defined data set.

If an error occurs, check the <**APM Gateway Server root directory>\log\datamarking.log file** for error information.

Partitioning Databases and Purging Historical Data from Databases

The APM database tables are created based on predefined database templates. The purging manager configures data partitioning for performance enhancement and automatic removal of historical data from profile databases.

To access

Select **Admin > Platform > Setup and Maintenance > Data Partitioning and Purging**.

Learn About

Partitioning

The database tables can quickly become very large due to the large amount of data generated by the APM data collectors. Over time, this can severely degrade system performance.

The Purging Manager automatically splits fast growing tables into partitions based on internal settings. Splitting the tables into partitions optimizes database performance.

New partitions are created based on an internal configuration regardless of whether or not the partition is filled.

New partitions for a table are created in the same Oracle tablespace or Microsoft SQL file group as the table's last partition. These partitions automatically acquire the storage parameters of this tablespace.

Note: The partitioning method used by the Partition and Purging Manager is Database Native Partitioning. (Refer to the database support matrix in the release notes for the SQL SERVER and Oracle Enterprise editions supported for this release). In an Oracle database, the Oracle Partitioning option must be enabled in order to partition or purge data from an Oracle database.

EPM

The size of each partition is determined by the EPM (Events per Minute) value displayed on the Purging Manager page. The default EPM value is preset according to the appropriate level for each database table.

If the data partitions are too large (accumulating much more than 1 million rows), you can raise the EPM value to create new partitions more frequently.

If the data partitions are too small (accumulating much less than 1 million rows), you can lower the EPM value to create new partitions less frequently.

Purging

By default, the Purging Manager does not purge data. However, you can configure the Purging Manager to purge data by defining the amount of time the data in a table's partition is retained.

The Purging Manager runs every hour and purges data older than the defined retention time.

Tasks

This task includes the following topics:

Prerequisites

Ensure that you have at least one profile database configured in your APM system.

- For details on configuring a profile database on a Microsoft SQL server, see "How to Create a Profile Database on a Microsoft SQL Server" on page 48.
- For details on configuring a user schema on an Oracle server, see "How to Create a Profile User Schema on an Oracle Server" on page 49.

How to Change a Database Template

To change settings for a database template, follow these steps:

1. Click **Admin > Platform > Setup and Maintenance > Data Partitioning and Purging**.
2. Click the **Template and Multiple Databases** tab.

   Note: The settings displayed in the Template and Multiple Databases tab are the settings configured for the template. To view the settings for a specific database tables, click the **Database Specific** tab.

3. Click the **Apply to** link at the top left of the page. The **Apply to** window appears with a list of databases and templates.
4. Select the required template.

   Note: We recommend that you also select all the available databases.

5. Click **OK**.
6. Select the check box next to the database tables whose database template you want to change. You can select multiple tables.
7. Modify the **Keep Data for** and **Change to EPM** fields as necessary, and click **Apply**.

How to Change Settings for Multiple Databases

To change settings for multiple databases, follow these steps:

1. Click **Admin > Platform > Setup and Maintenance > Data Partitioning and Purging**.
2. Click the **Template and Multiple Databases** tab.

   Note: The settings displayed in the **Template and Multiple Databases** tab are the settings configured for the template. To view the settings for a specific database tables, click the **Database Specific** tab.

3. Click the **Apply to** link at the top left of the page and ensure that the databases you want to change are selected. Clear the check box next to the template if you do not want your changes to apply to the template.
4. Click **OK**.
5. Select the check box next to the database tables you want to change. You can select multiple database tables.
6. Modify the **Keep Data for** and **Change to EPM** fields as necessary, and click **Apply**.

   Note: Changes made to the databases are displayed only in the Database Specific tab.

How to Change Settings for Individual Databases

To change settings for individual databases, follow these steps:

1. Click **Admin> Platform > Setup and Maintenance > Data Partitioning and Purging**.
2. Click the **Database Specific** tab.

   Note: The settings displayed in the **Database Specific** tab are the settings configured for the databases. To view the template settings, click the **Template and Multiple Databases** tab.

3. In the **Select a profile database** field, select the profile database to which you want your changes to apply.
4. Select the check box next to the database tables you want to change.
5. Modify the **Keep Data for** and **Change to EPM** fields as necessary, and click **Apply**.

How to Determine the Events Per Minute for a Database Table

You can determine the amount of events per minute (EPM) that arrives to a database table from the data collectors. You enter this number in the **Change to EPM** field at the top of the **Purging Manager** page.

To determine the Events Per Minute for a database table:

1. Open the file located at:

   <Gateway Server root directory>\log\db_loader\LoaderStatistics.log

2. Locate the line in the select data sample that reads:

   Statistics for: DB Name: <database name> Sample: <sample name> - (collected over <time period>):

3. Locate the line in the statistics section of the data sample that reads:

   Insert to DB EPS (MainFlow)

   The selected number represents the events per second. Multiply this number by 60 to determine the number of events per minute.

   To determine to which database table in the Purging Manager the sample belongs, follow the instructions for Generic Reporting Engine API in the APM Extensibility Guide. The resulting list displays the database

table in parentheses next to the name of the sample. You can then enter the EPM number for the correct table.

If you have more than one Gateway Server, add the values obtained from each server.

UI Description

Purging Manager Page

User interface elements are described below:

UI Element (A-Z)	Description
Apply to	Select the databases and template to which you want the configurations on the Template and Multiple Databases tab to apply. You can clear all databases to make changes only to the selected template.
Change to EPM	Enables you to configure the amount of data per minute that arrives in a database table from the data collectors. **Note:** Leave this field empty to retain the existing EPM value. For details on determining this value, see "How to Determine the Events Per Minute for a Database Table" on the previous page
Database Specific	This tab displays the configurations for the tables associated with the database selected in the **Select a profile database** drop-down list. From this tab you can change the EPM or data retention time a specific database table.
Description	Describes the corresponding database table.
Epm Value	The amount of data per minute that arrives in the database tables from the data collectors. For details on determining this value, see "How to Determine the Events Per Minute for a Database Table" on the previous page.
Keep Data for	The time range for retaining data in the database tables. This element appears as follows: • **Selection fields.** At the top of the page, set the time period for how long you want data kept in the selected database tables. • **Column heading.** Displays the amount of time data remains in a database table before it is purged. This value is configured in the **Keep Data for** selection fields at the top of the page. **Note:** The time period configured in the **Keep Data for** fields indicates that the data is stored for at least the specified amount of time; it does not indicate when the data is purged. By default, retention time is Infinite, meaning that the data is not purged.

UI Element (A-Z)	Description
Name of Table in Database	The name of the table in the database. Database tables are listed by the data collector from which the data was gathered. The following data types are available: • Alerts • Business Logic Engine • Business Process Monitor • DG (Diagnostics Business Transaction Sample) • Diagnostics • Real User Monitor • SOA • Service Level Management • SiteScope • UDX (Universal Data Exchange - custom data) • WebTrace
Select a profile database	Select a profile database for which you want to modify time range configurations for purging data. **Note:** This field is visible only on the Database Specific tab.
Template and Multiple Databases	This tab displays the configurations for the templates that are selected in the **Select a profile database** drop-down list. Select this tab to: • Change the partitioning and purging parameters for multiple profile databases. • Change the database template, for new databases added in the future.

Tips/Troubleshooting

Raw Data not Aggregated

Prior to purging, the Partition and Purging Manager performs an additional check to ensure that raw data is not purged before it has been aggregated and reported to APM.

If a particular set of data is scheduled for purging but its raw data has not yet been aggregated, the Partition and Purging Manager does not purge the data according to its schedule. The Partition and Purging Manager automatically purges the data on its next hourly run only after the data has been aggregated.

For example, if data was scheduled to be purged on Sunday at 8:00 but its data will only be aggregated on Sunday at 10:00, the Partition and Purging Manager checks the data at 8:00, does not purge the data, and automatically purges the data on its next hourly run only after Sunday at 10:00 after the data has been aggregated.

Data not Purged per Schedule

If data is not purged according to the schedules set in the Partition and Purging Manager and the profile databases are growing too large, check that the aggregator is running properly and view the Partition and Purging Manager logs located on the Data Processing Server at **<APM server root directory>\log\pmanager.log**.

Purging Principle

When defining purging for your raw and aggregated data make sure that the length of time raw data is kept is shorter than the length of time one-hour chunks of aggregated data are kept, which is shorter than the length of time one-day chunks of aggregated data are kept.

Purging policy is one year for raw data (for example, Business Process Monitor or SiteScope).

The purging policy for **Offline BLE States** limits the amount of data that can be used for SLA calculation. Even if raw data is available for longer periods of time, the SLAs can only be calculated for the Offline BLE States purging policy setting minus one month. By default, this means that SLA data can be calculated for just three months.

You cannot create an SLA or recalculate an SLA for a time period earlier than three months even if there is raw data for that time period.

New Profile Databases

Any changes made under the Template and Multiple Databases tab affect the default time periods for new profile databases created in the system. If a new profile database is created after you made changes to the time periods in the Template and Multiple Databases tab, data is kept in the tables of that new profile database for the time periods now defined in the Template and Multiple Databases for all tables.

Running Re-aggregation Only

By default, the Data Marking utility (see "Marking Data as Obsolete for Reports" on page 54) always runs the data marking process, followed by the re-aggregation process. If required, you can enable a feature that allows you to run re-aggregation only. This might be necessary if data marking passed successfully but re-aggregation failed.

Alternatively, you can use this feature to re-aggregate a defined set of data without marking it as unwanted for report generation (for example, if data was aggregated and then late-arriving data was inserted into the raw data tables in the database).

To access

On the Gateway Server, double-click the **<APM Gateway Server root directory>\tools\dataMarking\dataMarking.bat** file

Tasks

Prerequisite

You must enable the re-aggregation feature in the dataMarking.bat file in order to run the data re-aggregation process in the Data Marking utility.

1. Open the file **<Gateway Server root directory>\tools\dataMarking\dataMarking.bat** in a text editor.
2. Add the **DadvancedMode** property with a value of **true** to the **SET SERVICE_MANAGER_OPTS** line. For example:

   ```
   SET SERVICE_MANAGER_OPTS=-DhacProcessName=%PROCESS_NAME % -DadvancedMode=true
   ```
3. Save the file. The next time you open the Data Marking utility, the **Advanced** button appears.

How to Run Data Re-aggregation Only

1. On the Gateway Server, double-click the **<APM Gateway Server root directory>\tools\dataMarking\dataMarking.bat** file. A Command Prompt window opens, followed by the Data Marking Utility Login dialog box.
2. Enter the user name and password of an APM user with superuser privileges. The Data Marking Utility page appears.
3. Click **Advanced**. The Advanced window appears.
4. Select the **Run re-aggregation only** check box.
5. Select the categories of data for the re-aggregation and click **OK** to confirm selection.
6. Click **Start**.

UI Description

Data Marking Utility page

For information see "Data Marking Utility Page" on page 56.

Advanced Window

The Advanced window is accessed by clicking **Advanced** on the "Data Marking Utility Page" on page 56. User interface elements are described below:

UI Element (A-Z)	Description
Raw data status	Displays the status of the last re-aggregation.
Run Reaggregation only	Selecting this check box enables running re-aggregation without data marking.

Database Loader Persistence Folders

This topic provides an overview of the database loader persister and the loader persistence folders.

Learn About

Database Loader Persister - Overview

The database loader persister is responsible for storing incoming data samples until the data is processed by the loader in order to prevent data loss in case of system failure. The data samples are assigned a unique ID number when stored in the database loader persistence folder.This enables the data samples to be deleted from the database loader persistence folders after the data is processed.

The loader persister stores the data samples in files called partitions on a local disk. Each partition has a predefined number of data samples it can accommodate. When the limit is reached, a new partition is created. When removing data samples from the main persister, the corresponding partition is found and updated accordingly. When all samples from the partition are removed, the partition file is deleted from the disk.

Upon initialization, the loader persister reads the partition that remained on the disk from the previous run. After the partitions are fully and successfully read, they are deleted from the disk.

Loader Persister Folder Sub-directories

Each gateway server contains a folder named **persist_dir\db_loader** which contains the following sub-directories:

- **.persist_dir\db_loader\main\dlq** – contains samples that the system was not able to insert into the database, for example wrong sample, duplicated samples, or samples with time stamp older then data purging period.

  There is no size limit and no limit of the number of samples in this folder. Old files are not automatically purged. If these samples were added to this folder due to an error, for example, there was a data flow problem, you can reinsert these samples into the database.
- **.persist_dir\db_loader\main\current** – contains samples that are currently in the loader memory. The size of this folder is limited by memory restrictions of the database loader.
- **.persist_dir\db_loader\flattenfailure** – contains hierarchy samples (**trans_t**) that temporarily failed to open because of a database connectivity problem. There is no size limit.
- **.persist_dir\db_loader\recovery** – contains samples that the system was temporarily unable to insert. This is usually because of database availability issues. The limit for each sample type is five sub-folders. Each subfolder can contain up to 509 files with up to 8192 samples in each file (approximately 20M of samples for each sample type). After this limit is exceeded, the loader stops working and will not read data from the BUS.

Chapter 14: Infrastructure Settings

APM enables you to modify the value of many settings that determine how APM and its applications run. You configure most infrastructure settings using the Infrastructure Settings Manager.

Some infrastructure settings are configured outside the Infrastructure Settings Manager. For details, see How to Modify the Ping Time Interval, and Locations and Expirations of Temporary Image Files.

To access

Select **Admin> Platform > Setup and Maintenance > Infrastructure Settings**

Learn About

Infrastructure Settings Manager Overview

In the Infrastructure Settings Manager, you can select different contexts from which to view and edit settings. These contexts appear in the following groups:

- **Applications.** This list includes those contexts that determine how the various applications running within APM behave. Contexts such as Service Health Application, MyBSM, and Service Level Management are listed.
- **Foundations.** This list includes those contexts that determine how the different areas of the APM foundation run. Contexts such as RTSM (Run-time Service Model) and LDAP Configuration are listed.

Descriptions of the individual settings appear in the **Description** column of the table on the Infrastructure Settings Manager page.

Tasks

How to Modify Infrastructure Settings Using the Infrastructure Settings Manager

Caution: Modifying certain settings can adversely affect the performance of APM. It is highly recommended not to modify any settings without first consulting HPE Software Support or your HPE Services representative.

1. Select **Admin > Platform > Setup and Maintenance > Infrastructure Settings**.
2. Select a group of contexts: **Applications**, **Foundations**, or **All**.
3. Select a specific context from the drop-down box.
4. All configurable infrastructure settings relating to that context are displayed, along with descriptions and the current values of each setting. Click the **Edit Setting** button and modify the value of a specific setting.

UI Description

Infrastructure Settings Manager Page

User interface elements are described below:

UI Element (A-Z)	Description
	Click to edit the current value of the given setting in the relevant context table.
All	Select to view all the settings for both Applications and Foundations.
Applications	Select to edit one of the APM Applications.
Description	Describes the specific infrastructure setting. **Note:** This field is visible on both the Infrastructure Settings Manager page, and the Edit Setting dialog box after clicking the **Edit Setting**  button next to the relevant setting.
Foundations	Select to edit one of the APM Foundations.
Name	The name of the setting. **Note:** This field is visible on both the Infrastructure Settings Manager page, and the Edit Setting dialog box after clicking the **Edit Setting**  button next to the relevant setting.
Restore Default	Restores the default value of the setting. **Note:** This button is visible on the Edit Setting dialog box after clicking the **Edit Setting**  button next to the relevant setting.
Value	The current value of the given setting. **Note:** This field is visible on both the Infrastructure Settings Manager page, and the Edit Setting dialog box after clicking the **Edit Setting**  button next to the relevant setting.

Modifying the Ping Time Interval

Note: This infrastructure settings task is performed outside the Infrastructure Settings Manager.

You can modify the time interval after which APM pings the server to refresh a session.

To modify the ping time interval:

1. Open the file **<Gateway Server root directory>\conf\settings\website.xml** in a text editor.
2. Search for the parameter: **user.session.ping.timeinterval**.
3. Change the value (120, by default) for the ping time interval. This value must be less than half, and it is recommended that it be less than a third, of the value specified for the session timeout period (the **user.session.timeout** parameter).

4. Restart APM on the Gateway Server machine.
5. If you have multiple Gateway Server machines, repeat this procedure on all the machines.

Configuring the Database Statistics Age

The Database Statistics monitor checks the relevance of the database statistics. The default is to check the statistics for past day. You can configure the number of days to be used for verification of database statistics.

To configure the Database Statistics Age:

1. Select **Admin > Platform > Setup and Maintenance > Infrastructure Settings**.
2. Select **Foundations**.
3. Select **DB Health**.
4. In the DB Health - DB Health Settings table, locate **DB Statistics age**. Change the value as needed.

Configuring the Maximum Number of Late Arrival Samples

The WDE Late Arrivals monitor checks the number of data samples that reach the database more than an hour after the data is recorded. Late arriving samples are not included in the data aggregation for reports. You can configure the maximum number of late arrival samples, which if exceeded triggers an error. The default value is 1.

To configure the Maximum Number of Late Arrival Samples:

1. Select **Admin > Platform > Setup and Maintenance > Infrastructure Settings**.
2. Select **Foundations**.
3. Select **Offline Aggregator**.
4. In the Offline Aggregator - General table, locate **Maximum number of late arrival samples**. Change the value as needed.

Configuring the Maximum Number of CIs Marked as Candidate for Deletion

The CI Lifecyle monitor checks the number of CIs in RTSM that are marked as candidates for deletion by the aging mechanism. CIs that are marked as candidates for deletion are removed from RTSM in the next aging run. If the maximum number of CIs that can be marked for deletion is reached, a critical error is triggered. The default value is 1.

To configure the Maximum Number of CIs Marked as Candidate for Deletion:

1. Select **Admin > Platform > Setup and Maintenance > Infrastructure Settings**.
2. Select **Foundations**.
3. Select **Platform Administration**.
4. In the Platform Administration - CI Lifecycle monitor table, locate **Maximum number of CIs marked as candidate for deletion**. Change the value as needed.

Configuring the Maximum Number of Bus Queue Messages

The Bus Queue monitor checks the number of messages waiting in each of the HornetQ Bus Queues. You can configure the maximum number of messages in the HornetQ Bus Queues. If the maximum number of messages waiting in the HornetQ Bus queues is reached, a critical message is triggered. If half the maximum number is reached, a warning is triggered. The default value is 200.

To configure the Maximum Number of Bus Queue Messages:

1. Select **Admin > Platform > Setup and Maintenance > Infrastructure Settings**.
2. Select **Foundations**.
3. Select **Platform Administration**.
4. In the Platform Administration - Bus Queues monitor table, locate **Maximum number of messages in Bus Queues**. Change the value as needed.

Configuring the Mobile Health Report Locations Threshold

The Locations component in the Mobile Health report displays the ten locations with the worst performance or availability. You can define the minimal number of sessions per location to be displayed in the Locations component. The default value is 0 which means that all locations are displayed on the map and table in Mobile Health report.

To configure the Mobile Health report locations table threshold:

1. Select **Admin > Platform > Setup and Maintenance > Infrastructure Settings**.
2. Select **Applications**.
3. Select **End User/System Availability Management**.
4. In the End User/System Availability Management - Data table, locate **RUM Mobile Health report: Display locations that have at least x sessions**. Change the value as needed.

Locations and Expirations of Temporary Image Files

When you generate a report in APM applications, or when APM automatically generates a report to send through the scheduled report mechanism, images (for example, graphs) are created. APM saves these images, for a limited period of time, in temporary directories on the Gateway Server machines on which the images are generated.

Note: This infrastructure settings task is performed outside the Infrastructure Settings Manager.

Learn About

This section includes:

Accessing Temp Directories with Multiple Gateway Server Machines

APM reports access the Gateway Server machine using a virtual IP and the load balancer sends requests to any of the Gateway Server machines. Therefore, the image files need to be in a common location that is configured on all the Gateway Server machines and shared among them. This is typical when there are multiple Gateway Server machines running behind a load balancer in the APM architecture.

To support a shared location for temporary images in a Windows environment, the following configuration is recommended:

- All Gateway Servers—and the machine on which the shared image directory is defined, if different from the Gateway Servers—should be on the same Windows domain.
- The IIS virtual directory should be configured to use the credentials of an account that is a member of the domain users group.
- The account for the virtual directory should be given read/write permissions on the shared image directory.

> **Note:** If your server configuration requires placing servers on different Windows domain configurations, contact HPE Software Support.

If you set a custom path to temporary images, as defined in the **images.save.directory.offline** parameter (for details, see "How to Modify the Directory in Which Temporary Image Files Are Stored" on page 73), you must map the physical directory containing the images to a virtual directory in the web server on all Gateway Server machines.

Length of Time APM Keeps Temporary Image Files

You can modify settings that control how long APM keeps temporary image files generated by the Gateway Server machine, before removing them from the defined temporary directories. You can modify settings for the following directories in the **<APM Gateway Server root directory>\conf\topaz.config** file:

Directory Setting	Description
remove.files.0.path= ../../AppServer/webapps/site.war/Imgs/chartTemp/offline	Path to images created when generating reports
remove.files.1.path= ../../AppServer/webapps/site.war/Imgs/chartTemp/online	Path to images created when generating reports in APM applications
remove.files.3.path= ../../AppServer/webapps/site.war/snapshots	Path to images created by the Snapshot on Error mechanism and viewed in Error Summary reports

For the above temporary image directories, you can modify the following settings:

- **remove.files.directory.number=<number of directories>**
  Specifies the total number of directories for which you are defining settings.
- **remove.files.<num_of_path>.path=<path to directory>**
  Specifies the path to the directory that contains the files you want to remove. For the default directories that remove temporary image files, these values must match the **images.save.directory.online** and **images.save.directory.offline** parameters, also defined in the topaz.config file.

> **Note:** In Windows environments, use UNC path syntax (**\\\\server\\path**) when defining the path. In

Linux environments, use forward slashes (/) only when defining the path.

- **remove.files.<num_of_path>.expirationTime=<file expiration time in sec>**

  Specifies the time, in seconds, that APM leaves a file in the specified directory. For example, if you specify "3600" (the number of seconds in 1 hour), files older than one hour are removed.

  Leave this setting empty if you want APM to use only maximum size criteria (see below).

- **remove.files.<num_of_path>.maxSize=<maximum size of directory in KB>**

  Specifies the total size, in KB, to which the defined directory can grow before APM removes files. For example, if you specify "100000" (100 MB), when the directory exceeds 100 MB, the oldest files are removed in order to reduce the directory size to 100 MB.

  If you also define a value in the **remove.files.<num_of_path>.expirationTime** parameter, APM first removes expired files. APM then removes additional files if the maximum directory size limit is still exceeded, deleting the oldest files first. If no files have passed their expiration time, APM removes files based only on the maximum directory size criteria.

  This parameter is used in conjunction with the **remove.files.<num_of_defined_path>.deletePercents** parameter (see below), which instructs APM to remove the specified percentage of files, in addition to the files removed using the **remove.files.<num_of_path>.maxSize** parameter.

  Leave this and the **remove.files.<num_of_defined_path>.deletePercents** settings empty if you want APM to use only the expiration time criterion.

- **remove.files.<num_of_path>.deletePercents=<percent to remove>**

  Specifies the additional amount by which APM reduces directory size—expressed as a percentage of the maximum allowed directory size—after directory size has been initially reduced according to the **remove.files.<num_of_path>.maxSize** parameter. APM deletes the oldest files first.

  If you want APM to use only the expiration time criterion, leave this and the **remove.files.<num_of_path>.maxSize** settings empty .

- **remove.files.<num_of_path>.sleepTime=<thread sleep time in sec>**

  Specifies how often APM runs the mechanism that performs the defined work.

Example:

APM is instructed to perform the following work once every 30 minutes: APM first checks whether there are files older than 1 hour and, if so, deletes them. Then APM checks whether the total directory size is greater than 250 MB, and if so, it reduces directory size to 250 MB by removing the oldest files. Finally, APM reduces the total directory size by 50% by removing the oldest files. As a result, APM leaves files totaling 125 MB in the directory.

```
# remove files older than 1 hour (3600 sec.)
remove.files.0.expirationTime=3600
# reduce folder size to 250 MB
remove.files.0.maxSize=250000
# remove an additional 50% of max. folder size (125 MB)
remove.files.0.deletePercents=50
# perform work once every 30 min. (1800 sec)
remove.files.0.sleepTime=1800
```

Tip: You can configure the file removal mechanism to remove files from any defined directory. You define the parameters and increment the index. For example, to clean out a temp directory, you would specify **6** instead of **5** for the number of directories in the **remove.files.directory.number** parameter; then you would define the directory's path and settings using the index value **4** (since 0-4 are already being used by the default settings) in the **num_of_path** section of the parameter. Do not use this mechanism to remove files without first consulting with your HPE Software Support representative.

Tasks

This section includes:

How to Modify the Directory in Which Temporary Image Files Are Stored

You can modify the path to the directory where APM stores generated images used in scheduled reports. For example, you might want to save generated images to a different disk partition, hard drive, or machine that has a greater storage capacity than the partition/drive/machine on which the Gateway Server machine is installed.

To modify the path to the directory holding temporary image files:

1. Open the file **<Gateway Server root directory>\conf\topaz.config** in a text editor.
2. Search for the parameter **images.save.directory.offline**.
3. Remove the comment marker (#) from the line that begins **#images.save.directory.offline=** and modify the value to specify the required path.

   Note: In Windows environments, use UNC path syntax (**\\\\server\\path**) when defining the path. In a Linux environment, use forward slashes (/) and not backslashes (\) when defining the path.

4. Save the **topaz.config** file.
5. Restart APM on the Gateway Server machine.
6. Repeat the above procedure on all Gateway Server machines.
7. Map the newly defined physical directory containing the images to a virtual directory in the web server on all Gateway Server machines. For details, see "Accessing Temp Directories with Multiple Gateway Server Machines" on page 71.

How to Configure the Virtual Directory in IIS

1. Rename the default physical directory containing the temporary scheduled report images on the Gateway Server machine.

   For example, rename:

   ```
   <Gateway Server root directory>\AppServer\webapps\
   site.war\Imgs\chartTemp\offline
   ```

to

```
<Gateway Server root directory>\AppServer\webapps
\site.war\Imgs\chartTemp\old_offline
```

2. In the IIS Internet Services Manager on the Gateway Server machine, navigate to **Default Web site > Topaz > Imgs > ChartTemp**.

   The renamed offline directory appears in the right frame.

3. In the right frame, right-click and select **New > Virtual Directory**. The Virtual Directory Creation Wizard opens. Click **Next**.
4. In the Virtual Directory Alias dialog box, type `offline` in the Alias box to create the new virtual directory. Click **Next**.
5. In the Web Site Content Directory dialog box, type or browse to the path of the physical directory containing the temporary images, as defined in the **images.save.directory.offline** parameter (for details, see "Accessing Temp Directories with Multiple Gateway Server Machines" on page 71). Click **Next**.
6. If the physical directory containing the temporary images resides on the local machine, in the Access Permissions dialog box, specify **Read and Write** permissions.

   If the physical directory containing the temporary images resides on a machine on the network, in the User Name and Password dialog box, enter a user name and password of a user with permissions to access that machine.
7. Click **Next** and **Finish** to complete Virtual Directory creation.
8. Restart APM on the Gateway Server machine.
9. Repeat the above procedure on all Gateway Server machines.

How to Configure the Virtual Directory on Apache HTTP Web Server

1. Rename the default physical directory containing the temporary scheduled report images on the Gateway Server machine.

   For example, rename:

   ```
   <Gateway Server root directory>\AppServer\webapps\site.war\Imgs\chartTemp\offline
   ```

   to

   ```
   <Gateway Server root directory>\AppServer\webapps\site.war\Imgs\chartTemp\old_offline
   ```
2. Open the Apache configuration file **<Gateway Server root directory>\WebServer\conf\httpd.conf** with a text editor.
3. Map a virtual directory named **offline** to the physical location of the common directory as follows:
   a. Locate the line (note lower case "t" in topaz):

      ```
      Alias /topaz "C:\HPBSM/AppServer/webapps/site.war/"
      ```

   b. Above that line add the following line:

      ```
      Alias /topaz/Imgs/chartTemp/offline "<shared_temp_image_directory>"
      ```

   c. Locate the line (note upper case "T" in Topaz):

      ```
      Alias /Topaz "C:\HPBSM/AppServer/webapps/site.war/"
      ```

   d. Above that line add the following line:

      ```
      Alias /Topaz/Imgs/chartTemp/offline "<shared_temp_image_directory>"
      ```
4. Replace `<shared_temp_image_directory>` with the path to the physical directory containing the temporary scheduled report images, as defined in the **images.save.directory.offline** parameter (for

details, see "How to Modify the Directory in Which Temporary Image Files Are Stored" on page 73).

When specifying `<shared_temp_image_directory>` you must use double quotes and forward slashes, for example:

```
Alias /Topaz/Imgs/chartTemp/offline "//myhost.myurl.com/chartTemp/offline"
```

5. Save the file.
6. Restart APM on the Gateway Server machine.
7. Repeat the above procedure on all Gateway Server machines.

How to Configure the Virtual Directory on Sun Java System Web Server

1. Rename the default physical directory containing the temporary scheduled report images on the Gateway Server machine.

   For example, rename:

   ```
   <Gateway Server root directory>\AppServer\webapps\site.war\Imgs\chartTemp\offline
   ```

   to

   ```
   <Gateway Server root directory>\AppServer\webapps\site.war\Imgs\chartTemp\old_offline
   ```

2. Open the Sun Java System Web Server configuration file **<Sun Java System Web Server installation directory>\server\<server_nam>\config\obj.conf** with a text editor.
3. Add the following line inside the `<Object name=default>` directive (before the line **NameTrans fn=document-root root="$docroot"**, and before the line **NameTrans fn="pfx2dir" from="/Imgs" dir="ProductDir/Site Imgs/"**, if it exists):

   ```
   NameTrans fn="pfx2dir" from="/topaz/Imgs/chartTemp/offline"
   dir="<shared_temp_image_directory>"
   ```

   where `<shared_temp_image_directory>` represents the path to the physical directory containing the temporary scheduled report images, as defined in the **images.save.directory.offline** parameter (for details, see "How to Modify the Directory in Which Temporary Image Files Are Stored" on page 73).
4. Save the file.
5. Restart the Sun Java System Web Server on the Gateway Server machine.
6. Repeat the above procedure on all Gateway Server machines.

How to Modify Length of Time APM Keeps Temporary Image Files

1. Open the file **<APM Gateway Server root directory>\conf\topaz.config** in a text editor.
2. Before modifying the values, back up the file or comment out (using #) the default lines so that the default values are available as a reference.
3. Modify the settings as required.
4. Save the **topaz.config** file.
5. Restart APM on the Gateway Server machine.
6. Repeat the above procedure on all Gateway Server machines.

How to Specify the Directories from Which Temporary Image Files Are Removed

By default, temporary image files are removed from the root path of the specified directory. However, you can also configure APM to remove temporary image files from the subdirectories of the specified path.

To configure APM to remove temporary images files from subdirectories:

1. Open the file **<Gateway Server root directory>\conf\topaz.config** in a text editor.
2. Insert the following line after the specified path's other settings (described in the previous section):

   ```
   remove.files.<num_of_path>.removeRecursively=yes
   ```

3. Save the **topaz.config** file.
4. Restart APM on the Gateway Server machine.
5. Repeat the above procedure on all Gateway Server machines.

Enabling Docker Support for RUM Applications

You can configure whether to enable Docker monitoring options in RUM's Monitoring Settings to monitor applications deployed on Docker containers.

To enable Docker support for RUM applications:

1. Select **Admin > Platform > Setup and Maintenance > Infrastructure Settings**.
2. Select **Foundations**.
3. Select **EUM Administration**.
4. In the EUM Administration - EUM Administration table, locate **Enable Docker support for RUM applications**.
5. Set the value to **true**.

Enabling SMTP Server SSL/TLS Support

If you enable SSL/TLS for your email server, you need to enable SSL/TLS for APM.

To enable SMTP server SSL/TLS support :

1. Select **Admin > Platform > Setup and Maintenance > Infrastructure Settings**.
2. Select **Foundations**.
3. Select **Platform Administration**.
4. In the Platform Administration – SMTP Server Configuration – SSL/TLS Support table, locate **Enable TLS**and set to **true** to enable TLS. By default, this value is false.
5. After setting **Enable TLS** to true, set the following values:
   - **SMTP host** – Enter the SMTP host
   - **Secure SMTP port** – By default, the SMTP port is set to 465. Change this value if necessary.
   - **Enable authentication** – Set to **true** to enable authentication for the SMTP server. By default, this value is false.
   - **Username** – Enter your user name if you enabled authentication
   - **Password** – Create a password if you enabled authentication
   - **Supported protocols** – By default, TLSv1 TLSv1.1 TLSv1.2. You can change the list of supported

protocols.

Note: Separate the protocols with a space.

Chapter 15: JMX Console

This section provides an overview to the JMX console and instructions for changing the JMX password.

To access

Enter the relevant URL: **http://<Gateway or Data Processing Server name>:29000/**

where

<Gateway or Data Processing Server name> is the name of the machine on which APM is running.

Note: By default, for security reasons, the JMX console is accessible only from the localhost. You can disable this limitation so that you can access the JMX console remotely. See "How to Enable Accessing JMX Console Remotely" on the next page.

Learn About

JMX Console Overview

The JMX console comes embedded in APM, and enables you to:

- Perform management operations
- View performance of processes
- Troubleshoot problematic areas of APM

The credentials to access the JMX console were configured when you installed APM. To change your JMX password, see "How to Change the JMX Password" below.

You can configure the JMX console to work with SSL to encrypt JMX data for added security. For details, see "Configuring JBOSS to Work with SSL" in the APM Hardening Guide.

Tasks

How to Change the JMX Password

1. Stop the APM Gateway or Data Processing Server.
2. Run the appropriate file, depending on the operating system in use, on either the Gateway or Data Processing Server:

Operating System	File Name
Windows	<APM root directory>\tools\jmx\changeCredentials.bat
Solaris	<APM root directory>\tools\jmx\changeCredentials.sh

3. The Change Password dialog box opens. Enter and confirm your new password. The operating system registers and encrypts the password change on either the Gateway or Data Processing Server.
4. Restart APM.

Note: The login name cannot be changed.

How to Enable Accessing JMX Console Remotely

You can change the access level to the JMX console with the **Restrict remote access to JMX console** infrastructure setting. The default value is true which allows access to the JMX console only from the localhost.

1. Select **Admin > Platform > Setup and Maintenance > Infrastructure Settings**.
2. Select **Foundations**.
3. Select **Security**.
4. In the Security-Login table, locate **Restrict remote access to JMX console**. Change the value to **false**.

Chapter 16: Baselines

This section provides information about baselines and how to enable, configure, and manually invoke them.

Learn About

Baseline Overview

An application's status is determined by its transactions' actual performance and availability in relation to configured performance and availability thresholds. You can use this information in components such as Service Health, End User Management, Service Level Management, and Service Health Analyzer.

When you configure an application for monitoring by Business Process Monitor, you can determine whether its transactions' performance thresholds are static thresholds (specific threshold values that you configure), or are calculated using baselines based on historical transaction data.

You can configure APM to calculate baselines from actual performance metrics. Creating a baseline enables you to learn the normal performance of your applications. Knowing how an application typically performs enables you to determine whether a performance problem is an isolated incident or a sign of a trend.

Baselines are updated periodically as new metrics data are received.

Note: A minimum amount of accumulated data is necessary before baselines can be calculated. This depends on the number of samples collected and takes approximately one week after baselines are enabled in APM. You can speed up the process by manually invoking a baseline with limited data. For details, see "How to Manually Invoke a Baseline" on page 82 below.

Baseline Coefficient

When baselining is enabled, APM collects metric data from incoming samples over a period of time. After enough data has been collected, APM creates a baseline for the metric and calculates the mean and standard deviation.

Mean and standard deviation values for a metric are used to create a baseline sleeve and to identify metrics that deviate from the baseline. The mean and standard deviation are a statistical way of estimating the normal behavior of a metric. By default, the baseline sleeve is calculated using a coefficient of + or - 3 times the standard deviation from a metric's mean value.

This means that a metric is considered abnormal if its value is greater than the mean value plus 3 times the standard deviation, or less than the mean value minus 3 times the standard deviation.

This can be summarized as follows:
((Mean Value)-(3*STD)) <= NORMAL VALUE <= ((Mean Value)+(3*STD))

You can set a different coefficient for each data collector. For example you could set a coefficient of 2 for CIs received from BPM and a coefficient of 5 for CIs received from Diagnostics.

Seasonality and Trends

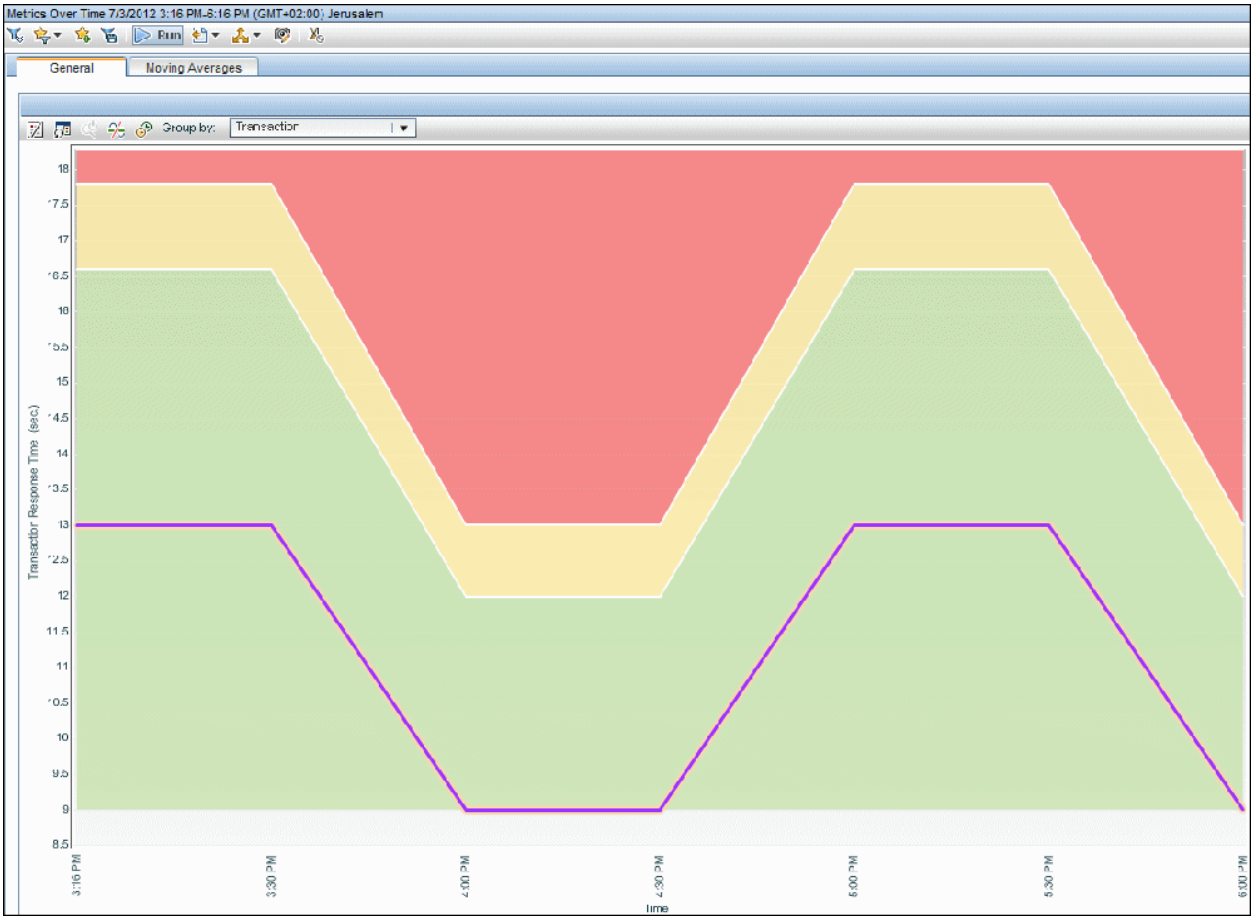
When calculating a metric's baseline, the baseline engine takes into account such things as seasonality and trends.

- **Seasonality** - When a repeated pattern at constant time intervals occurs, a metric has seasonality. For example a metric might have typical values at 8:00 every day when users log on, and different values at 12:00 when users take a break.
- **Trends** - When a metric's values have a consistent linear change over time, a trend is identified.

Seasonality and trends are considered to be part of the normal behavior of a metric, and the baseline sleeve is adjusted accordingly.

Baseline Example

The following example shows the baseline sleeve for the OK, minor, and critical thresholds for a transaction in the Metrics Over Time report:



Manually Invoking a Baseline

When you initially install and configure APM it takes a week for the system to gather CI data required to establish a baseline. You can speed up this process by manually creating a baseline using limited data from a single day after installing APM. This means that 24 hours after installing and configuring APM, the system can already identify anomalies.

If you manually create a baseline with less than a week's data, the baseline will not include any seasonal information such as different patterns over weekends, however, over time APM will automatically refine and improve the baseline as more data becomes available.

Note: You cannot manually create a baseline on the same day that you install APM. This is because the baseline process required an off-line process which runs automatically every night.

Tasks

How to Enable Baselines

1. Select the Baselining option in:
   - The **Setup and Database Configuration Utility** in a regular deployment (for details, see the APM Installation Guide).
   - The **Upgrade Wizard** if you are performing an upgrade (see the Upgrade Guide relevant to your upgrade path).
2. Create an Analytics database (**Admin > Platform > Manage Analytics Databases**) (see "Creating Databases" on page 48).

Note: You can also enable baselining after APM has been installed.

How to Set the Coefficient for a Data Collector

1. Select **Admin > Platform > Infrastructure Settings > Applications > Service Health Analyzer > Baseline Coefficient**.
2. Enter the required coefficient. Multiple values should be separated by a semi-colon, for example **BPM,2.0;SiS,2.5;DIAG,5.0;PA,3.5;RUM,2.0;NNM,4.0**.

   If you do not set a coefficient for a data collector, APM uses the default value of 3. For more information on coefficients, see "Baseline Coefficient" on page 80.

How to Manually Invoke a Baseline

1. In a web browser, open the baseline JMX page using the following link:
   http://<DPS>:29924/mbean?objectname=Topaz:service=Baseline+Services
2. Invoke the **showTasks** operation to identify the task IDs of your domain for example:

Task ID	Client	Metric Domain	Status	Start of period	End of period	Next run
33	1	RUM	idle	Sat Nov 29 00:00:00 IST 2011	Mon Dec 29 00:00:00 IST 2011	Mon Dec 29 00:01:00 IST 2011
34	1	BPM	idle	Sat Nov 29 00:00:00 IST 2011	Mon Dec 29 00:00:00 IST 2011	Mon Dec 29 00:01:00 IST 2011

3. Record the relevant task IDs and dates, and go back to the baseline JMX page (as listed above).
4. Invoke the **calculateNow** operation on each of the relevant task IDs.
5. To confirm that the process ran successfully, invoke the **showTasks** operation again and confirm that the dates have been updated. The process might take some time.

Tips/Troubleshooting

JVM Often Crashes in Baseline Processes while Running Baseline Tasks

This problem is caused by the Java Virtual Machine. You can identify the problem by the following errors in the file **hs_err_pid.log**:

- EXCEPTION_ACCESS_VIOLATION
- guarantee(result == EXCEPTION_CONTINUE_EXECUTION) failed: Unexpected result from topLevelExceptionFilter

The log file is located in the working directory at the time of process execution.

To resolve this problem, change the baseline process from 64 bit to 32 bit as follows:

1. In the JMX console, stop the service **basel_engine** as follows:
   a. In a browser, enter **http://<DPS>:11021/** and enter your user name and password.
   b. Under **Foundations**, click **Foundations:type=NannyManager**.
   c. Under **java.lang.String showServiceInfoAsHTML**, click **Invoke**.
   d. Next to **basel_engine**, click **Stop**.
2. On the Data Processing Server, copy the file **\HPBSM\JRE\bin\hpbsm_basel_engine.exe** to the directory **\HPBSM\JRE64\bin**, overriding the existing file with the copy.
3. Restart the **basel_engine** service.

Chapter 17: Audit Log

You use the audit log to keep track of different actions performed by users in the system, according to specific contexts.

To access

Select **Admin > Platform > Setup and Maintenance > Audit Log**

Learn About

About the Audit Log

You use the audit log to keep track of different actions performed by users in the system, according to the following specific contexts:

- **Alert Administration.** Displays actions related to creating and managing alerts.
- **CI Status Alert Administration.** Displays actions related to creating alert schemes for a configuration item (CI) status alert.
- **Data Collector Maintenance.** Displays actions related to removing Business Process Monitors and SiteScopes.
- **Database Management.** Displays actions related to creating, deleting, and modifying users and passwords for profile databases, as well as modifying the status of the Purging Manager.
- **Deleted Entities.** Displays actions related to adding and deleting data collectors (Real User Monitor engines and SiteScope monitors) from End User Management Administration.
- **Downtime/Event Scheduling.** Displays actions related to creating and modifying downtime and scheduled events.
- **End User Management Applications.** Displays actions related to adding, editing, updating, disabling and deleting event-based alerts, as well as registering and unregistering alert recipients.
- **IT World Configuration.** Displays actions, including editing, updating, and removing CIs and relationships, performed in the IT Universe Manager application.
- **Locations Manager.** Displays actions related to adding, modifying, and deleting locations, performed in the Location Manager application.
- **Notification Template Administration.** Displays actions related to modifying open ticket information, ticket settings, closed tickets, ticket templates, and subscription information: notification types (locations or general messages), and recipients.
- **Operations Management.** Displays actions related to Operations Management, such as the creating and modifying of content packs, event rules, and notifications.
- **Permissions Management.** Displays all actions related to assigning permissions, roles, and permission operations on resources for users and user groups.
- **Recipient Administration.** Displays actions related to modifying information about the recipients of audit logs.
- **Scheduled Report Administration.** Displays actions related to modifying the reporting method and schedule of reported events.
- **Service Health.** Displays actions related to the Service Health application.

- **Service Health Administration.** Displays actions related to configurations made in Service Health Administration.
- **Service Level Management Configuration.** Displays actions related to service level agreements performed in the Service Level Management application.
- **SLA Alert Administration.** Displays actions related to creating, modifying, or deleting SLA alerts.
- **System Availability Manager.** Displays actions related to system availability and SiteScope.
- **User Defined Reports.** Displays actions related to the creation and modification of Custom reports.
- **User/Group Management.** Displays actions related to adding, modifying, and deleting users and user groups.
- **View Manager.** Displays actions related to KPIs such as adding a KPI, editing a KPI, and deleting a KPI. Additionally, it displays actions related to changing the **Save KPI data over time for this CI** and the **Monitor changes** options.

Tasks

How to Use the Audit Log

1. Select **Admin > Platform > Setup and Maintenance > Audit Log**.
2. Select a context.
3. Where relevant, select a profile from the list. APM updates the table with the relevant information.
4. Optionally, click the Auditing Filters link to open the Auditing Filters pane and specify filter criteria. The following filters are available:
   - **User.** Specify a user in the system to view actions performed by only that user.
   - **Containing text.** Specify a text string that the action must contain to be displayed.
   - **Start after and End before.** Specify a starting and ending time period to view actions for only that period. Click the **More** button to open the Calendar dialog box where you can select a date.
5. Click **Apply**. APM updates the table with the relevant information.

If required, use the **Previous Page** or **Next Page** arrows to navigate to the previous or next page of the Audit Log.

How to Customize a Log File for Audit Log

The Audit Log uses the Apache log4j logging utility.

To customize the log file, edit its configuration file, located at:
<APM root directory>\conf\core\Tools\log4j\EJB\auditlog.properties
using the log4j configuration syntax. The log level should be set to **INFO** or higher.

Note: Do not change the appender name:
com.mercury.topaz.tmc.bizobjects.audit.AuditManager.writeAudit

UI Descriptions

Note: For details about the audit log for EUM Alert Administration, see Alerts Log Report in the APM User Guide.

Audit Log Page

This page enables you to keep track of different actions performed by users in the system.

User interface elements are described below (unlabeled elements are shown in angle brackets):

UI Element (A-Z)	Description
	Moves to the previous page or next page in the Audit Log.
<Audit log table>	Displays the contents of the audit log.
<EUM applications>	Select an <EUM application> for which you want to view the actions performed. **Note:** This field is displayed only if you have chosen the End User Management-Applications context.
Auditing Filters	Click the Auditing Filters heading to specify filter criteria.
Context	Select a context to view.
For user	Displays the user whose actions are displayed in the Audit Log, as specified in the Auditing Filters pane. **Default Value:** All
SiteScope	Select a SiteScope for which you want to view the actions performed. **Note:** This field is displayed only if you have chosen the System Availability Manager context.
Time period	Displays the time period whose actions are displayed in the Audit Log, as specified in the Auditing Filters pane. **Default Value:** All

Auditing Filters Pane

User interface elements are described below:

UI Element (A-Z)	Description
	Opens the Calendar dialog box enabling you to select a date.
	Expands the Auditing Filters pane.

UI Element (A-Z)	Description
	Collapses the Auditing Filters pane.
Apply	Applies the selected filters.
Cancel	Cancels filtering and closes the Auditing Filters pane.
Clear All	Clears the filters and displays all log items.
Containing text	Specify a text string to filter out all the actions that do not include this text string.
End before	Specify an ending time until which you want to view actions.
Start after	Specify a starting time from which you want to view actions.
User	Select a user to view actions performed by only that user.

Audit Log Table

User interface elements are described below:

UI Element (A-Z)	Description
Actions	Displays the actions performed by the specified user.
Additional Information	Displays additional information, where relevant.
Modification Date	Displays the date and time that the specified actions were performed.
Modified By	Displays the user who performed the specified actions.

Chapter 18: HPE System Health

System Health is a standalone application that uses the SiteScope monitoring system to enable you to monitor the servers, databases, and data collectors running as part of your APM system.

You can use System Health to:

- Measure performance by viewing the output from monitors running on the various system components.
- Monitor areas of the databases that influence performance.
- Display problematic areas of the servers, databases, and data collectors.
- Perform operations on your environment, such as:
  - **Move Backend Services**. You can move backend services from one server to another of the same type, in case the server machine is not functioning properly or requires downtime for servicing.
  - **Configure Backup Servers**. You can define a backup server in case the server machine is not functioning properly or requires downtime for servicing.
  - **Manage APM Processes**. You can start or stop various APM processes.
- View log files on specific components in a variety of formats.
- View information on components and monitors in .csv format (displaying current status) and Quick Report format (displaying status of the past 24 hours).

You can access System Health through APM or in a web browser.

For further information, see the System Health Guide.

Chapter 19: APM Server Time Synchronization

This section provides information about APM server clocks.

Learn About

Checking Server Time Against NTP Server

In order to ensure that the APM server clocks are accurate and synchronized, the APM servers check their system clocks against an NTP server every 20 minutes by default.

If no NTP server is reachable, the database clock is used for synchronization instead.

Viewing the Log for APM Server Time Synchronization

You can view the log for APM server time synchronization by accessing **<APM_HOME>\logs\topaz_all.ejb.log**.

Tasks

How to Add NTP Servers

Several NTP servers are configured by default, but you can manually add one in the configuration file:

<APM_HOME>\conf\settings\mtime\mtime.xml

How to View the APM Server Time

You can view the current APM server time via the following URLs:

- To view Unix time in plain text:

  http://<APM_Server>/topaz/services/technical/time?alt=text/plain

  Example results:

  ```
  1314089070858
  ```

- To view the current time in XML format:

  http://<APM_Server>/topaz/services/technical/time

  Example results:

  ```
  <entry xmlns="http://www.w3.org/2005/Atom">
  <id>timeService:1</id>
  <title type="text" xml:lang="en">Time service.</title>
  <summary type="text" xml:lang="en">The time is 2011-08-23 08:44:30,858</summary>
  <published>2011-08-23T11:44:31.382+03:00</published>
  <content type="text">1314089070858</content>
  </entry>
  ```

Chapter 20: APM Logs

This section provides information about APM Logs.

Learn About

This section includes:

APM Logs - Overview

APM records the procedures and actions performed by the various components in log files. The log files are usually designed to aid HPE Software Support when APM does not perform as expected.

You can view log files with any text editor.

Log File Locations

Most log files are located in the **<APM root directory>\log** directory and in subdirectories organized by component.

Log file properties are defined in files in the following directory and its subdirectories: **<APM root directory>\conf\core\Tools\log4j**.

Log File Locations in a Distributed Deployment

In one-machine or compact installations, all APM servers and their logs reside on the same machine. In the case of a distributed deployment of the servers among several machines, logs for a particular server are usually saved on the computer on which the server is installed. However, if it is necessary for you to inspect logs, you should do so on all machines.

When comparing logs on client machines with those on the APM server machines, keep in mind that the date and time recorded in a log are recorded from the machine on which the log was produced. It follows that if there is a time difference between the server and client machines, the same event is recorded by each machine with a different time stamp.

Log Severity Levels

Each log is configured so that the information it records corresponds to a certain severity threshold. Because the various logs are used to keep track of different information, each is preset to an appropriate default level. For details on changing the log level, see "How to Change Log Levels" on page 92.

Typical log levels are listed below from narrowest to widest scope:

- **Error.** The log records only events that adversely affect the immediate functioning of APM. When a malfunction occurs, you can check if Error messages were logged and inspect their content to trace the source of the failure.
- **Warning.** The log's scope includes, in addition to Error-level events, problems for which APM is currently able to compensate and incidents that should be noted to prevent possible future malfunctions.
- **Info.** The log records all activity. Most of the information is routine and the log file quickly fills up.
- **Debug.** This level is used by HPE Software Support when troubleshooting problems.

The default severity threshold level for log files differs per log, but is generally set to either **Warning** or **Error**.

Note: The names of the different log levels may vary slightly on different servers and for different procedures. For example, **Info** may be referred to as **Always logged** or **Flow**.

Log File Size and Automatic Archiving

A size limit is set for each type of log file. When a file reaches this limit, it is renamed and becomes an archived log. A new active log file is then created.

For many logs, you can configure the number of archived log files that are saved. When a file reaches its size limit, it is renamed with the numbered extension **1** (**log.1**). If there is currently an archived log with the extension **1** (**log.1**), it is renamed to **log.2**, **log.2** becomes **log.3**, and so on, until the oldest archived log file (with the number corresponding to the maximum number of files to be saved) is permanently deleted.

The maximum file size and the number of archived log files are defined in the log properties files located in **<APM root directory>\conf\core\Tools\log4j**. An example is:

```
def.file.max.size=2000KB
def.files.backup.count=10
```

JBoss and Tomcat Logs

The following **<APM root directory>\log** directory holds JBoss- and Tomcat-related log files:

- **jboss_boot.log.** Logs startup activities including running the JBoss process, deployment, and startup status, as well as the number of busy ports.
- **jboss_server.log.** Logs all JBoss activities including JBoss messages, deployment, and startup status.
- **jboss_tomcat.log.** Logs the Tomcat messages.

  Note: You can view the JMX Console at `http://<APM server>:29000/`

**.hprof Files*

*.hprof files contain a dump heap of an APM process's data structures. These files are generated by the JVM if a process fails with a Java Out Of Heap Memory condition.

You are rarely aware of a problem because the problematic process restarts automatically after a failure. The existence of many *.hprof files indicates that there may be a problem in one of the APM components, and its contents should be analyzed to determine the problem.

If you run out of disk space, you can delete the*.hprof files.

Logging Administrator Tool

The Logging Administrator tool enables you to temporarily modify the level of details displayed in APM logs, as well as create custom logs. You can access the APM Logging Administrator Tool from the following URL:

http://<APM Gateway Server>/topaz/logAdminBsm.jsp

Tasks

How to Delete APM Logs

You can delete all APM log files under **/opt/HB/BSM/log** and *.hprof files under **/opt/HP/BSM/bin** after stopping APM. This enables you to free up disk space. However, from a support perspective, it may be useful to save older logs.

Caution: Do not delete the log directory.

1. Stop APM.
2. Delete all files under **<APM>\log**. Do not delete the log directory.
3. Delete all .hprof files under **/opt/HP/BSM/bin/**.

Note: Some files cannot be deleted, because they are owned by IIS or Apache.

How to Change Log Levels

If requested by HPE Software Support, you may have to change the severity threshold level in a log, for example, to a debug level.

1. Open the log properties file in a text editor. Log file properties are defined in files in the following directory: **<APM root directory>\conf\core\Tools\log4j**.
2. Locate the **loglevel** parameter. For example,

   ```
   loglevel=ERROR
   ```

3. Change the level to the required level. For example,

   ```
   loglevel=DEBUG
   ```

4. Save the file.

Chapter 21: Port Usage

This sections provides a list of the ports that are used by APM. This list can be used as a tool for troubleshooting, monitoring and ensuring APM servers are configured correctly. In addition, instructions are provided for configuring these ports.

Learn About

This section includes:

Port Usage Overview

The APM suite uses a number of ports. A port is an application-specific or process-specific software construct serving as a communications endpoint in a computer's host operating system. Each port is associated with the IP address of the server, as well as the type of protocol used for communication.

Some of the ports listed below are optional (depending on which infrastructure is being used), others are mandatory. Some of the listed ports are only used for troubleshooting access to the application via the Java Management Extensions (JMX) consoles. It is important, however to have access to these ports so that data from APM can be quickly accessed and issues can be identified.

Each of the mandatory ports must remain open for proper APM operation. Optional ports may become mandatory if particular configurations of APM are used. For example, APM can use either SQL Server or Oracle as its database. Depending on which database is used, ports 1433/1434 (SQL Server) or port 1521 is mandatory.

System Health can be used to monitor the status of the APM applications, processes and services that utilize these ports. A mapping from each port to the infrastructure defined and monitored by System Health appears in each of the following tables. For some ports, there is no one-to-one mapping to infrastructure in System Health. In these situations the mapping will be listed as N/A.

Note: An extensive range of ports are used between the APM Data Processing Server (DPS) and Gateway (GW) server for the use of Java's Remote Method Invocation (RMI) protocol. HPE Software does not advise or support the use of operating system firewalls on either of these servers. HPE Software does not advise or support having firewall servers installed between these APM servers.

Note: In the following tables, OUTBOUND and INBOUND is windows terminology and OUTPUT/INPUT is Linux firewall/iptables packet filtering terminology.

Data Processing Server (DPS)

Port Number	Type of Traffic	Port Usage	Mandatory/Optional
25	OUTBOUND/OUTPUT	SMTP channel from the HPE Business Management Server to the SMTP mail server	Optional. Mandatory if SMTP is used for Alerts
161	OUTBOUND/OUTPUT	SNMP channel from the Data Processing Server to the SNMP manager	Mandatory
1099	INBOUND/INPUT	Naming service used by the JBOSS application server	Optional.
1433	OUTBOUND/OUTPUT	Connection between the HPE APM Servers and Microsoft SQL Server	Optional. Mandatory if SQL Server database used
1434	OUTBOUND/OUTPUT	Connection between the HPE APM Servers and Microsoft SQL Server Browser Server. This port is only used when a named instance is used.	Optional. Mandatory if SQL Server database used
1521	OUTBOUND/OUTPUT	Connection between the HPE APM Servers and Oracle Database Server	Optional. Mandatory if Oracle database used
4447	INBOUND/INPUT	Remote Method Invocation (RMI) channel between HPE Application Performance Management servers	Mandatory
5445	INBOUND/INPUT	HornetQ Bus port for the connection between the Data Processing Server and the Gateway Server	Mandatory
5455	INBOUND/INPUT	HornetQ Bus processes for the connection between HPE Application Performance Management servers	Mandatory.
8009	Localhost	Tomcat AJP13 connector	Mandatory for localhost access
8443	INBOUND/INPUT	Secure Connection to RTSM URL	Mandatory
11020	INBOUND/INPUT	RMI management channel for the HPE Application Performance Management Service (Nanny Manager)	Mandatory
11021	OUTBOUND/OUTPUT	HTTP channel for the HPE Application Performance Service (Nanny Manager)	Mandatory, JMX

Port Number	Type of Traffic	Port Usage	Mandatory/Optional
21212	OUTBOUND/OUTPUT	HTTP channel for the ODB process	Mandatory, JMX
21301	INBOUND/INPUT	RMI communication from backend to EPI server Admin services	Mandatory
29000	Localhost	HTTP channel for the JMX console and RMI communication	Mandatory for localhost access, JMX, JBOSS, Tomcat, Jetty
29602	INBOUND/INPUT	RMI management channel for the HornetQ Bus processes	Mandatory
29608	INBOUND/INPUT	RMI management channel for the Offline BLE process	Mandatory
29610	INBOUND/INPUT	RMI management channel for the Partition and Purging Manager	Mandatory
29612	INBOUND/INPUT	RMI management channel for the ODB process	Mandatory
29622	INBOUND/INPUT	RMI management channel for the OPR backend process	Mandatory
29628	INBOUND/INPUT	RMI for script execution for OPR backend process	Mandatory
29630	INBOUND/INPUT	RMI port for online BLE processes	Mandatory
29700	INBOUND/INPUT	RMI port for Marble Supervisor process	Mandatory
29711	INBOUND/INPUT	RMI port for Marble Worker 1 (online BLE)	Mandatory
29712	INBOUND/INPUT	RMI port for Marble Worker 2 (online BLE)	Mandatory
29713	INBOUND/INPUT	RMI port for Marble Worker 3 (online BLE)	Mandatory
29714	INBOUND/INPUT	RMI port for Marble (online BLE)	Mandatory
29720	INBOUND/INPUT	RMI port for Marble Matcher (online BLE)	Mandatory
29800	OUTBOUND/OUTPUT	HTTP port for Marble Supervisor process	Mandatory, JMX
29811	OUTBOUND/OUTPUT	HTTP port for Marble Worker 1 (online BLE)	Mandatory, JMX
29812	OUTBOUND/OUTPUT	HTTP port for Marble Worker 2 (online BLE)	Mandatory, JMX
29813	OUTBOUND/OUTPUT	HTTP port for Marble Worker 3 (online BLE)	Mandatory, JMX
29820	OUTBOUND/OUTPUT	HTTP port for Marble Matcher (online BLE)	Mandatory, JMX

Port Number	Type of Traffic	Port Usage	Mandatory/Optional
29908	OUTBOUND/OUTPUT	HTTP port for offline BLE processes	Mandatory, JMX
29910	OUTBOUND/OUTPUT	HTTP channel for the Partition and Purging Manager	Mandatory, JMX
29922	OUTBOUND/OUTPUT	HTTP channel for the OPR backend process	Mandatory, JMX
29930	OUTBOUND/OUTPUT	HTTP port for Business Impact process	Mandatory, JMX
30020	OUTBOUND/OUTPUT	HTTP port for marble loader processes	Mandatory, JMX
31000-32999	INBOUND/INPUT	HPE Application Performance Management service (Nanny Manager) uses the first available port in each range	Mandatory
49152-65535	INBOUND/INPUT	Dynamic ports are used for inter-component channels using Java RMI	Mandatory

Gateway Server (GW)

Port Number	Type of Traffic	Port Usage	Mandatory/Optional
25	OUTBOUND/OUTPUT	SMTP channel from the HPE Business Management Server to the SMTP mail server	Optional. Mandatory if SMTP is used for Alerts
80	OUTBOUND/OUTPUT	HTTP channel to Gateway Server Applications / Apache or IIS Web Server	Mandatory. Optional if you are accessing console through HTTPS (port 443)
123	OUTBOUND/OUTPUT	NTP channel from the Gateway Server to the NTP server	Optional. Not needed if Network Time Protocol not used, but we recommend using this to keep times between servers in sync.
389	OUTBOUND/OUTPUT	Connection between the Gateway Server and LDAP server for authentication	Optional. Mandatory if LDAP is used
443	OUTBOUND/OUTPUT	HTTPS channel to Gateway Server Applications. This is also used for reverse proxy / Apache or IIS Web Server	Optional. Mandatory if HTTPS access is used.

Port Number	Type of Traffic	Port Usage	Mandatory/Optional
1099	INBOUND/INPUT	Naming service used by the JBOSS application server	Mandatory
1433	OUTBOUND/OUTPUT	Connection between the HPE APM Servers and Microsoft SQL Server	Optional. Mandatory if SQL Server database used
1434	OUTBOUND/OUTPUT	Connection between the HPE APM Servers and Microsoft SQL Server Browser Server. This port is only used when a named instance is used.	Optional. Mandatory if SQL Server database used
1521	OUTBOUND/OUTPUT	Connection between the HPE APM Servers and Oracle Database Server	Optional, Mandatory if Oracle database used
5445	INBOUND/INPUT	HornetQ Bus port for the connection between the Data Processing Server and the Gateway Server	Mandatory
5455	INBOUND/INPUT	HornetQ Bus processes for the connection between HPE Application Performance Management servers	Mandatory
8009	Localhost	Tomcat AJP13 connector	Mandatory for localhost access
8443	INBOUND/INPUT	Secure Connection to RTSM URL	Mandatory
11020	INBOUND/INPUT	RMI management channel for the HPE Application Performance Management Service (Nanny Manager)	Mandatory
11021	OUTBOUND/OUTPUT	HTTP channel for the HPE Application Performance Management Service (Nanny Manager)	Mandatory, JMX
21302	INBOUND/INPUT	RMI communication from console web-app to admin web-app	Mandatory
21303	INBOUND/INPUT	RMI communication from console web-app to custom action script server running on the same host	Mandatory
29000	Localhost	HTTP channel for the JMX console and RMI communications	Mandatory for localhost access, JMX, JBOSS, Tomcat, Jetty

Port Number	Type of Traffic	Port Usage	Mandatory/Optional
29602	INBOUND/INPUT	RMI management channel for the HornetQ Bus processes	Mandatory
29603	INBOUND/INPUT	RMI management channel for the DB Loader process	Mandatory
29604	INBOUND/INPUT	RMI management channel for the Web Data Entry (WDE) process	Mandatory
29612	INBOUND/INPUT	RMI management channel for the ODB process	Mandatory
29616	INBOUND/INPUT	RMI management channel for the Scheduler process	Mandatory
29903	OUTBOUND/OUTPUT	HTTP channel for the DB Loader process	Mandatory, JMX
29904	OUTBOUND/OUTPUT	HTTP channel for the Web Data Entry (WDE) process	Mandatory, JMX
29916	OUTBOUND/OUTPUT	HTTP channel for the Scheduler process	Mandatory, JMX
29929	OUTBOUND/OUTPUT	HTTP port for the OPR process	Mandatory, JMX
31000-32999	INBOUND/INPUT	HPE Application Performance Management service (Nanny Manager), uses the first available port in range	Mandatory
49152-65535	INBOUND/INPUT	Dynamic ports are used for inter-component channels using Java RMI	Mandatory

Tasks

Note: The ports listed above are the ports APM uses. If you need to change a port assignment, it is strongly recommended that you first consult with HPE Software Support.

This section includes:

How to Manually Change Port 80

Port 80 is used by the APM Web Server. To modify this port, you must reconfigure other components on the APM server and restart APM.

1. Modify the virtual Gateway Server settings.
   a. Navigate to **Administration Tab > Platform > Setup and Maintenance Tab > Infrastructure Settings** and locate the **Platform Administration - Host Configuration table**. If this table is not visible, set the **Select Context** option to **All**.
   b. Modify the **Default Virtual Gateway Server for Application Users URL** to **http://<server name>:<new port>**.
   c. Modify the **Default Virtual Gateway Server for Data Collectors URL** to **http://<server name>:<new port>**.
2. Modify the direct Gateway Server settings
   a. In the same table, modify the **Direct Gateway Server for Application Users Server URL** to include the new port.
   b. Modify the **Direct Gateway Server for Data Collectors URL** to include the new port.
3. Modify the local virtual Gateway Server settings
   a. In the same table, modify the **Local Virtual Gateway Server for Application Users URL** to include the new port.
   b. Modify the **Local Virtual Gateway Server for Data Collectors URL** to include the new port.
4. Modify the Open APM URL
   a. Remotely connect to the APM Gateway server and select **Start > All Programs > HPE Application Performance Management**.
   b. Right-click **Open HPE Application Performance Management** and select **Properties**.
   c. In the **Web Document** tab, modify the **URL** field as follows: **http://<Gateway Server>:<new port>/topaz**.
5. Modify the web server settings

   Modify the web server settings. This procedure varies depending on your version of Windows and web server type. They should all be performed in the APM Gateway server. The following are examples for Windows Server 2008 using three different web servers:

   For IIS 7.x / 8.x with Windows Server 2008 / 2008 R2 / 2012 / 2012 R2:
   a. Open Microsoft's **Computer Management** tool by right-clicking **My Computer** and selecting **Manage**.
   b. Expand **Roles > Web Server** and select **Internet Information Services**.
   c. In the right-hand panel you can see the IIS Manager. In the left part of this panel (**Connections**), expand the connection of the current machine and expand the **Sites** node.
   d. Right-click **Default Web Site** and select **Edit Bindings**.
   e. Select the line that listens to port 80 and click **edit** to change the value to the new port.

   For Apache with Windows Server 2008:
   a. Open the file **<APM_Gateway_home>\WebServer\conf\httpd.conf** in a text editor.
   b. Go to the line that begins with **Listen**, and modify the port value as required.
   c. Go to the line that begins with **ServerName** and modify the port value as required.
6. Restart all APM servers and update data collectors.

Restart all APM servers and update any data collectors that were configured before you modified the port (for example, RUM, BPM, SiteScope). Modify the Gateway Server address in each data collector to reflect the new port as follows: **APM Gateway>:<new port>**.

How to Manually Change Ports 1433 and 1521

These ports control the communication between HPE APM and Database Servers.

1. Modify the Management Database port

   Run the Setup and Database Configuration Utility. Modify the port in the screen that specified the Management Database port. For details about the Setup and Database Configuration Utility, see the APM Installation Guide.

   Note: You can also perform this procedure manually as follows: On all APM servers (Gateway and DPS), open **<APM_home>\conf\TopazInfra.ini** in a text editor and modify the **dbPort** property as required.

2. Modify Profile Database port.

   Navigate to **Admin > Platform > Setup and Maintenance > Manage Profile Databases** and click the **Edit Database Properties** button  to modify the desired database configuration to include the new port.

3. Restart all APM servers.

How to Manually Change Port 8009

This port number is the port through which the Tomcat AJP13 connector enables communication between components on the APM server. Perform the following on each APM server whose Tomcat AJP13 connector port you want to redirect, and restart APM.

1. Change the Web Server Tomcat AJP13 connector port definition.
   a. In a text editor, open the file **/opt/HP/BSM/jboss-as/standalone/configuration/standalone.xml**.
   b. Locate the port 8009 section.
   c. Change the port number.
2. Change the Tomcat AJP13 listening port definition.
   a. In a text editor, open the files located in the folder **<BACroot>\WebServer\conf**.
   b. Change port 8009 wherever it appears in the files. Verify that port 8009 appears at least once.
3. Restart all APM servers.

How to Manually Change Port 29000

This port number is the port through which the Tomcat connector enables APM server HTTP communication. Perform the following on each APM server whose Tomcat connector port you want to redirect, and restart APM.

Note: After this port is changed, the HAC status will not be displayed in the APM Status page. This does not affect the normal execution of APM.

1. Change the Tomcat HTTP connector listening port definition.
   a. In a text editor, open the file **/opt/HP/BSM/jboss-as/bin/standalone.conf**.
   b. Locate the string **-Djmx.http.port=29000**.
   c. Change the port number.
2. Change the value of the topaz.adminserver.url parameter from 29000 to the new port number.
   a. In a text editor, open the file **<APM_home>\conf\topaz.config**.
   b. In a web browser, access **http://localhost:<new port number>/topaz**
   c. Under the **Internal Port** line, insert the following new row:
   internalport=<new port>

```
########################################################################
topaz.administrator.url+http://localhost:9090/topaz
########################################################################
#
#       Internal Port           At topaz.config file
#
########################################################################
internalport=9090
```

3. Restart all APM servers.
4. For changes on the Processing server,
   a. In a text editor, open the file **<APM_home>\conf\topaz.config**.
   b. In a web browser, access **http://localhost:<new port number>/topaz**.
   c. Under the **Internal Port** line, insert the following new row:
   internalport=<new port>
5. Restart all APM servers.

How to Manually Change Port 4447

This port number is the JBoss RMI/JRMP invoker.

1. Change the JBoss configuration.
   a. In a text editor, open the file **/opt/HP/BSM/conf/settings/jboss_config.xml**.
   b. Change the port number in the section **[jboss.config.socket_name.remoting]**.
   <value from="4000" to="99999" type="number">
   4447
   </value>
   c. In a text editor, open the file **/opt/HP/BSM/jboss-as/standalone/configuration/standalone.xml**.
   d. Locate **<socket-binding name="remoting" port="4447"/>**.
   e. Change the port number.

   Note: The port must be in the range of 4000 to 99999.

2. Restart the APM servers.

Chapter 22: File Backup Recommendations

APM directories that contain key configuration and data files should be backed up on a daily basis as a precautionary measure.

The table below lists the APM directories that contain such files and should therefore be backed up. All directories are under **<APM root directory>**.

Resource	Comments
\<APM root directory>\BLE	Configuration of business rules. Back up if business rules have been created.
\<APM root directory>\conf	Assorted APM configuration files.
\<APM root directory>\dat	Assorted APM configuration files.
\<APM root directory>\dbverify\conf	Configuration files for dbverify. This directory does not have to be backed up if dbverify has not been run.
\<APM root directory>\EJBContainer\bin	Configuration files for the scripts used to run APM, and environment settings.
\<APM root directory>\bin	APM binary files. Back up if changes were made to any of the installation defaults.
\<APM root directory>\lib	APM library files. Back up if changes were made to any of the installation defaults.
\<APM root directory>\AppServer\GDE	Configuration files for the Generic Reporting Engine, used for obtaining data for reports.
\<APM root directory>\odb\conf	RTSM main configuration directory
\<APM root directory>\odb\lib	RTSM library files. Back up if changes were made to any of the installation defaults.
\<APM root directory>\odb\classes	RTSM patch files. Back up if any patches were added.
\<APM root directory>\odb\runtime\fcmdb	RTSM adapter files.
\<APM root directory>_postinstall	Post-installation configuration files.
\<APM root directory>\AppServer\webapps\site.war\WEB-INF\sam\hi-mapping-monitors.xml	Custom EMS monitor types. Back up if any customer EMS SiteScope monitors were configured. This file is present only if APM was upgraded from versions 9.0 - 9.20.

Chapter 23: Working in Non-English Locales

This section describes how to configure APM to work with languages other than English and discusses some of the issues that arise when using a non-Latin character set.

Learn About

Multilingual User (MLU) Interface Support

The APM user interface can be viewed in the following languages in your web browser:

Language	Language Preference in Web Browser
French	French (France) [fr]
Spanish	Spanish [es-ES]
German	German [de-DE]
Russian	Russian [ru-RU]
Japanese	Japanese [ja]
Korean	Korean [ko]
Simplified Chinese	Chinese (China) [zh-cn]

The following are languages in which APM can operate but the user interface of only Run-time Service Model (RTSM)-related pages are presented in the language:

Language	Language Preference in Web Browser
Dutch	Dutch (Netherlands) [nl]
Portuguese	Portuguese (Brazil) [pt-br]
Italian	Italian (Italy) [it]

Use the language preference option in your browser to select how to view APM. The language preference chosen affects only your local machine (the client machine) and not the APM machine or any other user accessing the same APM machine.

Tasks

How to Display Non-Latin Languages in Service Health Top View

1. Verify that you correctly followed the instructions for installing the JRE on a non-Western Windows system. See the Oracle web site for details.
2. Make sure that you:

- Have administrative permissions to install the J2SE Runtime Environment on Microsoft Windows .
- (For users installing the JRE on non-Western 32-bit machines) - Select a **Custom** Setup Type. In Custom Setup under feature 2 (**Support for Additional Languages**), select **This feature is installed on local hard drive**.

3. Close all instances of the web browser.
4. Log into APM and access Service Health Top View. Verify that the Chinese or Japanese characters now appear correctly.

How to Set Up and View APM in a Specific Language

1. Install the appropriate language's fonts on your local machine if they are not yet installed. If you select a language in your web browser whose fonts have not been installed, APM displays the characters as squares.
2. If you are logged into APM, you must log out. Click **Logout** at the top of the APM window.

   Close every open browser window or, alternatively, clear the cache (if APM is running on Internet Explorer).
3. If APM is running on Internet Explorer, configure the web browser on your local machine to select the language in which you want to view APM (**Tools > Internet Options**).
   a. Click the **Languages** button and in the Language Preference dialog box, highlight the language in which you want to view APM.
   b. If the language you want is not listed in the dialog box, click **Add** to display the list of languages. Select the language you want to add and click **OK**.
   c. Click **Move Up** to move the selected language to the first row.
   d. Click **OK** to save the settings.
   e. Open the APM login window.
   f. From the Internet Explorer menu, select **View > Refresh**. APM immediately refreshes and the user interface is displayed in the selected language.
4. If APM is being viewed on Firefox, configure the web browser on your local machine as follows:
   a. Select **Tools > Options > Advanced**. Click **Edit Languages**. The Language dialog box opens.
   b. Highlight the language in which you want to view APM.

      If the language you want is not listed in the dialog box, expand the **Select language to add...** list, select the language, and click **Add**.
   c. Click **Move Up** to move the selected language to the first row.
   d. Click **OK** to save the settings. Click **OK** to close the Language dialog box.

Troubleshooting and Limitations

This section includes:

Installation and Deployment Issues

- If you use a CJK language in your browser, you must ensure that the Gateway Server machine running APM has East Asian languages installed. On the machine on which the APM Gateway Server is installed, select **Control Panel > Regional & Language Options > Languages > Install files for East Asian languages**.

  Note: This configuration will not work for an SQL Server installed in English.

- If you installed APM on a non-English Windows operating system, the command line tool output may not be displayed correctly because the Windows and OEM code pages differ. This may not be the case on many Asian language systems, but is often experienced on non-English European systems.

  To fix this, configure the Windows Command Prompt so that a TrueType font is used and the OEM code page is the same as the Windows code page.

  In a Windows Command Prompt window (run cmd.exe):

  a. Right-click the title bar, select **Properties**, and open the **Font** tab.

  b. Change the font from **Raster Fonts** to a TrueType font, and change the font size if necessary (for example: select Lucida Console, 12 pt).

  c. If prompted, modify the shortcut to make the font change global.

  Note: If you use other command line tools, such as `PowerShell` or `Cygwin Bash`, change the font for each of these tools separately.

  To change the codeset for the system, open the registry editor (regedit), and go to: `Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Nls\CodePage`. If the values of ACP and OEMCP differ, edit OEMCP to the same value as for ACP, and reboot the system.

  Note: If changing the OEM code page for the system is not acceptable, for each newly opened Comand Prompt window, change the code page value using the command: **chcp <APC value>**.

- Business Process Monitors and the Gateway Server must be installed on an operating system that has the same locale as the data.
- During Business Process Monitor installation, non-Latin characters cannot be used for the host name and location. If necessary, after installation you can change the names to include non-Latin characters, in **Admin > End User Management > Settings**.
- The installation path for all APM components must not contain non-Latin characters.
- When content packs are available in more than one language, the language of content packs automatically loaded during APM installation depends on the current locale of the host operating system. If there are matching content packs for the current locale, these are installed. If the locale does not have localized

content packs, English content packs are used. Later, a user can upload the content pack in another language manually.

At every Gateway Server startup, the contents of the following directory is checked: **<APM root directory>/conf/opr/content/<locale of server>**

Any package that has not already been loaded, and that does not have unresolved package dependencies (references to packages, which are neither already loaded nor in the same folder), is loaded during this startup.

The following directory is checked next: **<APM root directory>/conf/opr/content/en_US**

Any content packs that were not uploaded from the first location are uploaded. This can result in mixed-language content.

The packages are loaded with the standard import mode; already existing artifacts are not changed. Only new artifacts are added.

Note: Progress can be followed in the admin backend log file. The operation is done in the background and may still be in progress when a user logs in. The system prevents multiple content packages from being loaded at the same time.

Database Environment Issues

- To work in a non-Latin-character language APM environment, you can use either an Oracle Server database or a Microsoft SQL Server database. When using a Microsoft SQL Server database, it should use the same encoding as you use in your APM servers. When using an Oracle Server database, the encoding of the database can also be UTF-8 or AL32UTF-8, which supports both non-Latin-character languages as well as multiple languages. For a list of supported and tested database servers, refer to the APM System Requirements and Support Matrixes.
- When you create a new Oracle instance in an Oracle database, you must specify the character set for the instance. All character data, including data in the data dictionary, is stored in the instance's character set. For details on working with Oracle databases, refer to Deploying and Maintaining the Oracle Server Database in the APM Database Guide. For supported and certified Oracle character sets, refer to Oracle Summary Checklist in the APM Database Guide.
- The SiteScope Database Query Monitor can connect to an Oracle database but the Oracle user names and passwords must contain only Latin characters.

Administration Issues

- Email alerts sent with ISO-2022-JP encoding are supported only by an SMTP server running on a Windows platform. Use of this encoding affects all APM servers.
- When using the default authentication strategy, Lightweight SSO, to authenticate users logging into APM, user names and passwords can be in non-Latin characters.
- To support non-Latin characters in APM databases, the encoding for databases must be defined as UTF-8 or AL32UTF-8 (Oracle only), or set to the specific language.

  Note: This cannot be done for SQL Server.

- To support non-Latin characters in log files, set the log4j encoding property on the log4j configuration files.

  To write a specific log in UTF-8 encoding, do the following:

  a. Search the specific log name in log4j configuration at **conf/core/Tools/log4j**.

  b. In the properties file where this log file is configured, add the following property:

log4j.appender.<appender name>.Encoding=UTF-8

For example, the jboss_server.log configuration follows:

```
#######################################
### define appender: jboss.appender ###
#######################################
# jboss.appender is set to be a FileAppender which outputs to log/jboss_
server.log
log4j.appender.jboss.appender=org.apache.log4j.RollingFileAppender
log4j.appender.jboss.appender.File=${merc.home}/${log.file.path}/jboss_
server.log
log4j.appender.jboss.appender.MaxFileSize=${def.file.max.size}
log4j.appender.jboss.appender.Encoding=UTF-8
log4j.appender.jboss.appender.MaxBackupIndex=${def.files.backup.count}
log4j.appender.jboss.appender.layout=org.apache.log4j.PatternLayout
log4j.appender.jboss.appender.layout.ConversionPattern=${msg.layout}
```

Service Level Management Issues

Service Level Management does not support service names that contain more than 50 multibyte characters.

Application Management for Siebel Issues

- Non-Latin characters may not appear or may be corrupted in the Topology View. If you encounter this problem, install the Arial Unicode Microsoft font from the Microsoft web site.
- By default, APM only supports English language Siebel. Do not deliver data from a non-English version of Siebel to APM. You should use special translation adapters to enable APM to work with a non-English version of the Siebel application. For details, contact HPE Software Support.

Report Issues

- APM does not support Custom Report names that contain more than 50 multibyte characters.
- The Page Component Breakdown report does not support URLs that contain multibyte characters. When specifying a URL and a location from which to run the breakdown, you must enter Latin characters in the URL box.
- Excel reports must have Latin-character file names when uploading to APM running on a Chinese Simplified operating system. To view Excel reports, select **Applications > User Reports > Report Manager**.
- Reports downloaded from APM to Excel cannot be displayed properly on an operating system whose language differs from the data language.

  To download Excel files with multibyte data when APM is installed on an English-language machine, set the **user.encoding** entry in the **<APM root directory>\AppServer\resources\strings.properties** file to the correct encoding.

Business Process Monitor Issues

- If the Business Process Monitor (BPM) log files contain non-Latin-character data, you must open them in a viewer that supports UTF-8 format parsing, for example, Notepad, rather than from the View BPM Files window in the BPM Admin Console.

Log files that are saved in the default encoding of the server on which the BPM Admin Console is installed are shown correctly in the View BPM Files window.

- All BPM instances (such as application, scripts, and parameters) should be named with Latin characters or BPM Server locale characters only.

Real User Monitor Issues

- Real User Monitor supports non-Latin characters in UTF-8 format. For details on configuring the RUM probe to support non-Unicode encodings, see Configuring the HPE Real User Monitor Probe for I18N in the Real User Monitor Administration Guide.
- To support non-Latin characters from Real User Monitor, the encoding for APM databases must be defined as UTF-8, or set to the specific language. For further details, see "Database Environment Issues" on page 106.
- The Real User Monitor Probe Windows installation screens are in English only and are not translated. For details on installing the Real User Monitor Probe, see Installing the HPE Real User Monitor Probe in the Real User Monitor Administration Guide.

End User Management Administration Issues

- Global replace does not support non-Latin-character languages.
- When accessing the Status Snapshot in End User Management (**Applications** > **End User Management** > **Status Snapshot**), certain characters appear unreadable. To resolve this, ensure that you have installed files for East Asian Languages on your local machine, as follows:

  Select **Start > Control Panel > Regional and Language Options >** select the **Languages** tab **>** select **Install Files for East Asian Languages**.

Data Flow Management Issues

When exporting a CI instance to a PDF file, Japanese characters are not displayed in the PDF file. (**Data Flow Management > Discovery Control Panel > Basic Mode**. Run discovery. When discovery has finished, select a CIT in the **Statistics Results** pane. Click the **View Instances** button. In the Discovered by dialog box, select **Export Data to File > Export Displayed CIs to PDF**.)

Multilingual Issues

- The SNMP notification method does not support multilingual text, and can only send a notification in the character set of the Gateway Server machine. This is because APM uses SNMP version 1.0, which does not support multilingual data.
- Error messages in the Failed Transactions report do not display correctly when APM runs on an English operating system and the Business Process Monitor runs on a Japanese operating system. To access the Failed Transactions report, select **Applications > End User Management > Business Processes > Error Summary**. Locate the General Errors table, and click a link to open the Failed Transactions window.
- APM can store multilingual data only when Oracle is used and is set up as UTF-8 encoding. However, a regular executable cannot usually accept multilingual data on the command line.

  The following table describes the procedures that you must perform to add multilingual data to the command line when running an executable file upon alert:

Platform	Procedure
Windows	To prevent multilingual data from being lost, write the application with a wmain function instead of a main function. You can also use another main-type function that can take command line parameters of type wchar instead of type char. **Note:** When you use the SubAlerts command line option, the created XML file does not include an encoding attribute, and the encoding is different from the default UTF-8 encoding.
Solaris	Inform the writer of the application that the parameters passed to the application must be encoded in UTF-8.

For details on Using a Custom Command Line When Running an Executable File upon Alert, see "Run Executable File Dialog Box" in the APM Application Administration Guide.

- An executable file that was created for a previous version of APM is compatible with a multilingual version.

Multilingual User (MLU) Interface Support Issues

- There is no language pack installation. All translated languages are integrated into the APM Multilingual User Interface (MLU).
- Data remains in the language it is entered in, even if the language of the web browser changes. Changing the language of the web browser on your local machine does not change the language of any data that was entered by a user.
- You cannot deploy a package if the server locale is different from the client locale and the package name contains non-Latin characters. For details, see "Package Manager" in the RTSM Administration Guide.
- You cannot create a package that contains resources (for example, views and TQLs) having non-Latin characters in their names, if the server locale is different from the client locale. For details, see "Package Creation and Deployment in a Non-English Locale" in the RTSM Administration Guide.
- In the Modeling Studio, you cannot create a new view if the view's name contains more than 18 Japanese characters. For details on creating new views, see "Modeling Studio" in the Modeling Guide.
- In Location Manager, all geographical locations are in English, regardless of the UI language selected. Logical locations may be named in any language you choose, and remain in that language even if the UI language is subsequently changed.
- The APM server status HTML page appears only in English. It is not translated into any other language. For details, see Post-Deployment in the APM Installation Guide.

Part 3: Data Enrichment

Chapter 24: Location Manager

This section provides information about the Location Manager.

To access

- Select **Admin > Platform > Locations**
- To access Location Manager from End User Management Administration , select **Admin > End User Management > Settings > Business Process Monitor Settings > BPM Agents** and click  to open the Change Agent Location dialog box.

Learn About

Location Manager Overview

The Location Manager is used to define geographical and logical location CIs and assign them ranges of IP addresses. Location CIs can be attached to any other CI. They are used, for example, to attach a location to a Business Process Monitor (BPM) agent or a page discovered automatically by Real User Monitor (RUM).

Location Manager is accessible to users who have Administrator or System Modifier predefined permissions. Permissions are configured in **Admin > Platform > Users and Permissions**.

Location Details and Descriptions

- **Location Entity.** An entity that describes a place in the world. It may be a geographical location, such as a country or a city, or a logical location, such as a building. The location entity may be connected to devices and logical CIs representing end-users or data center locations.
- **Geographical Location.** An absolute location in the world, selected from a predefined list of cities/states/countries, and assigned specific geographical coordinates.
- **Logical Location.** A user-defined virtual location, which may or may not relate to a real location in physical space. If you assign geographical coordinates to a logical location, these coordinates can be changed or deleted.

  Note: All geographical locations are in English, regardless of the UI language selected. Logical locations may be named in any language you choose, and remain in that language even if the UI language is subsequently changed.

- **Hierarchy.** Locations may be nested under other locations, creating a hierarchical tree with a maximum of seven levels under the root.
- **Geographical Coordinates.** Longitude/latitude values, in degrees (expressed as decimal fractions). Coordinates are assigned to individual locations.
- **Default Container.** The parent location for all locations discovered automatically by Real User Monitor (RUM). By default, the Default Container is **World** (the root of the Locations tree), but any location on the tree can be set as the Default Container.
- **IP Ranges.** Each location may be assigned a set of IP ranges. An IP range is a range of IP addresses that have been designated for use by devices in a certain geographical area.

Populating the Location Manager

Location Manager can be populated with locations in a number of ways:

- **Using the Location Manager in Platform Admin.** For details on the user interface, see "Location Manager Page" on page 116.
- **Mass upload from an XML file.** APM enables you to create and define location CIs using an XML file external to the user interface. Mass upload is an alternative to using the user interface, and better suited for defining a large number of locations.

  For details, see "How to Create a Hierarchy of Locations using XML File" below.
- **Using Real User Monitor** (**RUM**)**.** When RUM encounters an IP address for which the location is unknown, that IP is propagated to the Location Manager for location discovery. The Location Manager then searches in the Hexasoft IP2Location repository for a geographical location that matches the given IP address. If a match is found, new locations are created in the Location Manager for the IP address. Depending on the information in the IP addresses repository, at most three locations (country, state, and city) may be created for each IP address.

  Note: If End User Management (EUM) is enabled after being disabled, it may take a few hours until automatic discovery of locations starts to work. This is the time that it takes for the IP-to-location information to load into the database.

Tasks

This section includes the following tasks:

How to Create a Hierarchy of Locations using XML File

You can define your own hierarchy of locations by creating an XML file and loading it through a Java Management Extensions (JMX) console. (For details on accessing and using the JMX, see "JMX Console" on page 78.)

The XML can be generated and edited in any tool that supports text. You can create the file yourself, or base it on an XML file created by APM in the JMX console, which already includes the tags, elements, and attributes necessary for the mass upload XML file.

XML File Details

For a reference detailing all the XML tags, elements, and attributes included in the mass upload file, see "XML Tag Reference" on page 122.

Each mass upload XML must begin with the following declarations:

- **<?xml version="1.0" encoding="UTF-8"?>** This states that this is an XML file with UTF-8 character encoding.
- **<!DOCTYPE locations_manager SYSTEM "./locations.dtd">** This is the document type declaration. The **locations.dtd** file is located in the **HPE APM/conf/locations** folder. The path to **locations.dtd** must

be specified relative to the location of your XML file, and may need to be updated. If your XML file is saved in the same location as **locations.dtd**, no path is necessary.

The XML file is validated using the **locations.dtd** file. If the XML structure is incorrect, you get a SAXParseException and the operation fails. If the DOCTYPE line does not correctly reference the path of the **locations.dtd** file, validation and the entire operation fails.

Note: Populating the location manager through XML results in deletion of all locations that were previously defined in the Location Manager.

XML File Example

In this example, customer 1 wants to upload an XML file to create a hierarchy of locations in Location Manager, as follows: The first location, a site in Los Angeles, includes geographical coordinates, ISP address ranges, and ISPs. Locations 2 and 3 are nested under the first location (Los Angeles), and 2a and 2b are under 2. Location 4 is parallel to Los Angeles in the hierarchy.

World

- Los Angeles; latitude 34.0396, longitude -118.2661; ISPv4 address range 4.38.41.136 to 4.38.80.152 (ISP = Level 3 Communications); ISPv6 address range 2002:0C19:8B00:0000:0000:0000:0000:0000 to 2002:0C19:B28F:0000:0000:0000:0000:0000 (ISP = AT_T WorldNet Services)
  - location_2
    - location_2a
    - location_2b
  - location_3
- location_4

There is no need to add the World root location.

The XML file used to upload this hierarchy of locations is as follows:

```
<?xml version="1.0" encoding="utf-8" ?>
<!DOCTYPE locations_manager SYSTEM "conf/locations/locations.dtd">
<locations_manager>
    <customer_hierarchy customer_id="1">
        <locations_list>
            <location location_name="Los Angeles">
                <latitude>34.0396</latitude>
                <longitude>-118.2661</longitude>
                <ip_ranges>
                    <ip_range>
                        <start_ip>4.38.41.136</start_ip>
                        <end_ip>4.38.80.152</end_ip>
                        <isp>Level 3 Communications</isp>
                    </ip_range>
                    <ip_range ip_v6="true">
                        <start_ip>2002:0C19:8B00:0000:0000:0000:0000:0000</start_ip>
                        <end_ip>2002:0C19:B28F:0000:0000:0000:0000:0000</end_ip>
                        <isp>AT_T WorldNet Services</isp>
                    </ip_range>
                </ip_ranges>
                <locations_list>
                    <location location_name="location_2">
                        <locations_list>
                            <location location_name="location_2a" />
                            <location location_name="location_2b" />
                        </locations_list>
```

```
                    </location>
                    <location location_name="location_3" />
                </locations_list>
            </location>
            <location location_name="location_4" />
        </locations_list>
    </customer_hierarchy>
</locations_manager>
```

For information on each of the XML elements and attributes, see "XML Tag Reference" on page 122.

How to Populate the Location Manager

The Location Manager can be populated with location CIs in a number of ways. You can:

- **Create locations with the user interface.** Use the Locations Manager user interface to create, edit, and manage locations and assign them IP ranges. For details about the user interface, see "Location Manager Page" on page 116.
- **Populate the Location Manager using an XML file.** Upload location CIs to the Location Manager using an XML file external to the user interface. Mass upload is an alternative to using the user interface, and better suited for populating the Location Manager with a large number of locations.

For details on this task, see "How to Update Locations Using Mass Upload" below.

How to Update Locations Using Mass Upload

This task describes how to load an XML file, change an existing location hierarchy using XML, and view the results.

The XML file must comply with the rules listed below. If any of the rules are violated, **buildLocationsHierarchyFromXML** aborts before any changes are made to the locations model:

- No two locations on the same hierarchical level (having the same parent) may have the same name. A location directly under customer_hierarchy (that is, directly under the root location, World) and a location in another place in the hierarchy may not have the same name unless one instance refers to a geographical location and the other to a logical location; or they refer to different types (country, state or city) of geographical locations, such as the country Mexico and city Mexico, or the state New York and city New York.
- A maximum of seven levels of hierarchy can be defined.
- No two locations may have the same ID.
- All location ID values in the XML must match an existing location with that ID.
- No two overlapping IP ranges are allowed.

Note: Saving the existing hierarchy in a file may lengthen the time required to load the new XML file.

To Upload Locations Using Mass Upload:

Create the file yourself in any tool that supports text. Save the XML file you created to a network location accessible to the APM server. For details, see "How to Create a Hierarchy of Locations using XML File" on page 112. For details on the XML file elements and attributes, see "XML Tag Reference" on page 122.

Or

1. Export the current hierarchy as XML using the JMX console, as described in the steps below.
2. Open the JMX console on this machine. (For detailed instructions, see "JMX Console" on page 78.)

3. Under the **APM-Platform** section, select **service=Locations Manager**.
4. Invoke the **convertLocationsHierarchyToXML** method with the following values:
   - **customerId**. By default, use `1` for **customerID**.
   - **target path.** The location where you want to save the XML file.
5. Open the XML file you just saved:
   - Check that the list of existing locations looks accurate. The World root location is not included in this XML file.
   - To add a new location, no ID should be defined.
   - To modify a location, change the fields, but do not change the real ID.
   - To delete a location, delete all its details from the XML file.
   - To change a location's position in the hierarchy, move the location with its real ID to another position in the XML file.
6. Save the XML file you created to a network location accessible to the APM server.

   Save the XML file into the same directory as the **locations.dtd** file so you do not have to reference a different path in the document type declaration line of the XML file. The **locations.dtd** is located in the **<APM root directory>\conf\locations** directory.
7. To upload your edited XML file, in the JMX **service=Locations Manager**, invoke the **buildLocationsHierarchyFromXML** method.
   a. In the **xmlFilePath** parameter, enter the path to the location where you saved the XML file.
   b. In the **saveInFile** parameter, select **True** to save the existing locations hierarchy in the file **<APM root directory>\conf\locations\current_locations_hierarchy.xml**.

The locations have now been uploaded to the Location Manager. They are visible on the Locations Tree of the user interface and through the JMX console.

How to View the Location Hierarchy through the JMX

1. Under **service=Locations Manager,** locate the **getAllLocations** method.
2. Enter the relevant customer ID. By default, use `1` for **customerID**.
3. Invoke the method and check that all your locations are there, including the World root location.

How to Set a Geographical Location

In the Location Properties area, you can set a geographical location and its coordinates from a predefined list of countries and areas, states, and cities; or name a logical location and set its geographical coordinates. Defining a location as a geographical location allows Discovery to automatically assign discovered IP addresses to the location.

To define a location as a geographical location:

1. In the Location Properties area, select the appropriate country/state/city (country alone, country/state, or country/city may be selected as well).

2. Click  .

How to View Location CIs in IT Universe Manager

1. Select **Admin > RTSM Administration > Modeling > IT Universe Manager**.
2. Select **Locations** view.

UI Descriptions

This section includes:

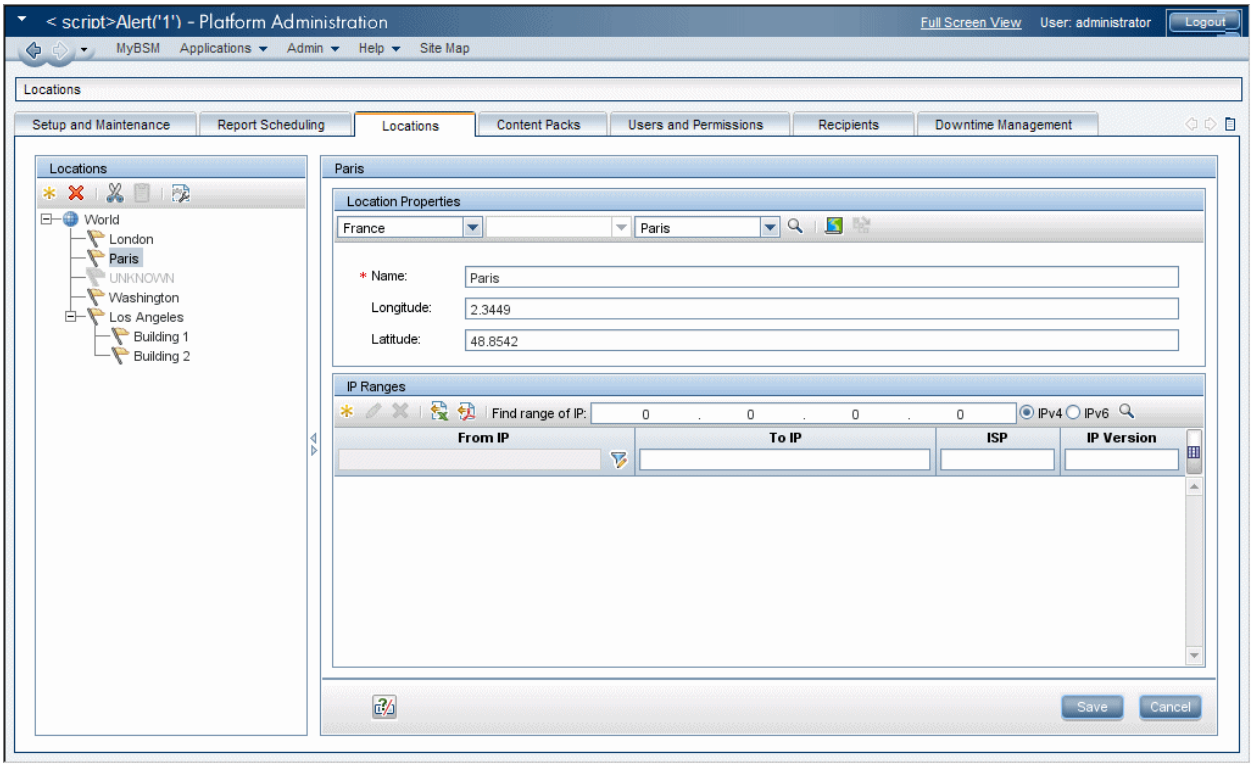
- "Location Manager Page" below
- "New/Edit IP Range Dialog Box" on page 120
- "Geographical Map Dialog Box" on page 120
- "XML Tag Reference" on page 122

Location Manager Page

The Location Manager page enables you to manage locations and assign the locations IP ranges.

The Location Manager page includes the following areas:

- "Locations Area Left Pane" on the next page
- "Location Properties Area" on the next page
- "IP Ranges Area" on page 118



Locations Area Left Pane

In the Locations area, on the left pane of the Locations page, you can add, delete, and move locations, and set a location as the default container. Locations appear in a tree structure, with a maximum of seven hierarchical levels, whose root (level zero) is called **World**.

User interface elements are described below. You can also access these actions from a context menu by right-clicking on the Locations area of the left pane.

UI Element	Description
	**Add location**. Click to add a new location below the selected location. Opens the Location Properties area. See "Location Properties Area" below
	**Delete location**. Click to delete a location and its children locations. If you delete a location, any IP ranges assigned to it or its children can be moved to its parent location. To do this, select the **Move IP Ranges to the Parent Location** check box in the **Confirmation** window that appears.
	**Cut location**. Click to cut a location. The location is copied to the clipboard, and can be pasted below another element in the locations tree. **Note:** When a location is cut, it remains visible, grayed out, in its former place on the tree, until it has been pasted in a different position. To deselect a cut location before it has been pasted to a different position, and return it to its original position, click **Cut location** again.
	**Paste location.** Available when a location has been cut and the user has navigated to another part of the tree.
	**Set as default container.** Click to set a particular location as the default container. This is the parent location for all automatically discovered locations. For more information, see "Location Manager Overview" on page 111.

Location Properties Area

In the Location Properties area, you can set a geographical location and its coordinates from a predefined list of countries and areas, states, and cities; or name a logical location and set its geographical coordinates. Defining a location as a geographical location allows Discovery to automatically assign discovered IP addresses to the location. To define a location as a geographical location, select the appropriate country/state/city (country alone, country/state, or country/city may be selected as well) and click  .

Note: Geographical location can be set only from a predefined list. If you manually enter the name of a location, it is created as a logical location.

User interface elements are described below:

UI Element	Description
<Country or Area>/<State>/<City>	Use the first and third drop-down controls to select country or area and city. When USA is selected as country, the middle dropdown becomes available, and can be used to select a particular state.
	**Set geographical location.** Click to locate the geographical coordinates (longitude and latitude) of the selected country/state/city and automatically enter name and coordinates into the appropriate fields under Location Properties, defining the location as a geographical location.
	**Select Location Coordinates.** Click to launch the Geographical Map dialog box, which can be used to select the geographical coordinates of any location. For more information, see "Geographical Map Dialog Box" on page 120.
	**Get coordinates from nearest parent.** Click to copy the geographical coordinates of the closest parent location with coordinates, to the selected location.
Name	Enter the name of the location in the **Name** text box. **Notes:** If you assign the same name to more than one location under different parents, a small caution symbol displays indicating that the name has already been defined for another location and suggesting that the name be changed. If you change the name of a geographical location, its association with the original geographical location is maintained.
Longitude/Latitude	Enter the longitude and latitude of the location. If you select a location from the predefined drop-down lists of countries, states, and cities, or from the Geographical Map dialog box, the longitude and latitude boxes are filled automatically.

IP Ranges Area

You can use the IP Ranges area to assign IP ranges to a location. Real User Monitor (RUM) then uses these ranges to assign newly discovered pages and other CIs to particular locations.

The table of IP ranges may contain thousands of pages. To view the table in a single file, you can export it in Excel or Adobe Acrobat (PDF) formats.

User interface elements are described below:

UI Element	Description
	**New IP Range**. Click to create a new IP range. Opens the New IP Range dialog box. **Note:** A particular IP range can be assigned to only one location. If you try to assign an IP range that overlaps with a parent IP range, a message displays, warning that this action will remove the IP range from the parent location. (Only the area of overlapping ranges is removed, and the parent IP ranges are adjusted accordingly.) Click **Remove from Parent** to remove the overlapping IP range from the parent and reassign it to the selected location, or **Cancel**. If you try to assign an IP range that overlaps with a range already assigned to another location (not a parent), an error message is displayed and you must select a different IP range.
	**Edit IP Range**. Click to edit a selected IP range. Opens the Edit IP Range dialog box. See "New/Edit IP Range Dialog Box" on the next page.
	**Delete IP Range**. Click to delete one or more selected IP ranges.
	**Export to Excel**. Click to export IP range information for the selected location to an Excel spreadsheet.
	**Export to PDF**. Click to export IP range information for the selected location to an Adobe Acrobat file.
Find Range of IP	To find an existing range in which a particular IP address is located: 1. Select the appropriate radio button: • **IPv4** (Internet Protocol version 4) for addresses consisting of four numbers, each ranging from 0 to 255, in dot-decimal notation) • **IPv6** (Internet Protocol version 6) for addresses consisting of eight hexadecimal numbers, each ranging from 0 to FFFF, in colon-separated notation) 2. Enter the IP address in the **Find Range of IP** box. 3. Click  . The system highlights the range in which the IP address is found. **Note:** This searches for the IP range in the currently selected location only.
From IP/To IP, ISP, IP Version	To filter the IP ranges for a particular string of text in their lower and upper IP range limits, ISP names, or IP versions, enter the string in the **From IP**, **To IP**, **ISP**, or **IP Version** boxes. These boxes may be used in combination with each other. An asterisk (*) may be used as a wildcard to represent one or more characters. For example: • To filter for IPv6 addresses, enter "`6`" in the **IP Version** box • To filter for IPv4 address ranges whose upper limits end in 0, enter "`*.*.*.0`" in the **From IP** box.

New/Edit IP Range Dialog Box

To access, select **Admin > Platform > Locations** and click  under IP Ranges.

User interface elements are described below:

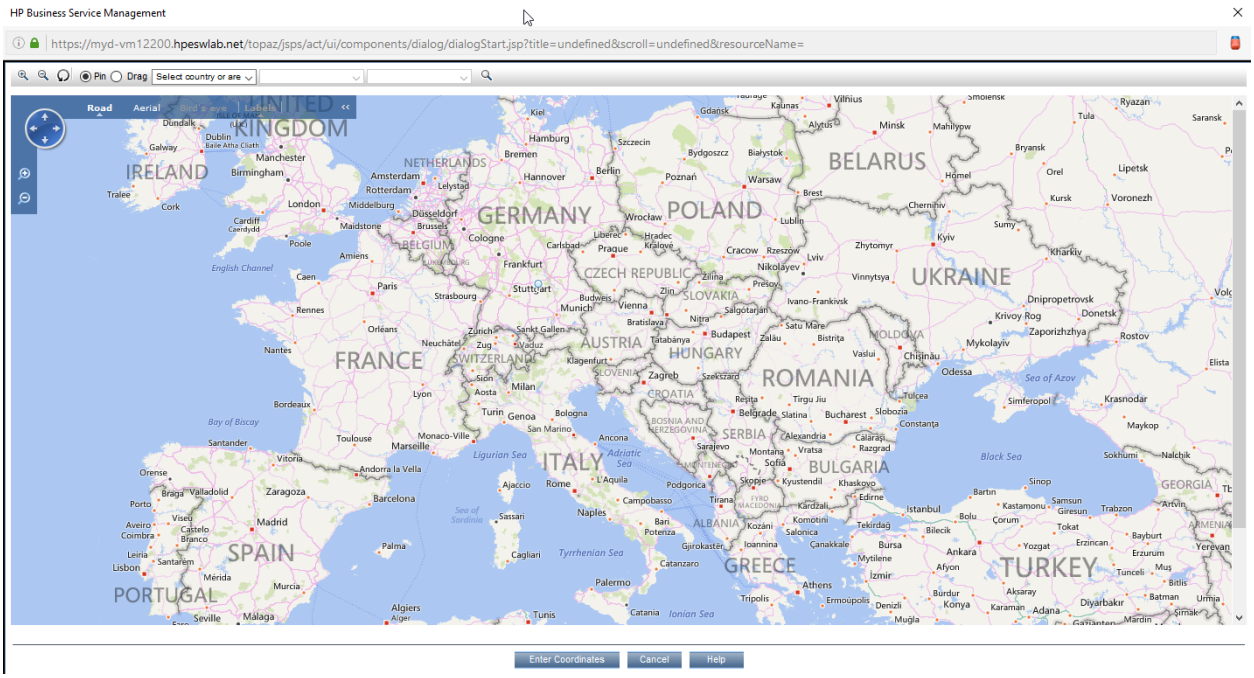
UI Element	Description
IP version	Choose **IPv4** or **IPv6** to select: • Internet Protocol version 4 (for IP addresses consisting of four numbers, each ranging from 0 to 255, in dot-decimal notation) • Internet Protocol version 6 (for IP addresses consisting of eight hexadecimal numbers, each ranging from 0 to FFFF, in colon-separated notation)
From IP/To IP	Use the **From IP** and **To IP** boxes to set the range of IP addresses for the location. • For IPv4, as you enter an IP address in the **From IP** box, a corresponding address ending with 255 is automatically entered into the **To IP** box. All values in both boxes may be changed to any permissible value (0-255), but the address in the **To IP** box must be the same or higher than the address in the **From IP** box. The IPv4 range must not exceed 50,000,000 IP addresses. • For IPv6, as you enter an IP address in the **From IP** box, the same address is automatically entered into the **To IP** box. All values in both boxes may be changed to any permissible value (0-FFFF), and the address in the **To IP** box may be higher, the same, or lower than the address in the **From IP** box.
ISP	Specify the Internet Service Provider in the **ISP** box.

Geographical Map Dialog Box

The Geographical Map dialog box enables you to select the geographical coordinates of any location. If geographical coordinates were previously entered into the **Longitude** and **Latitude** boxes, these are passed to the Geographical Map dialog box, which opens with a pin on that location.

Note: Users who are not connected to the Internet see another version of this map.

To access, from the Location Properties area of the Locations page, click  .



User interface elements are described below:

UI Element	Description
	**Zoom In**. Click to zoom in on the map. **Note:** This icon is located on the toolbar. Another **Zoom In** icon with identical functionality appears on the map.
	**Zoom Out**. Click to zoom out on the map. **Note:** This icon is located on the toolbar. Another **Zoom Out** icon with identical functionality appears on the map.
	**Reset**. If you open the Geographical Map at a particular set of coordinates and then pan elsewhere, clicking **Reset** recenters the map to the starting coordinates.
Pin/Drag radio buttons	Select **Pin** to move the pin to any location on the map by clicking on that location. Double-clicking moves the pin and zooms in on the location. Select **Drag** to drag the map.
<Country or Area>/<State>/<City>	Use the first and third drop-down controls to select country or area and city. When USA is selected as country, the middle drop-down becomes available, and can be used to select a particular state.
	**Find location on map.** Click to locate the selected country or area and city on the map.
	**Pan in Any Direction.** Click and hold on this control and drag to pan across the map.

UI Element	Description
Road View	Click to see a road map of the world.
Aerial View	Click to see an aerial photographic map of the world.
Bird's Eye	The bird's-eye view is disabled.
Labels	In Aerial View, click to display or hide map labels. This is disabled in Road View.
Enter Coordinates	Click to automatically copy the coordinates of the pinned location to the **Longitude** and **Latitude** boxes of the Location Properties area.

XML Tag Reference

Following are tables that list all the elements and attributes that are used in the mass upload XML file:

- Elements Table

Element	Description	Attributes
locations_ manager	Initial element in a block containing Location Manager data	
customer_ hierarchy	Initial element in a hierarchy of locations for a particular customer	customer_ id
locations_list	Initial element in a list of locations	
location	Initial element in block defining attributes for a particular location	location_ name
latitude	Latitude of the location, in degrees	
longitude	Longitude of the location, in degrees	
ip_ranges	Initial element in a list of IP address ranges for a particular location	
ip_range	Initial element in block defining attributes for a particular IP address range	ip_v6
start_ip	Lower limit of IP address range IP address ranges may be IPv4 or IPv6. Location Manager supports the following notation formats: IPv4 – number of 4 bytes IPv4 – string in x.x.x.x format IPv6 – number of 16 bytes IPv6 – string in x:x:x:x:x:x:x:x format IPv6 – IPv6 regular expression	

Element	Description	Attributes
end_ip	Upper limit of IP address range. For supported IPv4 and IPv6 notation formats, see start_ip, above. **Note:** IPv4 range must not exceed 50,000,000 IP addresses.	
isp	Name of ISP for the range	

- Attribute Table

Attribute	Parent Element	Description	Example
customer_id	customer_hierarchy	Number. Unique and mandatory. ID number of the customer for whom a hierarchy of locations is built.	<customer_hierarchy customer_id="1">
location_name	location	String. Mandatory. Not unique (several locations, if not siblings, can have the same name). Name of a particular location.	<location location_name="Los Angeles">
ip_v6	ip_range	Boolean. ="true" if IP addresses for a particular range are in IP version 6 format. Otherwise, they are in IP version 4 format.	<ip_range ip_v6="true">

- Implied Attribute Table

The following attributes are exported when exporting the current hierarchy as XML but are not required when defining new locations in the XML. When updating an existing location through XML, these attributes need to be preserved:

Attribute	Parent Element	Description
original_geo_location_id	location	Used to identify geographical locations
location_type	location	Possible values: • "undefined" (default) • "country" • "state" • "city"
location_id	location	The real ID of an existing location

Example:

```
<location_name="UNKNOWN" location_type="undefined" location_
id="47a3711c334fd8577858c6da60b3e0e6" original_geo_location_id="Unknown_Unknown">
```

Troubleshooting/Limitations

Location Export/Import XML via JMX Console Limitation

In the APM UI, you can create **two sub-locations** with the **same name**.

Using the JMX console, you can create an XML file of this location hierarchy.

However, using the JMX console, you cannot create a location hierarchy from the XML file that was created from a hierarchy that contains **sub-locations with the same name**.

Part 4: Users, Permissions, and Recipients

Chapter 25: User Management

This section describes the tasks you can perform through the user management interface.

To access

Select **Admin > Platform > Users and Permissions > User Management**

Learn About

Configure APM Users

Groups and Users Permissions enable you to restrict the scope of a user's access to predefined areas. You can grant permissions directly to an individual user or to a user group. User groups make managing user permissions more efficient; instead of assigning access permissions to each user one at a time, you can group users who are assigned the same permissions levels on the same resources.

To create users and groups, see "Configuring Users and Permissions - Workflow" on page 139.

You may want to create different groups based on how users access the different resources in APM. For example:

Functions Within the Organization	Locations and Territories
Customer service representatives	Users working in different sales territories
System administrators	Users based on geographical location
High-level management	Users accessing network servers in different locations

You can change a user's parameters, including username and password, on the General tab. For details, see "Create Users" on page 140.

Tip: To obtain more user management capabilities and security, we recommend using external LDAPs or Active Directory user management. For details about how to configure APM to work with LDAP, see "LDAP Authentication and Mapping" on page 227

Define a Superuser

One superuser is defined for every installation of APM. This superuser's login name is `admin` and the initial password for this account is specified in the Setup and Database Configuration utility. This original superuser is not listed among the users in User Management and therefore, this user's password can be changed only on the **General Settings** page in Personal Settings (**Admin > Personal Settings**).

You can apply superuser permissions to other users in the system. These users with superuser permissions can be modified in User Management.

UI Description

User Management Page

When you first access the User Management page or the cursor is located on the **All** node, the page displays:

- The **Groups/Users** pane. For details, see "Groups/Users Pane" below.
- The **Workflow** pane. The Workflow pane displays introductory information about the User Management application, and a suggested workflow for configuring groups and users. The Workflow pane consists of the following sub-panes:
  - General
  - "Recipient Management" on page 184
  - "Permissions Tab (User Management)" on page 177
  - "Hierarchy Tab (User Management)" on page 181
  - "Customization Tab (User Management)" on page 183

Groups/Users Pane

The Groups/Users pane appears on the left side of the page, and is visible on all tabs of the User Management application. This pane displays the list of users and groups of users configured to access APM.

Note: When selecting more than one user or group and modifying parameters, the changes take effect only for the first selected user. The exception is the Delete option, which deletes multiple users at once.

User interface elements are described below:

UI Element	Description
	Creates a user or group. Depending on whether you select to create a user or group, the **Create User** or **Create Group** window opens. When you create a new group or user, the **Groups/Users** pane refreshes and the newly created group or user is selected. When creating a group, the access permissions are automatically inherited by the group's users. When creating users with the cursor on a group, the users are automatically nested within that group. **Note:** In Firefox, after refresh, the **All** node is selected.
	Clones the settings of an existing user or group to a new user or group

UI Element	Description
	Deletes the selected user or group. **Note:** When you delete a user, the linked recipient is also deleted.
	Collapses or expands the groups selected in the hierarchy tree. **Note:** Only previously loaded nodes are expanded.
	Click **Delete Obsolete Users** to delete APM users no longer configured on the LDAP server. After selecting **Delete Obsolete Users**, choose a unique domain name. You can remove multiple users at once by holding the `Ctrl` button while selecting users.
	Click **Group Mappings** and select the unique domain name to map local groups to groups configured on the LDAP server. For details, see "Group Mappings Dialog Box" on the next page. **Note:** This button is displayed only if LDAP Configuration was added using the LDAP Configuration Wizard and enabled. For details, see "LDAP Configuration Wizard" on page 209.
	Click to assign or view the Security Officer. The security officer is a user who can configure certain sensitive reporting information in the system, such as which RUM transaction parameters to include or exclude from certain reports (such as Session Details or Session Analyzer). There can be only one security officer assigned in the system. Only a user with superuser permissions can assign the security officer for the first time. Only the security officer himself can assign it to another user or change his own password once it has been assigned. For details on this topic, see "Security Officer" on page 134.
	A configured user
	A configured group
	Security officer
	Root node
Browse	Displays a list of configured users and groups, and enables you to create or delete users and groups.
Search	Displays a table view of users and groups, and enables you to search for a user or group by any of the following criteria: • Group name • Login name • User name • User last login You can sort the columns by clicking the column headers above the boxes. You can include wildcards (*) in your search.

Group Mappings Dialog Box

This dialog box enables you to map groups configured in APM to groups configured on the LDAP server.

To access	Select **Admin > Platform > Users and Permissions > User Management**. In the Groups/Users pane, click the **Group Mappings**  button and select the unique domain name. The Group Mappings dialog box consists of the following panes: • **Remote Corporate Directory Pane.** For details, see "Remote Corporate Directory Pane" below. • **APM Local Directory For Remote Group Pane: <group name>.** For details, see "APM Local Directory for Remote Group: <group name> Pane" on the next page. • **Local Groups to Remote Group Mappings.** Displays a table of the LDAP groups and the APM groups that they are assigned to. The LDAP groups are displayed in the **Remote Group Name** column, and the APM Groups are listed in the **Local Group Name** column. Select the **Enable User Synchronization** check box to enable User Synchronization upon logging into APM, to synchronize LDAP users with APM users. **Note:** Ensure that you mapped LDAP groups to APM groups before selecting this check box. If you have not performed Group Mapping, all users are nested under the Root group and are assigned System Viewer permissions. For details on mapping groups, see "How to Map Groups and Synchronize Users" on page 233.
Important information	**Note:** This dialog box is accessible only if LDAP Configuration was added by the LDAP Configuration Wizard and enabled. For details, see "LDAP Configuration Wizard" on page 209. If you are switching from one LDAP server to another, ensure that you remove all existing group mappings from the original LDAP server before mapping to the new one.

Remote Corporate Directory Pane

This pane enables you to assign APM groups to LDAP groups, and to list the users in the LDAP groups.

Important information	• To synchronize LDAP groups with APM groups, click **Assign Groups** to open the Select Local Groups for Remote Group dialog box. • To view the list of users associated with the respective LDAP groups, click **List Users**. You can also select either of these options by right clicking on the group. • Once the LDAP groups have been mapped to the APM groups, the APM groups are managed only from the LDAP interface. This means that the following are fields are affected on the Users and Permissions interface: • The **Create User** field is disabled. • The **User Name** field is disabled. • The **Password** field is invisible. • The **Hierarchy** tab is enabled only for groups and not for users.

APM Local Directory for Remote Group: <group name> Pane

This pane displays the APM mapped to the LDAP group selected in the Remote Corporate Directory Pane, and enables you to remove the mapped APM groups.

Important information	• To remove groups, select the group you want to remove and click **Remove Groups**. • You can remove multiple groups at once by holding the `Ctrl` button while selecting groups.

Permissions

You can assign permissions to the groups and users defined in your APM platform, enabling access to specific areas of APM.

Learn About

Granting Permissions

Granting permissions has the following components:

- User
- Resource
- Role or operation being granted

For details on assigning permissions, see "Assign Permissions to Groups or Users" on page 141.

Permissions and Roles on Root Resource

Permissions and roles on the root resource (the top level resource relevant for all contexts) are exposed only for a Superuser, while other users with the relevant permissions, can assign roles and permissions for resources other than the root resource.

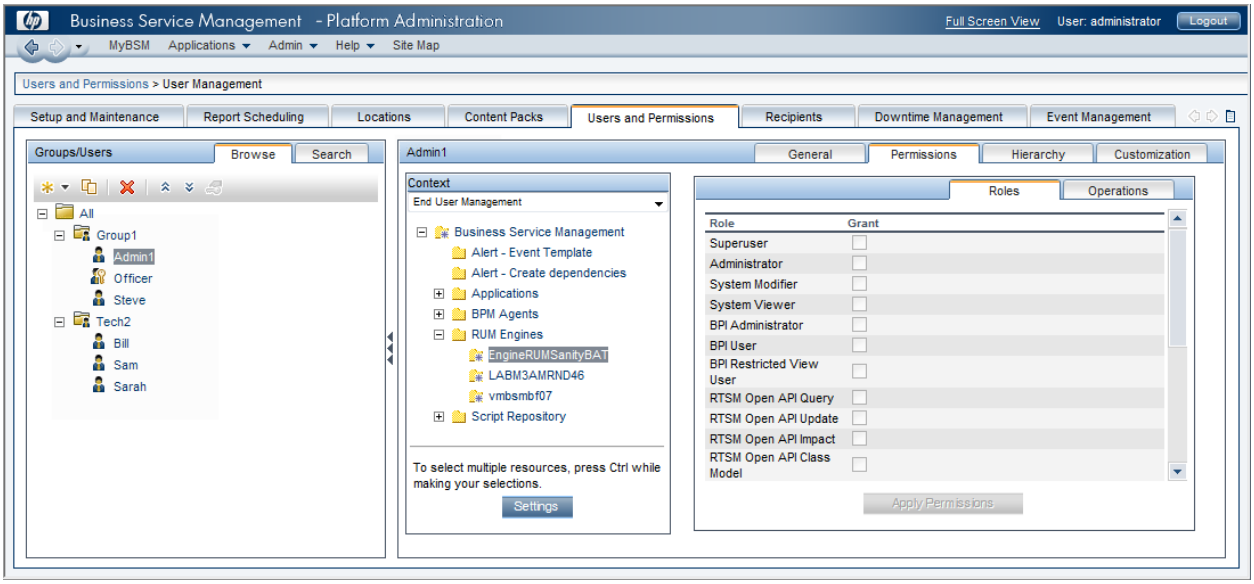
Permissions Tab

The Permissions tab includes the following areas:

- The resource tree area in the center of the page, containing the contexts, resources, and resource instances on which permissions are assigned. For details, see "Understanding Permissions Resources" below.
- The roles and operations area on the right side of the page. For details on roles, see "Roles" on page 133. For details on operations, see "Operations" on page 134.

Additionally, the **Groups/Users** pane is continually visible on the left side of the page.

The following is an example of Granting Permissions:



Upgrading and Maintaining Users and Security Levels

If you have upgraded from a previous version of APM and had specific users and security levels defined, those users and security levels are mapped to the new roles functionality in the Permissions tab. For details, see "Roles" on page 133.

Exporting Users, Groups, and Roles

You can export users and groups, together with their assigned roles, from one APM machine to another. For details, contact HPE Software Support.

Understanding Permissions Resources

APM enables you to fine-tune your permissions management by applying permissions at the resource level. All of the resources on which permissions can be applied are categorized in a hierarchical tree, representing the APM platform.

The resources and instances of those resources are organized according to logical groupings called **contexts**. Contexts make it easier to identify and select the area of the platform on which you want to apply permissions.

The resources are divided according to the context in which they function within the platform and not necessarily where they are found in the user interface.

Resources and Resource Instances

There are the following types of resources in Permissions Management:

	Resource collection (a resource that can have instances)
	Instance of a resource
	Resource that cannot have instances in the permissions resource tree

An instance of a resource is displayed only if it has been defined in the platform. The instance of a resource appears as a child object of the resource in the tree with the name as it has been defined in the application. After instances of a resource are defined in the system, the resource collection acts as the parent resource for those instances.

There are some resources, such as the different data collector profiles, that contain other resources within them in the resource tree hierarchy. Some of these sub-resource types appear only if there are instances of the resource defined in your platform, such as Monitor and Transaction resources within a profile resource.

Resources that cannot have instances in the permissions tree are divided into the following types:

- Resources that are functions or options within the system that do not have any other instances or types.

  Example:

  The Outlier Value resource determines whether the user can edit the outlier threshold value. It has no instances.

- Resources that do have instances; permissions can be applied only on the resource type and affect all instances of the resource.

  Example:

  The Category resource includes all categories defined in End User Management Administration. **Change** permissions granted on the categories resource enables a user to modify all the categories defined in the system. You cannot grant or remove permissions for specific categories, only for every category defined in End User Management Administration.

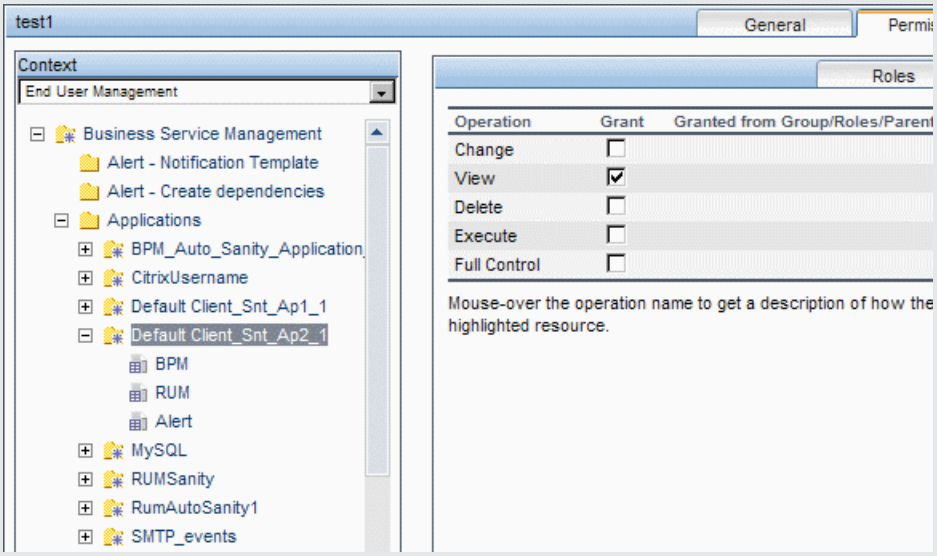
Examples of Resources and Instances:

An example of how resources and instances are displayed in the permissions hierarchy is the Applications resource collection within the End User Management context. The Applications resource includes instances only if applications have been defined in the system. Some instances may be defined by default, but others only exist if defined by the user. If there are applications defined in the system, each of these appears as an instance of the Applications resource.

Because BPM, RUM, and alerts are defined in your platform per application, the BPM, RUM, and Alerts resources appear under each of the instances of the application resource.

You can apply permissions to the Applications resource level. This provides the user with access to all applications created in the system. If you want to restrict a user's access to specific applications that relate to the user's tasks, you can apply permissions to those specific applications, and can also apply

or removed permissions to specific resources per application.



Guidelines for Working with Resources

- The Application Performance Management resource refers to all contexts in APM.
- Only roles and not operations can be applied to the Application Performance Management resource. For details, see "Roles" below.
- To manage the permissions on a sub-resource, you must provide the user with at least **View** permission on the selected resource's parent.
- You grant **Add** permission only on a resource and not on an instance of a resource.
- When a user defines or creates an instance of a resource, for example creates a Business Process profile, that user has **Full Control** permission on that resource instance and all of its sub-resources.

Roles

APM enables you to apply permissions using roles for specific users or groups in your organization. These roles include a preconfigured collection of resources and a set of operations that apply to those resources.

Roles are organized by context, which define what resources and operations have been preconfigured and included in the roles. For details on how each operation applies to a specific resource, see "Operations" on the next page.

Roles can be applied only to specific resources:

- Roles that include resources from several contexts can be applied only to the **Application Performance Management** resource. **Application Performance Management** appears as the first resource collection in every context.
- Roles whose resources are all within one context can be applied to specific resources within that context.

For a description of each role, including details of the resources on which roles can be applied, see " User Management Roles Applied Across APM" on page 151.

Operations

When working with operations, keep the following in mind:

- All of the operations that can be applied to a resource collection can also be applied to any instance of that resource. The one exception is the **Add** operation which cannot be applied to an instance of a resource.
- The **Full Control** operation automatically includes all the other operations available on the resource. When applied, the other operations are automatically selected.
- When the **Full Control** operation is applied to any resource, the user also has permissions to grant and remove permissions on that resource, or resource instance, for other users or groups.
- When the **View** operation is one of the resource's available operations and you select one of the other available operations, the **View** operation is also automatically selected.

For details on the available operations in APM, see "User Management Operations" on page 166.

Security Officer

The security officer is a user who has security privileges to view sensitive information in the system. The security officer is typically not a regular APM user and receives access to configure certain sensitive reporting information. In RUM, the security officer can configure settings for masking sensitive data. For details, see Sensitive Data Area in the APM Application Administration Guide.

This user does not generally access the other areas of APM.

There can be only one user in the system assigned as security officer. Only the user with superuser permissions can assign the security officer for the first time. Thereafter, only the user assigned as security officer can pass on the security office designation to another user, or change their own password. The superuser can no longer assign security officer status.

The security officer is designated by highlighting a user in the User Management tree and clicking on the Security Officer icon. For details on the user interface, see "Groups/Users Pane" on page 127.

No other user in the system can delete the user assigned as security officer. The security officer designation must be assigned to a different user by the security officer before the user who is the current security officer can be deleted from the system.

In unforeseen circumstances, when the security officer is no longer able to access the system and reassign the security officer designation to another user, the administrator can use the JMX console to clear the security officer designation from the user. For details on how to perform this task procedure, see "How to Remove Security Officer Status Using the JMX Console" below.

Tasks

How to Remove Security Officer Status Using the JMX Console

This task describes how use the JMX console to remove security officer status from a user. This may be necessary if under unforeseen circumstances, the security officer cannot remove the status himself. Once the security officer is assigned, there is no other user authorized to make this change within the User Management interface. For details on this topic, see "Security Officer" above.

To remove a security officer:

1. In a browser, enter the URL of the JMX console:
   http://<Gateway or Data Processing Server name>:29000/

2. Enter your JMX console authentication credentials. If you do not know your authentication credentials, contact your system administrator.
3. Locate:
   - Domain name: **Foundations**
   - Service: **Infrastructure Settings Manager**
   - Setting: **setSettingValuePerCustomerId**
4. Modify the parameter values as follows:
   - **Context Name**: enter `security`
   - **Setting Name**: enter `secured.user.login.name`
   - **New Value**: leave empty
5. Click **Invoke**.

Group and User Hierarchy

You can nest groups to make managing user and group permissions easier. Instead of assigning access permissions to each group one at a time, you can nest a group to inherit the permissions of its direct parent.

When nesting groups, note the following:

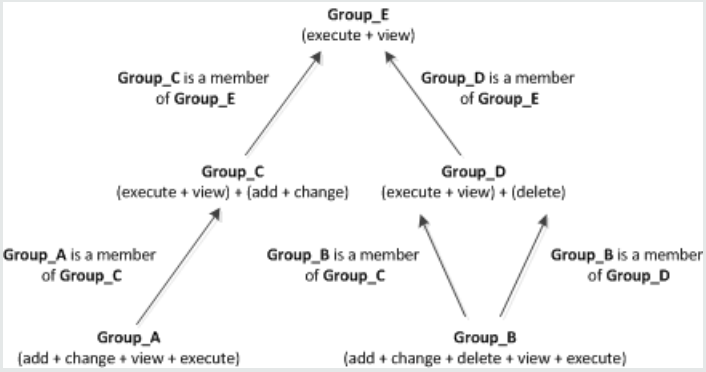
- A group can be a member of several groups.
- Permissions are assigned to nested groups in the same way as for regular, non-nested, groups. Changes in nested group permissions take effect at the user's next login.
- There is no maximum number of levels of nested groups.

Example:

In the example below:

- **Group_A** and **Group_B** are nested members of **Group_C**.
- **Group_B** is also a nested member of **Group_D**.
- **Group_A** and **Group_B** inherit the permissions of **Group_C** and indirectly inherit the permissions of **Group_E**.
- **Group_B** also inherits permissions from its other parent, **Group_D**.
- **Group_C** and **Group_D** are nested members of **Group_E.**

- **Group_C** and **Group_D** inherit the permissions of their parent, **Group_E**.



When permissions are added to, or removed from, a parent group, the changes are automatically implemented in the parent group's immediate children and continue to propagate onward. For example, if **delete** permission in **Group_D** is removed, **Group_B**'s permissions become **add + change + view + execute**.

A circle of nested groups is not permitted. For example, **Group_A** is a member of **Group_B**, and **Group_B** is a member of **Group_C**. **Group_C** cannot be a member of **Group_A**.

Note: All permissions in the previous example refer to the same resource.

For details on setting up nested groups, see "Configure User and Group Hierarchy" on page 141.

Application Health Permissions

The existing APM permissions model considers user operation permissions on resources and RTSM views.

In Application Health, permissions are enforced in the context of application. A user is allowed to see reports for specific application or edit its setting according to the permission level configured for him (for that application) in end user experience context (see "How to set permissions for applications" on page 138).

Learn About

Application Permissions

The following lists the operations you can perform on a RUM or BPM application and the permissions you need.

- To *view* an application on the Dashboard and in individual reports, you need **View** permission for the application.
- To *edit* an application, you need **View** , **Change** and **Execute** permission for the application. To select scripts and assign them to a specific location when configuring a BPM application, you need permission for the location and script repository.
- To *delete* an application, you need **View**, **Change**, and **Delete** permission for the application.
- To *add* an application, you need **Add** and **View** permission on the Applications folder in the End User Management context.

- To *add* a RUM configuration to an existing BPM application, or a BPM configuration to an existing RUM application, you need **Add** permission on the relevant application resource.

Report Permissions

- To *view* BPM reports , you need **view** permission for the relevant application resource.
- To *view* RUM reports, you need **view** permission on both the application's level as well as the RUM engine level.

Alert Permissions

The following lists the operations you can perform on an alert and the permissions you need.

- To *view* an alert, you need **View** permission on the application and the alert.
- To *add* or *edit* an alert, you need **View** permission on the application, and **Full Control** permission on the Alert.

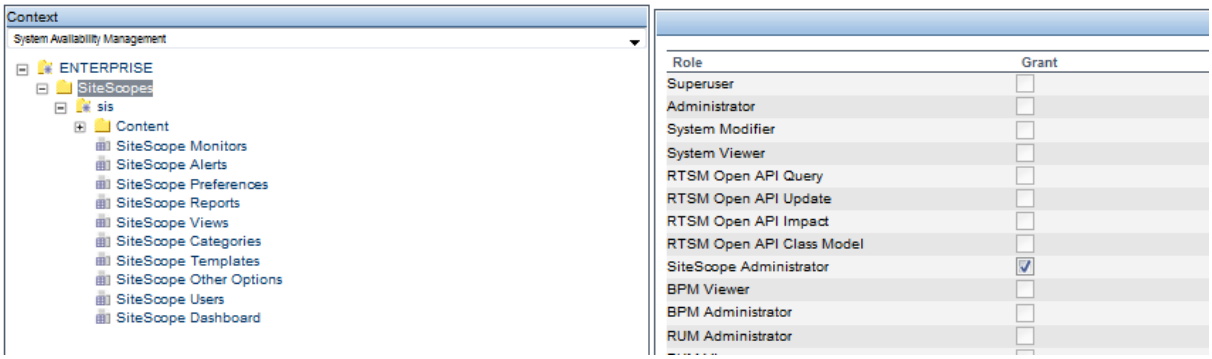
RUM Engine / BPM Agents / Script Repositories Permissions

The following lists the operations you can perform on the RUM Engine, BPM Agents, or Script Repositories and the permissions you need.

- To *edit* a RUM Engine or BPM Agent, you need **View** permission on the RUM Engine / BPM Agent or on the entire RUM Engine/BPM Agent folder.
- To *delete* a RUM Engine or BPM Agent, you need **View** permission on the RUM Engine / BPM Agent or on the entire RUM Engine/BPM Agent folder.
- To *edit* a BPM application, you need **Full Control** permission on the Script Repository folder.

SAM Permissions for SiteScope Users

- To *view ALL SiteScope instances*, you need to be assigned one of the following system roles: **Superuser**, **System Modifier**, or **System Viewer**.
- To *view a specific SiteScope instance*, you need to be assigned the **SiteScope Administrator** role on the specific instance or on the SiteScope parent group under the System Availability Management context.



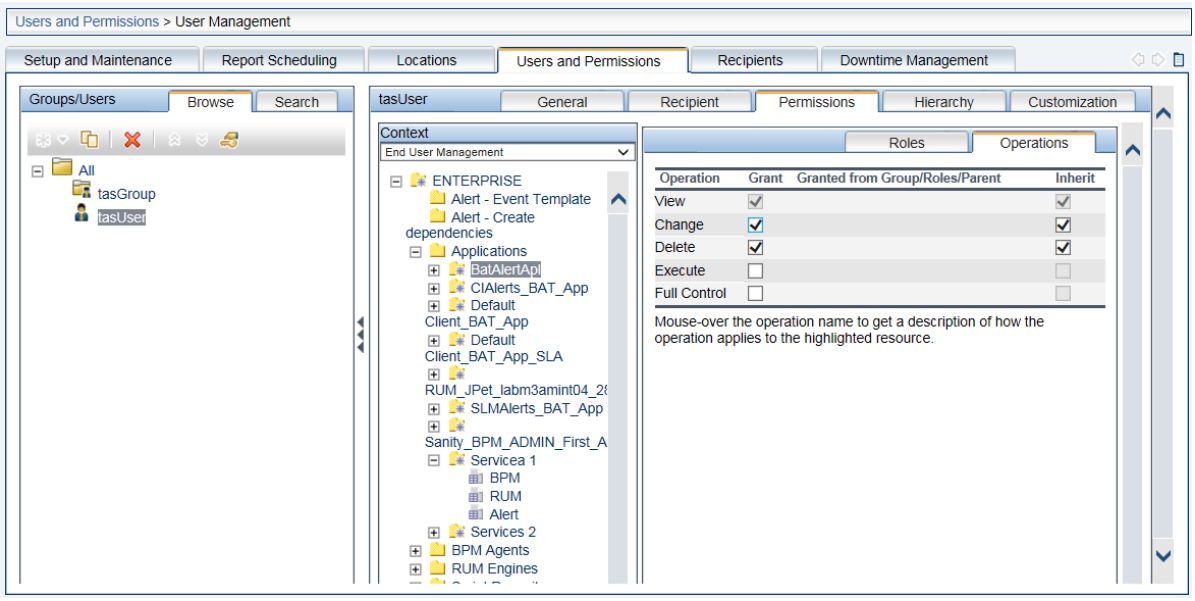
User roles and their default operations

Roles	Default Applications Operations	Description
Superuser	Add, Full Control	Can view reports and full control over BPM and RUM configuration of all applications, including adding new applications and viewing BPM Agents and RUM Engines properties
Administrator	Add , View	Can view reports for all applications and add new applications. Manage BPM Agents, RUM Engines, and scripts
BPM Administrator	Add, Full Control (BPM)	Can view BPM reports and full control over BPM configuration of all applications, including adding new apps. View BPM Agents properties and download scripts from all applications.
RUM Administrator	Add, RUM Full Control (RUM)	Can view RUM reports and full control over RUM configuration of all applications, including adding new apps. View RUM Engines settings.
BPM Viewer	View	Can view BPM reports for all applications, download scripts for all applications, and view BPM Agents settings
RUM Viewer	View	Can view RUM reports for all applications and view RUM Engines settings.
System Viewer	View	Can view all applications reports and view Agent settings.
System Modifier	View, Change	Can view all applications reports and view and edit BPM Agents settings.

Tasks

How to set permissions for applications

1. Select **Admin > Platform > Users and Permissions**.
2. In the Groups/Users pane, select a group or individual user.
3. Open the Permissions tab.
4. In the Context Pane, in the drop-down-list select **End User Management**, and select **Applications** to set permissions for all applications, or select a specific application.
5. On the Operations tab, select the required permissions for the user.



6. Click **Apply Permissions**.

How to set permissions for BPM agents or RUM engines

1. Select **Admin > Platform > Users and Permissions**.
2. In the Groups/Users pane, select a group or individual user.
3. Open the Permissions tab.
4. In the Context Pane, in the drop-down-list select **End User Management**, and select the required BPM agent or RUM engine or the entire BPM agent / RUM engine folder.
5. On the Operations tab, select the required permissions for the user.
6. Click **Apply Permissions**.

Configuring Users and Permissions - Workflow

Below is a suggested workflow for the User Management application. For a use-case scenario related to this task, see "How to Configure Users and Permissions — Use-Case Scenario" on page 143.

Prerequisites

Before you configure User Management, you should map out the required users and groups and their relevant permission levels. For example, enter the following information in an Excel page:

1. A list of users required to administer the system, as well as the end users who are to access Service Health and reports. Gather appropriate user details such as user names, login names, initial passwords, and user time zones. Although not needed to define users, at this stage it might be useful to also collect user contact information such as telephone numbers or email addresses.
2. If categorization of users into modes (operations and business) is required, specify into which user mode to categorize each user. For details, see Create KPIs for Operations and Business User Modes in the APM Application Administration Guide.
3. If multiple users require similar system permissions, create a list of groups, and the users that should belong to each group.
4. The permissions that each user or group requires. To aid in this process, review the Permissions

Management page to learn about the different contexts and resources for which permissions can be granted. For details, see "Understanding Permissions Resources" on page 131.

Create Groups

You can create groups as sub-groups nested under other groups. Sub-groups have the same access restrictions as the parent group.

1. Select **Admin > Platform > Users and Permissions > User Management**.
2. In the **Groups/Users** pane, select a location for the group, for example you may want to create the group as a sub-group under another group.
3. Click the **New Group/User** button, and then select **Create Group**.
4. In the Create Group dialog box, enter the group name and, if required, a group description.

Note:

- The group name must be unique, cannot exceed 40 characters, and cannot contain any of the following special characters: **" \ / [ ] : | < > + = ; , ? * % &**
- The group description is optional and cannot exceed 99 characters.

Create Users

You create users and then place them in the appropriate groups.

1. In the **Groups/Users** pane select the group that the user should belong to, click the **New Group/User** button, and then select **Create User**.
2. In the Create User dialog box, on the User Account tab, enter the following information:
   - **User name.** Cannot exceed 40 characters and cannot contain any of the following special characters: **" \ / [ ] : | < > + = ; , ? * % &**
   - **Login name.** The name that the user uses to log into the system. The Login name must be unique, cannot exceed 40 characters, and cannot contain special characters.
   - **User Mode.** Available options are:
     - **Unspecified.** Leaves the user without a particular mode. Select this option if your system does not work with user modes, or if the system works with user modes but you want this user to see KPIs for both modes in Service Health views.
     - **Operations User.** Enables the user to view the operations version of KPIs.
     - **Business User.** Enables the user to view the business version of KPIs.
   - **Time zone.** The time zone of the user's location.

     Note: When you modify the time zone, the linked recipient offset from GMT is also updated after you confirm the change. Half time zones (also known as offset time zones) are not supported.
   - **Password** and **Confirm password.** The password cannot exceed 20 characters.
3. **(Optional)** On the Recipient tab, enter required information. For information about the fields on this tab, see "New or Edit Recipient Dialog Box" on page 187.

After creating a user, you can modify user information in the Groups/Users page. For user interface details, see "Groups/Users Pane" on page 127.

Set Default Time Zone for New User Creation

APM enables you to set a default time zone for new user creation. When creating new users in APM (with or without LDAP), you can set up a timezone for that specific user. This enables you to change the time zone for a certain group of users or for all groups at one time.

1. Select **Admin > Platform > Setup and Maintenance > Infrastructure Settings**.
2. Select **Foundations**.
3. Select **Business Service Management Interface**.
4. In the Business Service Management Interface - Display table, edit **Default Time Zone** for user creation. You must specify the specific name of the time zone, such as Africa/Accra or Asia/Jerusalem. For a list of time zone, see

   ```
   HPBSM\AppServer\resources\ApplicationResources2.properties

   # Time Zones presentations  section
   ```

   The setting should contain a string such as: `ACT or Africa/Accra or Asia/Jerusalem`

Assign Permissions to Groups or Users

APM enables you to apply permissions to groups and users for specific resources and instances of those resources that are defined in the system. For more information about permissions, see "Permissions" on page 130.

1. In the **Groups/Users** pane, select the groups or users that you need to assign permissions to, and select the **Permissions** tab on the right side of the page.
2. Select a context for the groups or users from the **Context** dropdown list. For details on the available contexts, see "Resource Contexts" on page 179.
3. Select the required roles for the groups or users from the **Roles** dropdown list. For details on the available roles, see " User Management Roles Applied Across APM" on page 151.
4. **(Optional)** On the **Operations** tab, select the operations that the groups or users can perform. For details on the available operations, see "User Management Operations" on page 166.

Note: After you have changed user permissions, the user needs to log out of APM and log in again for the changes to take effect.

Configure User and Group Hierarchy

In the Hierarchy tab, you set user and group hierarchy by adding users to groups and nesting groups within other groups.

Note:

- When deleting a parent group, the child groups and users are not deleted.
- If APM groups have been synchronized with groups on an external LDAP server, APM users cannot be moved between groups, and only groups appear on the interface. For details on synchronizing groups, see "Synchronizing Users" on page 231.

1. Ensure that you have configured at least one group and one user in the **Groups/Users** pane.
2. Select a group or user in the **Groups/Users** pane, and select the **Hierarchy** tab on the right side of the page to view the parent and child groups of the group or user.
3. In the Hierarchy tab, click the **Edit Child Groups and Users** button.
4. Use the  or  buttons to add or remove groups or users from the list of nested items.

Customize User Settings

You can customize user settings to:

- Select the default context that is displayed for specific users or groups when they log into APM.
- Specify the first page that is displayed for specific users or groups in each of the different parts of APM.
- Select contexts, applications, tabs, and options that are available for users or groups.

You can customize settings for individual users or for all users in a group, including all members of sub-groups that are part of a parent group. If you restrict access to a feature or report for a group, all members of that group do not have access to the feature and you cannot override the setting for individual users.

Users who are members of more than one group, assume the restrictions of both groups. For example, the members of Group A are restricted from accessing all applications except App1 and App2, and the members in Group B are restricted from accessing all applications except App2 and App3. Therefore, users who are members of both Group A and Group B only have access to App2.

If you add users or sub-groups to a group that has group settings applied, the users or members of the sub-groups automatically get the access restrictions that were applied to the parent group.

Note: For the Service Health application, you cannot define user access to specific pages; you can only enable or disable user access at the application level.

For a use-case scenario related to this task, see "How to Customize User Menus — Use-Case Scenario" on page 148.

1. Select a group or user in the **Groups/Users** pane, and select the **Customization** tab on the right side of the page.
2. Select a context from the **Contexts** pane that you want to be the default entry context that this user or all users in a group see when they log into APM, and click **Set as Default Entry Context**.

   Note: The **Default Entry Page** icon  appears next to the specified context.
3. In the **Contexts** pane, clear the check boxes of the contexts and applications that you want hidden from the user or all members of the group.
4. In the **Pages and Tabs** pane, select the pages and tabs that you want to be visible on the selected context for the user or group.
5. If required, select a default page or tab for each context that appears by default when the user opens that context.

Configure and Manage Recipients

You create recipients by defining one or more notification methods, the template to use for alert notices, and a notification schedule to receive reports.

You create recipients and manage existing recipients in the Recipients page. For user interface details, see "Configure and Manage Recipients" on page 184.

How to Configure Users and Permissions – Use-Case Scenario

This use-case scenario describes how to configure users and groups in the User Management portal.

Note: For a task related to this scenario, see "Configuring Users and Permissions - Workflow" on page 139.

1. ## *Mapping Out Users and Groups*

   Jane Smith is the System Administrator at NewSoft Company, and wants to configure users and groups to be authorized to use APM, as well as end users who will be accessing Service Health and reports. Before doing so, she requests the following preliminary information from relevant staff members:

   - User names
   - Login names
   - Initial Passwords
   - User Time Zones
   - Contact Information (for example, telephone number, pager, and email address)

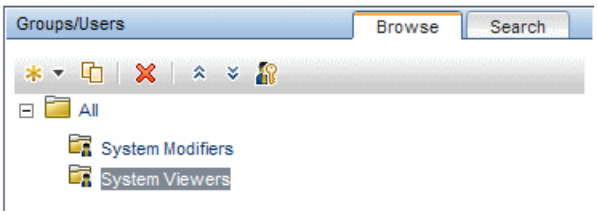
   With this information, she then decides to create one group with the permission level of System Modifiers, and another with the permission level of System Viewers. Further, one of the users is assigned additional roles of SiteScope Administrator.

2. ## *Creating Groups*

   Jane groups users together according to the level of permissions they are to be granted. She clicks the **New Group/User** button in the **Groups/Users** pane and creates the following groups:

   - System Viewers
   - System Modifiers

   The **Groups/Users** pane appears as follows:

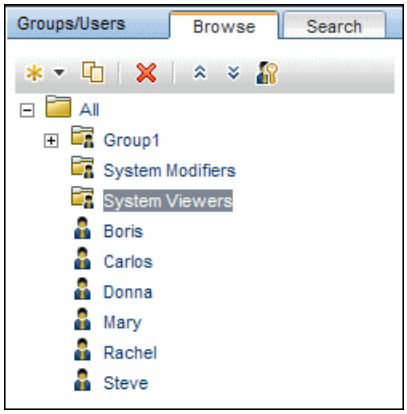
   

3. ## *Assigning Permissions to Groups*

   Once the groups have been created, Jane assigns the relevant permission levels to the groups. After selecting **System Modifiers** in the **Groups/Users** pane, she navigates to the **Permissions** tab in the **Information** pane, and selects the Root instance (**Enterprise**) from any context. In the **Roles** tab, she selects **System Modifier** and then clicks **Apply Permissions**. She then selects **System Viewers** in the **Groups/Users** pane and selects **System Viewer** in the **Roles** tab, clicking **Apply Permissions**.

4. ## *Creating Users*

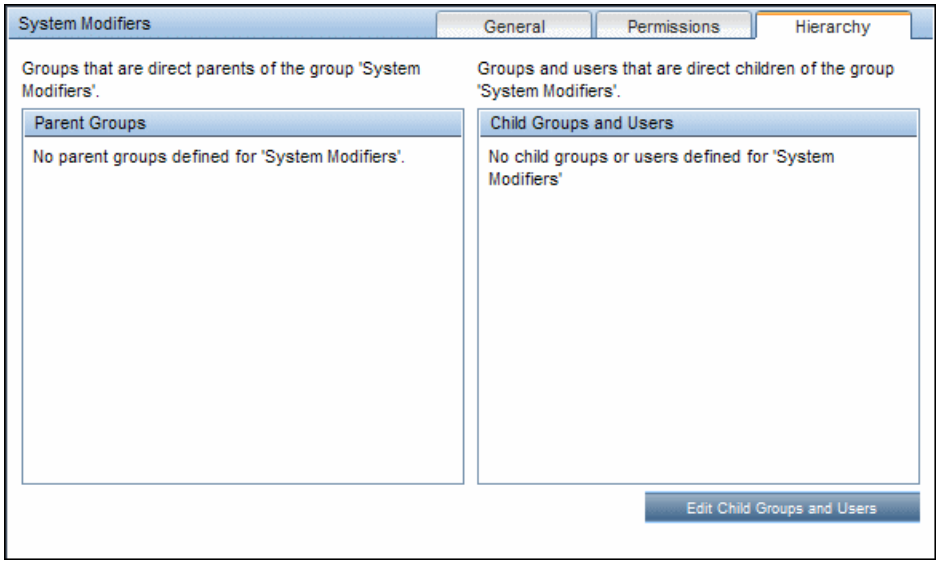
Jane must now create users to nest within the groups, based on the required permission levels of the individual users. She clicks the **New Group/User** button in the **Groups/Users** pane and while on the Root group, (**All**), she selects **Create User** and configures settings for each new user. The **Groups/Users** pane appears as follows:



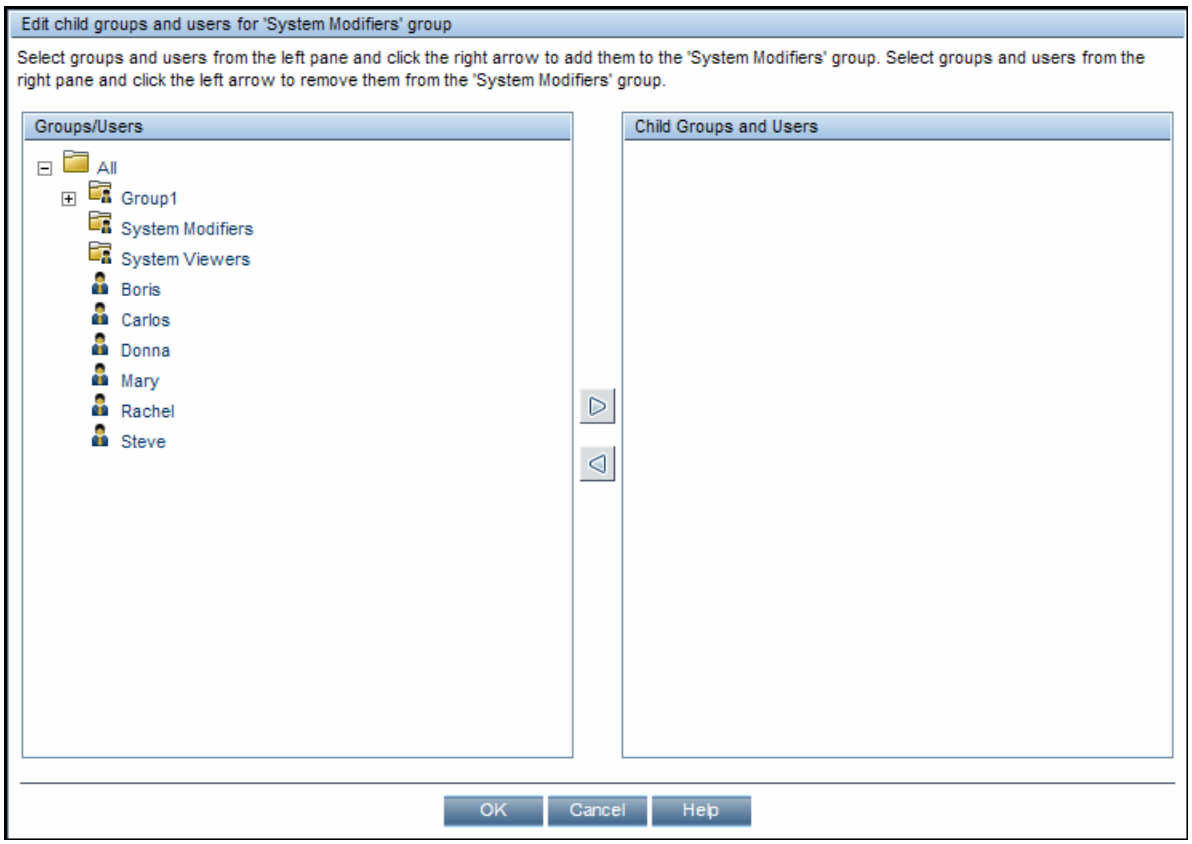
5. ## *Configuring User and Group Hierarchy*

Now that Jane has created users authorized to access APM, she assigns their permission level by nesting them within the appropriate group.

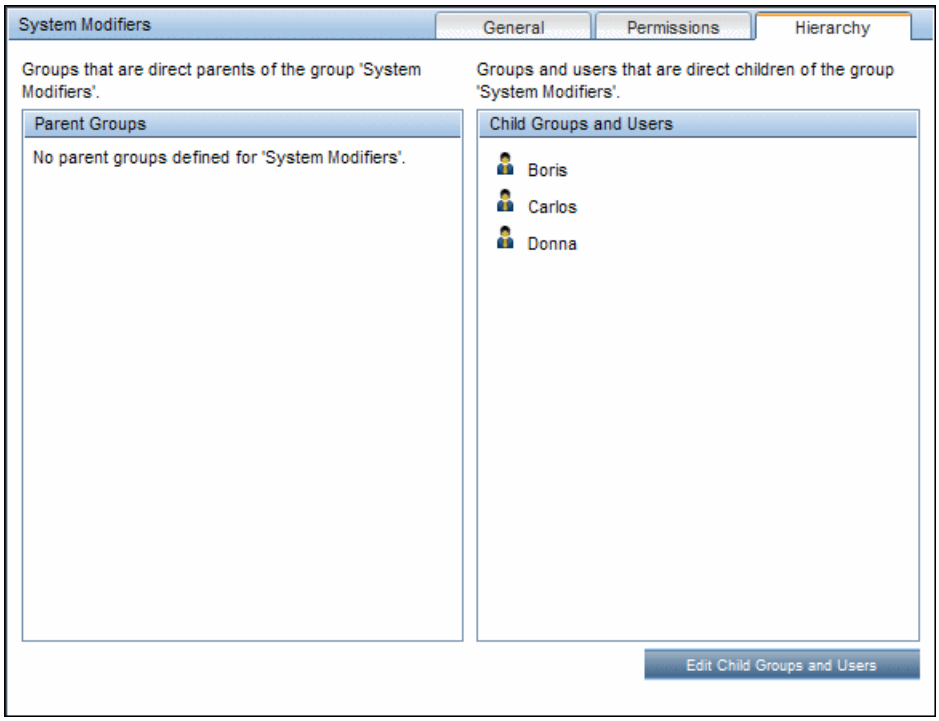
She selects the **System Modifiers** group from the **Groups/Users** pane to nest the appropriate users in this group. Jane then selects the **Hierarchy** tab from the **Information** pane on the right side of the page. The hierarchy tab indicates that the System Modifiers group has no child groups, as follows:



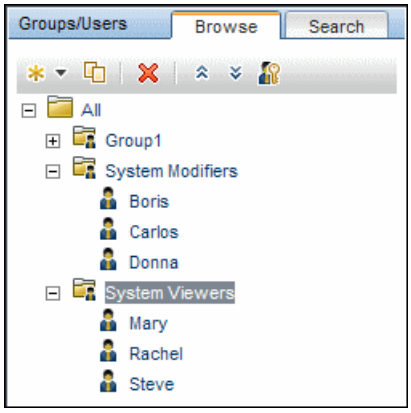
Jane clicks the **Edit Child Groups and Users** button to open the Edit Child Groups and Users dialog box:



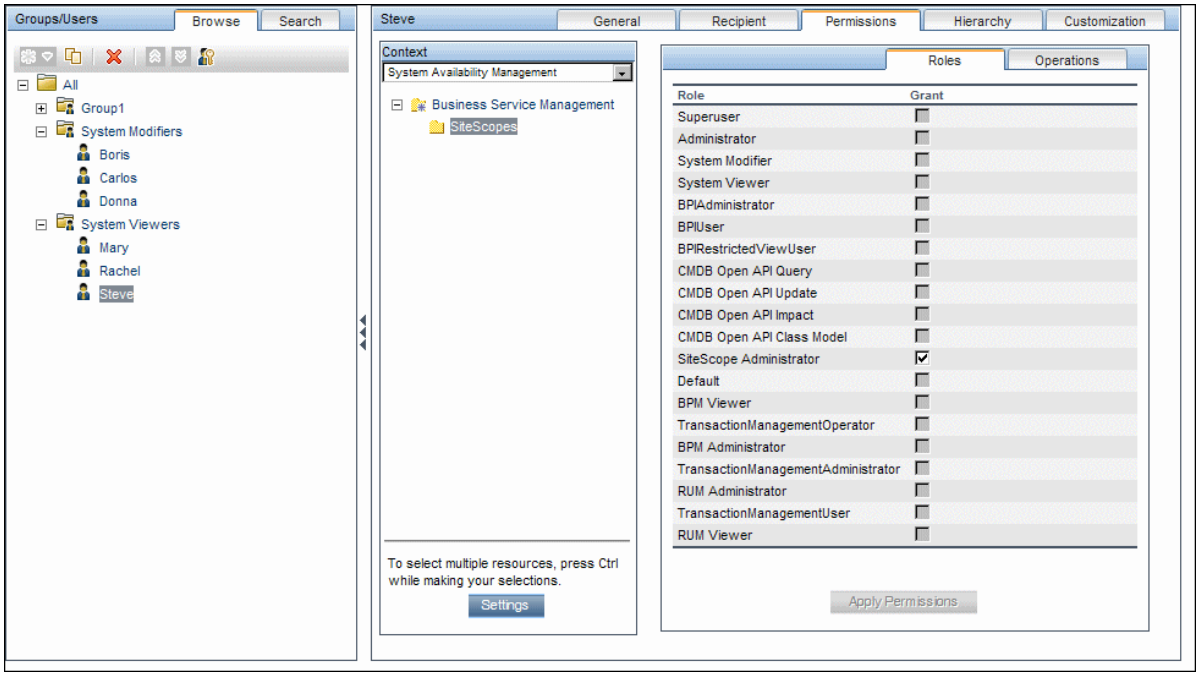
She then selects the relevant users from the **Groups/Users** pane and clicks the right arrow to move them to the **Child Groups and Users** pane. The Hierarchy tab indicates that these users are nested within the System Modifiers group, as follows:



After following the same procedure to nest the relevant users in the System Viewers group, the **Groups/Users** pane is displayed as follows:



Since Steve has the added permission level of SiteScope Administrator, Jane selects the username of the user in the **Groups/Users** pane whom she wants to give the added permission level of SiteScope Administrator, and in the **Permissions** tab, selects the **System Availability Management** context. After selecting a resource, she then selects **SiteScope Administrator** from the **Roles** tab, and clicks **Apply Permissions**. The resulting screen appears as follows:



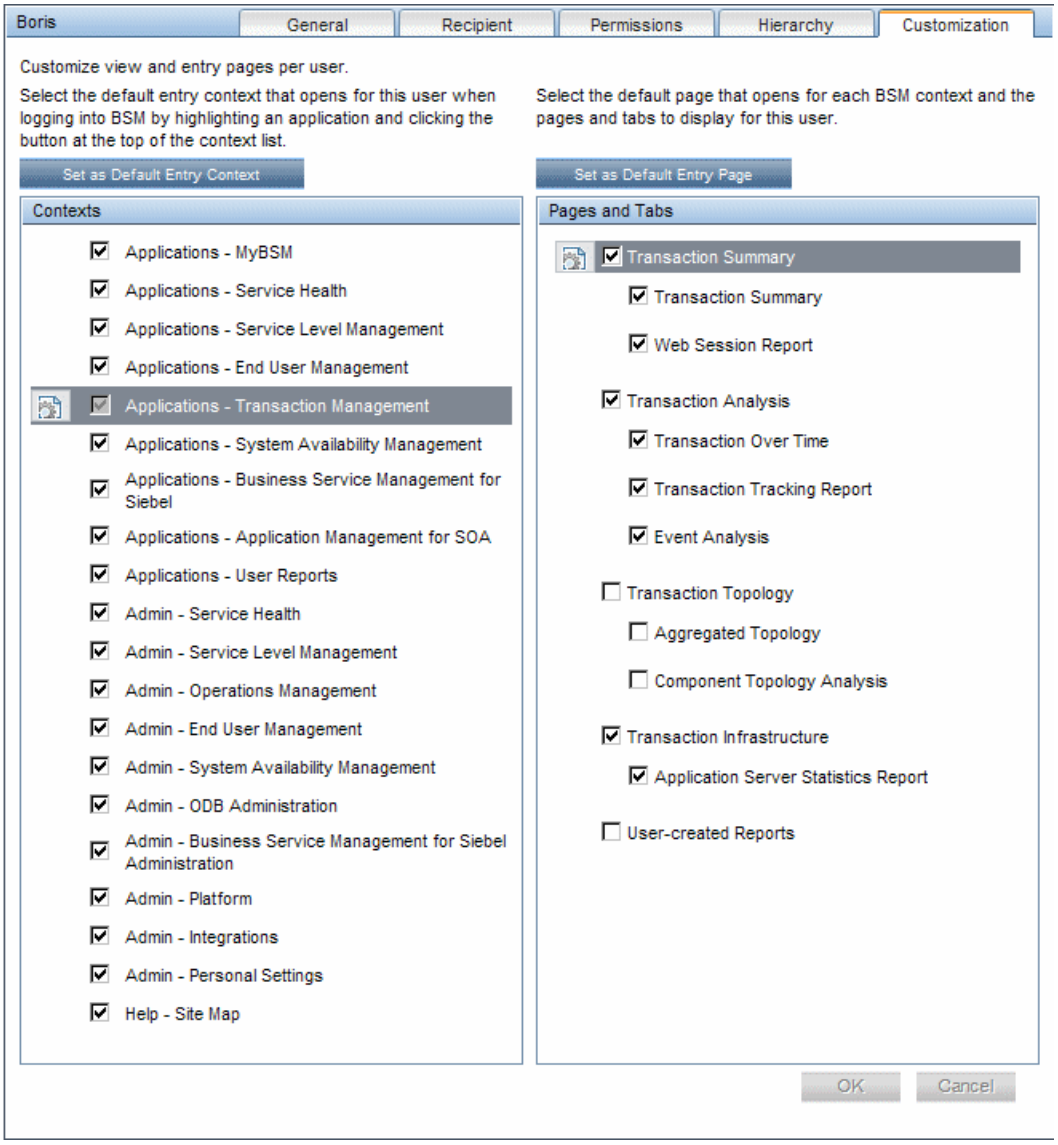
6. *Customizing User Settings*

Jane now sets the page each user sees when entering APM, and the menu items available to them on pages throughout APM. After selecting each user, she clicks the **Customization** tab and sets the following parameters:

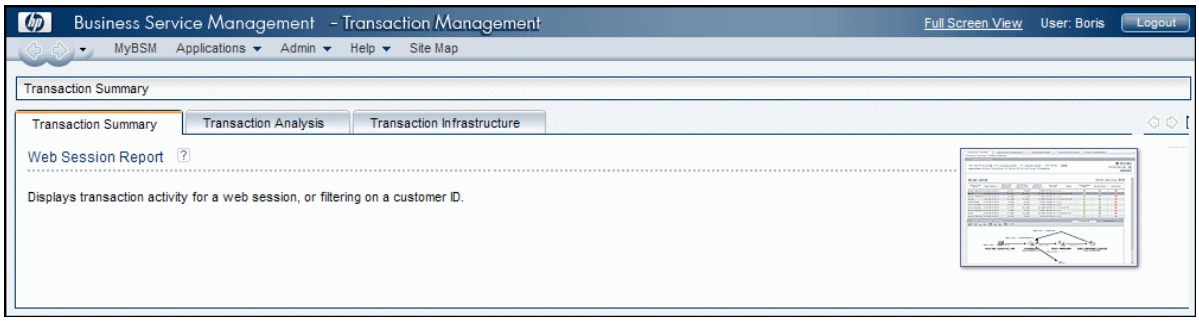
- The entry context that the user sees when logging into APM. For example, **Admin - End User Management**.
- The page within the entry context that the user sees on the selected context. For example, **Reports**.

- The pages and tabs that are to be visible on each APM page by selecting or clearing the relevant check boxes.

The configured settings are displayed on the customization tab as follows:



The login page that the user sees according to the customized configurations is as follows:



How to Customize User Menus – Use-Case Scenario

This use-case scenario describes how to customize user menus for individual users.

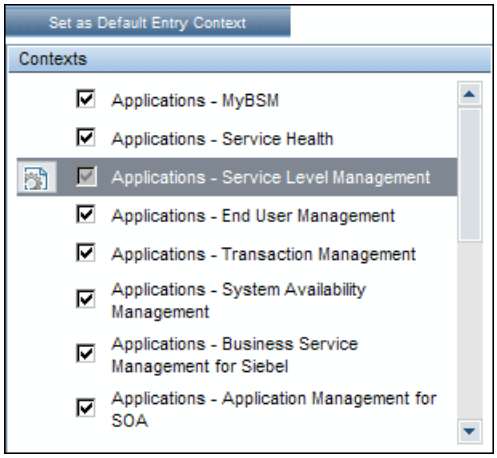
Note: For a task related to this scenario, see "Customize User Settings" on page 142.

1. ***Choosing a User***

   Mary, the administrator of ABC Insurance Company, is creating several users in the User Management section of APM. She decides that the user John Smith should be able to view only certain pages and tabs in APM, and that a specific page should appear on his screen when he logs into APM.

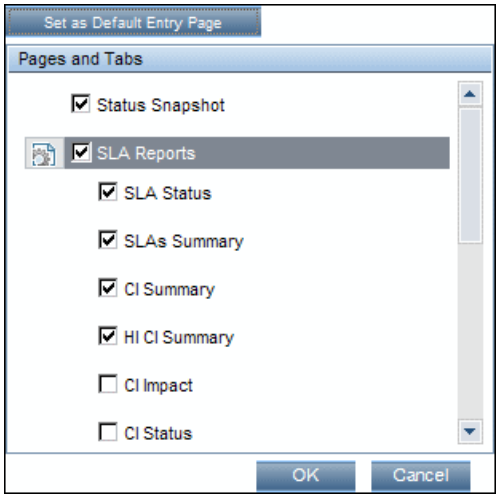
2. ***Assigning a Default Context***

   Since John's chief responsibility at ABC relates to service level management, Mary designates the Applications - Service Level Management page as the default entry context. Mary selects **Applications - Service Level Management** in the Contexts pane, and clicks **Set as Default Entry Context**. The **Applications - Service Level Management** context is indicated as the default entry context with the default entry icon, as appears in the following image:

3. ***Selecting Context Pages and Tabs***

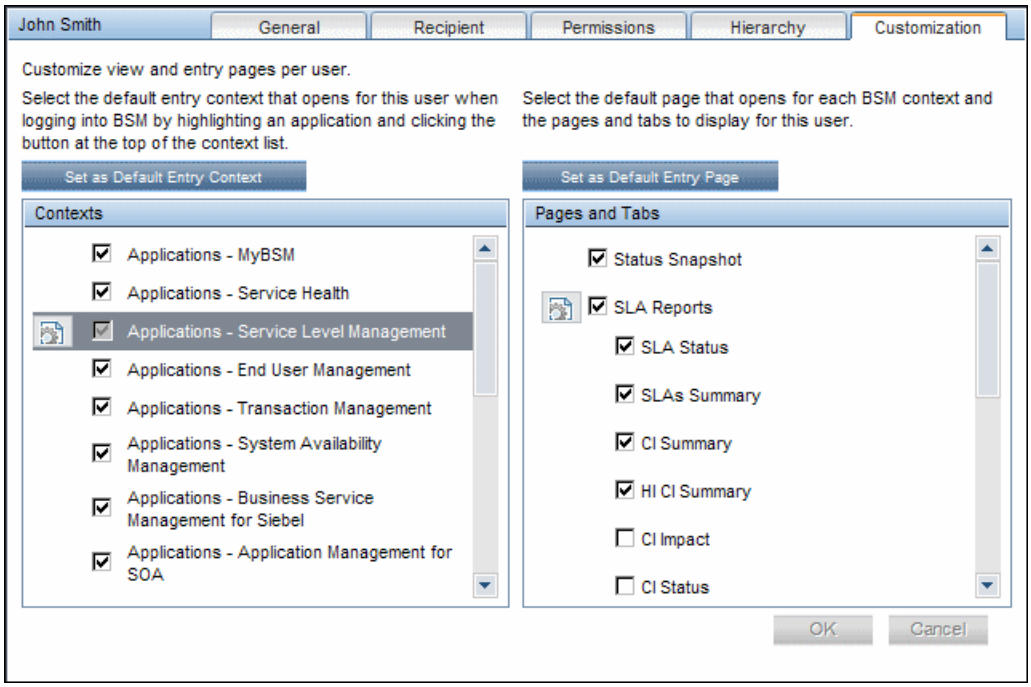
   Since John is not authorized to view Outage Reports, that option is cleared in the Pages and Tabs pane, leaving the remaining pages and tabs checked to be visible when John logs into APM. As SLA Reports are of the highest priority for ABC Insurance, Mary designates this as the first page for John to see upon logging in. She selects **SLA Reports** in the Pages and Tabs pane, and then clicks **Set as Default Entry Page**. **SLA Reports** is indicated as the default entry page with the default entry icon, as appears in the following image:



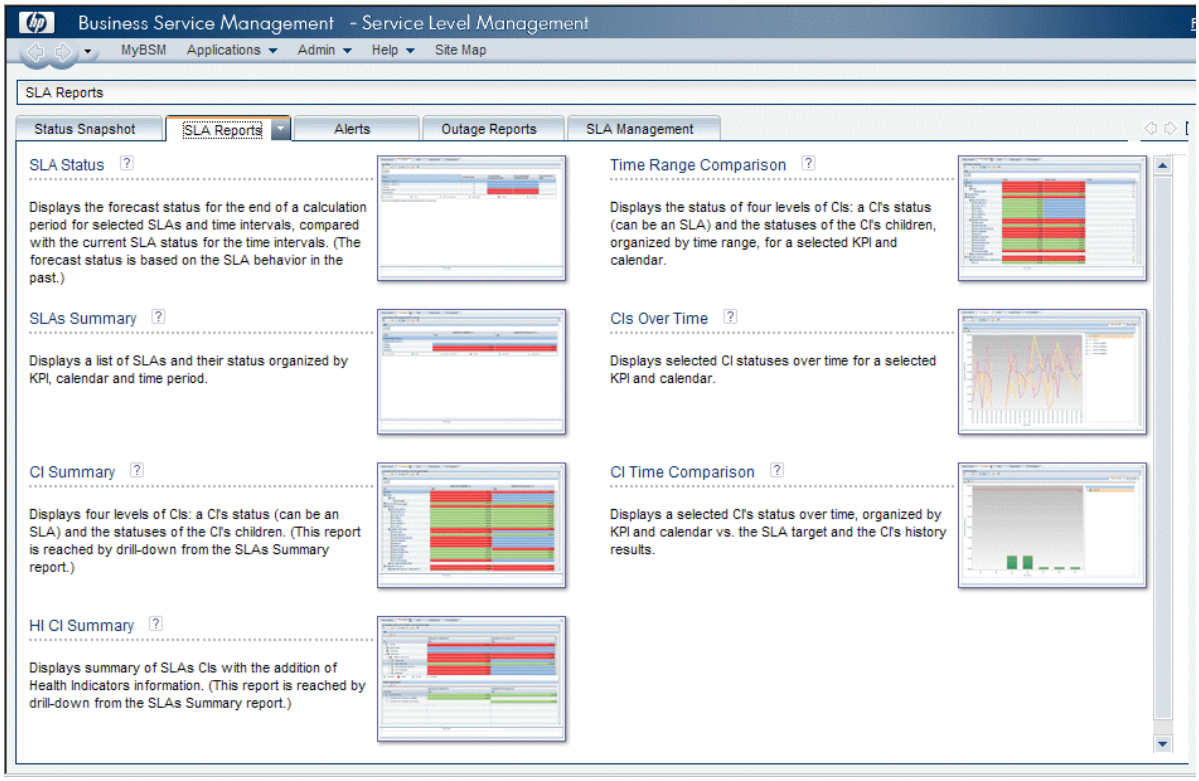
4. ***Results***

The context that opens when John Smith logs into APM is the **Service Level Management** context on the Applications menu. The **SLA Reports** page opens, and the Status Snapshot, Alerts, and SLA Management pages are also available to him.

The configured Customization tab in User Management appears as follows:



Screen that John sees when logging into APM:



How to Export and Import User Information Using the JMX Console

This task describes how use the JMX Console to copy user, role, and permission information from a source system to a target system. For example, if you need to configure a new APM database, you may need to copy user information from an existing database.

Set Contexts to Export

You can limit which contexts will be included in the export. You can view a list of available contexts in the JMX Console:

1. In a browser, enter the following URL:
   http://<SOURCE_Server>:29000/mbean?objectname=BSMPlatform%3Aservice%3DAuthorization+Service
2. Enter your JMX Console user name and password.
3. On the JMX MBean View page, click the **Invoke** button below **java.util.Set listAuthorizationContexts ()**. JMX Console displays all contexts in TAS.

If you need to limit the contexts included in the export:

1. On the source server, open the following file **<APM root directory>\conf\tas\exportedContexts.properties**
2. Modify the **contexts-to-export** property.

Contexts in the **contexts-to-export** property must be separated by commas only, without spaces.

3. Save your changes.

Export

Use JMX Console to create a .zip file that contains .xml files with user, role, and permission information.

1. In a browser, enter the following URL:
http://<SOURCE_Server>:29000/mbean?objectname=Topaz%3Aservice%3DAuthorization+Service+Data+Import+Export
2. On the JMX MBean View page, click the **Invoke** button below **void loadExportedContexts()** and then click the Browser's Back button to return to the JMX MBean View page.
3. Below **void exportAllTasEntities()**, in the **ParamValue** field, enter a location and file name for the export file on the source server. The file name must have a .zip extension for example:
C:\HPBSM\export.zip
4. Click the **Invoke** button below **void exportAllTasEntities()**.

Transfer

You need to copy the export .zip file from the source server to the target server.

1. On the source server, browse to the export file as defined above.
2. Copy the file to the target server.

Import

Import the users, roles and permissions from the .zip file to the target APM system.

Caution: Before you import user and group information, make sure that the target server does not have any created resources, such as reports, profiles, and monitors, that have user information that is not compatible with the information that you are importing.

1. In a browser, enter the following URL:
http://<TARGET_Server>:29000/mbean?objectname=Topaz%3Aservice%3DAuthorization+Service+Data+Import+Export
2. Enter your JMX Console user name and password.
3. Below **void importAllTasEntities()**, in the **ParamValue** field, enter the location and file name of the export file and click the **Invoke** button.

User Management Roles Applied Across APM

This section lists roles that can be applied across all contexts within APM and the resources that each role applies to.

For details about roles that can be applied only to specific contexts, see " User Management Roles Applied to Specific Contexts" on page 164.

The following are the roles that can be applied across all contexts within APM:

- "Superuser" on the next page
- "Administrator" on the next page

- "System Modifier" on page 157
- "System Viewer" on page 160
- "BPM Viewer" on page 162
- "BPM Administrator" on page 163
- "RUM Administrator" on page 163
- "RUM Viewer" on page 163

Superuser

The **Superuser** role can be applied only to the **Application Performance Management** resource.

This role includes all available operations on all the resources in all the contexts. Only a superuser can apply the **Superuser** role to another user.

Caution: The default superuser does not have permissions to write to Application Performance Management from the UCMDB WS API. Specific roles exist for that purpose. For details, see " User Management Roles Applied to Specific Contexts" on page 164.

Administrator

The **Administrator** role can be applied only to the **Application Performance Management** resource.

Administrators have a collection of permissions that enable them to add profiles to the system and manage the resources related to those profiles. After a profile has been added, the administrator has full control privileges on all resources within that profile instance.

Note: A user with the RUM administrator or BPM administrator role must also be assigned the Administrator role.

Diagnostics

Resource	Allowed Operations
Diagnostics	Change View Execute Full Control

End User Management

Resource	Allowed Operations
Alert - Create dependencies	Change
Applications	Add View
BPM Agents	View

Resource	Allowed Operations
RUM Engines	View
Script Repository	Add Change View Delete Full Control

MyBSM

Resource	Allowed Operations
User Pages	Full Control
Predefined Pages	View
	Full Control
User Components	Full Control

Operations Orchestration Integration

Resource	Allowed Operations
Administration	Add Change View Delete Full Control
Execution	Execute Full Control

Platform

Resource	Allowed Operations
Audit Log	View Full Control
Users	Add Change View Delete Full Control

Resource	Allowed Operations
User Groups	Add Change View Delete Full Control
Data Collectors	Change View
Scheduled Reports	Add Change View Delete Full Control
Recipients	Add Change View Delete Full Control
Custom Data Types	Add Change View Delete Full Control
Downtime	View Full Control
Databases	Add Change View Delete Full Control

RTSM

Resource	Allowed Operations
Views	Add Change View Delete Full Control
RTSM	Full Control
CI Search	Full Control

Resource	Allowed Operations
Data Modifier	Full Control
Get Related	Full Control
ITU Manager	Full Control
Modeling Studio	Full Control

Service Health Analyzer

Resource	Allowed Operations
Administration	Full Control
Application	Full Control

Service Level Management

Resource	Allowed Operations
SLAs	Add Change View Delete Full Control

SiteScope On-demand monitors

Resource	Allowed Operations
Administration	Add Change View Delete Full Control
Execution	Execute Full Control

System Availability Management

Resource	Allowed Operations
SiteScopes	Add

User Defined Reports

Resource	Allowed Operations
Custom Reports	Add Change View Full Control
Trend Reports	Add Change View Full Control
Custom Links	Change View Full Control
Excel Reports	Change View Full Control
Default Footer/Header	Change Full Control
Favorite Filter	Change View Delete Full Control
Annotation	Change Delete Full Control
Service Report	Change Delete Full Control
Custom Query Reports	Add View Full Control

System Modifier

The **System Modifier** role can be applied only to the **Application Performance Management** resource.

A system modifier can view and change any resources in APM. There are some resources on which the view or the change operation is not applicable. A system modifier has permissions for only those operations that are available in APM.

Diagnostics

Resource	Allowed Operations
Diagnostics	Change View

End User Management

Resource	Allowed Operations
Alert - Notification Template	Change View
Alert - Create dependencies	Change
Applications	Change View
BPM Agents	View
RUM Engines	View
Script Repository	View Full Control

MyBSM

Resource	Allowed Operations
Pre-defined Pages	View
User Pages	Full Control
User Components	Full Control

Operations Orchestration Integration

Resource	Allowed Operations
Administration	Change View
Execution	Execute

Platform

Resource	Allowed Operations
Audit Log	View
Users	Change View
User Groups	Change View
Data Collectors	Change View
Scheduled Reports	Change View
Recipients	Change View
Custom Data Types	Change View
Send SNMP trap	Change
Run executable file	Change
Log to Event Viewer	Change
Downtime	Full Control
Databases	Change View
System Recipient Template	Change View

RTSM

Resource	Allowed Operations
Views	Change View
CI Search	Full Control
Get Related	Full Control
ITU Manager	Full Control
Modeling Studio	Full Control

Service Health Analyzer

Resource	Allowed Operations
Administration	Full Control
Application	Full Control

Service Level Management

Resource	Allowed Operations
SLAs	Change View

SiteScopeOn demand monitors

Resource	Allowed Operations
Administration	Change View
Execution	Execute

System Availability Management

Resource	Allowed Operations
SiteScopes	Change View

User Defined Reports

Resource	Allowed Operations
Custom Reports	Add Change View
Trend Reports	Add Change View
Custom Links	Change View
Excel Reports	Change View
Default Footer/Header	Change

Resource	Allowed Operations
Favorite Filter	Change View Delete
Annotation	Change Delete
Service Report	Change Delete
Custom Query Reports	Add View

System Viewer

The System Viewer role can be applied only to the **Enterprise** resource.

A system viewer can only view resources within APM and does not have permission to change, add, or delete any resources or resource instance with the exception of the RUM Engine resource. There are some resources on which the view operation is not applicable, a system viewer has no access to those resources.

Diagnostics

Resource	Allowed Operations
Diagnostics	View

End User Management

Resource	Allowed Operations
Alert - Notification Template	View
Applications	View
BPM Agents	View
RUM Engines	View Edit
Script Repository	View

MyBSM

Resource	Allowed Operations
Predefined Pages	View

Operations Orchestration Integration

Resource	Allowed Operations
Administration	View

Platform

Resource	Allowed Operations
Audit Log	View
Users	View
User Groups	View
Data Collectors	View
Scheduled Reports	View
Recipients	View
Custom Data Types	View
Downtime	View
Databases	View
System Recipient Template	View

RTSM

Resource	Allowed Operations
Views	View
CI Search	Full Control
Get Related	Full Control
ITU Manager	Full Control
Modeling Studio	Full Control

Service Health Analyzer

Resource	Allowed Operations
Administration	Full Control
Application	Full Control

Service Level Management

Resource	Allowed Operations
SLAs	View

SiteScopeOn demand monitors

Resource	Allowed Operations
Administration	View

System Availability Management

Resource	Allowed Operations
SiteScopes	View

User Defined Reports

Resource	Allowed Operations
Custom Reports	Add View Edit (only if you are the user who created the report) Delete (only if you are the user who created the report)
Trend Reports	Add View Edit (only if you are the user who created the report) Delete (only if you are the user who created the report)
Custom Links	View
Excel Reports	View
Favorite Filter	View
Custom Query Reports	Add View

BPM Viewer

The **BPM Viewer** role can be applied only to the **Enterprise** resource.

These users have view permissions, but cannot modify transaction threshold settings and transaction descriptions.

Any regular user who was added as a user on a specific application in the previous version is upgraded to the BPM Viewer role for that application.

Resource	Allowed Operations
Applications	View
BPM Agents	View
Script Repository	View

BPM Administrator

The **BPM Administrator** role can be applied only to the **Enterprise** resource.

The BPM Administrator can manage all of the platform's BPM applications, including permissions.

Any administrator who was added as a user on a specific BPM application in the previous version is upgraded to the BPM application administrator role for that application. This is in addition to being assigned the administrator role as described above (for details, see "Administrator" on page 152).

Resource	Allowed Operations
Applications	Add Change View Delete Execute Full Control
BPM Agents	View
Script Repository	Add Change View Delete Full Control

RUM Administrator

The **RUM Administrator** role can be applied only to the **Enterprise** resource.

Resource	Allowed Operations
Applications	Add Change View Delete Execute Full Control
RUM Engines	View

RUM Viewer

The **RUM Viewer** role can be applied only to the **Enterprise** resource.

These users have view permissions, but can modify transaction threshold settings and transaction descriptions.

Any regular user who was added as a user on a specific RUM profile in the previous version is upgraded to the **RUM Viewer** role for that profile.

Resource	Allowed Operations
Applications	View
RUM Engines	View

User Management Roles Applied to Specific Contexts

The following roles can be applied only to specific contexts within APM. Details of the resources and contexts on which roles can be applied appear within the description of each role below.

For details about roles that can be applied across APM, see " User Management Roles Applied Across APM" on page 151.

CMDB Open API Query

The **CMDB Open API Query** role can be applied only to the **RTSM Open API** resource in the **RTSM** context.

This role enables users to query the CMDB (Configuration Management Database) for communication with third-party applications.

Context	Resource	Allowed Operations
RTSM	RTSM Open API	View

CMDB Open API Update

The **CMDB Open API Update** role can be applied only to the **RTSM Open API** resource in the **RTSM** context.

This role enables users to update the CMDB (Configuration Management Database) for communication with third-party applications.

Context	Resource	Allowed Operations
RTSM	RTSM Open API	Change

CMDB Open API Impact

The **CMDB Open API Impact** role can be applied only to the **RTSM Open API** resource in the **RTSM** context.

This role enables users to impact operations on the CMDB.

Context	Resource	Allowed Operations
RTSM	RTSM Open API	View

CMDB Open API Class Model

The **CMDB Open API Class Model** role can be applied only to the **RTSM Open API** resource in the **RTSM** context.

This role enables users to perform operations on CITs.

Context	Resource	Allowed Operations
RTSM	RTSM Open API	View

SiteScope Administrator

The **SiteScope Administrator** role can be applied only to the **SiteScope**s resource in the **System Availability Management** context or specific instances of the resource.

When granted this role at the resource collection level, the SiteScope administrator can manage all of the platform's SiteScopes, including permissions on the SiteScopes. When granted this role at the instance level, the administrator can manage only those resources associated with the specific SiteScope instance.

Any administrator who was added as a user on a specific SiteScope in the previous version is upgraded to the SiteScope administrator role for that SiteScope.

Context	Resource	Allowed Operations
System Availability Management	SiteScopes	Add Change View Delete Execute Full Control

Default

The **Default** role is automatically assigned if no other role was selected. It allows very limited permissions.

Note: To create meaningful reports, the user will likely need additional permissions to specific applications or configuration items.

Context	Resource	Allowed Operations
User Defined Reports	Custom Reports	Add Edit (only if you are the user who created the report) Delete (only if you are the user who created the report)
	Trend Reports	Add Edit (only if you are the user who created the report) Delete (only if you are the user who created the report)

User Management Operations

Within each context listed below is a table listing:

- Every resource
- Which operations can be applied to that resource
- A description of what the operation enables

Diagnostics

The **Diagnostics** context enables you to define operations permitted for the Diagnostics application.

Resources	Operation	Description
Diagnostics	Change	Enables viewing Diagnostics administration and configuring the Diagnostics settings.
	View	Enables viewing Diagnostics when accessing Diagnostics from APM.
	Execute	Enables changing the settings in the Diagnostics UI, such as setting thresholds.
	Full Control	Enables performing all operations on Diagnostics, and granting and removing permissions for those operations.

End User Management

The **End User Management** context enables you to define the operations permitted for the End User Management application. Operations assigned to a folder affect all folders contained beneath it.

Resources		Operation	Description
Alert - Notification Template		Change	Enables editing the properties of a customer-specific notification template.
		View	Enables viewing the properties of a notification template.
		Full Control	Enables performing all available operations on a notification template, and granting and removing permissions for those operations.
Alert - Create dependencies		Change	Enables creating and removing dependencies between alerts.
		Full Control	Enables creating and removing alert dependencies, and granting and removing permissions for those operations.
Applications		Add	Enables adding applications.
		Change	Enables editing applications, or a specific instance of applications.
		View	Enables viewing applications. Applies to End User Management (administration and reports) only.
		Delete	Enables deleting applications, or a specific instance of applications.
		Execute	Enables starting and stopping applications, or a specific instance of applications.
		Full Control	Enables performing all available operations on applications, or a specific instance of applications, and granting and removing permissions for those operations.
Applications (specific instances)	BPM	Add	Enables creating a Business Process configuration for a specific instance of applications.
		Change	Enables editing a Business Process configuration for a specific instance of applications.
		View	Enables viewing a Business Process configuration for a specific instance of applications.
		Delete	Enables deleting a Business Process configuration for a specific instance of applications.
		Execute	Enables activating and disabling a Business Process configuration for a specific instance of applications.
		Full Control	Enables performing all available operations on a Business Process configuration for a specific instance of applications.

Resources		Operation	Description
	RUM	Add	Enables creating a Real User Monitor configuration for a specific instance of applications.
		Change	Enables editing a Real User Monitor configuration for a specific instance of applications.
		View	Enables viewing a Real User Monitor configuration for a specific instance of applications.
		Delete	Enables deleting a Real User Monitor configuration for a specific instance of applications.
		Execute	Enables activating and disabling a Real User Monitor configuration for a specific instance of applications.
		Full Control	Enables performing all available operations on a Real User Monitor configuration for a specific instance of applications.
	Alert	View	Enables viewing an Alert configuration for a specific instance of applications.
		Full Control	Enables performing all available operations on an Alert configuration for a specific instance of applications.
BPM Agents		View	Enables viewing BPM agents and managing monitors on those agents.
RUM Engines		View	Enables viewing Real User Monitor engines and managing RUM configurations on those engines.
Script Repository		Add	Enables creating new folders in the script repository.
		Change	Enables renaming script repository folders and modifying scripts in those folders.
		View	Enables viewing script repository folders and the scripts in those folders, as well as downloading scripts from the script repository. **Note:** This does not enable uploading scripts to the script repository.
		Delete	Enables deleting folders in the script repository.
		Full Control	Enables performing all available operations on script folders and scripts in the script repository, and granting and removing permissions for those operations.

MyBSM

The **MyBSM** context enables you to define the operations permitted for user pages, predefined pages, and user components

Resources	Operation	Description
User Pages	Add	Enables creating new user pages.
	Change	Enables changing the user page on which this permission occurs.
	View	Enables viewing/opening the user page on which this permission occurs.
	Delete	Enables deleting the user page on which this permission occurs.
	Locked	Enables users to monitor information, but not to select a view or apply filters on a page. For details, see User Permissions in MyBSM in the APM User Guide.
	Full Control	Enables all the above permissions.
Predefined Pages	View	Enables viewing/opening the predefined page on which this permission occurs.
	Full Control	Enables granting permissions to predefined pages.
User Components	Add	Enables creating new user defined components.
	Change	Enables changing the definition of the user defined component on which this permission occurs.
	View	Enables viewing the component on which this permission occurs. **Note:** If you are viewing a page and don't have permission for a component in it, the page will appear without the component.
	Delete	Enables deleting the component definition for the component on which this permission occurs.
	Full Control	Enables all the above permissions.

Operations Orchestration Integration

The **Operations Orchestration Administration** context enables you to define the operations permitted for the Operations Orchestration Administration application.

Resources	Operation	Description
Administration	Add	Enables adding a run book.
	View	Enables viewing run book administration.
	Change	Enables editing run book administration.
	Delete	Enables deleting a run book.
	Full Control	Enables performing all available operations on run book administration, and granting or removing permissions for other users.

Resources	Operation	Description
Execution	Execute	Enables run book execution.
	Full Control	Enables performing all available operations on run book execution, and granting or removing permissions for other users.

Platform

The **Platform** context includes all the resources related to administering the platform.

Resources	Operation	Description
Authentication Strategy	Change	Enables creating and changing configurations on the Authentication Management page.
	View	Enables viewing the Authentication Management page.
	Full Control	Enables performing all available operations on the Authentication Management page.
Audit Log	View	Enables viewing the audit log.
	Full Control	Enables viewing the audit log, and granting and removing permission to view the audit log.
Users	Add	Enables adding users to the system.
	Change	Enables modifying user details.
	View	Enables viewing user details.
	Delete	Enables deleting users from the system.
	Full Control	Enables performing all available operations on users, and granting and removing permissions for those operations.
User Groups	Add	Enables adding user groups to the system.
	Change	Enables modifying user group details.
	View	Enables viewing user group details.
	Delete	Enables deleting user groups.
	Full Control	Enables performing all available operations on user groups, and granting and removing permissions for those operations.

Resources	Operation	Description
Data Collectors	Change	Enables performing remote upgrades, remote uninstalls, and settings updates on data collectors in Data Collector Maintenance.
	View	Enables viewing the data collectors in Data Collector Maintenance.
	Delete	Enables removing data collector instances.
	Full Control	Enables performing all available operations in Data Collector Maintenance, and granting and removing permissions for those operations.
Notification System	View	Enables viewing system tickets details.
	Execute	Enables executing system tickets in the system.
	Full Control	Enables performing all available operations on System Tickets, and granting and removing permissions for those operations.
Scheduled Reports	Add	Enables creating new scheduled reports.
	Change	Enables modifying scheduled reports.
	View	Enables viewing scheduled reports.
	Delete	Enables deleting scheduled reports.
	Full Control	Enables performing all available operations on scheduled reports, and granting and removing permissions for those operations.
Recipients	Add	Enables adding recipients to the platform.
	Change	Enables editing recipient details.
	View	Enables viewing recipients and recipient details.
	Delete	Enables deleting recipients from the platform.
	Full Control	Enables performing all available operations on recipients, and granting and removing permissions for those operations.
Custom Data Types	Add	Enables adding custom data types to the system.
	Change	Enables modifying custom data types in the system.
	View	Enables viewing custom data types in the system.
	Delete	Enables deleting custom data types in the system.
	Full Control	Enables performing all available operations on sample types, and granting and removing permissions for those operations.

Resources	Operation	Description
Send SNMP trap	Change	Enables selecting the option to send SNMP traps on alert, editing SNMP trap addresses, and clearing the option to send SNMP traps on alert.
	Full Control	Enables performing all available operations on sending SNMP traps on alerts, and granting and removing permissions for those operations.
Run executable file	Change	Enables selecting the option to run an executable file on alert, selecting and edition executable files to run on alert, and clearing the option to run an executable file on alert.
	Full Control	Enables performing all available operations on running an executable file on alert, and granting and removing permissions for those operations.
Log To Event Viewer	Change	Enables selecting whether alerts should be logged in the Windows Event Viewer which is accessed from Window Administrative Tools.
	Full Control	Enables selecting whether alerts should be logged in the Windows Event Viewer, and granting and removing permissions on that operation.
Downtime	View	Enables viewing downtime properties
	Full Control	Enables performing all available operations on downtimes, and granting and removing permissions for those operations.
Databases	Add	Enables adding profile databases to the system.
	Change	Enables modifying profile database details in database management.
	View	Enables viewing profile database management details.
	Delete	Enables deleting profile databases from the system.
	Full Control	Enables performing all available operations on profile databases in database management, working with the purging manager, and granting and removing permissions for those operations.
System Recipient Template	Add	Enables creating and cloning system recipient templates.
	Change	Enables editing system recipient templates properties.
	View	Enables viewing system recipient templates properties.
	Delete	Enables deleting a system recipient templates.
	Full Control	Enables performing all available operations on system recipient templates, and granting and removing permissions for those operations.

Resources	Operation	Description
Customer Recipient Template	Add	Enables adding a customer-specific recipient template.
	Change	Enables editing a customer-specific recipient template.
	View	Enables viewing the properties of a customer-specific recipient template.
	Delete	Enables deleting a customer-specific recipient template.
	Full Control	Enables performing all available operations on a customer-specific recipient template, and granting and removing permissions for those operations.
Package Work Manipulation (HPE Software-as-a-Service only)	Change	Enables modifying package locations, renaming packages, and selecting recipients for package notifications.
	View	Enables viewing package information.
	Delete	Enables removing packages from a location.
	Full Control	Enables performing all available operations on package information, and granting and removing permissions for those operations.

RTSM

The **RTSM** context enables you to define the operations permitted for the views defined in IT Universe Administration and viewed in the Model Explorer, Service Health, and Service Level Management.

Tip: If a user has permissions on a view in RTSM, all the profiles that are in that view are visible to the user, even if the user does not have permissions on the profile. To prevent a user from viewing profiles for which the user does not have permissions while enabling the user to access a view, create a view for the user including only those configuration items for which you want the user to have permissions and grant the user permission on that view.

Resources	Operation	Description
Views	Add	Enables adding and cloning views.
	Change	Enables editing views.
	View	Enables viewing views
	Delete	Enables removing views.
	Full Control	Enables performing all available operations on views.
RTSM	Full Control	Enables administrative operations for all of the Run-time Service Model (RTSM), except ITU Manager and Modeling Studio.
CI Search	Full Control	Enables the CI Search option from any location in the RTSM.

Resources	Operation	Description
Data Modifier	Full Control	Enables the Data Modifier option from any location in the RTSM.
Get Related	Full Control	Enables the Get Related CIs option from any location in the RTSM.
ITU Manager	Full Control	Allows the user to enter the ITU Manager. Once inside, the available functionality within the ITU Universe Manager depends on permissions the user has been granted on views.
Modeling Studio	Full Control	Allows the user to enter the Modeling Studio. Once inside, the available functionality within the ITU Universe Manager depends on permissions the user has been granted on views.
RTSM Open API	Change	Enables running of updates in RTSM Open API.
	View	Enables running of queries in RTSM Open API.

Service Health

Resources	Operation	Description
User Pages	Add	Enables adding user pages.
	Change	Enables editing user pages.
	View	Enables viewing user pages.
	Delete	Enables removing user pages.
	Full Control	Enables performing all available operations on user pages.
Predefined Pages	View	Enables viewing predefined pages.
User Components	Add	Enables adding and cloning component definitions.
	Change	Enables editing component definitions.
	View	Enables viewing component definitions.
	Delete	Enables removing component definitions.
	Full Control	Enables performing all available operations on component definitions.

Service Health Analyzer

The **Service Health Analyzer** context enables you to define the operations permitted for the Service Health Analyzer application.

Resources	Operation	Description
SHA application	Full Control	Enables performing all available operations on the SHA application, including permission management
SHA administration	Full Control	Enables performing all available operations on the SHA administration, including permission management

Service Level Management

Use the **Service Level Management** context to assign permissions to all SLAs or specific instances.

Resources	Operation	Description
SLAs	Add	Enables adding SLAs.
	Change	Enables renaming SLAs, adding descriptions to SLAs, viewing SLA configuration in administration pages, and changing SLA configurations.
	View	Enables generating and viewing reports and custom reports on SLAs.
	Delete	Enables deleting SLAs.
	Full Control	Enables performing all available operations on SLAs, and granting and removing permissions for those operations.

System Availability Management

Use the **System Availability Management** context to assign permissions to the various SiteScopes configured within the system.

Note: The permission levels granted in the System Availability Management context override any permission levels granted in the SiteScope standalone interface.

Resources	Operation	Description
SiteScopes	Add	Enables adding SiteScope profiles to System Availability Management.
	Change	Enables modifying a SiteScope profile in System Availability Management and enables adding the contents to the SiteScope root node (group, alert, report) and modifying contents to the SiteScope root node (alert, report), if the user has permissions for these resources.
	View	Enables viewing SiteScope profiles in System Availability Management.
	Delete	Enables deleting a SiteScope profile from System Availability Management and enables deleting the contents of the SiteScope root node (alert, report), if the user has permissions for these resources.
	Execute	Enables executing contents of the SiteScope root node (alert, report), if the user has permissions for these resources.
	Full Control	Enables performing all available operations on SiteScope profile and SiteScope root node.

User Defined Reports

Use the **User Defined Reports** context to assign permissions to the various types of user-defined reports and related settings.

Resources	Operation	Description
Custom Reports	Add	Enables adding custom reports.
	Change	Enables creating, editing, and deleting custom reports.
	View	Enables viewing custom reports.
	Full Control	Enables performing all available operations on custom reports, and granting and removing permissions for those operations.
Trend Reports	Add	Enables creating trend reports.
	Change	Enables creating, editing, and deleting trend reports.
	View	Enables viewing trend reports.
	Full Control	Enables performing all available operations on trend reports, and granting and removing permissions for those operations.
Custom Links	Change	Enables creating and deleting custom links.
	View	Enables viewing custom links.
	Full Control	Enables performing all available operations on custom links, and granting and removing permissions for those operations.

Resources	Operation	Description
Excel Reports	Change	Enables adding, deleting, and updating Excel open API reports.
	View	Enables viewing Excel open API reports.
	Full Control	Enables performing all available operations on Excel open API reports, and granting and removing permissions for those operations.
Default Header/Footer	Change	Enables modifying the default header and footer for custom and trend reports.
	Full Control	Enables modifying, and granting and removing permissions to modify, the default header and footer for custom and trend reports.
Favorite Filter	Change	Enables editing favorite filter.
	Delete	Enables deleting favorite filter
	Full Control	Enables performing all available operations on favorite filter, and granting and removing permissions for those operations.
Annotation	Change	Enables editing an annotation.
	Delete	Enables deleting an annotation.
	Full Control	Enables performing all available operations on annotations, and granting and removing permissions for those operations.
Service Report	Change	Enables editing a service report.
	Delete	Enables deleting a service report.
	Full Control	Enables performing all available operations on service reports, and granting and removing permissions for those operations.

User Management User Interface

Permissions Tab (User Management)

This tab enables you to apply permissions to groups and users for specific resources and instances of those resources that are defined in the system.

To access	Select **Admin > Platform > Users and Permissions > User Management > Permissions** tab. The **Permissions** tab is divided into the following areas: • **Groups/Users** pane on the left side of the page. For details, see "Groups/Users Pane" on page 127. • **Resource tree** pane in the center of the page. For details, see "Resource Tree Pane" below. • **Roles** tab on the right side of the page. For details, see "Roles Tab" on page 180. • **Operations** tab on the right side of the page. For details, see "Operations Tab" on page 180.
Important information	• You can grant permissions to only one user or group at a time. • Assigning **Add** permissions on the Operations tab **does not** automatically grant **View** permissions on the given resource. • If you have many users for whom you have to grant permissions, it is recommended that you organize your users into logical groups using the Hierarchy tab.
Relevant tasks	"Configuring Users and Permissions - Workflow" on page 139
See also	"Permissions" on page 130

Resource Tree Pane

This tab displays the instances and resources available within each APM context for which you set permissions.

To access	Select **Admin > Platform > Users and Permissions > User Management > Permissions** tab. The types of resources displayed in the Resource Tree pane are: • Resource with instances  • Instances of a resource  **Note:** When a user defines or creates an instance of a resource, for example creates a Business Process profile, that user has **Full Control** permission on that resource instance and all of its child resources. • Resource without instances
Important information	• The **Enterprise** resource refers to all contexts in APM and can have only roles applied to it. • The resources are divided according to the context in which they function within the platform and not necessarily where they are found in the user interface. • You can select multiple resources only when selecting instances. For information on instances, see "Understanding Permissions Resources" on page 131.
Relevant tasks	"Configuring Users and Permissions - Workflow" on page 139
See also	"Understanding Permissions Resources" on page 131

User interface elements are described below:

UI Element (A-Z)	Description
	An instance of a resource.
	A resource without instances.
	A resource that has instances (a resource collection).
Select Context	Select an APM context for which to configure permissions. For details on APM contexts, see "Resource Contexts" below.
Settings	Applies specific permissions settings for configurations in your User Management session. Select from the following options: • **Apply permissions automatically when selecting another resource.** Selecting this option removes the necessity for clicking the **Apply Permissions** button after each operation. If this option is not selected, you must click **Apply Permissions** before going on to the next operation. • **Do not display warning message when revoking VIEW from resource.** When the view operation is removed from a resource for a user, that user has no access to the resource or to any of its child resources or instances. Therefore, by default, a warning message appears when removing view permissions. Selecting this option will disable that warning message. **Note:** When you select the settings for applying permissions, the options selected apply only to the current APM session.

Resource Contexts

The following contexts are included:

UI Element (A-Z)	Description
Diagnostics	Includes all the resources relating to Diagnostics.
End User Management	Includes all the resources relating to operating and administering the End User Management application.
MyBSM	Includes resources needed to administer user pages, predefined pages, and user components.
Operations Orchestration Integration	Includes the resources enabling permissions for operating and administering the Operations Orchestration Administration application.
Platform	Includes all the resources for administering the platform.
RTSM	Includes all the resources for the Run-time Service Model (RTSM).
Service Health Analyzer	Includes all the resources relating to the Service Health Analyzer application.

UI Element (A-Z)	Description
Service Level Management	Includes the SLA resource.
SiteScope On Demand Monitors	Includes all the resources relating to the Service Health Analyzer to manage SiteScope monitors on demand.
System Availability Management	Includes the various SiteScope groups.
User Defined Reports	Includes the custom report, trend report, custom link, and Excel report resources.

Roles Tab

Displays the roles configurable for groups and users in APM.

To access	Select **Admin > Platform > Users and Permissions > User Management > Permissions** tab
Relevant tasks	"Configuring Users and Permissions - Workflow" on page 139
See also	• "Understanding Permissions Resources" on page 131 • " User Management Roles Applied Across APM" on page 151

User interface elements are described below:

UI Element (A-Z)	Description
Apply Permissions	Applies the permissions configured for the roles
Grant	Select the check box to assign the specified roles to the group or user.
Roles	The roles that can be assigned to a group or user for the selected resource or instances. For a description of the available roles, see " User Management Roles Applied Across APM" on page 151.

Operations Tab

Displays the predefined operations configurable for groups and users in APM.

To access	Select **Admin > Platform > Users and Permissions > User Management > Permissions** tab
Relevant tasks	"Configuring Users and Permissions - Workflow" on page 139
See also	• "Understanding Permissions Resources" on page 131 • "User Management Operations" on page 166

User interface elements are described below:

UI Element (A-Z)	Description
Apply Permissions	Applies the permissions configured for the resource.
Grant	Select the check box to assign the specified operation to the group or user.
Granted from Group/Roles/Parent	Displays those permissions that have been granted from either a group, a role, or a parent resource. **Note:** • You cannot remove any of these permissions individually, but you can grant additional permissions. • If you want to remove permissions that are granted from a group, role or parent resource, you must make the change at the group, role or parent resource level.
Inherit	Select the check box in the **Inherit** column for the operation to be inherited to all the child resources within the selected resource. **Note:** • The **Inherit** check box is enabled only for selected resources. • By default, the **Inherit** check box is selected when you assign an operation to specific resource instances. You can remove the **Inherit** option to prevent the operation from being inherited to all the child resources within the selected resource.
Operation	The operations that can be assigned to a group or user for the selected resource or instances. For details on the available operations, see "User Management Operations" on page 166.

Hierarchy Tab (User Management)

This tab enables you to assign users to a group, unassign users from a group, or nest one group within another.

To access, select **Admin > Platform > Users and Permissions > User Management**, select a group or user from the **Groups/Users** pane, and click the **Hierarchy** tab.

To access	Select **Admin > Platform > Users and Permissions > User Management**, select a group or user from the **Groups/Users** pane, and click the **Hierarchy** tab. The Hierarchy tab displays: • **Parent Groups.** The groups that the selected group is nested under. • **Child Groups and Users.** The groups and users that are nested directly beneath the selected group.

Important information	• To nest a user, you must select the group into which you want to nest it and click the **Edit Child Groups and Users** button. • When removing a nested group from its parent, the group itself is not deleted. • When deleting a parent group, the child groups and users are not deleted. • If APM groups have been synchronized with groups on an external LDAP server, APM users cannot be moved between groups, and only groups appear on the interface. For details on synchronizing groups, see Synchronizing Users.
Relevant tasks	"Configuring Users and Permissions - Workflow" on page 139
See also	"Group and User Hierarchy" on page 135

User interface elements are described below:

UI Element (A-Z)	Description
	Denotes a group that the selected group or user is nested under.
	Denotes a user that is nested beneath the selected group.
Child Groups and Users	Displays the groups and users that are nested directly beneath the group selected in the **Groups/Users** pane.
Edit Child Groups and Users	Opens the Edit Child Groups and Users window enabling you to nest or remove groups and users from the selected group. **Note:** This button is displayed only when selecting a group in the **Groups/Users** pane.
Parent Groups	Displays the groups that the group or user selected in the **Groups/Users** pane is directly nested under.

Edit Child Groups and Users Dialog Box

User interface elements are described below:

UI Element (A-Z)	Description
	Moves the group or user to the **Child Groups and Users** pane and nests the group or user under the specified group.
	Moves the group or user to the **Groups/Users** pane and removes the group or user from being nested beneath the specified group.
Child Groups and Users	Select a group or user you want to remove from the specified group.
Groups/Users	Select a group or user you want to nest under the specified group.

Customization Tab (User Management)

This tab enables you to select the page users see when entering APM, and select the menu items available on pages throughout APM.

To access	Select **Admin > Platform > Users and Permissions > User Management**, select a node from the **Groups/Users** pane, and click the **Customization** tab.
Important information	Properties are inherited based on the hierarchy of the nodes. If a context is deselected (hidden) for a group node, it cannot be selected for any child nodes.
Relevant tasks	• "Configuring Users and Permissions - Workflow" on page 139 • "How to Configure Users and Permissions — Use-Case Scenario" on page 143

User interface elements are described below:

UI Element (A-Z)	Description
Contexts	Select an APM context. You can perform the following actions on the context: • Select contexts and applications in the Contexts pane to be visible for the specified user or group. To hide a context or application, clear the check box. By default, all contexts are visible. • Select pages and tabs in the Pages and Tabs pane to be visible for the specified user or group. By default, all pages and tabs are visible. • Click the **Set as Default Entry Context** button to make it the context that is displayed when the user logs into APM. For details on APM contexts, see Resource Contexts.
Pages and Tabs	• Select the pages and tabs you want to be visible for the APM context selected in the Contexts pane. • Assign a page or tab as the default page that opens for the context selected in the Contexts pane. Note: For the Service Health application, you cannot define user access to specific pages; you can enable or disable user access only at the application level.
Set as Default Entry Context	Sets the selected context in the Contexts pane as the entry context that is displayed when a user logs into APM. **Note:** The **Default Entry Context** icon  appears next to the specified context.
Set as Default Entry Page	Assigns the specified page or tab as the default page that opens for the context selected in the Contexts pane. **Note:** The **Default Entry Page** icon  appears next to the specified page or tab.

Chapter 26: Recipient Management

A recipient definition includes information about how to communicate with the recipient. Recipients can receive triggered alerts or scheduled reports:

- **Alerts.** For each recipient, you define one or more notification methods (email, pager, or SMS) and the template to use for alert notices. You can configure alerts so specific recipients receive information about the alerts when they are triggered. For details about alerts, see "Setting Up an Alert Delivery System" on page 243.
- **Scheduled reports.** In the Report Manager, you can schedule the time intervals when recipients can receive reports or report items. Only those recipients who have been configured to receive email can be selected to receive scheduled reports. These recipients are listed in Available Recipients when configuring scheduled reports. For details about scheduled reports, see "Report Schedule Manager" on page 241.

For details on where to configure and manage recipients, see "Recipients Page" on the next page.

For more information about groups and users, see "Group and User Hierarchy" on page 135

Configure and Manage Recipients

This section provides information about configuring and managing recipients.

To access

Select **Admin > Platform > Recipients > Recipient Management**

Learn About

Creating Recipients

You create recipients by defining:

- One or more notification methods
- The template to use for alert notices
- A notification schedule to receive reports.

You create recipients and manage existing recipients in the Recipients page. For user interface details, see "Recipients Page" on the next page.

You can also create recipients while you are configuring users. Those recipients are automatically added to the list of recipients in the Recipients page in **Admin > Platform > Recipients > Recipient Management**.

The recipients you create in the Recipients page are automatically listed as available recipients when you configure users in **Admin > Platform > Users and Permissions > User Management**.

The Recipients Page

The Recipients page enables you to create or edit recipient information including the corresponding user and the email, SMS, and pager information. You can also, if you have the appropriate permissions, detach the current recipient from the user, attach existing recipients to the user, or delete the attached recipient.

How you access the Recipients page and what you see in the page depends on your user's permissions. For details, see "Permissions Tab (User Management)" on page 177.

There is a one-to-one relationship between the user and the recipient: a recipient can be assigned to one user or to no user, and a user can have a link to one recipient or to no recipient.

Tasks

This section includes:

- "How to Define Recipients" below
- "How to Attach Users to Recipients" below

How to Define Recipients

1. Select **Admin > Platform > Recipients.**
2. Click the **Recipient Management** tab.
3. Click  .
4. Complete the fields in the New Recipient dialog box. For information, see "New or Edit Recipient Dialog Box" on page 187.
5. Click **Save**.

How to Attach Users to Recipients

1. Select **Admin > Platform > Recipients.**
2. Click the **Recipient Management** tab.
3. Select a recipient in the table and click the **Attach user to selected recipient**  button in the Recipient page.
4. Complete the fields in the Attach user to selected recipient dialog box. For information, see "Attach Recipient to a User Dialog Box" on page 190.
5. Click **Save**.

UI Description

This section includes:

- "Recipients Page" below
- "New or Edit Recipient Dialog Box" on page 187
- "Attach Recipient to a User Dialog Box" on page 190

Recipients Page

User interface elements are described below:

UI Element (A-Z)	Description
	**Add new recipient.** Opens the New Recipient dialog box. For details, see "New or Edit Recipient Dialog Box" on the next page.
	**Edit selected recipient.** Opens the Edit Recipient dialog box. For details, see "New or Edit Recipient Dialog Box" on the next page.
	**Delete the recipient attached to the selected user.** Detaches the recipient and deletes the current recipient.
	**Attach user to selected recipient.** Select a recipient in the list of and click this button to open the Attach Recipient to a User dialog box where you can select the appropriate user. For details, see "Attach Recipient to a User Dialog Box" on page 190.
	**Detach user from selected recipient.** Detaches the current recipient from the corresponding user (listed in the page). A confirmation message is issued.
	**Update selected recipients email address from LDAP.** This icon appears only if LDAP is connected to the APM application. Click to synchronizes the user data, meaning that the email information stored in the User Repository for the specific user updates the email recipient information corresponding to the user linked to the recipient.
Email	The email address of the recipient as defined in the General tab.
Linked User	The name of the user linked to the recipient. **Important:** Cannot exceed 49 characters. **Syntax Exceptions:** The following characters are not supported: ` ~ ! @ # $ % ^ & * - + = [ ] { } \ | / ? . , " ' : ; < >
Pager	The pager numbers of the recipient. **Syntax Exceptions:** • Numbers and the following special characters are allowed: ( ) - _ + = [ ] { } | : ; . , • Letters and characters other than those specified above are not allowed.
Recipient Name	The name of the recipient. **Important:** Cannot exceed 49 characters. **Syntax Exceptions:** The following characters are not supported: ` ~ ! @ # $ % ^ & * - + = [ ] { } \ | / ? . , " ' : ; < >
SMS	The SMS numbers of the recipient. **Syntax Exceptions:** • Numbers and the following special characters are allowed: ( ) - _ + = [ ] { } | : ; . , • Letters and characters other than those specified above are not allowed.

New or Edit Recipient Dialog Box

The New/Edit Recipient dialog box enables you to define recipients, their email, pager, and SMS, and the template to use to send alert notices to those recipients.

User interface elements are described below:

UI Element (A-Z)	Description
	**Attach user to selected recipient.** Select a recipient in the list of and click the button to open the Attach Recipient to a User dialog box where you can select the appropriate user. For details, see "Attach Recipient to a User Dialog Box" on page 190. **Note:** This button is displayed only when you access the dialog box from **Admin > Platform > Users and Permissions > User Management**.
	**Detach user from selected recipient.** Detaches the current recipient from the corresponding user (listed in the page). A confirmation message is issued. **Note:** This button is displayed only when you access the dialog box from **Admin > Platform > Users and Permissions > User Management**.
	**Delete the recipient attached to the selected user.** Detaches the recipient from the user and deletes the recipient. **Note:** This button is displayed only when you access the dialog box from **Admin > Platform > Users and Permissions > User Management**.
	**Update selected recipients email address from LDAP.** This icon appears only if LDAP is connected to the APM application. Click to synchronize the user data, meaning that the email information stored in the User Repository for the specific user updates the email recipient information corresponding to the user linked to the recipient.
Communication Method Area	This area enables you to define the communication methods. For information, see "Recipient Management Communication Methods" on page 190.

UI Element (A-Z)	Description
EUM Alert notification template	Select the template you want to use for the EUM alert notification, or any custom template already created. **Note:** When you change the selection in the **EUM Alertnotification template** field in the top part of the page, the changes are propagated to the Email, Pager, and SMS tabs in the same page. If you modify the selection in the **EUM Alertnotification template** field in the Email, Pager, or SMS tabs, the **Schedule for receiving alerts** changes to **Mixed Value**. When you change once more, the selection in the **EUM Alertnotification template** field in the top part of the page, the changes are propagated to the Email, Pager, and SMS tabs in the same page and the **Mixed Value** button is cleared. For details on EUM alert notification templates and creating custom templates, see "How to Configure EUM Alerts Notification Templates" on page 260. **Note:** This field is relevant only for event-based alerts. For details on alert notification templates and creating custom templates, see "Notification Templates Page" on page 265. **Note:** • The default template is **LONG**. • For details on the parameters displayed in each template, see "Notification Template Properties Dialog Box" on page 261. • The field lists the default templates and the custom templates. • You must select the alert notification template and specify an alert notices schedule for alert recipients. You do not have to perform this procedure for recipients who are to receive only scheduled reports.
Link to user	This field is displayed only when you access this page from: • **Admin > Platform > Users and Permissions > User Management**, select a user in the tree and click the **Recipient** tab. • **Admin > Personal Settings > Recipient**.
Recipient name	The name of the recipient. **Important:** Cannot exceed 49 characters. **Syntax Exception:** The following characters are not supported: ` ~ ! @ # $ % ^ & * - + [ ] { } \ | / ? " ' < >

UI Element (A-Z)	Description
Schedule for receiving alerts	Enabled if you selected the **Per notification method** scheduling option for the recipient in the **Schedule for Receiving Alerts** in the General tab. Select: • **Mixed value.** When you change the selection in the **EUM Alertnotification template** field in the top part of the page, the changes are propagated to the Email, Pager, and SMS tabs in the same page. If you modify the selection in the **EUM Alertnotification template** field in the Email, Pager, or SMS tabs, the **Schedule for receiving alerts** changes to **Mixed Value**. When you change once more, the selection in the **EUM Alertnotification template** field in the top part of the page, the changes are propagated to the Email, Pager, and SMS tabs in the same page and the **Mixed Value** button is cleared. • **All Day.** If you want the recipient to receive email messages all day. • **From... to.** If you want the recipient to receive email messages during the specified time period. The time range is calculated based on the GMT offset selected for the recipient. Scheduled reports are sent based on the schedule configured in the Scheduled Reports page and not on the schedule configured for the recipient. For details, see How to Schedule a Report in the APM User Guide.
Time zone	Select the time zone for the recipient. Application Performance Management uses the time zone to send alert notices to the selected recipient. **Note:** • The time zone selected for the recipient is the time zone specified in the alert notifications that the recipient receives. For example, if an alert is triggered anywhere in the world and a notification is sent, the date and time of the alert are converted to the recipient local time. The alert also specifies the GMT offset of the recipient. • If you defined a notification schedule for the recipient, the time zone selected for the recipient is also the time zone that APM uses for calculating when to send the recipient notifications. For example, if you configure a recipient to receive pager alerts from 9:00 AM - 9:00 PM, and select a GMT offset of -5 hours, the recipient receives alerts through a pager only from 9:00 AM - 9:00 PM Eastern Time. Scheduled reports are sent based on the schedule configured in the Scheduled Reports page and not on the schedule configured for the recipient. For details, see How to Schedule a Report in the APM User Guide. • When you modify the time zone of the user to which the recipient is assigned, a confirmation message is issued to verify that you also want to propagate the time zone change to the recipient's offset from GMT. If you change the recipient's offset from GMT, the time zone of the user to which the recipient is assigned is not affected. • Half time zones (also known as offset time zones) are not supported.

Attach Recipient to a User Dialog Box

The Attach Recipient to a User dialog box enables you to select the user you want to attach to the selected recipient.

User interface elements are described below:

UI Element	Description
User Login	The name used to log into APM.
User Name	The name of the user, as configured in the User Management page.
Select	To assign a user to the selected recipient, select the user and click **Select**.

Recipient Management Communication Methods

This section provides information about recipient management communication methods.

To access

Select **Admin > Platform > Recipients > Recipient Management** and click  .

Learn About

Communication Method – Email

You can specify multiple email addresses for a recipient, the type of notification template (which overrides the notification template selected in the global level in the page), the schedule for sending email notifications, and the security certificate if necessary.

The text displayed in email messages can only be in Latin characters except for the contents of fields inserted by the user that can be in any supported and relevant language. Those fields can include, for example, Alert Name, Alert description, and KPI name.

Communication Method – SMS

You can specify the SMS (short message service) service provider, the SMS numbers, the type of notification template (which overrides the notification template selected in the global level in the page), and the schedule for sending alert notifications to the SMS.

SMS messages are useful to notify staff who are mobile, or who do not have email or pager access. The maximum message length of SMS text messages is generally 160 characters.

Note: You can use a pager or an SMS service provider that does not appear on the default list. For details, see "How to Add a Custom Pager or SMS Service Provider" on the next page.

Communication Method – Pager

You can specify the pager service provider, the pager numbers, the type of notification template (which overrides the notification template selected at the global level in the page), and the schedule for sending alert notification to the pager.

The text displayed in pager messages can only be in Latin characters except for the contents of fields inserted by the user that can be in any supported and relevant language. Those fields can include, for example, Alert Name, Alert description, and KPI name.

Note: You can use a pager or an SMS service provider that does not appear on the default list. For details, see "How to Add a Custom Pager or SMS Service Provider" below.

Custom Pager or SMS Service Provider

If you are configuring alerts to be sent by pager or SMS, and your pager or SMS service provider does not appear on the default provider list, and the provider uses an email gateway, you can manually add your provider to APM. After doing so, your provider appears on the list.

To add a provider that uses an email gateway, manually add the gateway information to the management database. If necessary, ask your database administrator for assistance.

See "How to Add a Custom Pager or SMS Service Provider" below for instructions on adding an SMS Service Provider.

Tasks

How to Add a Custom Pager or SMS Service Provider

1. Open the **NOTIFICATION_PROVIDERS** table in the management database.
2. In the **NP_NOTIFICATION_PROVIDER_NAME** column, add the name of the provider to the bottom of the list. Add the name exactly as you want it to appear in the provider list that opens in the SMS tab of the Recipient Properties wizard. For details, see "Communication Method Area - SMS Tab" on page 193. Note the ID number that is automatically assigned to the provider.
3. Close the **NOTIFICATION_PROVIDERS** table, and open the **NOTIFPROVIDER_NOTIFTYPE** table.
4. In the **NN_NOTIF_PROVIDER_ID** column, add the ID number that was assigned to the new provider.
5. In the **NN_NOTIF_TYPE_ID** column, assign the provider one of the following notification types:
   - **102** – for pager service provider
   - **101** – for SMS service provider
6. Close the **NOTIFPROVIDER_NOTIFTYPE** table, and open the **NOTIFICATION_PROVIDER_PROP** table.
7. In the **NPP_NOTIFICATION_PROVIDER_ID** column, add the ID number that was assigned to the new provider. Note that you add the ID number to two consecutive rows.
8. In the **NPP_NPROVIDER_PROP_NAME** and **NPP_NPROVIDER_PROP_VALUE** columns, add the following new property names and values for the provider, one beneath the other (for examples, see existing entries):

Property Name	Property Value	Description
EMAIL_SUFFIX	<email_suffix>	The gateway's email suffix. For example, if the gateway email address is 12345@xyz.com, enter `xyz.com` as the property value for EMAIL_SUFFIX.

Property Name	Property Value	Description
EMAIL_MAX_LEN	<max_length>	The maximum message length, in characters, of the body of the email message. For example, `500`. When determining this value, take into consideration the maximum length limit imposed by your service provider, as well as limitations to your pager or mobile phone.

9. In the **NPP_NPROVIDER_PROP_DATATYPE_ID** column, specify an ID value as follows:
   - for EMAIL_SUFFIX, specify: `1`
   - for EMAIL_MAX_LEN, specify: `2`
10. Restart APM.

UI Description

Communication Method Area - Email Tab

User interface elements are described below:

UI Element (A-Z)	Description
Email Addresses	Enter one or more email addresses. Separate multiple entries with a semi-colon (;). Only those recipients who have been configured to receive email can be selected to receive scheduled reports and are listed in Available Recipients when configuring scheduled reports.
Enable secure mail	Select this option if you want the recipient to receive encrypted mail. You must then copy, into the text box below the option, the contents of the certificate that the recipient uses to secure incoming email messages. **Note:** • The encrypted mail option is supported only for alerts. Encrypted mail is not supported for scheduled reports or subscription notification. • The encrypted mail option is supported only when the APM Data Processing Server is installed on a Windows machine.

UI Element (A-Z)	Description
EUM Alert notification template	Select the template you want to use. For details, see "EUM Alerts Notification Templates" on page 260. **Note:** When you change the selection in the **EUM Alert notification template** field in the top part of the page, the changes are propagated to the Email, Pager, and SMS tabs in the same page. If you modify the selection in the **EUM Alert notification template** field in the Email, Pager, or SMS tabs, the **Schedule for receiving alerts** changes to **Mixed Value**. When you change once more, the selection in the **EUM Alert notification template** field in the top part of the page, the changes are propagated to the Email, Pager, and SMS tabs in the same page and the **Mixed Value** button is cleared.
Schedule for receiving Email notifications	Select the schedule you want to use for receiving emails. For details, see **Schedule for receiving alerts** in "New or Edit Recipient Dialog Box" on page 187.

Communication Method Area - SMS Tab

User interface elements are described below:

UI Element (A-Z)	Description
EUM Alert notification template	Select the template you want to use. For details, see "EUM Alerts Notification Templates" on page 260. **Note:** When you change the selection in the **EUM Alert notification template** field in the top part of the page, the changes are propagated to the Email, Pager, and SMS tabs in the same page. If you modify the selection in the **EUM Alert notification template** field in the Email, Pager, or SMS tabs, the **Schedule for receiving alerts** changes to **Mixed Value**. When you change once more, the selection in the **EUM Alert notification template** field in the top part of the page, the changes are propagated to the Email, Pager, and SMS tabs in the same page and the **Mixed Value** button is cleared.
Provider	Select an SMS service provider from the list: • **Genie-UK** • **Itineris** • **SFR-France** • **GoSMS-Israel** • **MtnSMS-Global** **Note:** If your provider does not appear on the default provider list, and the provider uses an email gateway, you can manually add your provider to APM. For details, see "How to Add a Custom Pager or SMS Service Provider" on page 191.

UI Element (A-Z)	Description
Schedule for receiving SMS notifications	Select the schedule you want to use for receiving SMS text messages. For details, see **Schedule for receiving alerts** in "New or Edit Recipient Dialog Box" on page 187.
SMS numbers	Type one or more SMS access numbers in the box. Separate multiple entries with a semi-colon (;).

Communication Method Area - Pager Tab

User interface elements are described below:

UI Element (A-Z)	Description
EUM Alert notification template	Select the template you want to use. For details, see "EUM Alerts Notification Templates" on page 260. **Note:** When you change the selection in the **EUM Alert notification template** field in the top part of the page, the changes are propagated to the Email, Pager, and SMS tabs in the same page. If you modify the selection in the **EUM Alert notification template** field in the Email, Pager, or SMS tabs, the **Schedule for receiving alerts** changes to **Mixed Value**. When you change once more, the selection in the **EUM Alert notification template** field in the top part of the page, the changes are propagated to the Email, Pager, and SMS tabs in the same page and the **Mixed Value** button is cleared.
Pager Numbers	Enter one or more pager access numbers. Separate multiple entries with a semi-colon (;). **Note:** If your pager is numeric only, when creating an alert scheme in the Alert Wizard, you can only type a numeric user message.
Schedule for receiving pager notifications	Select the schedule you want to use for receiving pager messages. For details, see **Schedule for receiving alerts** in "New or Edit Recipient Dialog Box" on page 187.
Type	Select a pager service provider. The following providers are supported: • **MetroCall** • **Arch** • **AirTouch** • **PageMci** • **SkyTel** • **PageNet** • **PageMart** • **AmeriPage** • **Nextel** • **PageOne**

Chapter 27: Personal Settings

Personal settings enable customization of the way APM presents information to individual users. Individual users can configure personal settings to customize their specific user-related behavior of APM.

To access

- Select **Admin > Personal Settings**
- Click **Change the default page** on the Site Map

Learn About

User Account Settings

On the User Account tab, you can configure the following personal settings:

- User name
- User mode
- Time zone used when displaying reports
- Password
- Refresh rate of reports

For details on the user interface for changing your password and updating other Personal Settings, see "User Account Page" on page 198.

Menu Customization Settings

On the Menu Customization tab, you can:

- Specify the default context that is displayed when logging into APM.
- Specify the first page that is displayed in each of the different parts of APM.
- Specify the tabs and options that are available on pages throughout APM.

Customizing your entry page, menu items, and tabs enables your interface to display only the areas of APM that are relevant to you. For details on the Menu Customization User Interface, see "Menu Customization Page" on page 199.

Tasks

How to Customize APM Menus and Pages — Workflow

This task describes how to customize the page you see when entering APM, and select the menu items available on pages throughout APM.

Tip: For a use-case scenario related to this task, see "How to Customize APM Menus and Pages — Use-Case Scenario" on the next page.

1. **Assign a Default Context**

Select a context from the Contexts pane that you want to be the default entry context you see when logging into APM, and click **Set as Default Entry Context**. For user interface details, see "Menu Customization Page" on page 199.

2. **Select Context Pages and Tabs**

   In the Pages and Tabs pane, select the context of the pages and tabs that you want to be visible on the selected context for the user. Clear the check boxes of the pages and tabs that you want hidden from the user.

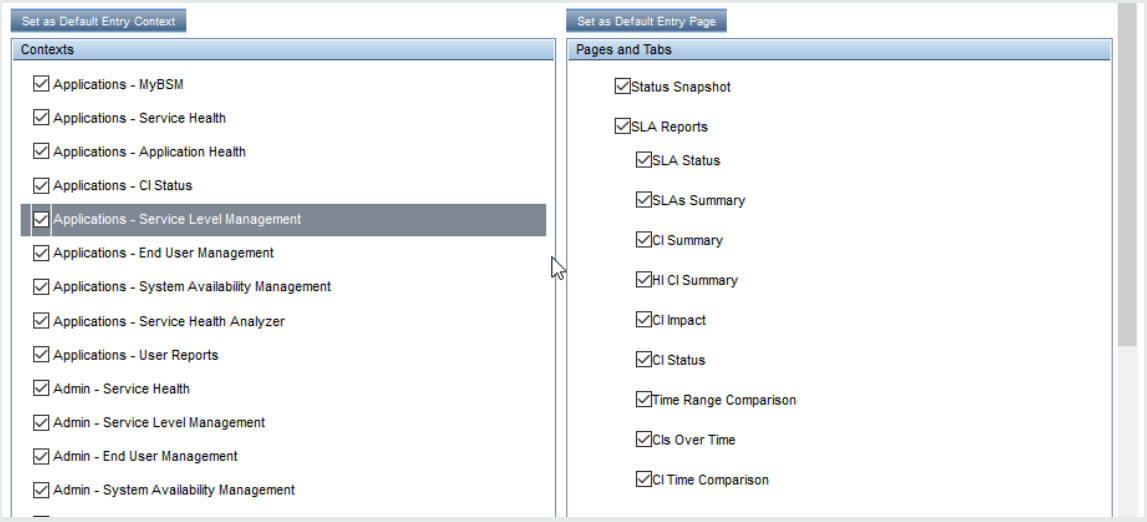
3. **Assign a Default Entry Page**

   Select a page or tab to be the default entry page for the selected context, and click **Set as Default Entry Page**.

4. **Results**

   The default entry icon appears next to the default entry context and page. Pages and tabs visible to the user are selected in the Pages and Tabs pane. Pages and tabs hidden from the user are cleared in the Pages and Tabs pane.

Example:



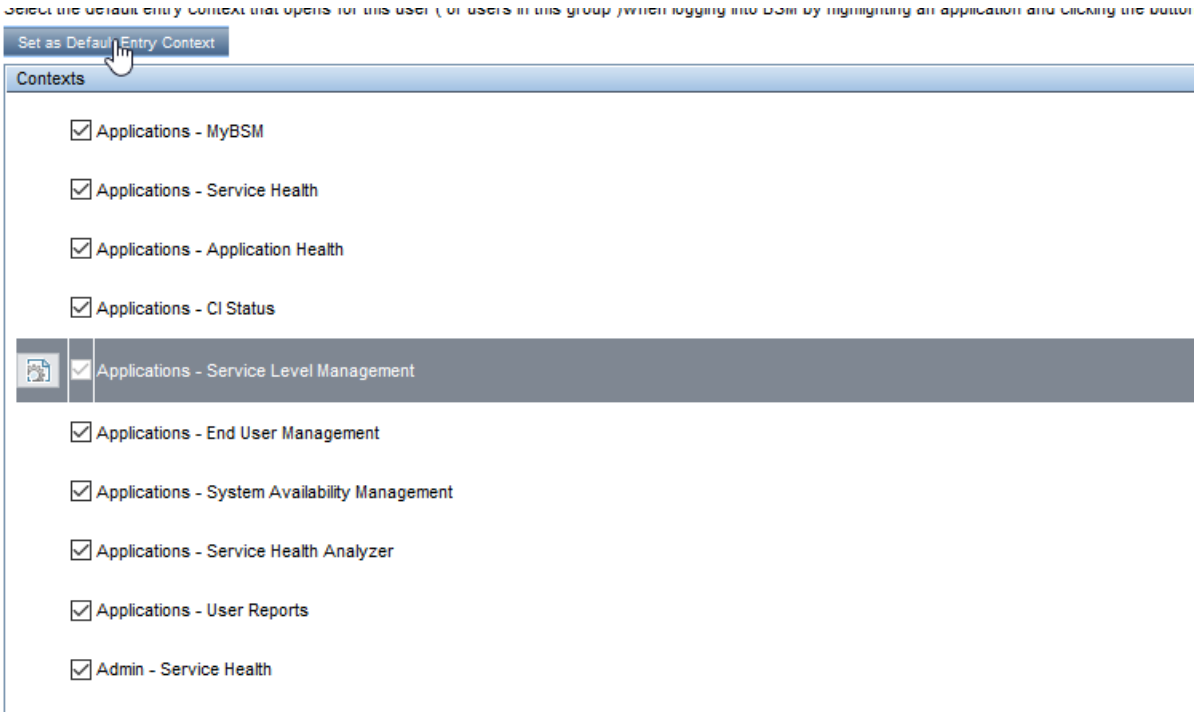
How to Customize APM Menus and Pages — Use-Case Scenario

This use-case scenario describes how to customize user menus for individual users.

Note: For a task related to this scenario, see "How to Customize APM Menus and Pages — Workflow" on the previous page.

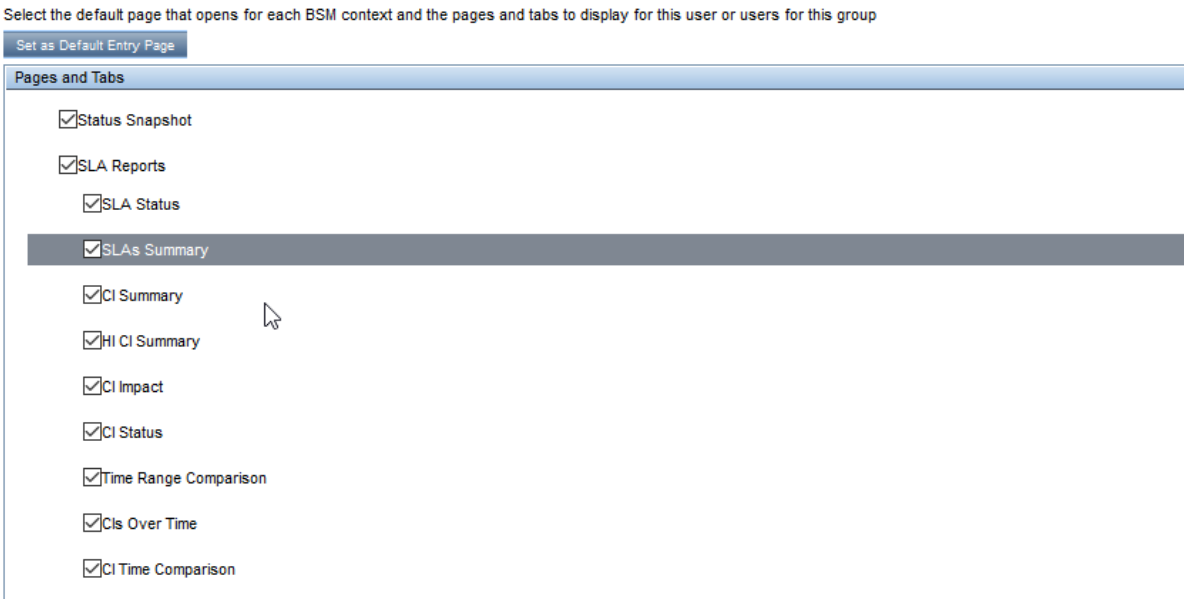
1. **Assigning a Default Context**

   John Smith is a registered APM user for the ABC Insurance Company. He wants to configure the Service Level Management application interface to be the default Application Performance Management context that he sees when logging in. He navigates to the Personal Settings option by selecting **Admin > Personal Settings**, and selects **Menu Customization** to open the Menu Customization page. He selects **Applications - Service Level Management** in the Contexts pane and clicks **Set as Default Entry Context**. The Applications - Service Level Management option is indicated as the default entry context:



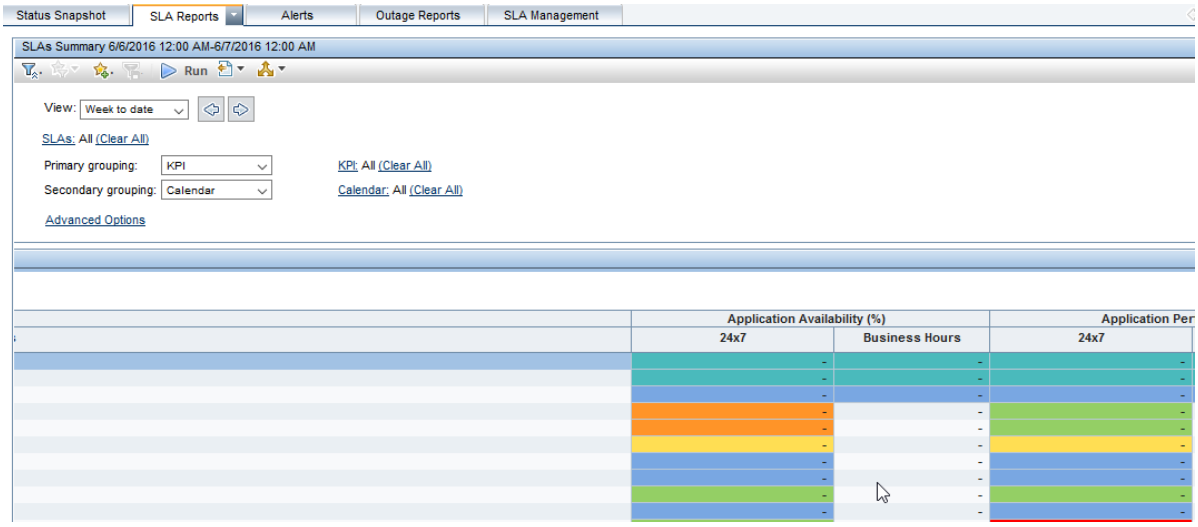
2. **Selecting Context Pages and Tabs**

   John wants to see only the pages and tabs that are relevant for his work, and wants to view the Service Level Agreements (SLAs) Summary report immediately upon logging into APM. In the Pages and Tabs pane, he deselects the SLA Management option, as the information presented on this tab is not relevant to his work. He selects the **SLAs Summary** option and clicks **Set as Default Entry Page**. The SLAs Summary page is indicated as the default entry page that John sees when logging into APM:



3. **Results**

   The context that opens when John Smith logs into APM is the **Service Level Management** context on the Applications menu. The **SLAs Summary Report** page is displayed on the SLA Reports tab:



UI Description

User Account Page

APM saves these settings per defined user. Any changes you make remain in effect for all future web sessions for only that user.

User interface elements are described below:

UI Element (A-Z)	Description
Confirm Password	Re-enter the password specified in the **Password** field.
Login name	The name used to log into APM. **Note:** You cannot change the entry in this field.
Old Password	Enter the existing password.
Password	Enter a password to be used when accessing APM.
Select auto-refresh rate	Select the rate at which you want APM to automatically refresh the browser and load the most up-to-date data from the database.
Time zone	Select the appropriate time zone, according to the user's location.

UI Element (A-Z)	Description

User mode	Select the user mode for the user, from the following options:
	• **Unspecified.** Leaves the user without a particular mode. Select this option if:
	  • APM is working with user modes and you want this user to see KPIs for both modes in Service Health views.
	  • Your system is not working with user modes.
	• **Operations User.** Enables the user to view the operations version of KPIs.
	• **Business User.** Enables the user to view the business version of KPIs.
	Note: For details on user modes, see Create KPIs for Operations and Business User Modes in the APM Application Administration Guide.

User name	The user name for the user. **Notes:** • The maximum number of characters you can enter is 50. • All special characters are allowed except the following: " \ / [ ] : | < > + = ; , ? * % &

Recipient Page

This page enables you to define recipients, their email, pager, and SMS information, and the template to use to send alert notices to those recipients.

For user interface details, see "New or Edit Recipient Dialog Box" on page 187.

Menu Customization Page

This page enables you to customize the view and entry pages per user. You can specify:

- The default context that is displayed when logging into APM.
- The first page displayed in each of the different parts of APM.
- The tabs and options available on pages throughout APM.

The Personal Settings tab can also be accessed by clicking **Change the default page** on the Site Map.

User interface elements are described below:

UI Element (A-Z)	Description
Contexts	Select an APM context. You can perform the following actions on the context: • Select pages and tabs in the Pages and Tabs pane to be visible for the specified user. • Click the **Set as Default Entry Context** button to make it the context that is displayed when the user logs into APM.

UI Element (A-Z)	Description
Pages and Tabs	• Select the pages and tabs you want to be visible for the APM context selected in the Contexts pane. • Assign a page or tab as the default page that opens for the context selected in the **Contexts** pane.
Set as Default Entry Context	Click to set the selected context in the Contexts pane as the entry context that is displayed when the specified user logs into APM. Note: The **Default Entry Context**  icon appears next to the specified context.
Set as Default Entry Page	Click to assign the specified page or tab as the default page that opens for the context selected in the Contexts pane. **Note:** The **Default Entry Page**  icon appears next to the specified page or tab.

Chapter 28: Authentication Strategies

APM authentication is based on a concept of authentication strategies. Each strategy handles authentication against a specific authentication service. Only one authentication service can be configured with APM at any given time.

To access

Select **Admin > Platform > Users and Permissions > Authentication Management**

Learn About

Authentication Strategies Overview

The default authentication strategy for logging into APM is the APM internal authentication service. You enter your APM user name and password from the Login page, and your credentials are stored and verified by the APM database.

Setting Up an SSO Authentication Strategy

Single Sign-On (SSO) is a method of access control that enables a user to log in once and gain access to the resources of multiple software systems without being prompted to log in again. The applications inside the configured group of software systems trust the authentication, and you do not need further authentication when moving from one application to another.

The default single sign-on authentication strategy for APM is Lightweight Single Sign-On (LW-SSO). LW-SSO is embedded in APM and does not require an external machine for authentication. For details on LW-SSO, see "Lightweight Single Sign-On Strategy" on page 220.

If the applications configured outside of APM do not support LW-SSO, or if you want a stronger Single Sign-On implementation, you can configure Identity Management Single Sign-On (IDM-SSO) using the SSO Configuration Wizard. When enabled as a Single Sign-On strategy, IDM-SSO also serves as an authenticator. Users authenticated through IDM-SSO can log into APM, provided they fulfill the criteria defined in the **Users Filter** field of the LDAP Vendor Attributes dialog box. For details, see "LDAP Vendor Attributes Dialog Box" on page 212.

Setting Up LDAP Authentication

The Lightweight Directory Access Protocol (LDAP) is an Internet protocol that email and other programs use to look up information from an external server. LDAP can be configured with APM in one of the following ways:

- As an authentication mechanism for users logging into APM.
- To map groups and synchronize APM users with users configured on the external LDAP server, thereby simplifying the process of managing users for APM administrators. For details, see "How to Map Groups and Synchronize Users" on page 233.

You can define multiple LDAP authentication module configurations under one realm. Although these additional configurations are visible from the User Management panel, they work in conjunction with the primary configuration if an initial search for the requesting user's authorization is not found. For example, one realm can define a search through LDAP servers for authentication in two different domains or it can configure multiple user naming attributes in one domain.

Smart Card Authentication

APM supports user authentication using smart cards. If smart card authentication is configured, you cannot log in without a valid smart card.

For more information on Smart Card Authentication, see "TLS and Smart Card Authentication" on the next page.

Authentication Modes in APM

The following table displays the Authentication Strategy used by APM, as determined by both the Single Sign-On mode and the selected LDAP mode.

Single Sign-On Mode	LDAP Mode	Authenticator
Disabled	Disabled	APM Internal
	Enabled	LDAP
LW-SSO	Disabled	APM Internal
	Enabled	LDAP
IDM-SSO	Disabled	IDM-SSO
	Enabled	IDM-SSO

UI Description

Authentication Management Page

This page displays the current authentication strategy and Single Sign-on configurations for logging into APM.

Access to the Authentication Management page is dependent on the following permission levels:

- **View.** Enables viewing the Authentication Management Page.
- **Change.** Enables you to access the Authentication Management page and create and change the configuration.

You configure permissions on the Users and Permissions interface. For details, see "Permissions" on page 130.

User interface elements are described below:

UI Element (A-Z)	Description
Add LDAP	Click to open the LDAP Configuration Wizard to add a new LDAP configuration. For details on the LDAP Configuration Wizard, see "LDAP Configuration Wizard" on page 209.

UI Element (A-Z)	Description
Configure	Click to open the SSO Configuration Wizard and configure an authentication strategy. For details on the SSO Configuration Wizard, see "SSO Configuration Wizard" on page 214. There is a separate **Configure** button for **Smart Card Authentication Configuration**. For information on Smart Card Authentication Configuration, see "TLS and Smart Card Authentication" below.
Delete	Click to remove an LDAP configuration.
Edit	Click to edit an LDAP configuration.
Enable/Disable	Click to enable/disable an LDAP configuration.
Lightweight Directory Access Protocol Configuration	The section displays: • **Name.** The name of the **Lightweight Directory Access Protocol** parameter. • **Value.** The value of the **Lightweight Directory Access Protocol** parameter as configured in the wizard.
Single Sign-On Configuration	The section displays: • **Name.** The name of the **Single Sign-On** parameter. • **Value.** The current value of the **Single Sign-On** parameter as configured in the wizard.
Smart Card Authentication Configuration	The section displays: • **Name.** The name of the **Smart Card Authentication Configuration** parameter. • **Value.** The current value of the **Smart Card Authentication Configuration** parameter as configured in the wizard.

TLS and Smart Card Authentication

APM supports user authentication using smart cards. If smart card authentication is configured, you cannot log in without a valid smart card.

To access the TLS and Smart Card Authentication Configuration Wizard:

Select **Admin > Platform > Users and Permissions > Authentication Management** and in the TLS and Smart Card Authentication Configuration pane, click **Configure**.

Learn About

Smart Card Authentication

Smart cards are physical devices used to identify users in secure systems. These cards can be used to store certificates both verifying the user's identity and allowing access to secure environments.

APM can be configured to use these certificates in place of the standard model of each user manually entering a user name and password. You define a method of extracting the user name from the certificate stored on each card.

When using smart cards with APM, users can only log in using the smart card. The option of logging in by manually typing in your username and password is locked for all users unless smart card configuration is disabled.

Tasks

Enable or Disable Smart Card Authentication

Smart cards are both enabled and disabled on the APM Gateway and Data Processing servers by using the Smart Card Authentication Configuration Wizard. This wizard is only a part of the overall workflow for configuring smart card authentication in your APM environment. For more details, see the Smart Card Authentication Configuration Guide.

Note: Your machine should have openssl installed. This is included as part of the Apache installation included on Windows APM and Linux environments. To check if this is installed on your machine run

/usr/bin/openssl

If you do not have this command, install it and make sure you can execute it from any path before configuring smart card authentication.

Emergency Disable of Smart Card Authentication

Note: This procedure should only be used if you cannot access APM normally.

If you cannot log in to APM using any smart card and want to disable smart card authentication, run the following batch file from any APM Gateway or Data Processing Server:

- **Windows:** <APM Installation Directory>\bin\RevertHardening.bat
- **Linux:** <APM Installation Directory>/bin/RevertHardening.sh

When the batch file is complete, restart all APM Gateway Servers to activate the change.

Manually Configure Reverse Proxy for Smart Cards

This procedure differs depending on whether your reverse proxy is using the IIS or Apache web server. This procedure describes the general settings that are required, but you may need to refer to the web server documentation for the details. It must be performed before you restart your APM Gateway servers to enable smart card authentication.

For the IIS web server:

1. Prerequisite: IIS is already configured to require client certificate
2. Configure the reverse proxy to forward the encoded client certificate in the header **CLIENT_CERT_HEADER**.

For the Apache web server:

1. Prerequisite: Apache is already configured to require a client certificate.
2. In httpd.conf, enable the **mod_headers.so**

3. In httpd-ssl.conf, add the following line before </VirtualHost>:
   requestHeader set CLIENT_CERT_HEADER "%{SSL_CLIENT_CERT}s"

UI Descriptions

TLS and Smart Card Authentication Configuration Wizard

This wizard guides you through the process of enabling and disabling smart card authentication configuration with APM.

To access the TLS and Smart Card Authentication Configuration Wizard:

Select **Admin > Platform > Users and Permissions > Authentication Management**, and in the TLS and Smart Card Authentication Configuration pane, click **Configure**.

Notes and Limitations

- User names are case sensitive
- When smart card authentication is enabled, the JXM console can only be accessed directly from the APM servers.
- When creating an admin user as directed in the smart card authentication wizard, make sure you enter a secure password even though no password is required for authentication with smart cards. If smart card authentication is disabled, the user will still exist on the system and if an insecure password is defined it could pose a security risk.
- If your deployment is distributed and it uses a high availability configuration with two or more APM Gateways and you intend to use TLS configuration on each APM Gateway which will be configured using TLS and Smart Card Authentication Configuration you need to use a single Server Certificate which is suitable for each APM Gateway according to its FQDN names.

  For example, you can use a wildcard Server Certificate for the domain OR a Subject Alternative Name (SAN) certificate with a list of APM Gateway FQDN names.

TLS and Smart Card Authentication Configuration - Introduction Page

This wizard enables you to configure server side secure communication using TLS and client side smart card authentication settings. Smart card authentication technology is used to identify users in secure systems. These cards can be used to store digital identity credentials, thereby providing access to secure environments. Once these settings are configured, you will not be able to log into APM without a valid smart card.

To access	Select **Admin > Platform > Users and Permissions > Authentication Management**, and in the TLS and Smart Card Authentication Configuration pane, click **Configure**.

Wizard map	This wizard contains: **TLS and Smart Card Authentication Configuration Wizard Introduction Page** > "TLS and Smart Card Authentication Configuration - Front End Server Page" below > "TLS and Smart Card Authentication Configuration - Configuration Mode Page" below > "TLS and Smart Card Authentication Configuration - Server Certificate Page" on the next page >"TLS and Smart Card Authentication Configuration - Client Certificate Page" on page 208 > "TLS and Smart Card Authentication Configuration - Admin Page" on page 208 > "TLS and Smart Card Authentication Configuration - Summary Page" on page 209

TLS and Smart Card Authentication Configuration - Front End Server Page

This wizard page enables you to select which APM front end server you are using in your APM deployment.

To access	Select **Admin > Platform > Users and Permissions > Authentication Management**, and in the TLS and Smart Card Authentication Configuration pane, click **Configure**. Navigate to the **Front End Server** page.

Choose which APM front end server you are using in your APM deployment. Options are:

- APM Gateway Server - Apache
- Reverse Proxy / Load Balancer

TLS and Smart Card Authentication Configuration - Configuration Mode Page

This wizard page enables you to select which CAC configuration you want to use.

To access	Select **Admin > Platform > Users and Permissions > Authentication Management**, and in the TLS and Smart Card Authentication Configuration pane, click **Configure**. Navigate to the **Configuration Mode** page.

User interface elements are described below:

UI Element (A-Z)	Description
Smart Card CAC mode	Options are: • **Custom** - This mode is by default similar to Full CAC. However, if your smart card software does not allow caching the pin code for the entire APM session, only per process, then this mode can be used instead of Full CAC. This will enforce smart card authentication for users logging into APM or data collectors accessing APM. In addition, Custom mode enables you to define URLs to require Smart card authentication. **Note:** This option is not available in IIS. • **Full** - Smart card authentication is required for any access to APM. This is the default mode. • **User login only** - Smart card authentication is required for logging in to APM only. This mode requires smart card authentication for users logging into APM, and SSL authentication for data collectors to access APM.
Server side TLS only mode	Selecting this option, means that you selected a server side configuration certificate. Therefore, all fields in the Client Certificate page are inaccessible.

TLS and Smart Card Authentication Configuration - Server Certificate Page

This wizard page enables you to enter the certificate of the CA that issued your APM gateway server certificate.

To access	Select **Admin > Platform > Users and Permissions > Authentication Management**, and in the TLS and Smart Card Authentication Configuration pane, click **Configure**. Navigate to the **Server Certificate** page.

User interface elements are described below:

UI Element (A-Z)	Description
APM java truststore password	Enter the APM Java truststore password. By default, the password is **changeit**.
CA certificate issuer for the APM gateway server (Base 64 - .cer format)	Enter the certificate for the CA that signed your APM gateway server certificate
Private key password	Enter the password for the private key contained in the server certificate .pfx file.
Server certificate (.pfx)	Enter the server certificate. The .pfx file must contain a public and private key (password protected).

TLS and Smart Card Authentication Configuration - Client Certificate Page

This wizard page enables you to enter the certificate of the CA that issued your APM gateway client certificate.

To access	Select **Admin > Platform > Users and Permissions > Authentication Management**, and in the TLS and Smart Card Authentication Configuration pane, click **Configure**. Navigate to the **Client Certificate** page.

User interface elements are described below:

UI Element (A-Z)	Description
CA certificate for the client certification (Base 64 - .cer format)	Enter the public certificate of the CA that issues the client certificates in your organization.
Revocation verification method	• **None (skip it)** - Disable revocation verification • **From local CRL** - Enter the path to the local CRL on the server (.pem) • **Obtain from Client Certificate**
Certificate data used for authentication	Attribute used to identify users - Define the attribute from the certificate that will be used to identify APM users. Relevant part of the attribute field - for example EMAILADDRESS

TLS and Smart Card Authentication Configuration - Admin Page

In CAC mode, make sure that you have an APM user with the super user roles defined according to the format you specified on the previous page.

For example, if you identify users through the EMAILADDRESS attribute, make sure you have a user whose login name fits this format and you have a valid smart card with a corresponding user.

Note: Without such a user, you will not have administrative permission in APM while smart cards are enabled. If you need to add a new admin user, you can do it after the completion of the smart card authentication wizard.

To access	Select **Admin > Platform > Users and Permissions > Authentication Management**, and in the TLS and Smart Card Authentication Configuration pane, click **Configure**. Navigate to the **Admin** page.

TLS and Smart Card Authentication Configuration - Summary Page

This page indicates if the TLS or smart card authentication configuration was successful. If successful, to activate smart card authentication, you need to restart all APM gateway and data processing servers.

To access	Select **Admin > Platform > Users and Permissions > Authentication Management**, and in the TLS and Smart Card Authentication Configuration pane, click **Configure**. Navigate to the **Summary** page.

LDAP Configuration Wizard

This wizard enables you to create an LDAP authentication strategy for logging into APM.

To access	Select **Admin > Platform > Users and Permissions > Authentication Management**, and click **Add LDAP**.
Important information	If the User Interface does not respond properly after upgrading your version of APM (for example, the page does not load, or an error message is displayed), clean the Java cache by following this procedure on your client PC: 1. Navigate to **Start > Control Panel > Java.** 2. In the Temporary Internet Files section, click **Settings**. 3. In the Temporary File Settings dialog box, click **Delete Files**.
Wizard map	This wizard contains: **LDAP Configuration Wizard** > "LDAP General Configuration Page" below > ("LDAP Vendor Attributes Dialog Box" on page 212) > "LDAP Group Mapping Configuration Page" on page 213 > "LDAP Summary Page" on page 214

LDAP General Configuration Page

This wizard page enables you to use an external LDAP server to store authentication information (user names and passwords) and to enable user synchronization between LDAP users and APM users.

To access	Select **Admin > Platform > Users and Permissions > Authentication Management**, and click **Add LDAP** for new or **Edit** for an existing LDAP Configuration. Navigate to the **LDAP General Configuration** page.
Important information	• When configuring LDAP parameters, consult your LDAP Administrator for assistance.

LDAP General Configuration Section

User interface elements are described below:

UI Element (A-Z)	Description
	Indicates that the value in the specified field is empty or invalid. You can view a description of the error in one of the following ways: • Hover over the error icon to display a tooltip with the error message. • Access the log file **<APM root directory>\log\Jboss\login.log.**
Advanced	Opens the LDAP Vendor Attributes dialog box enabling you to modify configurations for the selected LDAP vendor. For details, see "LDAP Vendor Attributes Dialog Box" on page 212.
Distinguished Name (DN) Resolution	Select to enable entering LDAP search user credentials. **Note:** If your LDAP requires user credentials to verify connection to LDAP server, you will need to use the users-remote-repository service in the JMX console to enter these credentials, because this UI will not let you past LDAP server URL without valid user credentials.
Distinguished Name of Search-Entitled User	Defines the Distinguished Name (DN) of a user with search privileges on the LDAP directory server. **Note:** Leave this entry blank for an anonymous user.

UI Element (A-Z)	Description

LDAP server URL	Enter the URL of the LDAP server. For Active Directory users, we recommend using the Global Catalog server (AD GC).
	
	To represent different trees in the same forest, enter multiple DNs, separated by semicolons.
	
	To allow failover, enter multiple LDAP (AD GC) server URLs, separated by semicolons.
	
	The required format is: **ldap://machine_name:port/scope??sub**
	
	• LDAP servers typically use port 389. Active Directory Global Catalog Servers typically use port 3268 or secure port 3269. We recommend using the Global Catalog server for Microsoft Active Directory.
	• Possible values of scope = **sub**, **one**, or **base**, and are case sensitive.
	• APM ignores the attribute between the two question marks, if one exists.
	• When the port number and scope value are empty, default values are used.
	  • **Default port number for regular communication:** 389
	  • **Default port number for SSL communication:** 636
	  • **Default scope value:** sub
	
	Examples:
	
	Single DN, single LDAP server:
	`ldap://my.ldap.server:389/ou=People,o=myOrg.com??sub`
	
	You can configure multiple domains by entering LDAP server URLs separated by a semicolon (;).The server names must be the same in order to search users in both LDAP servers.
	
	Multiple DNs: `ldap://my.ldap.server:389/ou=People,o=myOrg.com??sub;`
	`ldap://my.ldap.server:389/ou=Staff,o=my2ndOrg.net??sub`
	
	You can configure failover by entering different LDAP server URLs separated by a semicolon (;). For failover, the domain names must be the same.
	
	Failover LDAP servers: `ldap://my.ldap.server:389/ou=People,o=myOrg.com??sub;`
	`ldap://my.2ndldap.server:389/ou=People,o=myOrg.com??sub`
	
	Note: If you receive a red X after entering the URL with the following popup text:
	ERROR - sun.security.validator.ValidatorException: PKIX path building failed: sun.security.provider.certpath.SunCertPathBuilderException: unable to find valid certification path to requested target
	This means that you need to establish trust to the LDAP server. For details, see "How to Secure Communication Between the LDAP Server and APM Server Over SSL" on page 228.
	
	Note: The server names must be the same in order to search users in both LDAP servers.

UI Element (A-Z)	Description
LDAP vendor type	Enter the LDAP vendor you are using. Select from: • Common LDAP • Microsoft Active Directory • Other **Note:** If you click **Advanced** and modify the LDAP Vendor Attribute settings, the value of this field automatically changes to **Other**.
Password of Search Entitled User	Defines the password of the user entitled to search the LDAP server entities for groups. **Note:** Leave this entry blank for an anonymous user.
Unique domain	Enter a name for your LDAP configuration. This name should be unique in your APM system.

Test DN Resolution Section

Enables you to verify that both the configured LDAP parameters and the credentials of a specified user are valid.

User interface elements are described below:

UI Element (A-Z)	Description
Password	The password of the user whose credentials are entered in the **UUID** field. **Note:** This field is optional. If left empty, anonymous user is used.
Test	Tests the LDAP configuration and user credentials validity. A message is displayed indicating whether or not the validation was successful.
UUID	The actual login name (Unique User ID) of the LDAP user you want to verify.

LDAP Vendor Attributes Dialog Box

This dialog box page enables you modify the default LDAP settings that are specific to the selected vendor.

To access	Click **Advanced** on the **LDAP General Configuration Page** of the LDAP Configuration Wizard.
Important information	• If you modify the LDAP Vendor Attribute settings, the value of the **LDAP Vendor Type** field on the LDAP General Configuration page automatically changes to **Other**.

User interface elements are described below:

UI Element (A-Z)	Description
Group class object	Defines which LDAP entities are to be considered groups on the LDAP server.
Groups member attribute	Defines the specific attribute that determines which of the LDAP group's entities are to be considered members of the LDAP group.
Restore	Restores the LDAP vendor attributes to their state upon logging into the current session of APM.
Users filter	Defines which LDAP users are enabled to log into APM. **Note:** The filter should be as narrow as possible and include only users who require access to APM.
Users object class	Defines which LDAP entities are to be considered users on the LDAP server.
Users unique ID attribute	The attribute you want to log into APM with, as it appears on the LDAP server. **Example:** uid, mail

LDAP Group Mapping Configuration Page

This wizard page enables you configure the LDAP server to synchronize LDAP users with APM users.

To access	Select **Admin > Platform > Users and Permissions > Authentication Management**, and click **Configure**. Navigate to the **LDAP Group Mapping Configuration** page.
Important information	• This page is enabled only if the LDAP General Configuration page has been configured correctly.

User interface elements are described below:

UI Element (A-Z)	Description
	Indicates that the value entered in the specified field is invalid.
Groups base DN	The Distinguished Name (DN) of the LDAP entity from which you want to start your groups search. You can configure multiple domains by entering domains separated by a semicolon (;). For example: dc=devlab,dc=ad;dc=BSF_RND
Groups search filter	Enter the relevant parameters to indicate which attributes are to be included in the groups search.
Root groups base DN	The Distinguished Name (DN) of the LDAP groups that are to be first on the hierarchical tree of mapped groups. This value must be a subset of the Groups base DN.

UI Element (A-Z)	Description
Root groups filter	Enter the parameters to determine which LDAP entities are to be the hierarchical base for the LDAP groups. The specified entities are then available to be mapped to groups in APM.
Test	Verifies that the parameters entered to define the LDAP groups structure are valid. This button is disabled if the Test DN Resolution UUID field is empty
Test Groups Configuration Pane	Displays the groups available for mapping with APM groups and the LDAP groups' hierarchical structure. The displayed groups are determined by the parameters entered into the fields on the LDAP Users Synchronization Configuration page. The maximum number of groups that can be displayed is 1000. If there are more than 1000 groups, this list will be empty. If the list is empty, try to change the group search filter. For example, if the group search filter was (objectclass=groupOfUniqueNames) change it to (&(objectClass=groupOfUniqueNames)(cn=APM*)) or reduce the search range: ou=groups,dc=devlab,dc=ad

LDAP Summary Page

This wizard page displays a summary of the authentication strategies configured in the LDAP Configuration Wizard.

To access	Select **Admin > Platform > Users and Permissions > Authentication Management**, and click **Add LDAP**. Enter information in the LDAP pages, and navigate to the **Summary** page.

User interface elements are described below:

UI Element (A-Z)	Description
LDAP General Configuration	Displays the LDAP General Configuration parameters, as configured on the LDAP General Configuration page of the wizard.
LDAP Group Mapping Configuration	Displays the LDAP Group Mapping Configuration parameters, as configured on the LDAP Group Mapping Configuration page of the wizard.

SSO Configuration Wizard

This wizard enables you to create an SSO authentication strategy for logging into APM.

To access	Select **Admin > Platform > Users and Permissions > Authentication Management**, and click **Configure**.

Important information	If the User Interface does not respond properly after upgrading your version of APM (for example, the page does not load, or an error message is displayed), clean the Java cache by following this procedure on your client PC: 1. Navigate to **Start > Control Panel > Java.** 2. In the Temporary Internet Files section, click **Settings**. 3. In the Temporary File Settings dialog box, click **Delete Files**.
Wizard map	This wizard contains: **SSO Configuration Wizard** > "Single Sign-On Page" below > ("SAML2 Configuration Dialog Box" on page 217) > "SSO Summary Page" on page 218

Single Sign-On Page

This wizard page enables you to configure a Single Sign-On strategy. The elements displayed on the Single Sign-On page are determined by the Single Sign-On mode you choose.

Important information	• If a value in one of the wizard fields is blank or invalid, an error icon is displayed on the field's cell. You can view a description of the error in one of the following ways: • Hover over the error icon to display a tooltip with the error message. • Access the log file **<APM>/log/Jboss/login.log.**

User interface elements are described below:

UI Element (A-Z)	Description
Disabled	Select to disable the Single Sign-On (SSO) authentication strategy.
IdentityManagement	Select to configure the Identity Management Single Sign-On (IDM-SSO) authentication strategy. For details on the elements displayed this page, see below. For details on this topic, see "Identity Management Single Sign-On Authentication" on page 223. **Note:** If you have selected this option, LDAP can be configured only for group mapping and not for authentication.
Lightweight	Select to configure the Lightweight Single Sign-On (LW-SSO) authentication strategy. For details on the elements displayed on this page, see below. For details on this topic, see "Lightweight Single Sign-On Strategy" on page 220.

Identity Management Single Sign-On (IDM-SSO) Configuration

User interface elements are described below:

UI Element (A-Z)	Description
	Indicates that the value in the specified field is empty or invalid. Hover over this icon to view a tooltip describing the error.
Header Name	Enter the header name for the token name passed by the Identity Management Single Sign-On. **Example:** `sso_user` **Note:** Ensure that the Identity Management Single Sign-On strategy is securing APM resources before you enter this information.
Logout URL	Enter an alternate logout URL, to view a page other than the main login page when logging out of APM. **Example:** `\<alternativeLogoutURL>.jsp` **Note:** This field is optional.

Lightweight Single Sign-On (LW-SSO) Configuration

User interface elements are described below:

UI Element	Description
	Indicates that the value in the specified field is empty or invalid. Hover over this icon to view a tooltip describing the error.
Add	Adds the host/domain to the list of protected hosts/domains.
Enable SAML2 authentication schema	Select to enable authentication using the Security Assertion Markup Language 2.0 protocol.
HP Business Service Management Domain	Enter the relevant APM domain, to be used for token creation. This field may be needed for multi-domain support and normalized URLs when the domain cannot be parsed automatically, for example when using aliases. **Example:** `devlab.ad`
Parse automatically	Click to parse the APM domain automatically.
SAML2 Settings	Click to set parameters in the SAML2 Configuration Dialog Box.
JMX to get/set Token Creation Key (initString)	This non-editable field contains a link to the attribute in the JMX console where you can change the value of the initString.

UI Element	Description
Trusted Hosts/Domains	Displays the list of trusted hosts and domains that are participating in an LW-SSO integration. List of trusted hosts can contain DNS domain name (myDomain.com), NetBIOS name (myServer), IP address, or fully qualified domain name for the specific server (myServer.myDomain). To add a host or domain to the list of trusted hosts/domains, click the **Add** icon, enter the name of the host or domain in the text box under **Trusted Hosts/Domains**, and select the type of host or domain name from the **Type** drop-down box. **Examples:** `mercury.global, emea.hpqcorp.net, devlab.ad` To remove a host or domain from the list of trusted hosts/domains, select it and click the **Remove** button.

SAML2 Configuration Dialog Box

This dialog box page enables you to modify the SAML authentication parameters for your Lightweight Single Sign-On configuration.

To access	In the SSO Configuration Wizard, navigate to the Single Sign-On page, select **Lightweight**, and select the **Enable SAML2 authentication schema** check box. Click **SAML2 Settings** to open the SAML2 Configuration dialog box. The SAML2 Configuration dialog box consists of the following sections: • **SAML2 Creation.** Modify the SAML2 Authentication parameters for sending SAML authentication requests from APM. • **SAML2 Validation.** Modify the SAML2 Authentication parameters for decrypting SAML requests received by APM.
Important information	• APM comes with SAML enabled by default. If you want to disable SAML authentication, clear the **Enable SAML2 authentication schema** check box.

User interface elements are described below:

UI Element	Description
Restore	Restores the SAML2 configuration attributes to their state upon logging into the current session of APM.

SAML2 Creation Section

User interface elements are described below:

UI Element (A-Z)	Description
Keystore filename	The filename of the keystore in APM. • When **Look for keystore in classpath** is not selected, this value must be the full path of the keystore's location, for example: `C:\mystore\java.keystore.` • When **Look for keystore in classpath** is selected, this value must be just the file name of the keystore, for example: `java.keystore.`
Keystore password	The password which enables access to the keystore containing the private key used for encryption during the SAML authentication request.
Look for keystore in classpath	Select for the Lightweight Single Sign-On framework to search for the keystore in the classpath. **Note:** When this option is selected, you enter only the name of the actual keystore file in the **Keystore filename** field.
Private key alias	Indicates the alias of the private key used for encryption during the SAML authentication request.
Private key password	Indicates the password of the private key used for encryption during the SAML authentication request.

SAML2 Validation Section

User interface elements are described below:

UI Element (A-Z)	Description
Look for keystore in classpath	Select for the Lightweight Single Sign-on framework to search for the keystore in the classpath. **Note:** When this option is selected, you enter only the name of the actual keystore file in the **Keystore filename** field.
Keystore filename	The filename of the keystore in APM. • When **Look for keystore in classpath** is not selected, this value must be the full path of the keystore's location, for example: `C:\mystore\java.keystore.` • When **Look for keystore in classpath** is selected, this value must be just the file name of the keystore, for example: `java.keystore.`
Keystore password	The password of the public key used for decryption during the SAML authentication request.

SSO Summary Page

This wizard page displays a summary of the authentication strategies configured in the SSO Configuration Wizard.

To access	Select **Admin > Platform > Users and Permissions > Authentication Management**, and click **Configure**. Enter information in the Single Sign-On page, and navigate to the **Summary** page.

User interface elements are described below:

UI Element (A-Z)	Description
Single Sign-On Configuration	Displays the Single Sign-On parameters, as configured in the wizard.

Chapter 29: Lightweight Single Sign-On Strategy

This section provides information and instructions for configuring Lightweight Single Sign-On (LW-SSO).

Learn About

Lightweight Single Sign-On Overview

The default single sign-on authentication strategy for APM is LW-SSO. LW-SSO is embedded in APM and does not require an external machine for authentication. APM currently uses version 2.4 of LW-SSO.

For an overview of Single Sign-On strategies, see "Authentication Strategies" on page 201.

Configuring LW-SSO

You can configure LW-SSO in APM using the SSO Configuration Wizard. For details on the SSO Configuration Wizard, see "SSO Configuration Wizard" on page 214.

LW-SSO can be configured using the JMX console to accept client-side authentication certificates. Once a certificate is recognized, LW-SSO creates the token to be used by other applications. For details, see "Using Client-Side Authentication Certificates for Secure User Access to APM " on page 19.

For details on limitations of working with LW-SSO, see "LW-SSO Authentication – General Reference" on page 236.

LW-SSO Configuration for Multi-Domain and Nested Domain Installations

LW-SSO configuration, set in the SSO Configuration Wizard (for details, see "SSO Configuration Wizard" on page 214), depends on the architecture of your APM installation.

If you log into APM through a man-in-the-middle, such as reverse proxy, a load balancer, or NAT, the APM domain is the domain of the man-in-the-middle.

If you log in directly to the APM Gateway, the APM domain is the domain of the APM Gateway.

For LW-SSO to work with another application in a domain different from the APM domain, all of these domains must be listed in the **Trusted Hosts/Domains** list of the LW-SSO configuration.

If your APM domain and integrating application are located in nested domains, then the suffix of the domain should be the defined as the LW-SSO domain for both applications. In addition, you should disable automatic domain calculation (**Parse automatically** in the SSO Configuration Wizard) and explicitly state the domain suffix.

Tasks

How to Configure Unknown User Handling Mode

This task describes how to handle unknown users trying to log into APM—users that were authenticated by the hosting application but do not exist in the APM users repository:

1. Select **Admin > Platform > Setup and Maintenance > Infrastructure Settings**, click **Foundations**, and select **Single Sign On**.
2. Locate the **Unknown User Handling Mode** entry in the Single Sign On - Lightweight (LW-SSO) field, and select one of the following options:
   - **Integration User.** A user with the User name **Integration User** is created in place of the user who attempted to login. This user has System Viewer permissions.
   - **Allow.** The user is created as a new APM user and allowed access to the system. This user has System Viewer permissions, and his default password is his login name.
   - **Deny.** The user is denied access to APM, and is directed to the Login page.

   The changes take effect immediately.

Note: When User Synchronization is enabled between APM and the LDAP server, unknown users are always denied entry into APM.

How to Modify LW-SSO Parameters Using the JMX Console

This task describes how to modify options and parameters used with LW-SSO in the JMX console.

You can also use the JMX console if you are locked out of APM and must change SSO parameters to gain access.

1. Enter the URL of the JMX console (**http://<server name>:29000/**) in a web browser.
2. Enter your JMX console authentication credentials. If you do not know your authentication credentials, contact your system administrator.
3. Locate the Lightweight Single Sign-On context, as follows:
   a. Domain name: **Topaz**
   b. Service: **LW-SSO Configuration**
4. Modify parameters accordingly.

The changes take effect immediately.

Troubleshooting and Limitations

Unable to Access APM Due to Changes in LW-SSO Parameters

If you are locked out of APM, you can update selected Lightweight Single Sign-On (LW-SSO) parameters remotely using the JMX console on the application server that is embedded in APM.

For details on how to change LW-SSO parameters outside the APM interface, see "How to Modify LW-SSO Parameters Using the JMX Console" above.

Synchronizing Users When Using LW-SSO

LW-SSO does not ensure user synchronization between integrated applications. Therefore, you must enable LDAP and configure group mapping for the integrated application to monitor users. Failure to map groups and synchronize users may cause security breaches and negative application behavior. For details on mapping users between applications, see "How to Map Groups and Synchronize Users" on page 233.

Unable to Log into APM when Using an External Authentication Point

If you enabled an external authentication point (AP) and are unable to log in through it, make sure that the user whose credentials you are entering is defined as a user in APM.

Chapter 30: Identity Management Single Sign-On Authentication

Identity Management Single Sign-On (IDM-SSO) provides a more secure connection than that offered by LW-SSO. It also can be used if the applications configured outside of APM do not support LW-SSO.

Learn About

This section includes:

IDM Server

The IDM server is monitored by a single center Policy Server, and consists of a User Repository, a Policy Store (both could reside over the same server as the policy server), and a Web Server Agent installed over each of the application's web servers communicating with the Policy Server. The IDM server controls users' access to various organizational resources, protecting confidential personal and business information from unauthorized users. For details, see your IDM vendor's documentation.

Storing User Information

APM requires the IDM vendor to store user information to render it available as a header on http requests. You configure both the Header name and the IDM-SSO strategy in the SSO Configuration Wizard. For details, see "SSO Configuration Wizard" on page 214.

IDM Login

Before configuring IDM-SSO in APM, make sure you see your IDM login dialog box before the APM login screen.

If you do not see it, work with your IDM administrator. If the same LDAP was defined in APM as used by IDM, you should be able to authenticate through both the IDM and APM login screens using the same credentials. If not, verify that LDAP settings in APM match those used by IDM. Now you are ready to configure IDM-SSO in APM.

You can verify the correct IDM header to use in configuration using **http://<HPE APM server>/topaz/verifyIDM.jsp** in the same user session. Once it is verified as correct, you should be able to use it in the SSO Configuration Wizard.

Securing APM Resources Under IDM-SSO

When using IDM-SSO as a Single Sign-On strategy, APM resources may be protected with form or basic authentication schemes, or left unprotected.

Resources Accessed by Application Users

If you want to use IDM-SSO to secure APM resources accessed by application users, use **form authentication** on the following resources:

- /filters/*
- /hpbsm/*
- /mam-images/*
- /mcrs/*
- /MercuryAM/*
- /odb/*
- /opal/*
- /opr-admin-server/*
- /opr-console/*
- /opr-gateway/*
- /opr-web/*
- /ovpm /*
- /topaz/*
- /topazSettings/*
- /ucmdb-ui/*
- /uim/*
- /utility_portlets/*
- /webinfra/*

Examples of URL with form authentication

- The following URL verifies that the IDM header is correct:
  `https://<gateway server>/topaz/verifyIDM.jsp?headerName=sm_user`
  Expected Result: The system displays the user name of the current user (provided that SM authentication was performed prior to this action).
- The following URL shows values of all cookies in the session:
  `https://<gateway server>/topaz/DumpSession.jsp`
  Expected Result: The system displays a table of all cookies in the user session and their corresponding values.

Resources Accessed by Data Collectors

If you want to use IDM-SSO to secure APM resources accessed by data collectors in machine-to-machine communication, use an authentication method that allows **passing credentials**, or **basic authentication**.

The following resources are used by data collectors:

- /ext/* — used by RUM
- /mam/* — used by RTSM
- /topaz/topaz_api/* — used by all data collectors to get APM version, server time, etc.

Example of URL with basic authentication

- The following URL is used by data collectors to establish a connection to APM:

  `https://<gateway server>/topaz/topaz_api/api_getsystemkey.asp`

  Expected Result: The system displays the basic authentication window followed by a value, for example -7.

Resources Accessed by Web Services (Required)

If you use IDM-SSO with APM, you must protect the following resources with **basic authentication** as they are used by various APM web services:

- /opr-admin-server/rest/*
- /opr-console/rest/*
- /opr-gateway/rest/*
- /topaz/bam/*
- /topaz/bsmservices/*
- /topaz/eumopenapi/*
- /topaz/servicehealth/*
- /topaz/slm/*

Additional Resources to be Protected with Basic Authentication

- /topaz/rfw/directAccess.do — used with published URL to a report
- /topaz/sitescope/* — used for SAM Admin embedded in APM UI

Unprotected Resources

The following resources should remain **unprotected**:

- /mam-collectors
- /topaz/Charts
- /topaz/images
- /topaz/Imgs/chartTemp
- /topaz/js
- /topaz/rfw/static
- /topaz/services/technical/time
- /topaz/static
- /topaz/stylesheets
- /ucmdb-api

If you are using a Load Balancer, you should also **unprotect** the following resources:

- /topaz/topaz_api/loadBalancerVerify_core.jsp
- /topaz/topaz_api/loadBalancerVerify_centers.jsp

Troubleshooting and Limitations

Errors When Entering IDM-SSO Header in SSO Configuration Wizard

Make sure the correct header is used. Ask your Siteminder administrator to dump all headers and look for one that matches what you expect to use. For example, if you want to use an email address as your login username, look for a field containing only an email address. Or, for example, if it looks like **HTTP_SEA**, remove **HTTP_** from the name and use **sea** as the header name.

Verifying Correct User ID

To verify that you get the correct user ID with the header you provided, go to **https://<APM server>/topaz/verifyIDM.jsp?headerName=sea** (if **sea** is your header).

Chapter 31: LDAP Authentication and Mapping

This section provides an overview to LDAP authentication and mapping.

Learn About

LDAP Authentication Overview

You can use an external LDAP server to store users' information (usernames and passwords) for authentication purposes, instead of using the internal APM service. You can also use the LDAP server to synchronize APM and LDAP users. For optimal performance, it is recommended that the LDAP server be in the same subnet as the rest of the APM servers. For optimal security, it is recommended to either configure an SSL connection between the APM Gateway Server and the LDAP server, or to have APM servers and the LDAP server on the same secure internal network segment.

Authentication is performed by the LDAP server, and authorization is handled by the APM server.

You configure the LDAP server for authentication and user synchronization using the LDAP Configuration Wizard. For details on the LDAP Configuration Wizard, see "LDAP Configuration Wizard" on page 209

For details on securing communication between an LDAP server and your APM server over SSL, see "How to Secure Communication Between the LDAP Server and APM Server Over SSL" on the next page

Mapping Groups

You map groups to enable user synchronization between LDAP users and APM users. The Group Mapping feature is accessible through the Users and Permissions interface, by clicking the **Group Mappings**  button and selecting the unique domain name. This button is enabled only if the following conditions are met:

- There is at least one enabled LDAP Configuration on the Authentication Management page.
- The user has administrator permissions.

Once user synchronization is enabled, the User Management interface has the following limitations:

- You cannot create a user.
- The User name and Login name fields for individual users are disabled.
- The Password field is invisible.
- You cannot manually assign users to groups using the Hierarchy tab.

> **Note:** Users who are not assigned to any group will appear at the Root (All) level, with the role defined in **Automatically Created User Roles**, in **Infrastructure Settings**, under **LDAP Global Configuration**. If this does not give you sufficient control of user permissions, see "Achieving Finer Control over Default User Permission Assignments" on page 235.

> **Note:** Some customers like the concept of automatic user creation but prefer to put users into the appropriate APM groups manually. However, as noted above, with user synchronization enabled, manual group assignment is disabled in APM.

To manually assign users to the appropriate APM group when LDAP User Synchronization is enabled, do the following:

1) Disable User Synchronization in **Group Mappings.**

2) Assign users to groups manually using the **Hierarchy** tab.

3) Re-enable User Synchronization in **Group Mappings.**

You can optionally map an LDAP group to multiple APM groups, or multiple LDAP groups to an APM group.

When enabling the Group Mapping feature, you can log into APM with any unique user attribute that exists on the LDAP server (for example, an email address). For details, see "How to Modify the Attribute Used to Log into APM" below.

If you want to place all users not mapped to a specific group in the APM User Management (instead of assigning LDAP users to the root level in the APM User Management), you can create a group for them and activate the **Default LDAP Group** setting. For details, see "How to Activate Default LDAP Group" on the next page.

Mixed Authentication Mode

Mixed authentication mode enables users to be authenticated in the external LDAP and internally in APM. This mode is relevant only when there is at least one LDAP configuration defined and enabled.

If a user logs in when this mode is enabled, APM attempts to locate and authenticate the user in LDAP. If APM does not locate the user in LDAP, APM attempts to locate and authenticate the user in the internal APM users database.

This functionality enables you to create temporary APM users and integration users in APM and not in the external LDAP.

Note: Creating users only in the APM database is not recommended since a user that exists only in APM is a less secure user than a user that exists in the LDAP database.

Note that in mixed authentication mode, administrators can only modify user parameters in the User Management interface for users who do not exist in the LDAP database.

Tasks

How to Modify the Attribute Used to Log into APM

This task describes how to modify the LDAP attribute with which you want to log into APM.

1. Navigate to **Admin > Platform > Users and Permissions > Authentication Management**.
2. Click the **Edit** button under LDAP Configuration to activate the LDAP Configuration Wizard.
3. Navigate to the **LDAP General Configuration** page, and click the **Advanced** button.
4. Modify the **User unique ID** attribute to the attribute you want to log in with, as it appears on the LDAP server.

How to Secure Communication Between the LDAP Server and APM Server Over SSL

1. If the LDAP server requires a secure connection perform the following steps:

a. Obtain root CA certificate from the Certificate Authority that issued LDAP server certificate.
b. Import it into the truststore of JVM on each APM gateway (for both JRE and JRE64).
c. Restart the APM gateway servers.

Example

```
cd C:\HPBSM\JRE64\bin
keytool -import -trustcacerts -alias myCA -file c:\RootCA.cer -keystore
..\lib\security\cacerts
cd C:\HPBSM\JRE\bin
keytool -import -trustcacerts -alias myCA -file c:\RootCA.cer -keystore
..\lib\security\cacerts:
```

2. Verify that communication between the LDAP server and the APM server is valid over SSL, using the LDAP Configuration Wizard, as follows:
   a. Navigate to the LDAP Configuration Wizard by selecting **Admin > Platform > Users and Permissions > Authentication Management**, click **Edit** under LDAP Configuration and navigate through the LDAP Configuration Wizard to the LDAP General page.
   b. Enter the URL of your LDAP server, according to the following syntax: ldaps://machine_name:port/<scope>??sub.

      Ensure that the protocol is ldaps://, and the port number is configured according to the SSL port, as configured on the LDAP server (default is 636).
   c. Test your configuration on the LDAP General Configuration page by entering the UUID and password of a known LDAP user in the relevant fields. Click **Test** to authenticate the user. For details, see "LDAP General Configuration Page" on page 209.

How to Enable Mixed Authentication Mode

From the APM console:

1. Select **Admin > Platform > Setup and Maintenance > Infrastructure Settings**.
2. Select **Foundations > LDAP Global Configuration**.
3. Enable **Mixed Authentication mode**.

From the JMX console:

1. Enter the URL of the JMX console (http://<server name>:29000/) in a web browser.
2. Enter your JMX console authentication credentials. If you do not know your authentication credentials, contact your system administrator.
3. Locate **Foundations > service=users-remote-repository**.
4. Set the **IsMixedAuthenticationModeEnabled** parameter to **True**.

How to Activate Default LDAP Group

You need to obtain the unique ID of the created group in the GROUPS_AUTH table of management DB.

Select GRP_GROUP_ID from the GROUPS_AUTH table where GRP_GROUP_NAME='group_name'.

You should use the group ID for this setting only which enables you to rename the group as necessary.

From the APM console:

1. Select **Admin > Platform > Setup and Maintenance > Infrastructure Settings**.
2. Select **Foundations > LDAP Global Configuration**.

3. In the **LDAP Global Configuraiton - LDAP Options for Classes and Attributes** section, assign the group ID number to the **Default LDAP Group unique ID** setting.

Troubleshooting and Limitations

Secure Connection to LDAP Server

When setting the LDAP server URL, you see a red cross containing the following error:

ERROR - sun.security.validator.ValidatorException: PKIX path building failed: sun.security.provider.certpath.SunCertPathBuilderException: unable to find valid certification path to requested target

This means that you have not yet configured a secure connection to the LDAP server.

For details about securing a connection to the LDAP server, see "How to Secure Communication Between the LDAP Server and APM Server Over SSL" on page 228.

Case Sensitive Login

When APM is installed with an Oracle database and User Synchronization is enabled with an LDAP Active Directory server, ensure that you log into APM with the correct-case UID (uppercase or lowercase), as configured on the LDAP server. This is because while the Oracle database is case sensitive, the LDAP Active Directory is case insensitive, and logging in with an incorrect case UID can create undesirable results.

For example, if a user called **testuser** exists on the LDAP Active Directory server and logs into APM, he is automatically created as APM user **testuser**, who can be assigned permissions in the APM User Management interface. If you then log into APM as **Testuser**, the LDAP Active Directory server sends an acknowledgment that the user exists (because Active Directory is case insensitive) and he is allowed entry to APM. However, since the Oracle database does not identify this user as **testuser** (because the Oracle database is case sensitive), the user **Testuser** is treated as a new user, without the permissions that were assigned to **testuser**.

Empty User Fields

If when signing in to APM with LDAP, the authentication is working, but the user fields are empty, change the **User display name** attribute in Infrastructure Settings to **displayName**.

1. Select **Admin > Platform > Setup and Maintenance > Infrastructure Settings**.
2. Select **Foundations > LDAP Global Configuration**.
3. Under **LDAP Global Configuration - LDAP Options for Classes and Attributes** locate **User display name attribute** and change the value to **displayName**.

Cannot Login to APM with Administrator User Credentials

If LDAP contains an administrator user with the same login name as the APM local administrator user, the APM local administrator user credentials will be overwritten by LDAP, and you will not be able to login to APM through this user if LDAP is disabled.

To enable users to login to APM with local administrator user credentials when LDAP is disabled, remove the administrator user from the LDAP database, and update the authentication users parameters in the Users table in the APM database.

Synchronizing Users

The user synchronization feature maps users from an LDAP server to users in APM.

Learn About

Mapping Users from LDAP Servers to APM

Mapping users from an LDAP server to users in APM simplifies the process of managing users for APM administrators, as all of the user management functions are done through the LDAP server.

Granting Permissions

It is recommended to grant permissions on the group level in APM, and then nest users into groups according to their desired permission level. If users are moved between LDAP groups, they are moved between their corresponding mapped groups on the APM server after logging into APM.

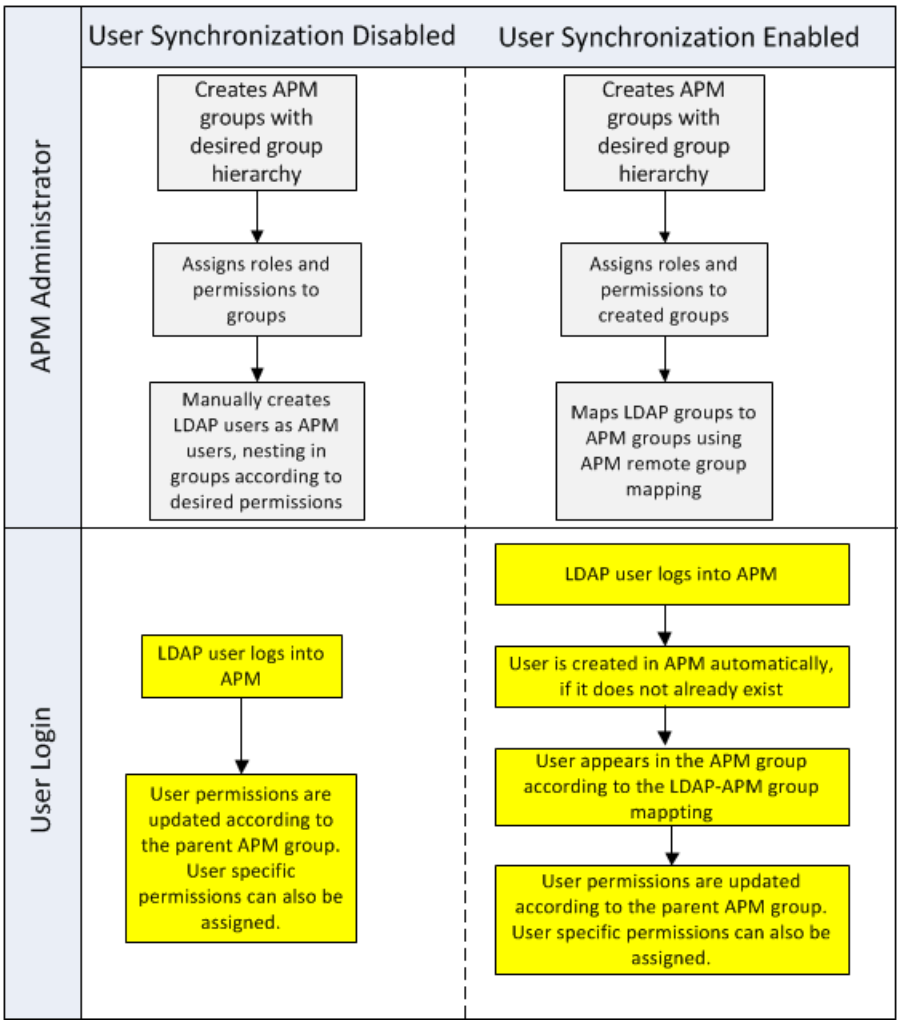
Status of LDAP Users not in APM

LDAP users who do not exist in, and log into, APM, are created as APM users. Their status is determined as follows:

- If the user belongs to a mapped LDAP group, she is automatically assigned to the APM group that is mapped to their LDAP group.
- If their group is not mapped to an APM group, or if they do not belong to an LDAP group, they are nested under the **Root** group and created as an APM user with **System Viewer** permissions. Their permissions and user hierarchy can be modified on the User Management interface.

LDAP User Management Process

The following flowchart displays the process of User Management when LDAP is enabled, as performed by the APM administrator and APM itself when the user logs in:



Matching the User Filter

For an LDAP user to log into APM, he must match the criteria defined in the **Users filter** field on the LDAP Advanced General Configuration dialog box in the LDAP Configuration Wizard. For details on the LDAP General Configuration page, see "LDAP Vendor Attributes Dialog Box" on page 212.

Note: Be aware that any new LDAP user who satisfies the user filter will be created as an APM user on first login. Ask your LDAP administrator to help you narrow down the filter definition so that only appropriate users can gain access to APM.

Synchronizing Users After Upgrading from a Previous Version of APM

When upgrading from a previous version of APM, User Synchronization becomes disabled by default.

For details on how to enable User Synchronization, see "How to Synchronize Users After Upgrading from a Previous Version of APM" on page 235.

Obsolete Users

Users that have been removed from the LDAP server are still displayed as APM users, even though they are no longer registered as LDAP users and cannot log into APM. These users are called **Obsolete Users**. For

details on removing Obsolete Users from APM, see " How to Delete Obsolete Users" on page 235.

Tasks

How to Map Groups and Synchronize Users

1. Configure Group Filters on the LDAP Server for Mapping Groups

   You can configure group filters on the LDAP Server for mapping groups using the LDAP Configuration Wizard. For task details, see "LDAP Configuration Wizard" on page 209.

2. Create APM Groups and Hierarchy

   You create local groups in APM with the appropriate roles to nest users into, and users adopt the permission level of the group they are nested in. For task details, see "Groups/Users Pane" on page 127.

3. Map LDAP Groups to APM Groups

   You map user groups on the LDAP server to groups in APM.

   Caution: Administrators must create an account in APM with superuser permissions after enabling the LDAP server but before configuring group mapping and user synchronization. Without an APM account with superuser permissions, you cannot configure group mapping and user synchronization because only a user with superuser permission can access the User Manager page.

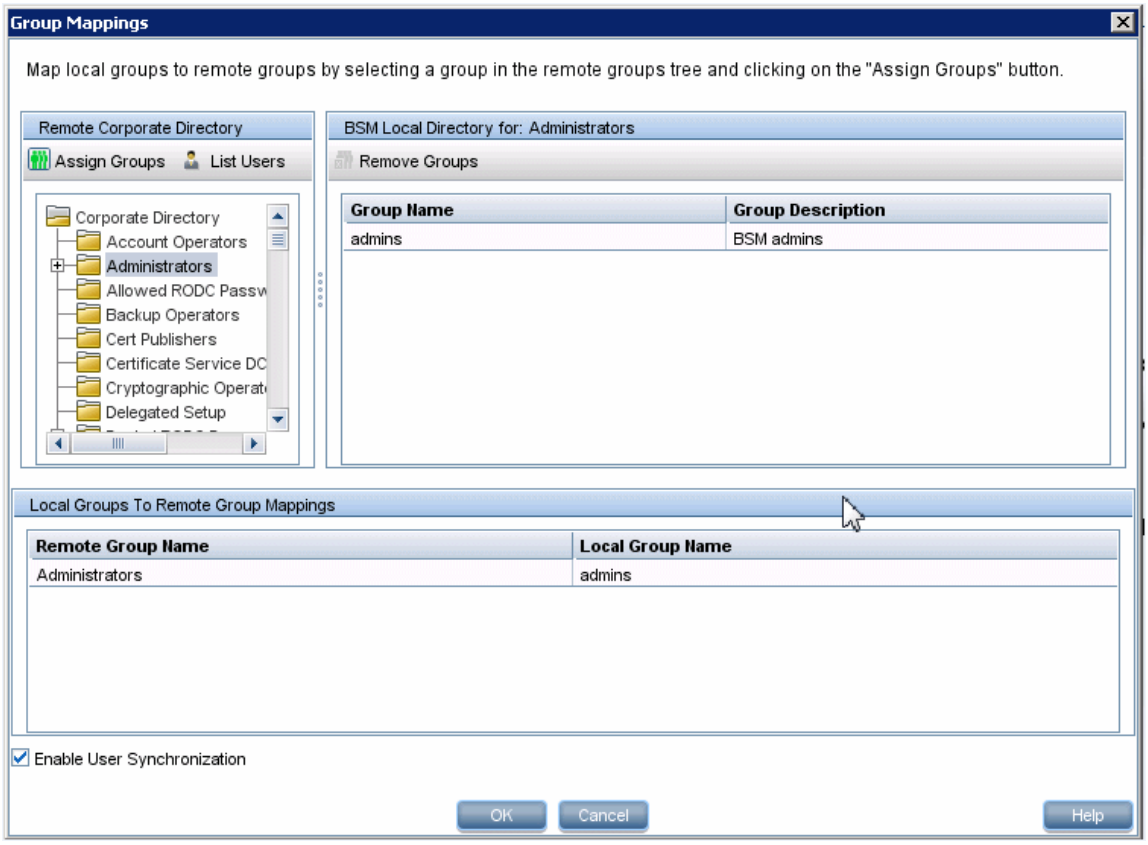
   a. On the Users and Permissions interface, navigate to the Groups/Users pane, click the Group Mappings  button and select the unique domain name to open the Group Mappings dialog box.

   b. In the **Remote Corporate Directory** pane, select a remote LDAP server group and click **Assign Groups**.

      The APM groups mapped to the selected LDAP group are displayed in the **APM Local Directory for Remote Group: <group name>** pane.

      Existing mapping of all LDAP groups is displayed in the **Local Groups to Remote Groups Mapping** pane.

Mapping local groups to remote groups:



4. Enable User Synchronization

   Select this option to enable User Synchronization upon logging into APM, to synchronize LDAP users with APM users. You enable synchronization of user groups on the LDAP server with user groups in APM by selecting the **Enable User Synchronization** check box in the **Group Mappings** dialog box.

   - Before enabling user synchronization, ensure that you have either created a superuser account in APM that matches your own LDAP user login, or mapped an appropriate LDAP group to an APM group that has the **superuser** role assigned to it. If you have not done so, and log out of APM after enabling LDAP but before group mapping is completed and user synchronization is enabled, the designated APM superuser account will be locked out of APM.
   - Ensure that you have mapped LDAP groups to APM groups before selecting this check box. If you have not performed Group Mapping, all users are nested under the Root group and are assigned System Viewer permissions.
   - To disable user synchronization and enable management of users through the User Management interface in APM, clear the **Enable User Synchronization** check box in the **User Management > Group Mappings** dialog box.

   For details on synchronizing users, see "LDAP Group Mapping Configuration Page" on page 213.

How to Synchronize Users After Upgrading from a Previous Version of APM

1. If you have upgraded from a version earlier than BAC 7.50, ensure that the **Enable User Synchronization** check box on the **User Management > Group mappings** dialog box is cleared.
2. Ensure that LDAP groups have been mapped to APM groups and enable **User Synchronization**. For details on performing this task, see "How to Map Groups and Synchronize Users" on page 233.

How to Delete Obsolete Users

This task describes how to delete APM users who no longer exist on the LDAP server. This option is enabled only if the following conditions are met:

- The needed LDAP Configuration is enabled on **Authentication Management** page.
- The user has **Delete** permissions.

To delete obsolete users:

1. Select **Admin > Platform > Users and Permissions,** click the click the **Delete Obsolete Users**  button and select the unique domain name.
2. Select the user you want to delete.

Achieving Finer Control over Default User Permission Assignments

If you need a default group mapping for all users who do not fit into any of the currently mapped groups, and the default APM user role (as defined in the infrastructure setting **Automatically Created User Roles** under **LDAP Configuration**) provides insufficient granularity, use the Dynamic LDAP group feature in APM.

Request that your corporate LDAP server administrator create a dynamic LDAP group based on the same user filter that you specified in the APM LDAP configuration.

This user filter automatically populates and maintains members of the dynamic group in your corporate LDAP.

In APM, create a local group with the roles and permissions that you require by default. Map the dynamic group created in your corporate LDAP to the APM local group. Any user who is allowed to enter APM but does not belong to any other mapped group will belong to the default group. Without such a default group, these users would be created at the root level in the User Management tree and their permissions would need to be handled individually.

To enable dynamic LDAP groups in APM, go to **Infrastructure Settings**, select the **LDAP Configuration** context and set **Enable Dynamic Groups** to true. The change takes effect immediately.

Before dynamic groups are enabled, **List Users**, in the Group Mappings dialog box under **Users and Permissions**, will not display members of the dynamic group.

Note: Because corporate LDAP groups can be very large, **List Users** will display only up to the first 100 users. To see the whole user list or search for specific users, use a standard LDAP browser.

Chapter 32: LW-SSO Authentication – General Reference

LW-SSO is a method of access control that enables a user to log on once and gain access to the resources of multiple software systems without being prompted to log on again. The applications inside the configured group of software systems trust the authentication, and there is no need for further authentication when moving from one application to another.

The information in this section applies to LW-SSO version 2.4.

- LW-SSO Token Expiration

  The LW-SSO Token's expiration value determines the application's session validity. Therefore, its expiration value should be at least the same value as that of the application session expiration value.
- Recommended Configuration of the LW-SSO Token Expiration

  Each application using LW-SSO should configure token expiration. The recommended value is 60 minutes. For an application that does not require a high level of security, it is possible to configure a value of 300 minutes.
- GMT Time

  All applications participating in an LW-SSO integration must use the same GMT time with a maximum difference of 15 minutes.
- Multi-domain Functionality

  Multi-domain functionality requires that all applications participating in LW-SSO integration configure the trustedHosts settings (or the **protectedDomains** settings), if they are required to integrate with applications in different DNS domains. In addition, they must also add the correct domain in the **lwsso** element of the configuration.
- Get SecurityToken for URL Functionality

  To receive information sent as a **SecurityToken for URL** from other applications, the host application should configure the correct domain in the **lwsso** element of the configuration.

LW-SSO System Requirements

The following table lists LW-SSO configuration requirements:

Application	Version	Comments
Java	1.5 and higher	
HTTP Sevlets API	2.1 and higher	
Internet Explorer	6.0 and higher	Browser should enable HTTP session cookie and HTTP 302 Redirect functionality
FireFox	2.0 and higher	Browser should enable HTTP session cookie and HTTP 302 Redirect functionality
JBoss Authentications	JBoss 4.0.3 JBoss 4.3.0	

Application	Version	Comments
Tomcat Authentications	Standalone Tomcat 6.0.29 Standalone Tomcat 5.0.28 Standalone Tomcat 5.5.20	
Acegi Authentications	Acegi 0.9.0 Acegi 1.0.4	
Spring Security Authentication	Spring Security 2.0.4	
Web Services Engines	Axis 1 - 1.4 Axis 2 - 1.2 JAX-WS-RI 2.1.1	

LW-SSO Security Warnings

This section describes security warnings that are relevant to the LW-SSO configuration:

- **Confidential InitString parameter in LW-SSO.** LW-SSO uses Symmetric Encryption to validate and create a LW-SSO token. The **initString** parameter within the configuration is used for initialization of the secret key. An application creates a token, and each application using the same initString parameter validates the token.

  Caution:
  - It is not possible to use LW-SSO without setting the **initString** parameter.
  - The **initString** parameter is confidential information and should be treated as such in terms of publishing, transporting, and persistency.
  - The **initString** parameter should be shared only between applications integrating with each other using LW-SSO.
  - The **initString** parameter should have a minimum length of 12 characters.

- **Level of authentication security.** The application that uses the weakest authentication framework and issues a LW-SSO token that is trusted by other integrated applications determines the level of authentication security for all the applications.

  It is recommended that only applications using strong and secure authentication frameworks issue an LW-SSO token.

- **Symmetric encryption implications.** LW-SSO uses symmetric cryptography for issuing and validating LW-SSO tokens. Therefore, any application using LW-SSO can issue a token to be trusted by all other applications sharing the same **initString** parameter. This potential risk is relevant when an application sharing an initString either resides on, or is accessible from, an untrusted location.

- **User mapping (Synchronization).** The LW-SSO framework does not ensure user mapping between the integrated applications. Therefore, the integrated application must monitor user mapping. We recommend that you share the same user registry (as LDAP/AD) among all integrated applications.

  Failure to map users may cause security breaches and negative application behavior. For example, the same user name may be assigned to different real users in the various applications.

  In addition, in cases where a user logs onto an application (AppA) and then accesses a second application (AppB) that uses container or application authentication, the failure to map the user will force the user to manually log on to AppB and enter a user name. If the user enters a different user name than was used to log on to AppA, the following behavior can arise: If the user subsequently accesses a third application (AppC) from AppA or AppB, then they will access it using the user names that were used to log on to AppA or AppB respectively.
- **Identity Manager.** Used for authentication purposes, all unprotected resources in the Identity Manager must be configured with the **nonsecureURLs** setting in the LW-SSO configuration file.

LW-SSO Troubleshooting and Limitations

Known Issues

This section describes known issues for LW-SSO authentication.

- **Security context.** The LW-SSO security context supports only one attribute value per attribute name.

  Therefore, when the SAML2 token sends more than one value for the same attribute name, only one value is accepted by the LW-SSO framework.

  Similarly, if the IdM token is configured to send more than one value for the same attribute name, only one value is accepted by the LW-SSO framework.

Limitations

Note the following limitations when working with LW-SSO authentication:

- **Client access to the application**.

  If a domain is defined in the LW-SSO configuration:
  - The application clients must access the application with a Fully Qualified Domain Name (FQDN) in the login URL, for example, http://myserver.companydomain.com/WebApp.
  - LW-SSO cannot support URLs with an IP address, for example, http://192.168.12.13/WebApp.
  - LW-SSO cannot support URLs without a domain, for example, http://myserver/WebApp.

  If a domain is not defined in the LW-SSO configuration: The client can access the application without a FQDN in the login URL. In this case, an LW-SSO session cookie is created specifically for a single machine without any domain information. Therefore, the cookie is not delegated by the browser to another, and does not pass to other computers located in the same DNS domain. This means that LW-SSO does not work in the same domain.
- **LW-SSO framework integration.** Applications can leverage and use LW-SSO capabilities only if integrated within the LW-SSO framework in advance.
- **Multi-Domain Support**.
  - Multi-domain functionality is based on the HTTP referrer. Therefore, LW-SSO supports links from one application to another and does not support typing a URL into a browser window, except when both

applications are in the same domain.

- The first cross domain link using **HTTP POST** is not supported.

  Multi domain functionality does not support the first **HTTP POST** request to a second application (only the **HTTP GET** request is supported). For example, if your application has an HTTP link to a second application, an **HTTP GET** request is supported, but an **HTTP FORM** request is not supported. All requests after the first can be either **HTTP POST** or **HTTP GET**.

- LW-SSO Token size:

  The size of information that LW-SSO can transfer from one application in one domain to another application in another domain is limited to 15 Groups/Roles/Attributes (note that each item may be an average of 15 characters long).

- Linking from Protected (HTTPS) to non-protected (HTTP) in a multi-domain scenario:

  Multi domain functionality does not work when linking from a protected (HTTPS) to a non-protected (HTTP) page. This is a browser limitation where the referrer header is not sent when linking from a protected to a non-protected resource.

- **SAML2 token.**
  - Logout functionality is not supported when the SAML2 token is used.

    Therefore, if the SAML2 token is used to access a second application, a user who logs out of the first application is not logged out of the second application.
  - The SAML2 token's expiration is not reflected in the application's session management.

    Therefore, if the SAML2 token is used to access a second application, each application's session management is handled independently.
- **JAAS Realm.** The JAAS Realm in Tomcat is not supported.
- **Using spaces in Tomcat directories.** Using spaces in Tomcat directories is not supported.

  It is not possible to use LW-SSO when a Tomcat installation path (folders) includes spaces (for example, Program Files) and the LW-SSO configuration file is located in the **common\classes** Tomcat folder.
- **Load balancer configuration.** A load balancer deployed with LW-SSO must be configured to use sticky sessions.

Part 5: Reports and Alerts Administration

Chapter 33: Report Schedule Manager

This page enables you to edit, delete, resume, or pause scheduled reports.

To access	Select **Admin > Platform > Report Scheduling**
Important information	You cannot create a new schedule from the Report Schedule Manager. For details on creating schedules, see How to Schedule a Report in the APM User Guide.

Caution: Scheduled reports place pressure on the system and can cause performance issues for users who are logged on. When possible, you should schedule reports for off hours when fewer users access the system. If your system does not have off hours, you should stagger reports at different times of the day to minimize the number of reports running simultaneously.

User interface elements are described below:

UI Element (A–Z)	Description
	Opens the Edit Schedule for the <Report Name> dialog box enabling you to edit the selected schedule. For details, see Creating a New Schedule Dialog Box in the APM User Guide. **Note:** This dialog box enables you only to edit an existing schedule - you create a new schedule from the Report Manager interface. For details, see Creating a New Schedule Dialog Box in the APM User Guide.
	Deletes the selected schedule.
	Resumes the selected schedule, this button is only available if the selected report has been paused.
	Pauses the selected schedule.
	Refreshes the Report Schedule Manager page.
	Resets the width of the columns to the default setting.
	Enables you to select columns to be visible in the table.
Generation Time	The time (in the indicated time zone) that the schedule is to be generated.
Recipients	The individuals configured in the Report Manager to receive the report or report item at scheduled intervals. For details on configuring Schedules, see Creating a New Schedule Dialog Box in the APM User Guide.
Recurrence	The recurrence pattern for the selected schedule.
Report Name	The name of the report for which the schedule is configured.

UI Element (A–Z)	Description
Report Type	The type of report for which the schedule is configured.
Status	The status of the schedule. Possible values are: • Active • Paused

Chapter 34: Setting Up an Alert Delivery System

APM alerts proactively inform you when predefined performance limits are breached, by triggering alerts.

For task details, see "How to Set Up an Alert Delivery System" on page 245.

Alert Recipients

Alerts can be configured to send notification to specified recipients. For task details on configuring recipients, see "Recipient Management" on page 184.

Notification Template

For each recipient, you can specify the notification method (any combination of email, pager, and/or SMS) and the template to use for alert notices. You can also create a notification schedule for the alerts. For details, see "How to Configure EUM Alerts Notification Templates" on page 260.

Alert Schemes

In each alert scheme, you define a unique set of alert properties. After you create an alert scheme, you view and edit it in the appropriate Alerts user interface. For detailed tips and guidelines, see "Planning for Effective Alert Schemes" on the next page.

You can configure alerts and assign recipients to the alerts for:

- **CIs in a view.** CI Status alerts are triggered by a pre-defined status change for the selected configuration item (CI) detected by the Business Logic Engine. For details, see CI Status Alerts Administration in the APM User Guide.
- Service Manager automatically opens incidents when a CI Status alert is triggered in APM. For details, see Service Manager in the APM section of the HPESW Solution and Integration Portal.
- **SLAs.** SLA status alerts are triggered by changes to an SLA's key performance indicator status. For details, see SLA Alerts Administration in the APM User Guide.
- **EUM alerts.** EUM alerts are triggered when pre-defined conditions, such as transaction response time, availability, success or failure, or completion time, are reached. For details, see End User Management Alerts Administration in the APM User Guide.

Open Events in OMi

You can automatically submit events to OMi, when a CI Status alert, an SLA alert, or an EUM alert is triggered in APM when APM is configured to do so. For details, see the OMi Integration Guide.

Alert History

You can view the history of the alerts in the following:

- **CI Status Alerts Report tab.** Enables you to list all of the CI Status alerts that were triggered during the specified time range. For details, see Configuration Item Status Alerts Report in the APM User Guide.
- **SLA Alerts Report tab.** Enables you to list all of the Service Level Management alerts that were triggered during the specified time range. For details, see Alerts Log Report in the APM User Guide.
- **EUMAlerts Report tab.** Enables you to access the following reports:

- **Alert Log report.** Enables you to track all the details for the EUM alerts sent by APM during the specified time range. For details, see Alerts Log Report in the APM User Guide.
- **Alert Count Over Time report.** Enables you to display an overview of the frequency of alerts. For details, see Alerts Count Over Time Report in the APM User Guide.

Delivery of Alerts

If the online components are experiencing downtime, the Alerts application makes sure that the data is stored in the bus for one hour by default. After the components are back online, the Alerts engine generates alerts from data in the bus.

Alerts and Downtime

When you configure a CI Status alert, downtime can affect the CIs and skew the CI's data.

When you configure an EUM alert scheme for CIs whose status is based on data from Business Process Monitor or SiteScope data sources, downtime can affect the CIs and skew the CI's data.

You may decide to trigger a CI Status alert or an EUM alert during downtime or not. For concept details about downtime, see "Downtime Management Overview" on page 268.

To specify how to handle the CI Status alerts and the EUM alerts during downtime, select **Admin > Platform > Downtime**, and select one of the following options:

- **Take no actions**
- **Suppress alerts and close events**
- **Enforce downtime on KPI calculations; suppress alerts and close events**
- **Enforce downtime on Reports and KPI calculations; suppress alerts and close events**
- **Stop active monitoring (BPM & SiteScope); enforce downtime on Reports & KPI calculations; suppress alters and close events (affects all related SLAs)**

CI Status or EUM alerts for CIs that are in a scheduled downtime are not sent for all the options listed above apart from the **Take no action** option.

The CI alert is sent even if one of the options listed above is selected (apart from the **Take no action** option), if you configured the alert to be triggered when the status of the CI changes to the **Downtime** status. For user interface details, see General Page in the APM User Guide.

For task details, see "How to Set Up an Alert Delivery System" on the next page.

For user interface details, see "Downtime Management Page" on page 272.

Planning for Effective Alert Schemes

Before creating alert schemes, you should consider how to most effectively alert users to performance issues. The information described below can assist you with effective alert planning.

Note: HPE Professional Services offers best practice consulting on this subject. For information on how to obtain this service, contact your HPE representative.

- When creating alert schemes, categorize alerts by severity. Create critical alerts for events that require immediate corrective action (for example, transaction failure, or excessive response times for critical

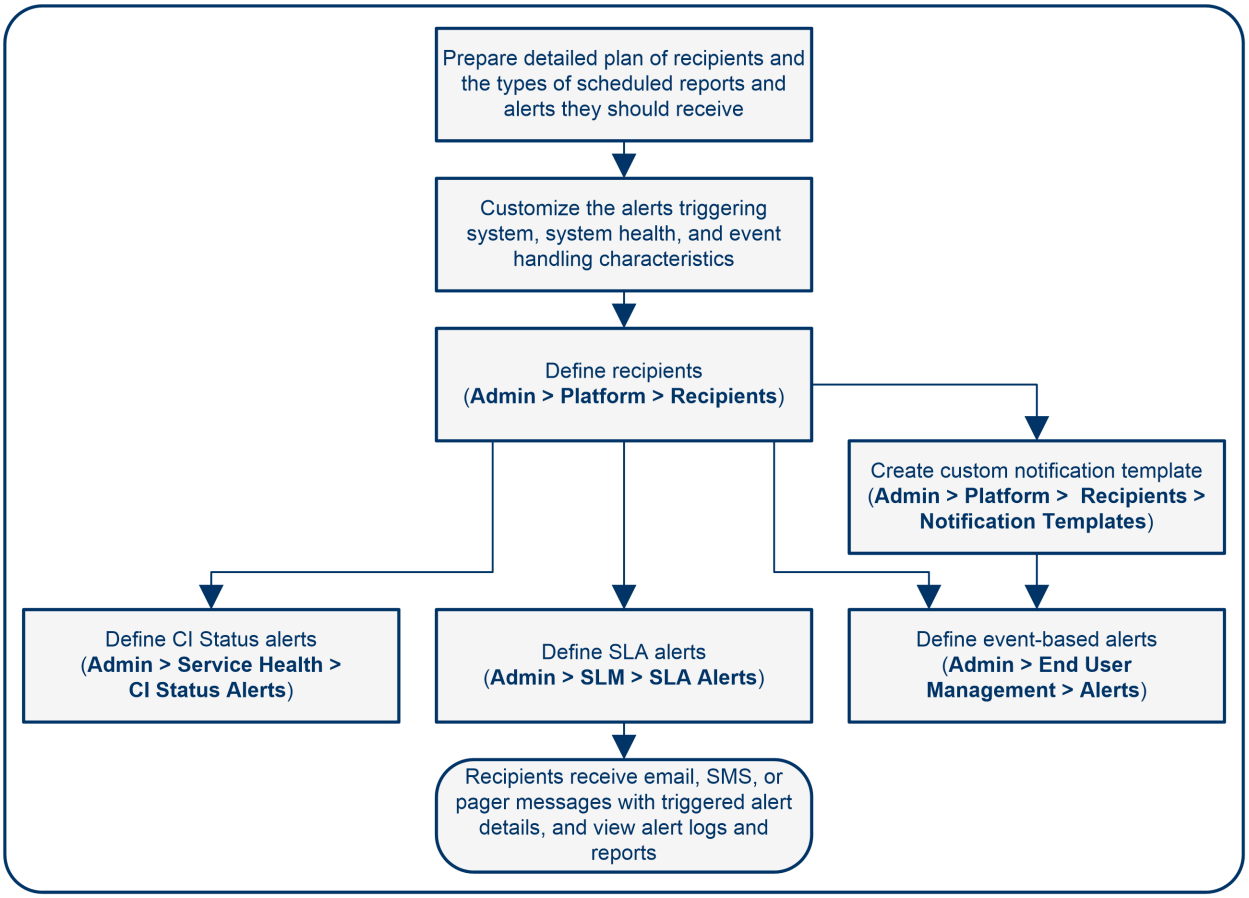
transactions). Create non-critical alerts for events that require early notification (for example, slow response times).

- Determine the users that receive the different types of alerts, and consider the alert delivery method that best suits the alert type. For example, pager delivery as opposed to email delivery might be more effective for critical alerts. When determining the delivery method, take the time of day into account as well. For example, email alerts might not be effective during non-business hours.
- Set APM to alert you to a recurring problem, not one-time events. Recurring alerts are the most accurate indicator of problems with your application. For example, as a rule, you should compare the number of recurring events to the number of Business Process Monitor locations from which you are monitoring. For example, if you had three failures, but you were monitoring from 100 locations, it would not be as critical as if you had five failures in all five locations.

How to Set Up an Alert Delivery System

This task and the associated flowchart describe how to set up a system for delivering alerts to recipients.

Setting Up an Alert Delivery System - Flowchart



Plan the alert recipient requirements

Before you start, we recommend that you:

- List the required recipients of alerts, including contact information and required delivery method to the recipient (email, SMS, pager). For suggestions on how to proceed, see "Planning for Effective Alert

Schemes" on the previous page.

- Map out the types of alerts you plan to deliver. For details on the types of alerts, see "Result - define the alerts schemes" on the next page.

Specify the appropriate user permissions

Specify the appropriate user permissions for the following. To set these permissions:

1. Select **Admin > Platform > Users and Permissions > User Management**.
2. Create or edit a user, and open the **Permissions** tab.
3. Select the required option from the Context drop-down list as described below.

- **The EUM alerts.**

  You can specify that a user can have a **View** or **Full Control** permission per application.

  - In the **End User Management** context, select **Enterprise > Applications >** `<Application>` **> Alert**

  You must also specify the permission for the CEM event template.

  - In the **End User Management** context, select **Alert - Notification template**.

- **The CI Status alerts.**

  You can specify that a user can have a **Change**, **View**, **Delete**, or **Full Control** permission per view.

  - In the **RTSM** context, select **Enterprise > Views >** `<view_name>`.

- **The SLA alerts.**

  You can specify that a user can have an **Add, Change**, **View, Delete,** or **Full Control** permission per SLA.

  - In the **Service Level Management** context, select **Enterprise > SLAs >** `<sla_name>` context.

- **The alert external actions** (**Run executable**, **Send SNMP trap**, or **Log to Event Viewer**).

  You can specify that a user can have a **Change** or **Full Control** permission at the global level.

  - In the **Platform** context, select **Enterprise > Run executable**, **Send SNMP trap**, or **Log to Event Viewer** contexts separately.

- **The notification template you can specify for the alerts.**

  You can specify that a user can have an **Add, Change, View, Delete**, or **Full Control** permission for the template.

  - In the **End User Management** context, select **Enterprise > System Recipient Template** context.

  These permissions are defined at the global level.

For user interface details, see "Operations" on page 134.

Specify how alerts are triggered during downtime

When you configure a CI Status alert or an EUM alert scheme for CIs whose status is based on data from Business Process Monitor or SiteScope data sources, downtime can affect the CIs and skew the CI's data.

You may decide to trigger a CI Status alert or an EUM alert during downtime or not. To specify how to handle the CI Status alerts and the EUM alerts during downtime, select **Admin > Platform > Downtime**, and select one of the available options.

For concept details, see "Alerts and Downtime" on page 244.

For user interface details, see "Downtime Management Page" on page 272.

Customize the alerts triggering system, alerts system health, and event handling characteristics – optional

Customize the alerts triggering system, system health, and event handling characteristics. For more information, see "How to Customize Alerts" below.

Define recipients

On the Recipients page, you define system recipients for alerts (except SiteScope alerts). You can specify email, SMS, or pager delivery methods. If required, enter specific alert delivery schedules (for example, recipients who receive alerts during business hours as opposed to evenings and weekends). For more information, see "Recipient Management" on page 184.

Create custom notification templates – optional

If required, when defining EUM alerts, you have the option to create custom notification templates that customize the format and information included in alert emails. For more information, see "How to Configure EUM Alerts Notification Templates" on page 260.

Set up to open an event in OMi 10 and later versions when an alert is triggered in APM

You can set up to open events in OMi 10 and later versions when an alert is triggered in APM. For details, see the OMi Integrations Guide.

Result - define the alerts schemes

You have planned the alert schemes, set up the relevant recipients, customized the alerts general settings and customized the notification templates. You can now define the alert schemes you require:

- **CI Status Alerts.** Define CI Status alerts as required to alert recipients to KPI status changes for specific CIs and KPIs being monitored in Service Health. For more information, see How to Create a CI Status Alert Scheme and Attach it to a CI in the APM User Guide.
- **SLA Alerts.** Define SLA alerts as required to alert recipients to changes in the current and forecasted status for service agreements. For more information, see How to Define an SLA Alert Scheme in the APM User Guide.
- **EUM Alerts.** Define EUM alerts as required to alert recipients to performance variance of Real User Monitor entities or Business Process Monitor transactions. For more information, see How to Create EUM Alert Schemes in the APM User Guide.

How to Customize Alerts

Note: All the steps in the task are optional and can be performed in any order.

This task describes the customization you can perform for CI Status, SLA, and EUM alerts.

To customize alerts:

1. Select **Admin > Platform** > **Setup and Maintenance** > **Infrastructure Settings**.
2. Select **Foundation > Alerting** and modify the required settings as described below.

Modify the way events are handled

You can modify the following parameters in the **Event handling** area:

Parameter	Does the Following
Acceptable event delay (minutes)	The system discards alerts after the number of minutes defined here.
Alert persistency during Downtime	If this option is set to **true**, the system does not reset the alert persistent state when an application goes into Downtime. This means that the system retains data and uses it when generating alerts after the Downtime ends. Applies to EUM alerts only.
Calculation persistency	If this option is set to **true**, if the system goes down, the system retains data and uses it when creating alerts when the system comes back up.

Modify the Alerting System Health parameters

You can modify the following parameters in the **System Health monitors** area:

Parameter	Does the Following
Error threshold for the notification queue monitor	The maximum number of messages that can wait in the alert queue of the notification queue monitor. When the maximum is reached the notification queue monitor status changes to **error**.
Error threshold for the alert queue monitor	The maximum number of messages that can wait in the alert queue of the alert queue monitor. When the maximum is reached the alert queue monitor status changes to **error**.
Warning threshold for the notification queue monitor	The maximum number of messages that can wait in the alert queue of the notification queue monitor. When the maximum is reached the notification queue monitor status changes to **warning**.
Warning threshold for the alert queue monitor	The maximum number of messages that can wait in the alert queue of the alert queue monitor. When the maximum is reached the alert queue monitor status changes to **warning**.

Modify the alerts triggering defaults

You can modify the following parameters in the **Triggered alerts** area:

Parameter	Does the Following
Command line execution timeout (seconds)	The default timeout for an action (by default 30 seconds) after which a command line alert action is not executed.

Parameter	Does the Following
Command line substitution pairs	When specifying a command in the Executable Files action of an EUM alert, you can use special tokens that are replaced with actual values when the command is prepared for execution. Those values might include a double quote (") or other tokens that may cause the resulting command line to be inappropriately interpreted by the operating system. To avoid this misinterpretation, you can modify the default value of the **Command line substitution pairs** infrastructure setting, as follows: • Each pair is written using the **|a|b|** format, the first character (**a**) is replaced by the second (**b**). • Multiple pairs are separated by a comma (,). For example: `|a|b|,|c|d|,|e|f|`.
Default EXE path	The default path to the default executable for EUM alerts.
• Default SNMP Port • Default SNMP Target Address • Default SNMP v3 user name • Default SNMP v3 authentication protocol • Default SNMP v3 authentication passphrase • Default SNMP v3 privacy protocol • Default SNMP v3 privacy passphrase	The default SNMP Trap host address. You can enter the IP address or server name in the **Default SNMP Target Address** parameter, and the port number in the **Default SNMP Port** parameter. For SNMP v3 traps you must enter the following security settings: • Default SNMP v3 user name (HPBSMUSER by default) • Default SNMP v3 authentication protocol (MD5, SHA, or no authentication) • Default SNMP v3 authentication passphrase • Default SNMP v3 privacy protocol (CBS-DES, or no privacy protocol) • Default SNMP v3 privacy passphrase You can specify only one SNMP target address. The default host address of the SNMP trap appears automatically in the **Enter host destination** box in the Create New/Edit SNMP Trap dialog box. For details, see Create New/Edit SNMP Trap Dialog Box in the APM Application Administration Guide or Create SNMP Trap/Edit SNMP Trap Dialog Box in the APM Application Administration Guide. If, when you create or edit an SNMP trap, you select the default host address and then modify it afterwards in the Infrastructure Settings, the address in all the SNMP traps you created are updated to the new default. Any alert that is sent causes the SNMP trap to be sent to the new default address.
Default URL	The default URL address for EUM alerts.
Enable alert dependencies across CIs	If this option is set to **true**, alert dependencies are allowed between CIs.

Parameter	Does the Following
Enable alert timer reset	If this option is set to **true**, an alert is triggered by a specific condition, then the condition that triggered the alert does not exist any more. If the condition that triggered the alert occurs again before the end of time period specified in the **Acceptable events delay** parameter ends, the alert is sent because the trigger condition has reset the notification frequency timer. The default is **false**.
Enable logging to DB	If this option is set to **true**, alerts and notifications are not logged in the Profile database. The default is **false**.
Enable notifications and actions	If this option is set to **true**, the alert engine is able to perform actions and send notifications. This customization is available only for EUM alerts. The default is **true**.
• Legacy SNMP Port • Legacy SNMP Target Address • Legacy SNMP v3 user name • Legacy SNMP v3 authentication protocol • Legacy SNMP v3 authentication passphrase • Legacy SNMP v3 privacy protocol • Legacy SNMP v3 privacy passphrase	The default SNMP Trap host address for EUM alerts. Modify the default SNMP trap host address, by entering the IP address or server name in the **Default SNMP Target Address** parameter, and the port number in the **Default SNMP Port** parameter. For SNMP v3 traps you must enter the following security settings: • Legacy SNMP v3 user name (HPBSMUSER by default) • Legacy SNMP v3 authentication protocol (MD5, SHA, or no authentication) • Legacy SNMP v3 authentication passphrase • Legacy SNMP v3 privacy protocol (CBS-DES, or no privacy protocol) • Legacy SNMP v3 privacy passphrase You can specify only one SNMP target address. The default host address of the SNMP trap appears automatically in the **Enter host destination** box in the Create New/Edit SNMP Trap dialog box. For details, see Create New/Edit SNMP Trap Dialog Box in the APM Application Administration Guide or Create SNMP Trap/Edit SNMP Trap Dialog Box in the APM Application Administration Guide. If, when you create or edit an SNMP trap, you select the default host address and then modify it afterwards in the Infrastructure Settings, the address in all the SNMP trap you created are updated to the new default. Any alert that is sent causes the SNMP trap to be sent to the new default address.
Notification execution retries	Specifies the number of retries of a notification. This customization is available only for EUM alerts. By default, a notification is sent once. Change the default using the **Notification execution retries** parameter. The number of retries that is performed equals the number you specify plus one.
Notification URL	The URL embedded in the notifications.

Parameter	Does the Following
Recipient information format in template	Use to modify how to display the recipient list in Emails or SMSs.You can assign the following values: • **Address**. Select this option to display the email address of the recipients in the **To** field of Emails and SMS notifications. For example, if you set **Recipient information format in template** to **Address** and the template includes the following parameters: To:<<Recipients>>, Profile Name: <<Profile Name>>, Severity: <<Severity>>, then the Email would look as follows: To:JSmith@example.com;MBrown@example.com Profile Name: forAlert Severity: Major • **Logical Name**. Select this option to display the logical name of the recipients in the **To** field of Emails and SMS notifications. For example, if you set **Recipient information format in template** to **Logical Name** and the template includes the same parameters as the example above, then the Email is as follows: To:John Smith, Mary Brown Profile Name: forAlert Severity: Major
SNMP alerts charset	The character set used to send SNMP alert traps. By default, the setting uses the platform's default character set. If your operating system supports multi-byte characters, it is recommended to use the "UTF-8" character set.
Symphony request timeout (seconds)	The number of seconds until an alert action times out.
Wait interval between retries (seconds)	The number of seconds between each attempt to execute a notification.

Modify the way alerts are sent by email

To modify the way email alerts are handled:

1. Select **Admin > Platform > Setup and Maintenance > Infrastructure Settings**.
2. Select **Foundation > Platform Administration**.
3. In the **Alerts E-Mail Settings** area, modify the following:

Parameter	Does the Following
Password for authorized email sending	The default password for authorized sending of email alerts.
SMTP server (Windows only)	The primary SMTP server used. In windows, set as <SMTPSVC> if you want to send using the SMTP service.
SMTP server port (Windows only)	The SMTP server port
User for authorized email sending	The default user for authorized sending of email alerts. If not set, email alerts are sent without authorization

Modify the way alerts are sent by pager

To modify the way pager alerts are handled:

1. Select **Admin > Platform > Setup and Maintenance > Infrastructure Settings**.
2. Select **Foundation > Platform Administration**.
3. In the **Alerts Pager Settings** area, modify the following:

Parameter	Does the Following
Password for authorized pager sending	The default password for authorized sending pager alerts.
SMTP server (Windows only)	The primary SMTP server used. In windows, set as <SMTPSVC> if you want to send using the SMTP service.
SMTP server port (Windows only)	The SMTP server port
User for authorized pager sending	The default user for authorized sending pager alerts. If not set, the system sends pager alerts without authorization.

Modify the way alerts are sent by SMS

To modify the way SMS alerts are handled:

1. Select **Admin > Platform > Setup and Maintenance > Infrastructure Settings**.
2. Select **Foundation > Platform Administration**.
3. In the **Alerts SMS Settings** area, modify the following:

Parameter	Does the Following
Password for authorized SMS sending	The default password for authorized sending SMS alerts.
SMTP server (Windows only)	The primary SMTP server used. In windows, set as <SMTPSVC> if you want to send using the SMTP service.

Parameter	Does the Following
SMTP server port (Windows only)	The SMTP server port
User for authorized SMS sending	The default user for authorized sending SMS alerts. If not set, the system send SMS alerts without authorization.

Modify the way notifications are handled

To modify the way notifications are handled:

1. Select **Admin > Platform > Setup and Maintenance > Infrastructure Settings**
2. Select **Foundations > Platform Administration**.
3. In the **Platform Administration - Recipient Notification Service** area, modify the following:

Parameter	Does the Following
Alerts email sender address	Used to modify the default sender email address used in emails. Use the parameter to modify the default value (**HP_BSM_Alert_Manager**) that appears in the **From** field when APM sends alerts is set when you install the Data Processing Server.
Alternate SMTP server, (Windows only) Alternate SMTP server port (Windows only)	Used to modify the alternate SMTP server: • **A designated server with a defined port number.** Enter a server name for sending SMTP emails as the value in the **Alternate SMTP server** field and enter a port number for the server in the **Alternate SMTP server** field. • **Microsoft's SMTP services.** Enter `<SMTPSVC>` as the value in the **SMTP server** or **Alternate SMTP server** field. **Limitation:** The following characters are invalid: _ . -
Email notifications charset	When an alert is triggered, recipients for the generated alert can be notified by email, SMS, or pager messages. You can select one of the following character sets: • **UTF-8.** The default character set. • **ISO-2022-JP**.
Email sender	The name of the sender of alert emails. If this value does not contain domain info, APM will use **<Email sender>@ <SMTP server>** to send notification email. If this value contains domain info, APM will use **<Email sender>** to send notification email. You can enter a fake email address. However, If you need a reply to the notification email, you must enter a real email address.
Enable recipient notifications	If this option is set to **false**, the system will not send email notifications.
Notification date format	The format used to display dates in notifications.

Parameter	Does the Following
Pager notifications charset	The character set used to send pager notification messages You can select one of the following character sets: • **UTF-8.** The default character set. • **ISO-2022-JP**.
Password for authorized message sending	The default password for authorized message sending. If this option is not set, the system sends messages without authorization.
SMS notifications charset	The character set used to send SMS notification messages You can select one of the following character sets: • **UTF-8.** The default character set. • **ISO-2022-JP**.
SMTP server (Windows only)	The primary SMTP server used. In windows NT, set as <SMTPSVC> if you want to send using the SMTP service.
SMTP server port (Windows only)	The SMTP server port
SMTP server socket connection timeout (seconds) (Windows only)	The default timeout (60 seconds) after which an SMTP server socket is disconnected.
User for authorized message sending	The default user for authorized message sending. If this option is not set, the system sends messages without authorization.

How to Test Your Email Notification Configuration

The following provides instructions for testing your email notification configuration. Before beginning, ensure that the Telnet Client is enabled on your Windows machines.

To test your email notification configuration:

From the command line in the DPS/GW, enter the following:

```
>telnet <your smtp server according to your APM Infra Settings> <port defined in your APM Infra Settings>
>ehlo
>mail from: <mail from the sender. For example, name@hpe.com>
>rcpt to: <mail from the receiver. For example, name@hpe.com>
>data
><Whatever you want to write in the body of the email>
>.
>quit
```

For example:

```
>telnet smtp-xyz.hpe.com 25
>ehlo
>mail from: john.smith@hpe.com
```

```
>rcpt to: john.smith@hpe.com
>data
>Whatever I want to write here (this is the body of the email)
>.
>quit
```

Alert Logs

You can use the following logs to debug the CI Status, SLA, and EUM alerts.

Alert Type	Path to Log and to Properties File for Log Level Setup	Description
All alerts	**Log:** <APM_data_processing_server>\log\alerts\alerts.ejb.log **Setup:** <APM_data_processing_server>\conf\core\Tools\log4j\EJB\alerts.properties	Alerts and notifications handling in the MercuryAs process
	Log: <APM_Gateway_server>\log\alerts\alerts.reports.log **Setup:** <APM_Gateway_server>\conf\core\Tools\log4j\EJB\alerts.properties	For all alert reports

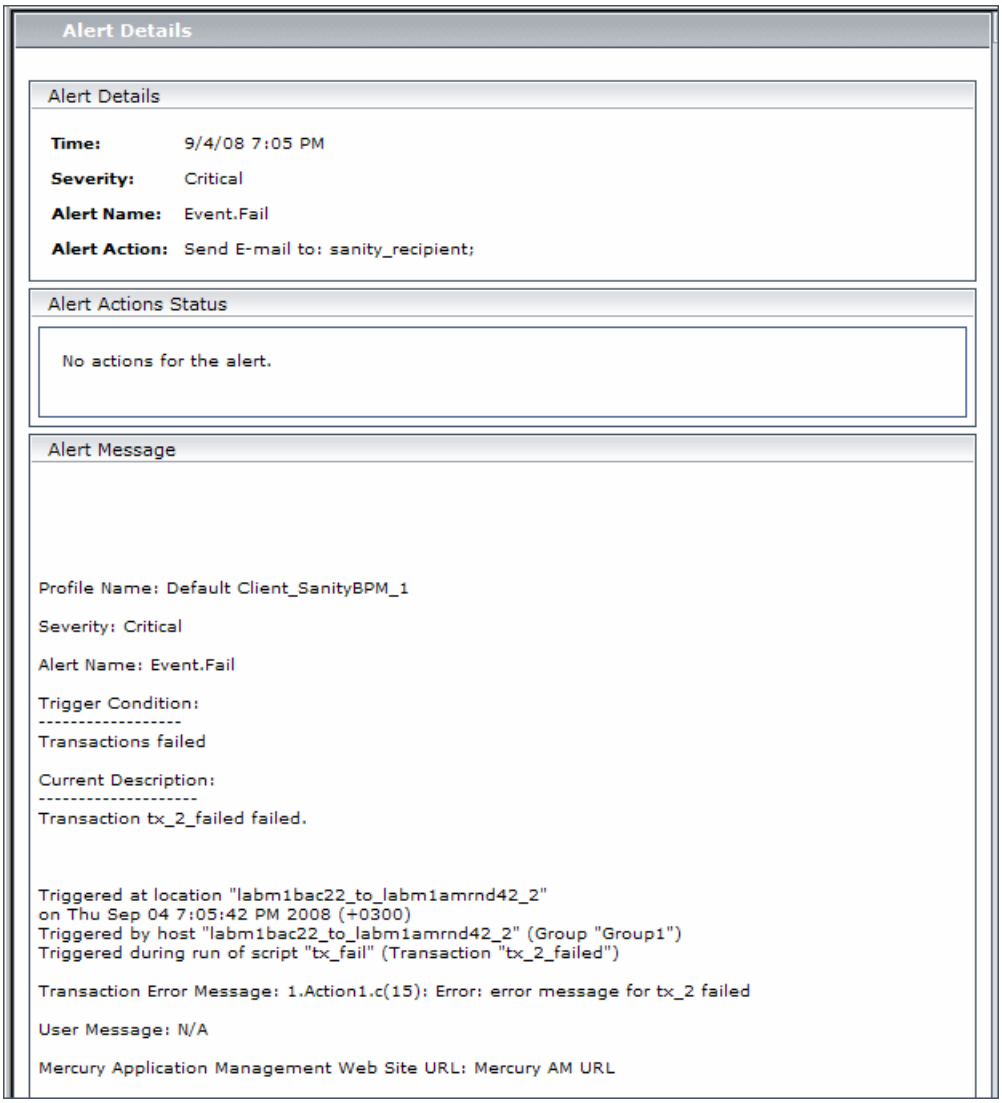
Alert Type	Path to Log and to Properties File for Log Level Setup	Description
CI Status alerts and SLA alerts	**Log:** <APM_data_processing_server>\log\marble_worker_1\status.alerts.log **Setup:** <APM_data_processing_server>\conf\core\Tools\log4j\marble_worker\cialerts.properties	Alert init and calculation in the MAR Business Logic Engine worker process
	Log: <APM_data_processing_server>\log\marble_worker_1\status.alerts.downtime.log **Setup:** <APM_data_processing_server>\conf\core\Tools\log4j\marble_worker\acialerts.properties	Alert downtime handling in the MAR Business Logic Engine worker process
	Log: <APM_Gateway_server>\log\alerts\alertui.log **Setup:** <APM_Gateway_server>\conf\core\Tools\log4j\EJB\alerts.properties	Alert administration

Alert Type	Path to Log and to Properties File for Log Level Setup	Description
EUM alerts	**Log:** <APM_data_processing_server>\log\alerts\alert.rules.log **Setup:** <APM_data_processing_server>\conf\core\Tools\log4j\marble_worker\alerts-rules.properties	Alert calculation in the MAR Business Logic Engine worker process
	Log: <APM_data_processing_server>\log\alerts\alerts.rules.init.log **Setup:** <APM_data_processing_server>\conf\core\Tools\log4j\marble_worker\alerts-rules.properties	Alert initialization in the MAR Business Logic Engine worker process
	Log: <APM_data_processing_server>\log\alerts\alerts.downtime.log **Setup:** <APM_data_processing_server>\conf\core\Tools\log4j\marble_worker\alerts-rules.properties	Alert downtime handling in the MAR Business Logic Engine worker process

Note: When you modify a log properties file on one of the APM processing servers, it affects only the logs on this APM processing server.

Alert Details Report

This report displays the triggering information that is available for the alert, including the actual conditions at the time of the alert.
The following is an example of the Alert Details report.



To access	Click  in the Configuration Item Status Alerts page, SLA Status Alerts page, or Alerts Log reports.
Important information	For details about CI Status Alerts, see Configuration Item Status Alert Notifications Report in the APM User Guide. For details about SLA Status Alerts, see SLA Status Alert Notifications in the APM User Guide. For details about EUM alerts, see Alert Details in the APM User Guide.

Troubleshooting and Limitations

This section describes troubleshooting and limitations for alerts.

Emails Are Not Received by Recipients When an Alert Should Have Been Triggered

If emails are not received by recipients, check the following possibilities:

- The alert definition is not as expected. Check the alert definition in the relevant alert administration.
- The data does not behave as expected so the alert triggering condition might not exist. Check the alert calculation log or check the specific data origin logs and reports. For details, see "Alert Logs" on page 255.
- There might be a connection problem with the SMTP email server. To check if the server works, **run telnet <smtp_server_host_name_or_IP_nbr> 25**.
- The email address of the recipient might not be valid. Examine the recipient definition in the user interface, and manually send an email to the recipient to check the address's validity.
- The recipient considers the alert email as spam. You might have to ask the recipient's administrator to reconfigure the spam filter.

Chapter 35: EUM Alerts Notification Templates

To determine the contents and appearance of the EUM alert notices, you can select predefined templates or configure your own template for notifications.

Alerts notification templates specify the information that APM includes when it sends various types of alert notices. The available default templates are pre-configured with selected parameters for each section of the alert notice. For details on the information included in the default templates, see "Notification Templates Page" on page 265.

You can also create custom templates. For example, you can create different templates for different alert notice delivery methods (email, pager, SMS), or for different recipients. A custom template is defined in the Notification Template Properties page. Each section of the alert notice includes a list of parameters that you can select. For details on the information that can be included in a custom template, see "Notification Templates Page" on page 265.

Clear Alert Notification Templates

When configuring alert schemes, you can set up an alert scheme to automatically send a clear alert notification. For details on selecting this option while creating your alert scheme, see How to Create EUM Alert Schemes in the APM Application Administration Guide.

The default template for clear alert notifications is automatically used by APM. If you do not want APM to use the default template, you can create your own clear alert template. The clear alert template must be based on an existing notification template. APM uses the clear alert notification template that you create under the following circumstances:

- An alert has been triggered.
- Notification is sent to a recipient based on an existing template (default or user-defined).
- The alert scheme has been configured to send a clear alert.

For details on configuring a clear alert notification template, see "How to Configure a Template for Clear Alert Notifications" on the next page.

How to Configure EUM Alerts Notification Templates

You can select predefined templates, modify existing templates, or create your own notification templates to determine the contents and appearance of the alert notices. For details on notification templates, see "EUM Alerts Notification Templates" above.

Create custom templates

APM gives you the flexibility to create different notification templates for the different alert schemes and recipients that are defined for your platform.

Every template is divided into sections. You specify the information that you want to appear in each section. For details, see "Notification Template Properties Dialog Box" on the next page.

Manage existing templates

Over time, you may find it necessary to make changes to notification templates that you create, because of organizational changes, changes in notification policies, changes to service level monitoring contracts, and so on. You use the Notification Templates page to edit, clone, and delete notification templates defined in APM. For details, see "Notification Templates Page" on page 265.

How to Configure a Template for Clear Alert Notifications

You can select predefined clear alert notification templates, modify existing templates, or create your own clear alert notification templates to determine the contents and appearance of the clear alert notices. For details on notification templates, see "Clear Alert Notification Templates" on the previous page.

Note: The notification template selected for the recipient has a clear alert template based on the notification template's name. For details on naming a clear alert template, see "Notification Template Properties Dialog Box" below. For details on clear alerts, see Advanced Settings Tab in the APM User Guide.

To create, modify, or manage clear alerts notification templates, see "Notification Templates Page" on page 265.

EUM Alerts Notification Templates User Interface

This section describes:

Notification Template Properties Dialog Box

This dialog box enables you to define a new alerts notification template.

To access	**Admin > Platform > Recipients > End User Management Alerts Notification Templates** • To create a new template, in the End User Management Alerts Notification Templates page, click the **New** button. • To edit an existing template: in the End User Management Alerts Notification Templates page, select an existing template, and click  .

Important information	**Clear alert notifications:** To set up a clear alert notification, select the notification template to use as the basis for your clear alert template and clone it. Make you determination based on the notification templates that was selected for users likely to receive a clear alert notification. Change the name of the template by deleting `Copy of` and adding `_FOLLOWUP` (all caps, one word). Edit the template details as required. It is recommended that you include in the Subject of a clear alert email, the Header, the Alert Specific Information, or both. **Example:** If you are creating a clear alert template based on the LONG default template, you would call the clear alert template LONG_FOLLOWUP. If the clear alert template is based on a user-defined template called MyTemplate, name the clear alert template MyTemplate_FOLLOWUP. **Default:** The _FOLLOWUP string is the default string recognized by APM as the template name for a clear alert message. **Customization:** You can customize the _FOLLOWUP string. For details, see "How to Configure a Template for Clear Alert Notifications" on the previous page.
Relevant tasks	"How to Configure a Template for Clear Alert Notifications" on the previous page

General Information Area

User interface elements are described below (unlabeled elements are shown in angle brackets):

UI Element (A-Z)	Description
<Insert>	Select a parameter to add to the section. Repeat to add as many text parameters as you want from the list. Add free text before or after the text parameters. The text parameters available for this section are: • **Alert Name.** The name of the alert, as defined in the alert scheme. • **Severity.** The severity label assigned to the alert in the alert scheme. • **HP BSM URL.** The URL of the APM web site. • **Entity Name.** The name of the CI attached to the alert. • **Entity Type.** The type of the CI attached to the alert. • **Alert User Description.** The description you specified in the alert scheme. • **Actions Result.** A description of the results of the alert actions specified in the alert scheme.
Message format	Select the format for the message: **Text** or **HTML**.

UI Element (A-Z)	Description
Name	Enter a name for the template. If possible, use a descriptive name that includes information on the type of alert (email, pager, SMS) for which you plan to use the template, or the recipients who receive alerts using this template.
Subject	Specify the information that you want APM to include in the subject of the email, pager message, or SMS message. Use the **<insert list for Subject / Header / Footer>** to add parameters and free text to create a customized subject. Use as many parameters as you want from the list.

Header Area

Use this area to specify the information that you want to appear at the top of the alert notice. Select parameters from the **<Insert>** list and free text to create a customized header. Use as many parameters as you want from the list.

User interface elements are described below (unlabeled elements are shown in angle brackets):

UI Element (A-Z)	Description
<Insert>	Select a parameter to add to the section. Repeat to add as many text parameters as you want from the list. Add free text before or after the text parameters. The text parameters available for this section are: • **Alert Name.** The name of the alert, as defined in the alert scheme. • **Severity.** The severity label assigned to the alert in the alert scheme. • **HP BSM URL.** The URL of the APM web site. • **Entity Name.** The name of the CI attached to the alert. • **Entity Type.** The type of the CI attached to the alert. • **Alert User Description.** The description you specified in the alert scheme. • **Actions Result.** A description of the results of the alert actions specified in the alert scheme. • **Entity ID.** The ID of the CI attached to the alert.

Alert Specific Information Area

Use this area to add alert information to the notification.

User interface elements are described below (unlabeled elements are shown in angle brackets):

UI Element (A-Z)	Description
<insert list for Alert Specific Information>	Select a text parameter to add to the section. Repeat to add as many text parameters as you want from the list. • **Trigger Cause.** A description of the alert trigger conditions, as specified in the alert scheme. • **Actual Details.** A description of the actual conditions at the time of the alert.

Transaction Area

Use this area to specify the BMP transaction details relevant only for the BPM alert type.

User interface elements are described below (unlabeled elements are shown in angle brackets):

UI Element (A-Z)	Description
<Insert>	Select a parameter to add to the section. Repeat to add as many text parameters as you want from the list. Add free text before or after the text parameters. The text parameters available for this section are: • **Data Collector Name.** The name of the data collector running the transaction related to the alert. • **Script Name.** The name of the script containing the transaction related to the alert. • **Transaction Time.** The date and time of the alert. • **Transaction Description.** A description of the transaction, if it has been defined in System Availability Management. • **Transaction Name.** The name of the transaction related to the alert. • **Transaction Error.** The error message generated by the data collector for the transaction, if a transaction error occurred at the time of the alert. • **Location Name.** The location of the data collector running the transaction related to the alert.

Footer Area

Use this area to specify the information that you want to appear at the bottom of the alert notice. Select parameters from the **<Insert>** list and free text to create a customized footer. Use as many parameters as you want from the list.

User interface elements are described below (unlabeled elements are shown in angle brackets):

UI Element (A-Z)	Description
<Insert>	Select a parameter to add to the section. Repeat to add as many text parameters as you want from the list. Add free text before or after the text parameters. The text parameters available for this section are: • **Alert Name.** The name of the alert, as defined in the alert scheme. • **Severity.** The severity label assigned to the alert in the alert scheme. • **HP BSM URL.** The URL of the APM web site. • **Entity Name.** The name of the CI attached to the alert. • **Entity Type.** The type of the CI attached to the alert. • **Alert User Description.** The description you specified in the alert scheme. • **Actions Result.** A description of the results of the alert actions specified in the alert scheme. • **Entity ID.** The ID of the CI attached to the alert.

Notification Templates Page

This page lists the default templates and any custom template that has been defined. It enables you to manage default and custom templates and to create new templates, or to edit clear alert notification templates.

To access	**Admin > Platform > Recipients > End User Management Alerts Notification Templates**
Important information	When configuring alert schemes, you can instruct APM to automatically follow up the alert by sending a clear alert notification. For details on selecting this option while creating your alert scheme, see "How to Configure a Template for Clear Alert Notifications" on page 261. The default template for clear alert notifications is automatically used by APM. If you do not want to use that default template, you can create your own clear alert template. It is recommended to clone an existing notifications template and then to modify the cloned template. APM uses the clear alert notification template that you create under the following circumstances: • An alert has been triggered. • Notification is sent to a recipient based on an existing template (default or user-defined). • The alert scheme has been configured to send a clear alert. • The notification template (DEFAULT_POSITIVE_FORMAT) selected for the recipient has a clear alert template based on the notification template's name.
Relevant tasks	"How to Configure EUM Alerts Notification Templates" on page 260

User interface elements are described below:

UI Element (A-Z)	Description
	**Click to duplicate notification template.** Clones the selected notification template. The Notification Template Properties dialog box opens where you can edit the cloded notification. For details, see "Notification Template Properties Dialog Box" on page 261.
	**Click to modify notification template properties.** Click to edit the selected template. For details, see "Notification Template Properties Dialog Box" on page 261.
	**Click to delete notification template.** Delete the selected templates simultaneously. To delete multiple templates simultaneously, select their check boxes, and click the  button located at the bottom of the templates list.
New Template	Click the **New Template** button to open the Notification Template Properties dialog box. For details, see "Notification Template Properties Dialog Box" on page 261.
Notification Template Name	Lists the default templates and the custom templates. The default templates are: • **DEFAULT_LOG_FORMAT.** Includes all the elements needed to create a default long format notification for reports. • **DEFAULT_POSITIVE_FORMAT.** Includes all the elements needed to create a default long format notification for positive or clear alerts. For details on clear alerts, see "How to Configure a Template for Clear Alert Notifications" on page 261. • **LONG.** Includes all the elements needed to create a default long format notification. • **SHORT.** Includes all the elements needed to create a default short format notification. **Note:** For details on the parameters displayed in each template, see "Notification Template Properties Dialog Box" on page 261.

Part 6: Downtime Management

Chapter 36: Downtime Management Overview

Downtime management enables you to exclude periods of time from being calculated for events, alerts, reports, views, or SLAs that can skew CI data. This section provides information and instructions for creating downtimes.

To access

Select **Admin > Platform > Downtime Management**

Learn About

Downtime Management

Downtime or other scheduled events can skew CI data. You may want to exclude these periods of time from being calculated for events, alerts, reports, views, or SLAs.

Downtimes are configured based on associated CIs. For example, you might want to exclude a recurring maintenance event or a holiday for a specific host CI whose physical host you know will be down for that period of time.

When defining downtimes, you configure how often the downtime will occur and select the specific instances of CIs that are affected by the downtime. You can select CIs of the following CI types:

- Node
- Running software
- Business application
- CI collection
- Infrastructure service
- Business service

Downtime Actions

You can select what action is taken during the downtime on the CIs specified in the downtime configuration. Downtime can impact the following:

- **Alerts and Events**. Events are suppressed and no CI Status alerts, EUM alerts, or notifications are sent for any of the CIs associated with the downtime.
- **KPIs**. KPIs attached to the CI and impacted CIs are not updated and display the downtime for the CI in Service Health. For details on how downtime configurations affect Service Health, see KPI Status Colors and Definitions in the APM User Guide.
- **Reports**. End User Management Reports are not updated and display the downtime for the CI. For details on how downtime configurations affect reports, see Downtime Information in Reports in the APM User Guide.
- **SLAs**. Selected SLAs that are attached to the CI are not updated. You can select which SLAs to include in the downtime. For details on how downtime configurations affect SLAs, see Retroactive SLA Data Corrections in the APM Application Administration Guide.
- **Monitoring**. Business Process Monitor and SiteScope monitoring stops for any of the CIs associated

with the downtime. For details on how downtime configurations affect SiteScope monitoring, see CI Downtime in the APM Application Administration Guide.

The options you select in the downtime wizard are combinations of the above actions, grouped in this order. This means that each option includes the previous options listed. The actions that are taken in APM during the downtime depend on the option selected during downtime configuration.

Permissions

To add, edit, or delete downtimes, you must have Full permission on the Downtime resource. In addition, you should have View permission on the Views to which CIs in the downtime belong. For details on permissions, see "Permissions" on page 130.

Maximum Number of Downtimes and CIs

By default, there is a maximum number of CIs and downtimes. These values are the recommended number of CIs and downtimes that are appropriate for your deployment and are based on capacity calculator values. These limits are enforced in both the APM UI and REST.

When adding a new downtime, APM checks that the number of downtimes configured in the system is less than the downtime threshold. You will only be able to continue adding a new downtime if the number of downtimes in the system is below the threshold.

When adding CIs to a new or existing downtime, APM checks that the number of CIs configured in the system is less than the CI threshold. You will only be able to continue the process if the number of CIs is below the threshold.

Although you can edit the downtime and CI thresholds, we recommend that you first try deleting unnecessary CIs or downtimes. Increasing the downtime and CI thresholds could adversely affect your system's efficiency.

Periodic Purging Downtimes

You can purge downtimes based on how long ago the downtime completed. By default, periodic purging is active and the time period from which completed downtimes should be purged is 1095 days. This means that by default, all downtimes that were completed more than 3 years ago are purged.

From the JMX console, you can also set how often periodic purging should be run. The default value is 7 days.

When starting the downtime service, the frequency for which the periodic purging is run is offset by 10 minutes. Therefore, if the periodic purging downtime runs every 7 days, and you start the downtime service at 9 am on Monday, the periodic purging downtime is performed every Monday at 9:10 am.

Note: After a downtime is purged, the downtime info in APM reports is inconsistent.

Downtime REST Service

You can retrieve, update, create, and delete downtimes through a RESTful web service running on the Gateway Server. For details, see Downtime REST Service in the APM Extensibility Guide.

Tasks

How to Configure Maximum Number of Downtimes

1. Select **Admin > Platform > Setup and Maintenance > Infrastructure Settings**. For user interface

details, see "Infrastructure Settings Manager Page" on page 68.

2. Select **Foundations**.
3. From the **Foundations** drop-down list, select **Downtime**.
4. From the **Fuse for number of downtimes in the System** parameter, click the **Edit Setting** button .
5. In the **Value** field, enter a new value.
6. Click **Save**.
7. Restart the server for the new value to take affect.

How to Configure Maximum Number of CIs in Downtimes

1. Select **Admin > Platform > Setup and Maintenance > Infrastructure Settings**. For user interface details, see "Infrastructure Settings Manager Page" on page 68.
2. Select **Foundations**.
3. From the **Foundations** drop-down list, select **Downtime**.
4. From the **Fuse for total number of CIs in downtime in the System** parameter, click the **Edit Setting** button .
5. In the **Value** field, enter a new value.
6. Click **Save**.
7. Restart the server for the new value to take affect.

How to Disable Periodic Purging

By default, periodic purging is enabled. To disable periodic purging, change the value of the of the Run Periodic Purging parameter to false.

1. Select **Admin > Platform > Setup and Maintenance > Infrastructure Settings**. For user interface details, see "Infrastructure Settings Manager Page" on page 68.
2. Select **Foundations**.
3. From the **Foundations** drop-down list, select **Downtime**.
4. From the **Periodic Purging Period** parameter, click the **Edit Setting** button .
5. In the **Value** field, enter the time period from which completed downtimes should be purged .
6. To disable periodic purging, from the **Run Periodic Purging** parameter, click the **Edit Settings** button and select **False**.
7. Click **Save**.
8. Restart the server for the new value to take affect.

How to Configure Periodic Purging Frequency

1. In a browser, enter the URL of the JMX console:
http://<Gateway or Data Processing Server name>:29000/
2. Enter your JMX console authentication credentials.
3. Go to **service=Infrastructure Settings Manager**.
4. Invoke the function **setSettingValuePerCustomerId** with **context=downtime** and **downtime.periodic.purging.days.interval**.

5. Restart the server.

How to Create and Manage Downtimes

1. Plan how you want the downtime to affect the CIs in your system. Before working in the wizard:
   - When determining which CIs may need downtimes, take into consideration CIs that impact the CIs that you selected. In some cases, these CIs are also affected by downtime.

     To understand the downtime impact model, see the **BSMDowntime_topology TQL** in the RTSM Modeling Studio.

     Note: By default, **BSMDowntime_topology TQL** is hidden. To view this TQL, in the Modeling Studio go to **Admin > RTSM > RTSM Administration > Administration > Package Manager > Tools > User Preferences > General > Show hidden queries** and set the value to **True**. The maximum depth that the impact can affect is 15 steps.

     You can only select CIs from the following CI types:
     - node
     - running_software
     - business_application
     - ci_collection
     - infrastructure_service
     - business_service

     Note: Even though SiteScope URL monitors are not included in this list of CI types, you can define a downtime on a SiteScope URL monitor by using a CI type computer. For example:

     1. In SiteScope, define a SiteScope URL monitor as a Computer named HPSERVER.
     2. In Platform Admin, create a downtime on a server name called HPSERVER.

   - Determine which actions should be applied to which CIs.

2. Run the Create Downtime wizard

   Go to **Admin** > **Platform** > **Downtime Management** and click the **Create New Downtime** button .

   For user interface details, see "New Downtime Wizard" on page 274.
3. Review the Results

   After running the wizard, the details of the downtime are displayed in the "Downtime Management Page" on the next page. You can export the details of the downtimes to a PDF or Excel file.

   For user interface details, see "Downtime Management Page" on the next page.

   Tip: To limit the downtimes in the exported file to a specified selection, you can filter the visible downtimes in the "Downtime Management Page" on the next page and then export to a PDF or Excel file. You can filter by any combination of one or more columns, including: Name, CIs, Status, Action, Scheduling, Next Occurrence, Modified By, Approved By, Planned, and Category.

How to Filter the Downtimes List

1. Click the column head of the column by which you want to filter the list.

2. From the column's drop-down list, select an option. Only items of the selected type appear in the list.

How to View Completed Downtimes

By default, downtimes with status of "*Completed*" are hidden.

To view completed downtimes, click the **Edit the Filter** button at the top of the Status column.

UI Description

Downtime Management Page

Information displayed on this page is view only. To edit any of the values, double-click on a downtime or select a downtime and click the **Edit** button.

User interface elements are described below.

UI Element (A–Z)	Description
	Create new downtime. Opens the New Downtime wizard where you configure a new downtime. For details, see "New Downtime Wizard" on page 274.
	Edit downtime. Opens the Edit Downtime wizard, which enables to you edit the configuration of an existing downtime. This wizard contains the same screens as the New Downtime wizard. For details, see "New Downtime Wizard" on page 274.
	Duplicate downtime. Clones the settings of an existing downtime to a new downtime.
	Delete downtime(s). Deletes selected downtime(s). Downtimes that are active now or were active at any time in the past cannot be deleted. This is designed to prevent the loss of historical data.
	Terminate Active Downtime. Cancels all future occurrences of the selected downtime and marks the downtime status as *Completed*.
	Export to Excel. Exports the table of configured downtimes to a file in Excel format.
	Export to PDF. Exports the table of configured downtimes to a PDF file.
Action	The action that takes place when the downtime is in active status. You configure the action for the downtime in the New Downtime wizard. For details about the possible actions, see "Action Page" on page 280.
CIs	The CIs associated with the downtime. These are the CIs that are impacted when the downtime is in active status.
Modified by	The user who last created or modified the downtime configuration.
Name	The name of the downtime as configured in the Downtime wizard.

UI Element (A–Z)	Description
Next Occurrence	The date and time of the next occurrence of the downtime. This field is updated automatically.
Scheduling	Displays the: • Date, time, time zone, and duration For recurring downtimes, also displays: • What day of the week or month the downtime is scheduled to recur • Range of recurrence
Status	Displays whether the downtime is currently: • **Active.** The CIs are currently in downtime and the action selected for the downtime is now taking place. • **Inactive.** The downtime is configured but it is currently not the time for the downtime to take place. • **Completed**. The time for the downtime has passed and the actions configured for the downtime have occurred.
Optional Columns	
Approved by	Indicates if there was an approval for the downtime and who approved it.
Category	The category assigned to the downtime. Options include: • Application installation • Application maintenance • Hardware installation • Hardware maintenance • Network maintenance • Operating system reconfiguration • Other • Security issue You can also create your own customized categories using Infrastructure Settings. To add a custom downtime category: 1. Select **Admin > Platform > Setup and Maintenance > Infrastructure Settings**. 2. Select **Foundations** > **Downtime**. 3. In the **Downtime - General settings** table, edit the **Downtime categories** value to the name you want to use as a customized category for the downtime. The name you enter will appear as an option in the list of available downtime categories.
Planned	Indicates whether the downtime is planned or not.

New Downtime Wizard

To access the New Downtime Wizard, from the Downtime page, click  , or select and existing downtime and click  .

Wizard Map	The New Downtime Wizard contains: "Properties Page " on page 277> "Select CIs Page " on page 278> "Scheduling Page " on page 279> "Action Page" on page 280 > "Notification Page " on page 281> "Preview Page " on page 282

Troubleshooting and Limitations

Editing Downtimes

- If while editing a downtime in the Downtime wizard its status changes from **Idle** to **Active**, the downtime cannot be saved.
- If you want to cancel a recurring downtime that already occurred at least once, edit the downtime's **End by** date in the Scheduling page.

Downtime and Daylight Saving Time

In time zones that observe Daylight Saving Time (DST), downtime calculations take into account the transitions between Standard and Daylight Time, using the following rules:

Note: The examples that follow use the daylight saving changes observed throughout most of the United States.

- March 14 2010 -- when 2:00 am arrives, the clock moves forward to 3:00 am. Thus, the period 2:00-2:59 am does not exist.
- November 7 2010 -- when 2:00 am arrives, the clock moves back to 1:00 am. Thus, the period 1:00-1:59 am appears twice.

  In other time zones, the behavior is the same, but the transition dates and times may vary.

  These examples are summarized in the table "DST Changes Affecting Downtime — Example Summary" on page 276.

Spring (Standard to Daylight Time)

- When downtime starts before the DST change and ends the day after the change, its end time is as expected, but the duration is 1 hour less than defined.

  Example 1:

  Monthly downtime starting 14th day of month at 1:30 am and ending on 15th day of month at 2:40 am. Duration is 1 day, 1 hour, and 10 minutes.

  No DST change: Downtime starts on 14th at 1:30 am and ends on 15th at 2:40 am. Duration is 1 day, 1 hour, 10 minutes.

  DST change on March 14 2010: Downtime starts on 14th at 1:30 am and ends on 15th on 2:40 am, but the duration is 1 day, 0 hours, 10 minutes (1 hour less than defined).
- When downtime starts before the DST change and ends the same day as the change, but after the change, its end time is 1 hour more than defined, but its duration is as defined.

Example 2:

Monthly downtime on 13th day of month, starting at 11 pm (23:00), for a duration of 5 hours.

No DST change: Downtime starts on 13th at 11:00 pm and ends on 14th at 4:00 am.

DST change on March 14 2010: Downtime starts on 13th at 11:00 pm and ends on 14th at 5:00 am, and the duration remains 5 hours.

- When downtime is defined to start during the skipped hour, the start time shifts 1 hour forward and keeps the defined duration.

  Example 3:

  Monthly downtime on 14th day of month, starting at 2:30 am, for a duration of 2 hours.

  No DST change: Downtime starts on 14th at 2:30 am and ends on 14th at 4:30 am.

  DST change on March 14 2010: Downtime starts on 14th at 3:30 am and ends on 14th at 5:30 am, and the duration remains 2 hours.

- When downtime is defined to start before the DST change and end during the skipped hour, the end time shifts 1 hour forward and keeps the defined duration.

  Example 4:

  Monthly downtime on 13th day of month, starting at 1:30 am, for a duration of 1 day, 1 hour, and 10 minutes.

  No DST change: Downtime starts on 13th at 1:30 am and ends on 14th at 2:40 am. The duration is 1 day, 1 hour, and 10 minutes.

  DST change on March 14 2010: Downtime starts on 13th at 1:30 am and ends on 14th at 3:40 am, and the duration remains as defined -- 1 day, 1 hour, and 10 minutes.

- When downtime is defined to start and end during the skipped hour, downtime takes place one hour later than defined.

  Example 5:

  Monthly downtime on 14th day of month, starting at 2:00 am, for a duration of 1 hour.

  No DST change: Downtime starts on 14th at 2:00 am and ends on 14th at 3:00 am.

  DST change on March 14 2010: Downtime starts on 14th at 3:00 am and ends on 14th at 4:00 am, and the duration remains as defined -- 1 hour.

Fall (Daylight Time to Standard Time)

- When downtime starts and ends after the DST change, its end time and duration are as defined.
- When downtime starts before the DST change (same day as change or day before) and ends after the change during the day of the change, the end time is 1 hour less than expected, and duration is as defined.

  Example 6:

  Two monthly downtimes, both starting on the 7th day of month at midnight. The first downtime duration is 1 hour, and the second is 2 hours.

  No DST change: The first downtime is on 7th from 0:00 to 1:00 am (1 hour duration), and the second on 7th from 0:00 to 2:00 am (2 hours duration).

  DST change on November 7 2010: The first downtime starts on 7th at 0:00 Daylight Time and ends on 7th at 1:00 am Daylight Time, with a duration of 1 hour. The second downtime starts on 7th at 0:00 Daylight Time and ends on 7th at 1:00 am Standard Time, and the duration remains 2 hours.

  Example 7:

  Monthly downtime on 7th day of month, starting at midnight, for a duration of 4 hours.

  No DST change: Downtime starts on 7th at 0:00 and ends on 7th at 4:00 am.

DST change on November 7 2010: Downtime starts on 7th at 0:00 and ends on 7th at 3:00 am, and the duration remains as defined -- 4 hours.

Example 8:

Monthly downtime on 6th day of month, starting at 8:00 pm (20:00), for a duration of 7 hours.

No DST change: Downtime starts on 6th at 8:00 pm and ends on 7th at 3:00 am.

DST change on November 7 2010: Downtime starts on 6th at 8:00 pm and ends on 7th at 2:00 am, and the duration remains as defined -- 7 hours.

- When downtime starts before the DST change and ends the day after the change, the end time is as expected, and duration is 1 hour more than defined.

  Example 9:

  Monthly downtime on 7th day of month, starting at midnight (0:00), for a duration of 1 day, 1 hour (25 hours).

  No DST change: Downtime starts on 7th at 0:00 and ends on 8th at 1:00 am.

  DST change on November 7 2010: Downtime starts on 7th at 0:00 and ends on 8th at 1:00 am, but the duration is 26 hours.

DST Changes Affecting Downtime — Example Summary

Example	Downtime as Set/With DST Change	Start Time	End Time	Duration
1	Set	14th at 1:30 am	15th at 2:40 am	1 day, 1 hour, 10 minutes
	With DST Change	14th at 1:30 am	15th at 2:40 am	1 day, 0 hours, 10 minutes
2	Set	13th at 11:00 pm	14th at 4:00 am	5 hours
	With DST Change	13th at 11:00 pm	14th at 5:00 am	5 hours
3	Set	14th at 2:30 am	14th at 4:30 am	2 hours
	With DST Change	14th at 3:30 am	14th at 5:30 am	2 hours
4	Set	13th at 1:30 am	14th at 2:40 am	1 day, 1 hour, and 10 minutes
	With DST Change	13th at 1:30 am	14th at 3:40 am	1 day, 1 hour, and 10 minutes
5	Set	14th at 2:00 am	14th at 3:00 am	1 hour
	With DST Change	14th at 3:00 am	14th at 4:00 am	1 hour

Example	Downtime as Set/With DST Change		Start Time	End Time	Duration
6	1st	Set	7th at 0:00	7th at 1:00 am	1 hour
		With DST Change	7th at 0:00	7th at 1:00 am	1 hour
	2nd	Set	7th at 0:00	7th at 2:00 am	2 hours
		With DST Change	7th at 0:00	7th at 1:00 am Standard Time	2 hours
7	Set		7th at 0:00	7th at 4:00 am	4 hours
	With DST Change		7th at 0:00	7th at 3:00 am	4 hours
8	Set		6th at 8:00 pm	7th at 3:00 am	7 hours
	With DST Change		6th at 8:00 pm	7th at 2:00 am	7 hours
9	Set		7th at 0:00	8th at 1:00 am	25 hours
	With DST Change		7th at 0:00	8th at 1:00 am	26 hours

Properties Page

This wizard page enables you to configure the general properties of the downtime. For information about downtimes, see "Downtime Management Overview" on page 268.

This page is part of the "New Downtime Wizard" on page 274.

User interface elements are described below:

UI Element	Description
Downtime name	Cannot exceed 200 characters.
Downtime description	This description also appears in the Downtime Information Area in the APM User Guide. The description cannot exceed 2000 characters.
Approved by	You can enter the person or department who approved this downtime. Cannot exceed 50 characters. **Note:** In Oracle, if you are using East Asian Languages (Chinese, Japanese, or Korean), the maximum number of characters for **Downtime Name**, **Downtime Description**, or **Approved by** may be less than specified above.
Planned	Select if you want this downtime marked as planned. You can create downtimes that are unplanned. This is for information purposes only.

UI Element	Description
Downtime Category	Select a category that describes the reason for the downtime. You can also create your own customized categories using Infrastructure Settings. To add a custom downtime category, select **Admin > Platform > Setup and Maintenance > Infrastructure Settings**: • Select **Foundations**. • Select **Downtime**. • In the **Downtime - General settings** table, edit the **Downtime category** value to the name you want to use as a customized category for the downtime. The name you enter appears as an option in the list of available downtime categories after you restart APM.

Select CIs Page

This wizard page enables you to select the CIs that are affected by the downtime. For information about downtimes, see "Downtime Management Overview" on page 268.

You cannot edit the selected CIs for downtimes that already occurred.

This page is part of the "New Downtime Wizard" on page 274.

User interface elements are described below:

UI Element (A-Z)	Description
Available CIs	Select from the list the view that contains the CIs to be affected by this downtime. Click  to browse and search for the CI from the available views. Highlight a CI from the view to move it to the Selected CIs list. Press the `Ctrl` key to select multiple CIs. You can select any view that you have permission to see. You can select CIs only of the following CI types: • Node • Running software • Business application • CI collection • Infrastructure service • Business service
Selected CIs	Once CIs are selected, they appear in the Selected CIs list. To remove a CI from a downtime, select the CI in the Selected CIs and click the back arrow to move it back to the Available CIs list.

Scheduling Page

This wizard page enables you to configure the schedule for the downtime. For information about downtimes, see "Downtime Management Overview" on page 268.

Note: You cannot schedule a downtime in the past.

For downtimes that have already occurred, only the following field is editable in the Scheduling page:

End by date in **Range of recurrence**

To cancel a recurring downtime that occurred at least once, edit the downtime and modify this field.

This page is part of the "New Downtime Wizard" on page 274.

User interface elements are described below:

UI Element	Description
Time of occurrence	• **Start**. The drop-down list includes times set for every half hour on the hour and half hour. To select a different time of day, select the closest half hour and edit the field to enter the actual time you want the downtime to start. For example, for 2:10 am, select 2:00 am and edit the minutes to indicate 2:10 am. • **End**. When you select an end time, the duration field automatically updates. Or you can select the duration and the end time field automatically updates. • **Duration.** Includes options from 5 minutes to one week. The downtime duration must be in increments of 5 minutes and be defined in lengths of minutes, hours, days, or weeks. If the length of time you want to specify does not appear, for example 1-1/2 hours, enter the end time and the duration automatically updates. To select a time greater than 1 week, select 1 week and edit the field to the correct number of weeks.
Recurrence pattern	Select one of the following: • **Once.** The downtime happens only once as scheduled and does not recur. Select the calendar date for the occurrence. • **Weekly.** Select the day of the week for the scheduled weekly recurrence. • **Monthly.** Select a day in the month or a monthly repeated downtime pattern. For example, you can schedule a downtime event on the first Sunday of every third month.
Range of recurrence	If you selected **Weekly** or **Monthly**: 1. Define a **Start** date. 2. Select either an **End by** date or **No end date**.
Time zone	All time zones are displayed in relation to GMT.

Action Page

This wizard page enables you to define the set of actions taken during the downtime. For information about downtimes, see "Downtime Management Overview" on page 268.

You cannot edit fields in teh Action page for downtimes that already occurred.

This page is part of the "New Downtime Wizard" on page 274.

User interface elements are described below:

UI Element	Description
Take no actions	There is no action taken on the associated CIs or the CI monitoring, alerts, reports, or SLAs. **Note:** During this downtime, the affected CI doesn't change its status to **Downtime**. CI status alerts are configured to be triggered if the CI changes its status.
Suppress alerts and consider events	• No alerts or their associated notifications or actions are sent for any of the CIs associated with the downtime. • By default, events are submitted as closed. • Monitoring continues, and reports, status in Service Health, and SLAs are updated. **Note:** During the downtime period, the affected CI may change its status, and the status change may trigger the relevant CI status alert.
Enforce downtime on KPI calculations; suppress alerts and consider events	• KPI calculations are not run and the status in Service Health is not updated. The downtime for the CI is displayed. • No alerts or their associated notifications or actions are sent for any of the CIs associated with the downtime. • By default, events are submitted as closed. • Reporting and monitoring continue. SLAs are updated.
Enforce downtime on Reports and KPI calculations; suppress alerts and consider events	• Report data is not updated and the downtime is displayed for the associated CIs. • Selected SLAs are not updated for the SLAs affected by the CIs associated with the downtime. • KPI calculations are not run and the status in Service Health is not updated. The downtime for the CI is displayed. • No alerts or their associated notifications or actions are sent for any of the CIs associated with the downtime. • By default, events are submitted as closed. • Monitoring continues.

UI Element	Description
Stop active monitoring (BPM & SiteScope); enforce downtime on Reports & KPI calculations; suppress alerts and consider events (affects all related SLAs)	• Business Process Monitor and SiteScope monitoring stops. • Report data is not updated and the downtime is displayed for the associated CIs. • SLAs are not updated for the SLAs affected by the CIs associated with the downtime. • KPI calculations are not run and status in Service Health is not updated. The downtime for the CI is displayed. • No alerts or their associated notifications or actions are sent for any of the CIs associated with the downtime. • By default, events are submitted as closed. **Note:** If you configure a downtime period for an Application CI (whose data is updated by BPM monitoring), the Downtime Manager automatically sends an event to the BPM Agent when the downtime period starts. The agent stops sending samples to APM. The samples that are suppressed are the BPM samples that correspond to the Transaction CIs, which are child CIs of the Application CIs on which the downtime is configured. There is one sample per transaction.

Notification Page

The New Downtime wizard - Notification page enables you to select recipients to receive notification of the downtime. Notifications are sent by email at the time of downtime occurrence and immediately after it completes. You can select only those recipients with an email address defined. For information about downtimes, see "Downtime Management Overview" on page 268.

Note: You can edit the **Selected Recipients** for downtimes that already occurred.

This page is part of the "New Downtime Wizard" on page 274.

User interface elements are described below:

UI Element	Description
	Opens the **New recipient** dialog box that enables you to create a recipient that is not yet in the list of available recipients. The recipients you create are available as recipients in all of APM. For details on creating recipients, see "Recipient Management" on page 184.
Available Recipients	Lists the available recipients for downtime notification by means of email, SMS, or pager.
Selected Recipients	Lists the selected recipients for downtime notification by means of email, SMS, or pager. You can select either one, two or all three notification options.

Preview Page

The New Downtime wizard - Preview page enables you to preview a summary of your Downtime settings. For information about downtimes, see "Downtime Management Overview" on page 268.

This page is part of the "New Downtime Wizard" on page 274.

User interface elements are described below:

UI Element	Description
Preview table	Displays a table listing all the values configured for this downtime. You can click the **Back** button to return to a page in the wizard that contains a value that should be modified or deleted. When you click **Finish**, the downtime is added to the system and displayed in the Downtime Manager page.

Part 7: Troubleshooting

Chapter 37: Troubleshooting and Limitations

This section describes common problems that you may encounter when working in the Platform Administration area of APM.

For additional troubleshooting information, use the HPE Software Support Website (https://softwaresupport.hpe.com/).

Forgot my Admin password

Rerun the Setup and Database Configuration Utility to create a new Admin password. Refer to the instructions in *Running the Setup and Database Configuration Utility* in the APM Installation Guide.

Need to change password for access from data collectors (RUM, Diagnostics) to RTSM

During deployment, you can optionally set an **Access to RTSM password** to secure communication between APM data collectors (such as Real User Monitor and the Run-time Service Model. This password can be changed later using the JMX console.

To modify the password for RTSM access using the JMX console:

1. Enter the URL of the JMX console (**http://<Gateway or Data Processing Server name>:29000/**) in a web browser. (For detailed instructions, see "JMX Console" on page 78.)
2. Enter your JMX console authentication credentials. If you do not know your authentication credentials, contact your system administrator.
3. In the **Foundations** domain, select the service **RTSM passwords manager**.
4. Modify **changeDataCollectorsOdbAccessPwd**. The operation gets customer ID and new password as parameters and changes all data collector passwords to the new one.

RTSM Administration pages do not load

If the links from RTSM Administration do not work, this may be caused by one of the following:

- Make sure that the APM Gateway Server is able to access the Default Virtual Server for Application Users URL. This URL can be found in **Admin > Platform > Setup and Maintenance > Infrastructure Settings.** In the **Foundations** field, specify **Platform Administration**. The URL is located in the **Host Configuration** table.
- If you are using a reverse proxy or load balancer, make sure you log in through the URL specified above.

Java applets fail to load with "class not found" error

Make sure that you created a Profile Database. This database must be created manually in Platform Administration. For more information, see "Creating Databases" on page 48.

Java applets fail to load

Open **Control Panel > Java > Temporary Internet Files > Settings** and make sure **Keep temporary files on my computer** is checked. If the problem persists, clear the Java cache by clicking **Delete Files** in the same location.

Intermittent UI failures after connecting through Load Balancer

APM requires sticky sessions for users. Make sure the persistency settings are set to **stickiness by session enabled** or **Destination Address Affinity** (depending on the Load Balancer).

APM Login page does not appear when connecting through Load Balancer

- Check the KeepAlive URIs.
- Virtual hosts and Load Balancer should be configured with a fully qualified domain name (and not an IP) for LW-SSO to work.

APM dialog boxes and applets, such as the Configuration Wizards, do not load properly

Possible Cause:

Old java files on your client PC.

Solution:

Clear the java cache by following this procedure:

1. Navigate to **Start > Control Panel > Java**.
2. In the Temporary Internet Files section, click **Settings**.
3. In the Temporary File Settings dialog box, click **Delete Files**.

APM has been installed, but the Downloads page is empty

Possible Cause:

The components setup files have not been installed to the Downloads page.

Solution:

Install the components setup files to the Downloads page. For details on installing the component setup files on a Windows platform, see Installing Component Setup Files.

General connectivity problems related to ports

Verify that all ports required by APM servers are not in use by other applications on the same machine. To do so, open a Command Prompt window, and run netstat (or use any utility that enables you to view port information). Search for the required ports.

You can also check the **<APM root directory>\log\Jboss \jboss_boot.log** for ports in use. If the **jboss_boot.log** reports "`Port <> in use`" but you do not see that this port is in use when you run netstat utility, restart the server and then start APM.

For details on the ports required by APM, see Port Usage in the APM Hardening Guide.

> **Tip:** To troubleshoot port usage problems, use a utility that lists all ports in use and the application that is using them.

APM connectivity is down, but the Tomcat servlet engine and jboss application server appear to be working

Connectivity problems include the inability to log into APM, and the inability of Business Process Monitor to

connect to the Gateway Server.

Possible Cause:

This can happen if the **TopazInfra.ini** file is empty or corrupt.

To verify that this is the problem:

1. In the browser, type http://<Gateway Server>:29000/ to connect to the JMX Console.

   If prompted, enter the JMX Console authentication credentials (if you do not have these credentials, contact your system administrator).
2. Under **System > JMX MBeans > Topaz**, select **Topaz:service=Connection Pool Information**.
3. Click the **showConfigurationSummaryInvoke** button toward the bottom of the page. If the Operation Result page is blank, the **TopazInfra.ini** file is empty or corrupt.

Solution:

To solve this problem, rerun the Setup and Database Configuration utility and either reconnect to your existing management database or define a new management database. If you did not discover a problem with the **TopazInfra.ini** file, contact HPE Software Support.

Inability to log into APM, and JBoss application server fails to initialize

Run the database schema verify program to verify that the database server on which the management database is located is up and running. For details, see Database Schema Verification in the APM Database Guide.

Browser unable to reach APM and an error about insufficient heap space

A message box opens indicating that APM is not available and you should try logging in at a later time.

Possible Cause:

The page file size is too small.

Solution:

Configure the page file size to be at least 150% of RAM size. Restart the server.

Browser unable to reach APM or the .jsp source code appears in the browser window

A message box opens indicating that the APM page does not exist.

Solution:

Ensure that the Jakarta filter path is correct. The path might be incorrect—for example, if you uninstall APM servers and then reinstall to a different directory. In this case, the Jakarta filter path is not updated, causing redirection problems.

To update the Jakarta filter path:

1. Open the IIS Internet Services Manager.
2. Right-click the machine name in the tree and select **Properties**.
3. With **WWW Service** displayed in the Master Properties list, click **Edit**.
4. Select the **ISAPI Filter** tab.
5. Select **jakartaFilter** and click **Edit**.

6. In the **Filter Properties** box, update the path to point to the drive and directory of the current APM installation.
7. Apply your changes and quit the Internet Services Manager.
8. Restart the IIS service.

APM is sitting behind a proxy and the server name is not recognized by the proxy

The problem occurs for both Microsoft IIS and Apache web servers.

Possible Cause:

The web server redirects the browser page to a URL that replaces the server name entered by the user.

Solution:

Add the APM server name to the **<Windows system root directory>\system32\drivers\etc\hosts** file on the proxy server machine.

Host names of Gateway or Data Processing Server have changed

You can no longer access APM using the server names on which they were installed and must change the names of the servers.

Processes do not resume restart automatically after automatic failover

If the High Availability Controller's Automatic Failover mode is enabled and the management database has been down for some time, some processes may be stopped and will not resume automatically when the management database returns to normal operation. These processes will have the status **STARTING** on the APM Status page, accessible on the Windows operating system from **Start > Programs > HPE Application Performance Management > Administration > HPE Application Performance Management Status**.

Solution:

Restart these processes once the management database is available again.

Applets may take longer to open for clients with JRE 7 update 25 and later

This is due to Java security enhancements. Before Java applets and Java Web Start applications run, the signing certificates are checked to ensure that a signing certificate was not revoked.

If there is a proxy problem or any other network issue, you should disable this Java feature.

To disable Java from performing certificate revocation checks:

1. Click the **Start** button and select the **Control Panel** option.
2. Click the **Java** icon to open the Java Control Panel.
3. Click the **Advanced** tab.
4. Locate and deselect the option to perform certificate revocation checks.

Unable to access an APM component that requires the Java applet (Windows system only)

If a user tries to access an APM component that requires the Java applet, the component may not open and the following error appears int he Java console log:

```
java.io.IOException: Error 0 writing to WindowsNamedPipe: server: false; readPipe: jpi2_
pid20984_pipe8, readBufferSz: 4096; writePipe: jpi2_pid20984_pipe9, writeBufferSz:
at sun.plugin2.message.transport.NamedPipeTransport$SerializerImpl.flush(Unknown Source)
at sun.plugin2.message.transport.NamedPipeTransport.signalDataWritten(Unknown Source)
at sun.plugin2.message.transport.SerializingTransport.write(Unknown Source)
at sun.plugin2.message.Pipe.send(Unknown Source)
```

This error is due to a link (or 'heartbeat') between the browser's JRE and the client's JRE. If the browser's virtual machine and the local system's Java virtual machine are not able to communicate for that thread within 10 seconds, the local machine's JVM kills the thread.

If this situation occurs, create the following environment variable JPI_PLUGIN2_NO_HEARTBEAT = 1 on the customer's client system.

To create the environment variable:

1. On the desktop of the customer's client system, right-click the Computer icon and select **Properties**.
2. Click **Advanced system settings**. The System Properties dialog box appears.
3. Click **Environment Variables**. The Environment Variables dialog box appears.
4. In the System variables area, click **New**. The New System Variable dialog box appears.
5. Enter the following information:
   - **Variable Name:** PI_PLUGIN2_NO_HEARTBEAT
   - **Variable Value:** 1
6. Click **OK**.

Send Documentation Feedback

If you have comments about this document, you can contact the documentation team by email. If an email client is configured on this system, click the link above and an email window opens with the following information in the subject line:

Feedback on APM Platform Administration Guide (Application Performance Management 9.31)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to SW-doc@hpe.com.

We appreciate your feedback!