MICRO FOCUS

Silk Performance Manager 19.0

Administration Help

Micro Focus
The Lawn
22-30 Old Bath Road
Newbury, Berkshire RG14 1QN
UK
http://www.microfocus.com

2018-06-06

Contents

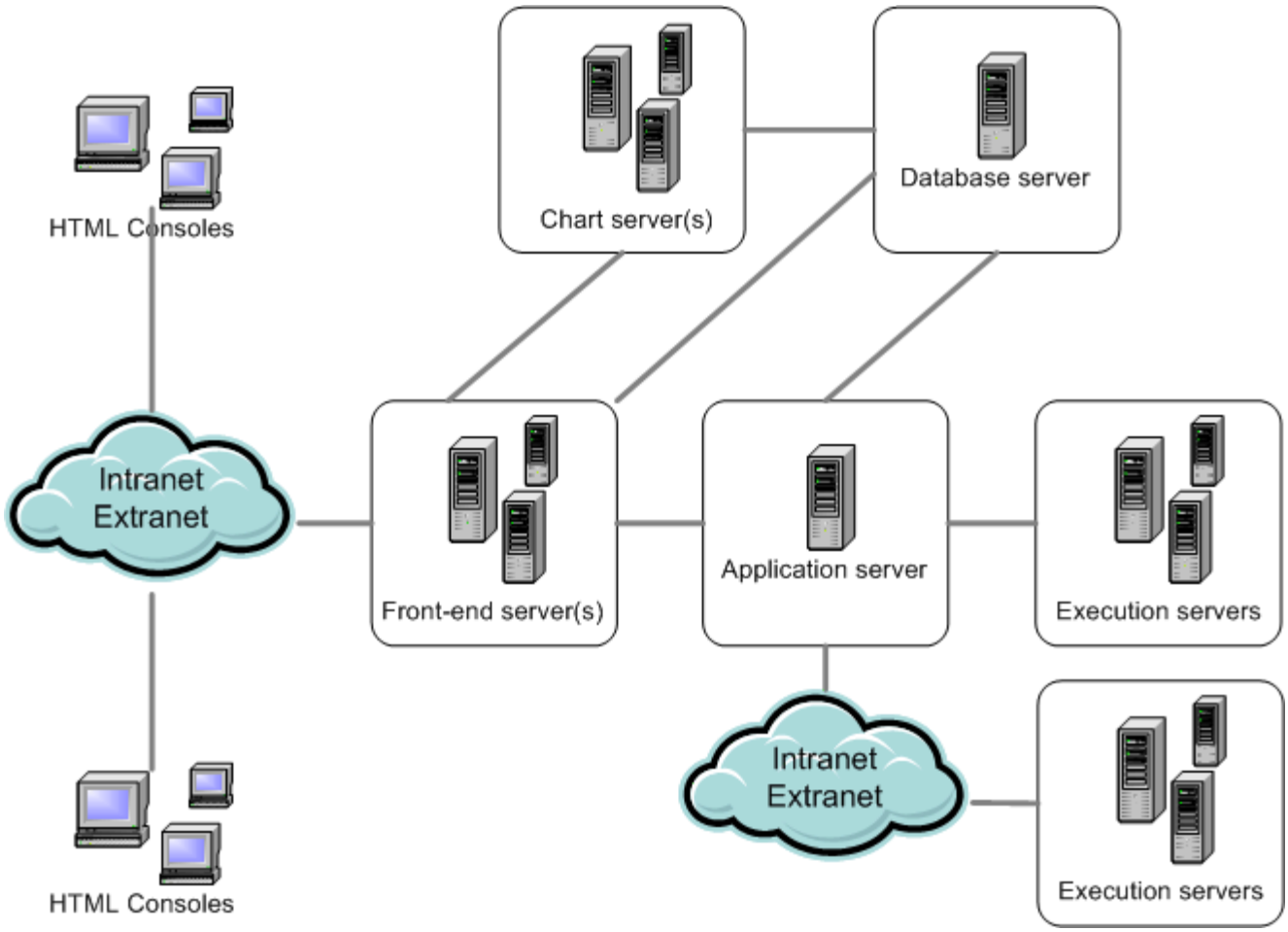
Getting Started

This section provides overview information on how to work with Performance Manager.

Silk Performance Manager Architecture

The following sections describe the Performance Manager components.

Overview



Front-End Server

The front-end server is responsible for the graphical user interface. This server is based on HTML and is accessible from any Web browser, such as Internet Explorer or Firefox. A user sends an appropriate HTTP request to the front-end server and receives a login page for authentication. After successful login, the user can use the corresponding application based on the respective user rights. The front-end server can operate as a stand-alone HTTP server, or it can be attached to a Web server, such as IIS via ISAPI filter.

Application Server

The application server synchronizes tasks such as the distribution of schedules, control of execution servers, and management of database configuration. These tasks require a centralized agency to ensure the consistent, reliable behavior of the application. The application server also evaluates results, saves them to the database, and sends alerts based on success conditions.

Execution Server

The execution server executes automated tests that are scheduled by authorized users. Users are responsible for the proper configuration of execution servers and additional resources that are required for test executions. The system allows for the installation and configuration of multiple execution servers working independently of one another.

Chart Server

The chart server is used to generate charts that are viewed in reports. The system allows for the configuration of a pool of chart servers. A built-in load balancing mechanism uses the pool to distribute chart generation. The chart server is also used to generate reports and deliver them directly to the end-user for viewing within a browser.

Database Server

System persistency is implemented using a RDBMS (Relational Database Management System).

Performance Monitoring with Silk Performance Manager

Silk Performance Manager (Performance Manager) includes an enterprise-monitoring product that allows users to manage the performance and reliability of their web-based applications.

Performance Manager helps users implement complex performance and functional transaction monitoring. It offers support for enterprise applications that are based on a wide range of technologies, including Web/HTML, client/server databases, J2EE, .NET, Web services, and ERP/CRM—including both client-side business transaction monitoring and infrastructure (server) monitoring. It lets users define and schedule monitors distributed around the globe to measure site health based on server metrics and end-user experience metrics such as availability, accuracy and performance. Monitoring can be maintained on an ongoing basis across all tiers of an application, with data reported back in a single, intuitive interface.

Real-time reporting of collected data helps users identify performance and functional issues within production environments and is vital for trend analysis and capacity planning. Performance Manager's configurable alarm notification system enables immediate alerting of operations personnel when application performance falls below defined threshold levels. Powerful notification features such as email, pager notification, SNMP traps, and SMS messages can also be configured.

Configuring the System

This section describes how to make the initial configurations that are required to work with Performance Manager. These configurations must be performed by an administrator.

Secure Web Server Connections with SSL

If you intend to work using a secure connection and have opted to install the ISAPI Web Server, then you must configure Microsoft Internet Information Services (IIS) to use the Secure Sockets Layer (SSL). You must first obtain a certificate from a Certificate Authority to gain access to the Secure Sockets Layer.

The Performance Manager default standalone Web server (Tomcat) can also be configured to use SSL (Secure Sockets Layer).

Configuring Secure Connections with Microsoft IIS

To use Performance Manager with Secure Sockets Layer (SSL), you must first obtain a certificate from a *Certificate Authority* and then apply the certificate to Internet Information Services (IIS). For detailed information on SSL enablement for sites, refer to the IIS documentation or contact Micro Focus SupportLine.

Configuring Secure Connections with Tomcat Web Server

You need to be familiar with Tomcat and SSL configuration to perform this task.

Set up the Performance Manager default standalone Web server (Tomcat) to use SSL (Secure Sockets Layer).

To enable secure communication with Performance Manager:

1. Log on to the Performance Manager server as an Administrator.
2. Stop all Performance Manager services (application, chart, execution, and front-end servers).
3. To generate a unique certificate for your Tomcat Web server, execute the following command in the Performance Manager Java directory: `C:\Program Files\Silk\Silk Performance Manager 19.0\lib\jre\bin\keytool -genkey -alias tomcat -keyalg RSA`. Note: The `alias` specifies the logical name in the keystore, for example `tomcat` or `Silk`. For additional information on Keytool, refer to the *Java SE Technical Documentation*.
4. Specify a keystore password value of `changeit`.

   If you desire to use a unique password, specify it here.
5. The keytool command prompt sequence will be similar to the following. Respond accordingly.

```
What is your first and last name?
[Unknown]: hostname (the name of the host as your users use it to access
the system)
What is the name of your organizational unit?
[Unknown]: IT Department (if that is the group creating the certificate)
What is the name of your organization?
[Unknown]: Company Name
What is the name of your City or Locality?
[Unknown]: City
What is the name of your State or Province?
[Unknown]: State
```

```
What is the two-letter country code for this unit?
[Unknown]: US
Is CN=xxxx, OU=xxxxxxx, O=xxxxxx, L=xxxxxxxxx, ST=xxxxx, C=xx correct?
[no]: Yes (These values will reflect what you entered previously)
Enter key password for <tomcat> same as keystore password
(RETURN if same as keystore password):
```

A file named `.keystore` is generated in the profile folder of the user you are logged in with, for example `C:\Users\Administrator`.

Note: By default Tomcat will look for your Keystore with the file name `.keystore` in the home directory with the default password `changeit`. The home directory is generally `/home/<username>/` on Unix and Linux systems, and `C:\Users\<username>\` on Microsoft Windows systems.

6. Move the `.keystore` file to a safe location of your choice.

Note: On some operating systems, Tomcat may encounter problems if you use a location that contains space characters.

7. Edit the Tomcat configuration file:

   Locate the `server.xml` file in the `conf\frontendserver\conf` subdirectory of the directory where Performance Manager is installed.

8. Open the file in a text editor such as Notepad. Comment out the current `Connector` entry and add the following text:

```
<!-- Define a SSL Coyote HTTP/1.1 Connector on port 8443 -->
<Connector port="8443" minSpareThreads="25" URIEncoding="UTF-8"
compression="on"
compressableMimeType="text/html,text/xml,text/plain,text/css,application/
javascript,application/xml"
debug="0" scheme="https" secure="true" SSLEnabled="true" clientAuth="false"
sslProtocol="TLS" keystorePass="changeit" keystoreFile="C:\<file location>
\.keystore"/>
```

Note: Make sure that the path specified in the `keystoreFile` parameter matches the location that you copied the `.keystore` file to. If you choose to use a different password other than `changeit`, you will need to add the `keystorePass` parameter to the `server.xml` file entry:

```
<Connector port="8443" minSpareThreads="25" URIEncoding="UTF-8"
compression="on"
compressableMimeType="text/html,text/xml,text/plain,text/
css,application/javascript,application/xml"
debug="0" scheme="https" secure="true" SSLEnabled="true"
clientAuth="false"
sslProtocol="TLS" keystorePass="newpassword" keystoreFile="C:\<file
location>\.keystore"/>
```

For more information, visit the *Apache Tomcat 7 Documentation*.

9. *Optional:* Change the **Port** of the front-end server in the `<Connector>` tag from `19120` to the desired port.
10. To enable BIRT reports on SSL environments, edit the registry key of the chart server in `HKEY_LOCAL_MACHINE\SOFTWARE\(Wow6432Node)\Apache Software Foundation\Procrun 2.0\SPMChartServer190\Parameters\Java\Options`. Add the following text to the key:

```
-Djavax.net.ssl.trustStore=C:\<file location>\.keystore
-Djavax.net.ssl.trustStorePassword=<Password>
```

The `<Password>` is the `keystorePass` you have defined.

11. Save the file and close the editor.
12. Restart all services that were stopped at the beginning of this procedure.
13. Log on to your Performance Manager server using HTTPS:

```
https://hostname:8443/login
```

Configuring Tomcat for Sending Secure Reports

You need to be familiar with Tomcat and SSL configuration to perform this task.

If your Performance Manager system uses secure connections, sending reports per email from the Performance Manager UI will result in `SSLHandshakeException` errors. To enable sending reports in a secure Performance Manager environment you need to configure Tomcat to trust the certificate.

1. Log on to the Performance Manager server as an administrator.
2. Open your browser and go to the application's home URL, for example `https://hostname:8443`. A dialog box warning you about the certificate appears.
3. Click **View Certificate**. The certificate detail page appears.
4. Click **Install certificate** and complete the subsequent certificate import wizard. Store the certificate in `Trusted Root Certification Authorities`. A confirmation message like `The import was successful` displays.
5. In your browser, export the certificate. In Internet Explorer for example, choose **Tools** > **Internet Options** and select the **Content** tab. Click **Certificates**, select the **Trusted Root Certification Authorities** tab, select the certificate you have installed before and click **Export**.
6. Select `DER encoded binary X.509` and click **Next**. Choose a location for the storage of the certificate file, for example `c:\hostname.cer`, and complete the export wizard.
7. Use the `keytool -import` command to import the file into your JRE's Certification Authorities keystore on your Performance Manager machine (on the front-end and application server): `"%SPM_HOME%\lib\jre\bin\keytool" -import -alias tomcat –keystore "%SPM_HOME%\lib\jre\lib\security\cacerts" -file c:\hostname.cer`
8. Type in the keystore password when prompted . The initial password is `changeit`.
9. Confirm the following prompt `Trust this certificate?` with `yes`. A message like `Certificate was added to keystore` should display. This confirms that your private certificate has been added to the application's keystore as a Trusted Certificate Authority.
10. Restart all services.

Application Server Location

The application server synchronizes tasks such as the distribution of schedules, control of execution servers, and management of database configuration. Before you can start working with Performance Manager, you need to specify the location of the application server.

Specifying a Location for the Application Server

When you use the `Standard Setup` option for installing Performance Manager, you do not need to specify an application server location. Setup automatically configures the localhost to be the application server. In this case you can skip this procedure. For additional information on setup options, see the application’s installation instructions.

To specify a location for the application server:

1. Once you have installed the Performance Manager software, connect to Performance Manager using a Web browser.

   Tip: The default URL is `http://<computer name>:19120/login` (no port information required if Performance Manager runs on IIS).

   You will receive a confirmation stating that the application server connection has not yet been defined.

2. Enter the **Host** or **IP address** and the **Port** of the application server.

   The application server is the computer where you installed Performance Manager's application server component. The default port is 19122.
3. Click **Login** to proceed. If your specifications are correct and the respective computer is running with the installed software, you will be returned to the login page.

The **Database Administration** page displays.

Silk Performance Manager Repositories

The terms "database" and "repository" are sometimes used interchangeably, but generally a repository is defined as a central place in which an aggregation of data is kept and maintained. The conceptual model for Performance Manager is that of a data repository that contains the application data.

A repository is a database used by Performance Manager to store, maintain, and analyze data. You must first choose which database system you want to use for your repository and take the necessary steps in the Performance Manager GUI to access the repository. You must be connected to a repository to work with Performance Manager.

You may set up multiple repositories, though only one repository at a time may be active.

To connect to a new Performance Manager database, you must first disconnect from the current database.

Note: You will receive error messages if you try to work with Performance Manager while the database is disconnected.

We recommend to perform administrative tasks that require the database to be disconnected during off-hours. If this is not possible, make sure to inform the users about the system-outage and its duration.

Note: If you are not planning on using LDAP authentication, user accounts will be stored in the repository. If you plan to use multiple repositories, you will have to maintain separate user accounts for each repository.

Creating a New Repository

Note: If you are currently connected to a Performance Manager repository, you must disconnect from the repository before you can create a new repository.

To create a new repository:

1. If you have already set up your Performance Manager application server, the **Database Administration** page will display in a browser window, and you can proceed to step 3 of this procedure.

   Tip: Alternatively, you can browse to your Performance Manager site with a Web browser. The default URL is `http://<computer name>:<port>/login`. When you use the *Standard Setup* option for installing Performance Manager, the **Database Administration** page displays immediately after you connect to the application.
2. If not already logged in, log in.

   `admin` is the default value for both the **username** and the **password**.
3. In the menu, click **Administration** > **System** .
4. Click **Database**.
5. Enter the information for the new database, then click **Connect**.

   You can create a database on the locally installed Microsoft SQL Server Express, a locally installed Microsoft SQL Server, or on a network server that has Microsoft SQL Server installed. Performance Manager supports:

   - Microsoft SQL Server 2012, 2014, 2016

Tip: For detailed information on the individual connection settings, see the *Database Settings Page*.

The **Create Database** dialog box displays.

6. To create a new database, provide the database administrator credentials.

   Tip: If you are creating a local or network database, enter the login information provided to you by your database administrator, then click **OK**.

   Note: This process can take up to a few minutes.

7. A **Messages** dialog box may display, informing you of servers that were found on the local computer and have automatically been added to the system configuration. Confirm this dialog box by clicking **OK**. If you receive a warning message stating `Couldn't define localhost as Execution Server`, you need to configure your execution servers manually.
8. You will be notified that the repository has been created successfully. Confirm the message by clicking **OK**. The login page displays.
9. Log in using your standard **username** and **password**.

   The default is `admin`/`admin`. Do not log in as a database administrator. Information about the currently connected database is displayed in **Administration** > **System Settings** > **Database**, but other available databases are not displayed anywhere in the Performance Manager user interface. You must make a note of the database name for future reference.

Your system is now ready for use.

Accessing an Existing Repository

To access an existing repository:

1. In the menu, click **Administration** > **System** .
2. Click **Database**.
3. If you are already connected to a repository, click **Disconnect**. A confirmation dialog box displays, asking you if you really want to disconnect from the current repository. Click **Yes** to disconnect.
4. Type or confirm the information for the database, then click **Connect**.

   For detailed information on the individual connection settings, see *Database Settings Page*.
5. After the database connection is established, a confirmation message displays. Confirm the message by clicking **OK**. The Performance Manager login page displays.
6. Log in to Performance Manager. After you log in, you should have access to Performance Manager.

   The default value for both the **username** and **password** is `admin`.

Repository Maintenance

This topic outlines common causes for performance decreases and recommends usage of features and common maintenance tasks to improve the performance of your database.

Note: For an overview of the performance of your system at a given time, open the **System Health** page. The **System Health** page provides a compact overview of the load status, because it displays the overall measure-writing performance and data load for each project.

System Capacity

There is a limit to the number of measures that can be written in an hour without overloading the system. This limit depends on the architecture, hardware resources, and database configuration, and not on a product limitation.

When the limit is reached you must remove non-essential measures or implement a second Performance Manager instance to reduce the number of measures.

Performance Impact

The most common causes of performance issues are improper hardware, sub-optimal database setups, and insufficient database maintenance and monitoring. To optimize the performance of your database, ensure that the hardware is appropriate and your database is properly set-up and maintained. The following product areas should be checked in regards to performance:

Product Area	Recommended Usage
Installed Performance Manager version	Use the latest version as it contains the latest optimizations to queries that build the different views.
Application Server	To enhance performance, Performance Manager caches measure objects in the systems RAM. When new results arrive the health data is calculated based on the cached objects instead of a database query, reducing the number of database calls required. Each time the Application Server is restarted this cache is lost and must be rebuilt when the Application Server starts. The cache is filled by querying the database, which means that during the rebuilding of the cache the database write times for measures will grow and results may be queued in the **System Health** page. The duration of the performance decrease is limited because once the cache is rebuilt the write time decreases and the results writing clears the queue.
Implementing storage reduction mechanism	Implementing storage reduction mechanism creates a data-delete job that physically deletes data from the database based on the configured settings. This job causes an increased workload on the database and therefore reduces overall performance. The data-deletion job is designed to pause to allow measure writing and therefore reduce the impact on measure write-times. The `BackgroundDeleteIdlePercentage` setting in the `SVAppServerHomeConf.xml` file specifies how long the data deletion process should pause in relation to the duration of the previous deletion command. For example, if the setting is set to 100, and a deletion packet took 200ms to complete, then the process will wait 200ms longer before it continues. We recommend to run the background deletion process only once a week, and to rebuild the indexes on the database afterwards.
The requested view or page	Different views or pages in Performance Manager use different queries to collect the data to build the view or page. Views and pages can be based on different periods of time, and some views and pages require less data to be read from the database than others. In some views and pages you can reduce the returned amount of data by collapsing unneeded sections.
Amount of measures or monitors	Although there is no logical limit to the amount of measures or monitors in a project, bigger numbers result in more data being read from the database, therefore increasing the time required to build a view. We recommend that you distribute the measures and monitors over projects, because results are written on a round-robin basis, where each project gets equal amount of time for writing the results.
Deleting a monitor	When you delete a monitor from a project, a data-deletion task is spawned, which deletes all information related to the monitor, and re-aggregation takes place. When you delete a single monitor instead of the entire project, the project-wide health cache is continuously re-aggregated and could result in a performance decrease. We recommend that you delete the entire project wherever possible.

Common Maintenance Tasks

In order to prevent performance decreases, regularly perform the following maintenance tasks:

- Rebuild the indexes on the `SV_TimeSeriesData` table.

- Rebuild the statistics on the entire database.

Disconnecting from a Repository

Note: Buffered results are deleted when you disconnect from the repository. Since it is possible to connect to a different database later, the buffered results would be invalid.

To disconnect from a repository:

1. Browse to your Performance Manager site with a Web browser.
   The default URL is `http://<computer name>/login`.
2. Log in.
   The default value for both the **username** and **password** is `admin`.
3. In the menu, click **Administration** > **System** .
4. Click **Database**.
5. Click **Disconnect** to disconnect from the current database.

Database Settings Page

Administration > **System** > **Database**

On the **Database** page you can create databases, connect a database with Performance Manager and disconnect the database again.

Configure the database connection with the following UI controls:

Item	Description
DBMS type	The type of DBMS you want to access (`MSSQL Server`).
DBMS hostname or IP address	The computer name or IP address of the computer hosting the database management system (DBMS) in the format `<computer name>\<instance name>`. **Database System** — **Hostname Description** **Microsoft SQL Server** — `<computer name>\<instance name>`, for example `localhost`. **Note:** An instance name only needs to be provided if the DBMS was installed using an instance. **Microsoft SQL Server Express** — `<computer name>\<instance name>`. The default MS SQL Server Express instance is `localhost\SQLExpress`.
Port	The port on which the DBMS listens. The default port for Microsoft SQL Server, including Express, is `1433`.
Database / SID	MS SQL Server database name.
Username	Database user with sufficient credentials. The default Microsoft SQL Server user, including Microsoft SQL Server Express, is `sa`, if not changed by your database administrator.
Password	Valid password for the specified **Username**.

Item	Description	
	Database System	**Password**
	Microsoft SQL Server, including Express	These databases enforce password usage. Ask your database administrator for the correct login credentials if you are not sure.
Read-only Username (optional)	An optional database user with read-only rights on all tables and views in the specified database. This user is used for executing reports. This will ensure that running reports with advanced queries will not change any data in the database, as executing advanced queries could have a detrimental effect on the data. For Microsoft SQL Server, Performance Manager automatically creates this user if you specify a name and password.	
Read-only Password (optional)	Valid password for the specified **Read-only Username (optional)**.	
Status	Displays the status of the Performance Manager connection to the DBMS.	
DBMS version info	Displays DBMS and operating system version information.	
Connect / Disconnect	Depending on the current connection status, use this button to connect to or disconnect from a DBMS.	

Initial Login

Once connected to a repository, you are ready to login using the default system administrator account.

Caution: Because the *SuperUser* account `admin` has all administrative privileges, you should immediately create a new password for this user to prevent unlimited access to these privileges. For more information on changing the password, see **Changing the Password of the System Administrator Account**.

Logging in for the First Time

Once connected to a repository, you are ready to login using the default system administrator account.

To login to Performance Manager for the first time:

1. Type `admin` in the **Username** text box and `admin` in the **Password** text box.
2. Click **Login**.

Caution: Because the *SuperUser* account `admin` has all administrative privileges, you should immediately create a new password for this user to prevent unlimited access to these privileges. For more information on changing the password, see **Changing the Password of the System Administrator Account**.

Login Page

Use this page to connect to Performance Manager. The page displays the following items:

Item	Description
Username	Type your LDAP or Performance Manager username. The default username for the SuperUser is `admin`.

Item	Description
Password	Enter a valid password for the **Username** that you entered.
Remember login	If you check the **Remember login** check box, you will not have to log in again after being automatically logged out by the application. You are logged out when you are idle for more than 30 minutes.
Login	Logs you in to Performance Manager, if the entered credentials are valid.

System Administrator Accounts

Adding user accounts allows different users to create projects and have access rights to work with them.

By default, the *SuperUser* account `admin` is available in the set-up installation with the password `admin`. For information on the other user types and their capabilities, see *User Roles and Permissions*.

Caution: Because the *SuperUser* account `admin` has all administrative privileges, you should immediately create a new password for this user to prevent unlimited access to these privileges. For more information on changing the password, see **Changing the Password of the System Administrator Account**.

Changing the Password of the System Administrator Account

Describes how to change the password of the default *SuperUser* account.

To designate a new password for the default *SuperUser*:

1. In the menu, click **Administration** > **Users**.
2. Click the **Accounts** tab.
   The page displays all available user accounts. When you access this page for the first time, the *SuperUser* account `admin` is the only user listed.
3. Click the name of the `admin` user.
   The **Configure existing user account** page displays.
4. Enter a password of your choice.
   Click **OK**.
5. Enter the password again to confirm it.
6. Click **OK**.

You are returned to the **User accounts** page and notified that the update was successful.

Chart Server Location

A chart server is a service that computes data and produces graphs. These graphs are viewable within the Performance Manager application. This service can be installed with the Performance Manager setup on a computer of your choice. You must specify the location of your chart server in order to display graphs.

Note: You can define as many chart servers as you want; Performance Manager automatically implements a load balancing mechanism for chart generation.

Adding Chart Servers

Describes how to add a chart server.

Note: You can only add a chart server if the respective *chart server service* is installed on the computer you want to add to the list of available chart servers. For more information, refer to the installation instructions of Performance Manager.

To add a new chart server:

1. In the menu, click **Administration** > **System** .
2. Click **Chart Servers**.
3. If a chart server was installed with the application server on the same computer, Setup will have already defined `localhost` as the chart server.
4. Click **New Chart Server**. The **Configure chart server** page displays.
5. On this page you are asked to specify the hostname or IP address, the port, and the URL where the charting service has been installed. The only change you will have to make to the default settings is the name of the computer on which the server is located. The default port is `19126` and the default URL is `ChartServer`.
6. Click **Check** to establish a test connection to the chart server. The **Chart Server Check** dialog box appears.

   Note: If the test is successful, a test image appears. If the test fails, an error message appears. Check the entered data and verify that a chart server is installed on the target machine.
7. Click **Back** to return to the chart server configuration. If the test connection was successful, check the status check box and click **Save**.
8. You will be returned to the list of chart servers, which now includes the chart server you have just added.

You can click **New Chart Server** to add more chart servers.

Editing Chart Servers

Describes how to edit a chart server.

To modify the settings of a chart server:

1. In the menu, click **Administration** > **System** .
2. Click **Chart Servers**.
3. Click the chart server you want to modify. The **Configure chart server** page displays.
4. On this page you can modify the hostname or IP address, the port, and the URL where the charting service has been installed. You can also activate/deactivate the chart server by checking/un-checking the **Active** check box. If you only want to activate or de-activate the chart server, please proceed with step 5.
5. Click **Check** to establish a test connection to the chart server. The **Chart Server Check** dialog box appears.

   Note: If the test is successful, a test image appears. If the test fails, an error message appears. Check the entered data and verify that a chart server is installed on the target machine.
6. Click **Back** to return to the chart server configuration. Since the test connection was successful, set the status check box to active.
7. Click **Save**. You will be returned to the list of chart servers.

Removing Chart Servers

Describes how to remove a chart server.

Note: Removing a chart server does not remove the installation of the service; it only removes the availability of the service to the application. To reconnect to the service at a later time, see *Adding Chart Servers*.

To remove a chart server:

1. In the menu, click **Administration** > **System** .
2. Click **Chart Servers**.
3. Click the **Chart Server URL** of the chart server that you want to remove.
4. Uncheck the **Active** check box and click save. You are returned to the **Chart Servers** page.
5. Click ✕ in the **Actions** column of the chart server you want to remove.
6. A confirmation dialog box displays, where you can confirm the deletion by clicking **Yes**.

Chart Servers Page

Administration > **System** > **Chart Servers**

Use this page to manage your chart servers. The page displays the following columns for each listed chart server:

Column	Description
Chart Server URL	The URL to connect to the chart server. Syntax: `http://<computer name or IP address>:<port>/ChartServer`. The default port is `19126`.
Status	Displays whether the connection to the chart server is active or inactive.
Created On	Date when the chart server connection was created.
Created By	The user who created the chart server connection.
Changed On	Date when the chart server connection was modified.
Changed By	The user who modified the chart server connection.
Actions	Perform a trial connection to the chart server by receiving a sample chart, or delete a chart server connection.

LDAP Authentication

Configure LDAP authentication to enable Performance Manager logins through an LDAP server.

Lightweight Directory Access Protocol (LDAP) is an open network protocol standard that is designed to provide access to directory services. LDAP provides a mechanism for querying and modifying information that resides in a directory information tree (DIT). A directory information tree typically contains a broad range of information about different types of network objects including users, printers, applications, and other network resources.

Performance Manager LDAP Integration

The most important aspect of LDAP integration in Performance Manager is user authentication. In most directories it is not possible to retrieve a user's password, so LDAP must be accessed each time a user needs to be authenticated.

Performance Manager LDAP integration supports plain-text authentication and SSL authentication. The directory service must either allow anonymous queries or a user with read rights on the directory must be provided.

LDAP Authentication Logic

Standard mode authentication means that a user can only authenticate against LDAP, if an LDAP server is defined and active. Mixed mode authentication means that a user can login with either LDAP or local credentials. If a user is known on an LDAP server, but the credentials are incorrect, access is denied.

Note: For either authentication mode, a user can only be logged in when their username exists in the Performance Manager database.

Standard Mode Authentication

Standard mode authentication is enabled when at least one LDAP server is active. Each defined LDAP server is checked to determine if a user (with specific username and password) can be authenticated. Access is granted when authentication succeeds on one of the servers.

Mixed Mode Authentication

When no LDAP server is defined, users will only be able to login with local credentials. If at least one LDAP server is active and a user account is set to use mixed mode authentication, each defined LDAP server is checked to determine if a user (with specific username and password) can be authenticated. If the user is unknown on all defined LDAP servers, then local database authentication is attempted. Access is denied when a user is also unknown based on local credentials. If a user is known on an LDAP server, but the credentials are incorrect, access is denied.

Importing a Certificate for Communicating with an LDAP Server Over SSL

To communicate with an LDAP server through SSL, a root authority certificate must be added to the default Java keystore.

If you receive an SSL handshake error when trying to connect to an LDAP server, perform the following steps:

1. Receive the SSL certificate from your IT department.
2. Start the key- and certificate-management tool *Keytool*.

   Keytool is part of Performance Manager's JRE installation, and is located in `C:\Program Files \Silk\Silk Performance Manager 19.0\lib\jre\bin`. For additional information on Keytool, see *keytool - Key and Certificate Management Tool*.
3. To add the certificate to the default Java keystore on the front-end server and application server, type for example the following command in Keytool:

   ```
   keytool
     -importcert
     -file CERTIFICATE.crt
     -keystore "C:\Program Files (x86)\Silk\Silk Performance Manager
                  19.0\lib\jre\lib\security\cacerts"
   ```

   Note: Make sure you enter the correct name of your certificate, `CERTIFICATE.crt` is just an example.

   You are prompted to type the password.
4. Type the default keystore password, `changeit`.
5. Restart the front-end server and the application server to reload the keystore.

Adding LDAP Servers

To configure an LDAP server for usage with Performance Manager:

1. In the menu, click **Administration** > **System** .
2. Click the **LDAP Servers** tab.
3. Click **Add New Server**. The **Add LDAP Server** dialog box appears.
4. Type a **Name** for the server and optionally a **Description**. You can define any name for the LDAP server; this field has no impact on the actual LDAP settings.
5. Check the **Active** check box to activate the server for use with Performance Manager. If unchecked, the LDAP server's services are not available to Performance Manager.
6. Type the **Hostname** or IP-address of the LDAP server and the **Port** used for the LDAP service. The default port is 389. When using SSL, the default LDAP port is 636.
7. Check the **Use SSL** check box to connect to the server through SSL. This check box is closely related to the settings defined in the **Port** field. For additional information on setting up the communication with SSL, see *Communicating with an External System Over SSL*.
8. *Optional:* In the **Bind DN** field, type the domain name of the user who is to be used to bind to the LDAP service. This user must have read rights on the directory from the given **Base DN** root. If this field is left empty, anonymous access will be used, except for LDAP servers that do not support anonymous access.
9. Type the **Password** of the user defined by **Bind DN**. This is not required when anonymous access is allowed.
10. Type the **Base DN** root for LDAP queries. For example `DC=yourcompany,DC=com`.
11. Type the **Filter** that is to be used for querying LDAP. Filters must contain a placeholder enclosed in braces.

    - Example 1: `(sAMAccountName={%username})`

      This example queries the LDAP server for the `sAMAccountName` with the value of the login name of the logged in Performance Manager user.
    - Example 2: `(&(sAMAccountName={%username})(memberOf=CN=Development,CN=Users,DC=yourcompany,DC=com))`

      This example queries the LDAP server for the `sAMAccountName` with the value of the login name of the logged in Performance Manager user, but only if the user is a member of the `Development` team. This may be useful for example if you enable the automatic account creation, but want Performance Manager to create accounts only for members of a certain LDAP group.
12. Click **Test** to perform a test connection to the LDAP server.

    For more information, see *Testing LDAP Servers*.
13. Click **OK** to save your settings.
14. If you are using multiple LDAP servers: Specify an **Order** number to prioritize the order in which the LDAP servers are queried for authentication.

Editing LDAP Servers

To edit an LDAP server profile:

1. In the menu, click **Administration** > **System** .
2. Click the **LDAP Servers** tab.
3. Click the name of the LDAP server profile you want to edit. The **Edit LDAP Server** dialog box appears.
4. Type a **Name** for the server and optionally a **Description**. You can define any name for the LDAP server; this field has no impact on the actual LDAP settings.
5. Check the **Active** check box to activate the server for use with Performance Manager. If unchecked, the LDAP server's services are not available to Performance Manager.
6. Type the **Hostname** or IP-address of the LDAP server and the **Port** used for the LDAP service. The default port is 389. When using SSL, the default LDAP port is 636.

7. Check the **Use SSL** check box to connect to the server through SSL. This check box is closely related to the settings defined in the **Port** field. For additional information on setting up the communication with SSL, see *Communicating with an External System Over SSL*.
8. *Optional:* In the **Bind DN** field, type the domain name of the user who is to be used to bind to the LDAP service. This user must have read rights on the directory from the given **Base DN** root. If this field is left empty, anonymous access will be used, except for LDAP servers that do not support anonymous access.
9. Type the **Password** of the user defined by **Bind DN**. This is not required when anonymous access is allowed.
10. Type the **Base DN** root for LDAP queries. For example `DC=yourcompany,DC=com`.
11. Type the **Filter** that is to be used for querying LDAP. Filters must contain a placeholder enclosed in braces.

    - Example 1: `(sAMAccountName={%username})`

      This example queries the LDAP server for the `sAMAccountName` with the value of the login name of the logged in Performance Manager user.
    - Example 2: `(&(sAMAccountName={%username})(memberOf=CN=Development,CN=Users,DC=yourcompany,DC=com))`

      This example queries the LDAP server for the `sAMAccountName` with the value of the login name of the logged in Performance Manager user, but only if the user is a member of the `Development` team. This may be useful for example if you enable the automatic account creation, but want Performance Manager to create accounts only for members of a certain LDAP group.
12. Click **Test** to perform a test connection to the LDAP server.

    For more information, see *Testing LDAP Servers*.
13. Click **OK** to save your settings.

Testing LDAP Servers

To test the connection to an LDAP server:

1. When adding or editing an LDAP server profile in Performance Manager, the **Add LDAP Server** dialog box, respectively the **Edit LDAP Server** dialog box displays a **Test** button.
2. Click **Test** to display the **Test LDAP Configuration** dialog box.
3. In the **Test username** field, enter a username to be used for testing LDAP authentication.
4. Fill in the **Test password** associated with the user who is to be used for testing LDAP authentication.
5. Click **Test** to execute an authentication test.

   Note: LDAP error codes are included when tests fail.

   A dialog box shows you whether or not the test was successful.
6. Click **Close** to return to the **Add LDAP Server** dialog box, respectively the **Edit LDAP Server** dialog box. If the test connection was not successful, edit your settings or ask your system administrator for assistance. Then start over at step 2 again.

Deleting LDAP Servers

To delete an LDAP server profile:

1. In the menu, click **Administration** > **System** .
2. Click the **LDAP Servers** tab.
3. If the LDAP server is active, you need to deactivate it before you can delete it. Click the name of the LDAP server profile that you want to delete. The **Edit LDAP Server** dialog box appears.

4. Uncheck the **Active** check box to deactivate the server and click **OK**.
5. Click ✕ (**Delete**) in the **Actions** column of the LDAP server you want to delete.
6. Click **Yes** to confirm the deletion.

LDAP Servers Page

Administration > **System** > **LDAP Servers**

The **LDAP Servers** page lists all configured LDAP servers. Use this page to manage your LDAP servers.

In this page you can perform the following actions:

- Click **New LDAP Server** to configure a new LDAP server.
- Specify an **Order** number to prioritize the order in which the LDAP servers are queried for authentication.
- Click an existing LDAP server in the list to edit the settings.
- Click ✕ (**Delete**) in the **Actions** column to delete an LDAP server (you need to deactivate the LDAP server beforehand).

New LDAP Server Dialog Box

Note: The **Edit LDAP Server** dialog box contains the same items as the **Add LDAP Server** dialog box.

The dialog box includes the following items:

Item	Description
Name	Specifies the name of the LDAP server as it should appear in the Performance Manager GUI. You can define any name for the LDAP server; this field has no impact on the actual LDAP settings.
Description	A description of the LDAP server. You can enter any text for the description of the LDAP server; this field has no impact on the actual LDAP settings.
Active	Activates the LDAP server, if checked. If unchecked, the LDAP server's services are not available to Performance Manager.
Hostname	The LDAP server URL.
Port	The LDAP port. The default port is `389`. When using SSL, the default LDAP port is `636`.
Use SSL	Defines whether Performance Manager connects to the LDAP server through SSL (if checked) or without SSL (if unchecked). This check box is closely related to the settings defined in the **Port** field.
Bind DN (optional)	The distinguished name of the user who is to be used to bind to the LDAP service. This user must have read rights on the directory from the given **Base DN** root. If this field is left empty, anonymous access will be used, except for LDAP servers that do not support anonymous access.
Password (optional)	The password of the user defined in the **Base DN** field. This is not required when anonymous access is allowed.
Base DN	Base Distinguished Name (DN) root node for LDAP queries. For example `DC=comp,DC=net`.
Filter	The filter that is to be used for querying LDAP. Filters must contain a placeholder enclosed in braces. Example 1: `(sAMAccountName={%username})`

Mail Host Location

To have reports emailed to you to update you about results from your application, you must specify the location of your mail server. You may only configure email settings if you have administrator privileges.

Note: Performance Manager supports basic SMTP authentication (*LOGIN PLAIN*).

Specifying a Location for the Mail Host

To specify the location of up to three mail servers:

1. In the menu, click **Administration** > **System** .
2. Click the **Notification** tab.
3. Click the **Email** tab, if it has not already been selected automatically.
4. In the **Server 1**, **Server 2** and **Server 3** fields, type the mail server hostname or IP address of your email server(s).
5. Type the **Email address of system administrator**, and the **'From' address to use for emails**.
6. To test the configuration, click **Check**. Verify that the system administrator receives a test email notification from the application.

   If you receive an error message, or if you do not receive an email, review your mail settings. Ensure that the hostname of your email server is correct and that the SMTP protocol is running on that computer.
7. If you receive a notification that the test mail has been sent, click **Save**.

Email notification is now ready for use.

Email Notification Page

Administration > **System** > **Notification**

Use this page to configure a mail server for your Performance Manager applications. The page displays the following items:

Item	Description
Email address of system administrator	Specifies the mail address of the Performance Manager system administrator. You must enter an address here to complete the configuration. You may add any valid email address.
'From' address to use for emails	Specifies the name that is to appear in the **From** field when someone receives an email from the system. This can be any email address, for example `System_message@mycompany.com`.
Server 1 **Server 2** **Server 3**	The names or IP addresses of the servers that send your mail. For many companies, this server is simply called mail. If your mail server uses SMTP authentication (*LOGIN PLAIN*), you must enter a valid user and password for the mail server. Contact your mail server administrator if you do not know the login credentials.
Check	Sends a test email to the recipient defined in the **Email address of system administrator** text box.
Reset	Clears all items on this page.
Save	Saves your settings.

SMS Host Settings

You may configure Performance Manager to send notifications of results from your application through Short Messaging Service (SMS). To do so, you must specify information about your mobile phone provider. Your mobile network provider should be able to give you the required information.

To make optimal use of the Performance Manager SMS service, you may need to define a standard set of abbreviations or short-hand “codes” that your team can use for system communications.

Note: This service only works after you configure email notification; messages are sent to your mobile provider through email. For additional information, see *Specifying a Location for the Mail Host*. You may only configure these settings if you have administrator privileges.

Configuring Settings of an SMS Host

To configure the settings of an SMS host:

1. If not already done, you first need to configure a mail host.

   For more information, see *Specifying a Location for the Mail Host*.
2. In the menu, click **Administration** > **System** .
3. Click the **Notification** tab.
4. Click the **SMS** tab.
5. Type the **Email address of mobile provider**, the **Email address of sender**, and the **Mobile phone number for test SMS**.

   For more information, see *SMS Notification Page*.
6. In the **Subject** text box, enter a subject for the SMS to be sent.
7. To confirm that the configuration has been successful, click **Check** and verify that the SMS recipient, **Mobile phone number for test SMS**, receives a test SMS notification.
8. If you receive an error message, review your SMS settings. Make sure that you have entered the correct data as given to you by your network provider.
9. If you receive confirmation that the test SMS has been sent, click **Save**.

Your SMS notification is now ready for use.

SMS Notification Page

Administration > **System** > **Notification** > **SMS**

Use this page to configure an SMS server for your Performance Manager applications. The page displays the following items:

Item	Description
Email address of mobile provider	Can be obtained from the network provider that offers mobile services for sending SMS messages. The address includes a `{#}` symbol as a place holder, which should be replaced by the phone number receiving the SMS message. For example `MyProvider@NetCompany.com`.
Email address of sender	Is provided by your service provider.For example `MyUser@MyCompany.com`.
Mobile phone number for test SMS	Any cellular phone number that you want to send a test SMS to by clicking **Check**.

Item	Description
Subject	The subject of an SMS that is sent by the system. The subject of the SMS should be a series of letters, numbers, or symbols, for example `Alarm`.
Check	Sends a test SMS to the recipient defined in the **Mobile phone number for test SMS** text box.
Reset	Clears all fields on this page.
Save	Saves your settings.

PageGate Gateway Access

To receive pages that include reports regarding results from your application, configure Performance Manager to page you through PageGate™. You must already have PageGate installed and configured to use this service and you must specify information regarding how Performance Manager is to send messages through PageGate.

PageGate is a third-party product that is used to send text messages to wireless devices, for example pagers, SMS, and others. Performance Manager uses the GetAscii interface of PageGate.

Configuring Access to the PageGate Gateway

To configure access to the PageGate gateway:

1. In the menu, click **Administration** > **System** .
2. Click the **Notification** tab.
3. Click the **PageGate** tab.
4. Type the **Polling directory of the GetAscii interface**, the **Name of sender**, the **Timeout (in seconds)**, and the **Recipient of checks**.

   For additional information, see *PageGate Gateway Settings Page*.
5. To confirm that the configuration has been successful, click **Check** and verify if the pager recipient, **Recipient for checks**, receives the test message.
6. If you receive an error message, review your PageGate settings. Make sure that the polling directory is accessible. Verify that PageGate's GetAscii interface is configured and points to the correct polling directory. Verify that the sender and recipient users are registered in the PageGate list of recipients.
7. If you confirm that a test message has been sent and that the test recipient has received the message, click **Save**.

PageGate notification is now ready for use.

PageGate Gateway Settings Page

Administration > **System** > **Notification** > **PageGate**

Use this page to configure PageGate Gateway (pager) notification for your Performance Manager applications. The page displays the following items:

Item	Description
Polling directory of the GetAscii interface	The **Polling directory of the GetAscii interface** is the name of the directory in PageGate from which messages are sent. You can find the name of this directory in your PageGate configuration. If PageGate is not installed on the same computer as the application server, the directory must be on a network drive of the computer on which PageGate is installed. In

Item	Description
	such an instance, you must map the directory on the application server (map network drive) so that it can be specified in pages. For example `F:\polling`.
Name of sender	The name of the sender is the name of the registered user in your PageGate configuration. This must be a name included in the PageGate list of recipients.
Timeout (in seconds)	The timeout is the number of seconds that Performance Manager is to check in PageGate to see if messages have been sent. The default setting of `10` seconds is normally a reasonable time period, though the ideal value depends on the interval at which PageGate is configured to retry message delivery.
Recipient of checks	The recipient for checks is the address of a recipient who will receive test notifications when you click **Check**. This name must also be included in the PageGate list of recipients.
Check	Sends a test pager message to the recipient defined in the **Recipient for checks** text box.
Reset	Clears all items on this page.
Save	Saves your settings.

SNMP Trap Notification

To have reports sent to you with results from your application, you may configure Performance Manager to notify you through a Simple Network Management Protocol (SNMP) Version 2 trap message. You must already have this software installed and configured on a computer in your LAN to use this service and to view data through the third-party software. This type of notification can be used for transferring alarms directly into your existing system management tool.

Configuring SNMP Trap Notification

Describes how to configure SNMP trap notification.

To configure access to SNMP trap messaging:

1. In the menu, click **Administration** > **System** .
2. Click the **Notification** tab.
3. Click the **SNMP trap** tab.
4. Type the **SNMP trap destination hostname or IP-address**, the **Port**, and the **Community**.
   For additional information, see *SNMP Trap Settings Page*.
5. To confirm that the configuration has been successful, click **Check** and verify if the message has arrived in your SNMP database.
6. If you receive an error message, review your SNMP trap settings. Make sure that the SNMP software is installed and running on the host you specified and that the community string is available for use.
7. Once you receive confirmation that the SNMP trap has been sent, click **Save**.

SNMP trap notification is now ready for use.

SNMP Trap Settings Page

Administration > **System** > **Notification** > **SNMP trap**

Use this page to configure SNMP trap notification for your Performance Manager applications. The page displays the following items:

Item	Description
SNMP trap destination hostname or IP-address	The name of the computer or the IP-address to which messages are sent (the location of your SNMP database). For example `MySNMPHost.MyDomain`.
Port	The number of the port you have configured in the SNMP trap software through which you will receive the message. You may use the default port number `162` as specified in the GUI as it is the standard port for SNMP trap messages.
Community	The SNMP Community string is like a user ID or password that allows access to a router's or other device's statistics. Most equipment ships from the factory with the read-only community string of `public`. It is standard practice for network managers to change all community strings so that outsiders cannot see information about the internal network. If you need more information on the communities used in your organization, please consult your network administrator.
Check	Sends a test SNMP trap message to the defined SNMP trap database.
Reset	Clears all items on this page.
Save	Saves your settings.

System Proxies

Configure a system proxy to enable execution servers of a certain location to communicate with the application server through the proxy. Once you have specified the location of a proxy server, you can select the defined proxy server in your location configuration. Enabling this setting will force all execution servers of the location to communicate with the application server through the defined system proxy.

Configuring a System Proxy

This procedure explains how to configure a system proxy. To use a proxy for your location you must configure a system proxy.

To configure a system proxy:

1. In the menu, click **Administration** > **System** .
2. Click the **System Proxy** tab.
3. Specify the **Host** and the **Port** of the proxy that should be used.
4. Specify **Username** and **Password** if required by the proxy.
5. To confirm that the configuration has been successful, click **Check**. A message informs you whether or not connection to the proxy server has been successful.
6. If you receive an error message, review your system proxy settings. Make sure that a system proxy is installed and running on the host you specified.
7. Click **Save**.

Your system proxy is now ready for use.

System Proxy Page

Administration > **System** > **System Proxy**

Use this page to configure a system proxy. The page displays the following items:

Item	Description
Host	The hostname or IP-address of the computer that is intended to serve as system proxy.
Port	The port number on which the system proxy listens. The default port is `8080`.
Username (if required)	Type a valid username if the proxy server requires login credentials.
Password (if required)	A valid password for the specified **Username**.
Reset	Clears all items on this page.
Check	Tests the connection to the proxy with the credentials you provided.
Save	Saves your settings.

Configuring the Application

This section contains conceptual information about user accounts, projects, locations, and execution servers. It also covers the administration of custom reports and managing uploaded files, and the configuration of other common entities.

Once you have completed the initial configuration of Performance Manager (system configuration), this section will guide you through the steps required to set up user accounts, projects, locations, execution servers, and more. These tasks must be performed by an administrator.

User Roles and Permissions

When working with Performance Manager, tasks are assigned to designated groups of users who have access to assigned projects. Within groups, users are granted specific roles within those projects. User permissions are configured based on user role type and group membership. This topic defines each permission type and details the specific permissions that are associated with each user role.

Each user account can belong to one or multiple groups. A group specifies which roles a user has within that group. Groups are assigned to projects. So the permissions that each individual user has are derived from the group/role assignments that have been defined for them. Defined permissions apply only to the projects that are assigned to the groups in which each user has a group/role assignment.

User Roles

There are five predefined user roles:

- SuperUser
- Administrator
- Project Manager
- Analyst
- Reporter

These roles cannot be modified or deleted.

SuperUser

The SuperUser role is a special role that is granted all privileges across Performance Manager.

Administrator

Administrator tasks include the configuring of application-, front-end, and chart-server locations; setting up and maintaining repositories and notification settings; creating accounts; configuring locations and execution servers, and others.

Project Manager

Project Managers maintain the projects for which they are responsible. Project Managers do not have write access to the Performance Manager Administration area. Project Managers can only access the projects to which they have been assigned as Project Managers, where they have full write access to all project-related features, including creating, editing and deleting blackout periods related to their assigned projects. If a blackout period involves just one project that a project manager is not assigned to, they will not be able to make any modifications though.

Analyst

Analysts analyze the results of projects that have been assigned to them. They cannot modify project settings or schedules and have read-only privileges.

Reporter

In addition to having all the rights of Analysts, Reporters additionally have the right to edit and delete reports in *Advanced mode*. Advanced mode allows reporters to enter, modify, and delete SQL statements for advanced reports. For details on advanced reports, refer to the Performance Manager Help.

Permission Definitions

This section explains the permissions that govern user ability to perform tasks and access secure areas within Performance Manager. There is a separate list for each permission category.

Note: Permissions for predefined roles cannot be edited.

User Type Permissions

The following permissions and security areas are associated with the appropriate user types:

Role	System	Administration	Configuration	Simple Reports	Advanced Reports
SuperUser	RWD	RWD	RWD*	RWD	RWD
Administrator	RWD	RWD	RWD*		
Project Manager	R	R	RWD*	RWD*	R*
Analyst				R*	R*
Reporter	R	R		RWD*	RWD*

* only for assigned projects

The following table explains the abbreviations that are used above:

Abbreviation	Permission Type
R	Read permission
W	Write/Edit permission
D	Delete permission

The following table details the particular permissions that are associated with each security area:

Security Area	Permissions
System	Connecting database, chart server, locations and execution servers, and more
Administration	Users, projects, reports, user/project assignment, audit logs, and more
Configuration	Manage monitors, rules, conditions, and custom incidents
Simple Reports	Manage reports
Advanced Reports	Manage reports in the advanced mode (entering SQL statements)

User Accounts and Groups

A user account must be created for each user working with Performance Manager. One or more groups of users are assigned to specific projects. Only with a user account, a user role, and a group assignment can a user work with a Performance Manager project.

Maintaining User Accounts

User accounts track login data and configuration settings for individual users. They also enable user login. User accounts are typically assigned to group accounts with one or more specific user roles for specific projects. The SuperUser is the only user role that can, among other things, configure the application-, Web-, and chart server locations; and set up and maintain repositories and notification settings.

Caution: Because the *SuperUser* account `admin` has all administrative privileges, you should immediately create a new password for this user to prevent unlimited access to these privileges. For more information on changing the password, see **Changing the Password of the System Administrator Account**.

Adding User Accounts

To add a user account:

1. In the menu, click **Administration** > **Users**.
2. Click the **Accounts** tab.

   The page displays all available user accounts. When you access this page for the first time, the *SuperUser* account `admin` is the only user listed.
3. Click **New User**. The **Add new user account** page displays.
4. Type a username and password for the user. Type the password a second time to confirm it.
5. Check the **Mixed mode authentication (LDAP)** check box to enable both LDAP and local-credential based authentication.
6. Set the login to **Locked** if you want to prevent the user from logging in.
7. Type the user's first name, last name and email address.
8. Type the user's local time zone and select a date format, a short date format, and the first day of the week.
9. Type the **Page refresh time** in seconds and the **CSV separator string**.
10. Select a group and role definition from the respective list boxes.
11. Click **Add Assignment** to add the group and role combination to the user account.
12. Repeat the previous two steps to assign all desired group and role combinations to the user account.
13. To remove a group and role combination from the current user account, click the **Delete** icon in the **Actions** column.
14. Click **Save** to save your settings.

Editing User Accounts

Once a user account is set up you may edit any of the parameters, except the **Login** name.

Note: Changes to a user account become active upon the next login of the changed user account. Please notify the user to logout and login again.

To edit a user account:

1. In the menu, click **Administration** > **Users**.

2. Click the **Accounts** tab.

   The page displays all available user accounts. When you access this page for the first time, the *SuperUser* account `admin` is the only user listed.
3. Click the **Login** name of the user account that you want to edit. The **Configure existing user** page displays.
4. Edit the password of the user as required. Type the password a second time to confirm it.
5. Check the **Mixed mode authentication (LDAP)** check box to enable both LDAP and local-credential based authentication.
6. Edit other user settings as required.
7. Select a group and role definition from the respective list boxes.
8. Click **Add Assignment** to add the group and role combination to the user account.
9. Repeat the previous two steps to assign all desired group and role combinations to the user account.
10. To remove a group and role combination from the current user account, click **Delete** in the **Actions** column.
11. Click **Save** to save your settings.

Deleting User Accounts

Caution: Deleting a user account is not reversible. You may lock a user account instead, if you want to temporarily make an account unavailable. For additional information about locking user accounts, see *Editing User Accounts*.

To delete a user account:

1. In the menu, click **Administration** > **Users**.
2. Click the **Accounts** tab.

   The page displays all available user accounts. When you access this page for the first time, the *SuperUser* account `admin` is the only user listed.
3. In the **Actions** column of the user account you want to remove, click **Delete**. A confirmation dialog box displays.
4. Click **Yes** to confirm the operation; click **No** to abort. If you choose **Yes**, you will be returned to the list of user accounts where the deleted account will no longer be listed.

User Settings Page

Administration > **Users** > **Accounts** > **New/Edit User**

Use the **User Settings** page to configure user accounts. User account settings are closely related to group account settings.

You can click on the name of the user in the menu to access the **User Settings** page for the logged-in user.

Note: You must define at least one group and role assignment to save a user account.

Login Data Item	Description
Login	The username to be stored in the Performance Manager repository. If you check **Mixed mode authentication (LDAP)** below, the entered username must match the defined LDAP username.
Password	Enter a valid password for the **Login** that you entered. This password is not related to the LDAP password.
Confirm password	Enter the password again to confirm it.

Login Data Item	Description
Mixed mode authentication (LDAP)	Check this check box to enable both LDAP and local-credential based authentication. If an LDAP server exists, not checking this check box results in LDAP-only authentication.
Locked	Check this check box if you want to prevent the user from logging in with the given credentials. This makes the user account inactive.

General Data Item	Description
First name	Type the user's first name. This information does not affect the behavior of Performance Manager; it simply tracks user contact information.
Last name	Type the user's last name. This information does not affect the behavior of Performance Manager; it simply tracks user contact information.
Email	Type the user's email address. This information is used for notification purposes.
Time zone	The user's local time zone. Time zone information is used to display times and dates in the user's local time zone.
Date format	The selected date format is presented to the user in lists, reports, and in the calendar whenever Performance Manager displays a long date format.
Short date format	The selected date format is presented to the user in lists, reports, and in the calendar whenever Performance Manager displays a short date format.
First day of week	The first day of the week determines the weekly view in reports.
Page refresh time	The page refresh time in seconds. This setting determines the time interval at which report pages are refreshed automatically. Type `0` (default value) if you do not want reports to refresh automatically. The page refresh time only affects pages that support automatic page refreshing.
CSV separator string	This string is used as a row separator for the user's downloaded CSV-files. Reports can be downloaded as CSV-files.

Group and Role Assignments Item	Description
Group and Role Assignments table	Lists all existing user group/user role assignments of the user. You can also delete group and role assignments by clicking ✕ next to the assignment you want to remove.
Group	Select a group to which the user is to be assigned. This list box lists the user groups that have been defined by a Performance Manager administrator.
User role	Select the user role with which the user is to be assigned to the selected group. Available user roles are predefined by the system.
Add Assignment	Click this button to create a new user group/user role assignment with the group and user role you selected.

Maintaining Groups

Groups define access to specific projects. Each user can be associated with one or more groups from which they inherit the access rights to the projects that are defined for the selected group.

Note: Users can be added to groups with multiple roles, allowing advanced user permission configuration.

Adding Groups

To add a group:

1. In the menu, click **Administration** > **Users**.
2. Click the **Groups** tab.
3. Click **New Group**.
4. In the **Group name** field, type a group name for the new group.
5. In the **Description** field, enter a description for the new group.
6. Select a user with a role assignment from the respective list boxes, then click **Add Selection** to add the user and role combination to the new group.
7. Repeat the previous step to assign all desired user and role combinations to the group.
8. To remove a user and role combination from the current group, click ✕ in the **Actions** column.
9. In the **Project Assignment(s)** section you can assign any existing projects to this group.
10. Click **Save**.

Editing Groups

To edit a group:

1. In the menu, click **Administration** > **Users**.
2. Click the **Groups** tab.
3. Click the group name of the group you want to edit. The **Configure existing user group** page displays.
4. In the **Group Name** field, edit the name as required.
5. In the **Description** field, edit the group's description as required.
6. Select a user with a role assignment from the respective list boxes, then click **Add Selection** to add the user and role combination to the new group.
7. Repeat the previous step to assign all desired user and role combinations to the group.
8. To remove a user and role combination from the current group, click ✕ in the **Actions** column.
9. In the **Project Assignment(s)** section you can assign any existing projects to this group.
10. Click **Save** to return to the **Groups** page.

Deleting Groups

Before you can delete a group, you must remove all user and role assignments from the group. For additional information about modifying groups, see *Editing Groups*.

To delete a group:

1. In the menu, click **Administration** > **Users**.
2. Click the **Groups** tab.
3. In the **Actions** column of the group you want to remove, click ✕. A confirmation dialog box displays.
4. Click **Yes** to confirm the operation; click **No** to abort.

Group Settings Page

Administration > **Users** > **Groups** > **New/Edit Group**

Use the **Group Settings** page to configure user groups. Group settings are closely related to user account settings. The page displays the following items:

Item	Description
Group name	Specifies the name of the group as it should display in the GUI. You can define any name for the group.
Description	A description of the group. You can enter any text for the description.
Account and Role Assignment(s)	Lists all existing user/role assignments of the group. You can also delete user and role assignments by clicking ✕ next to the assignment you want to remove.
User	This list box lists the user accounts that have been defined by an administrator. Select a user to be assigned to the group.
Role Definition	Available user roles are predefined by the system. Select the user role with which the user is to be assigned to the group.
Add Selection	Click to create a new user account and user role assignment with the selected user and user role.
Project Assignment(s)	Lists all existing projects and whether they are assigned to the group account. Check the check box next to a project to assign the project to the group account. If no projects exist, you may assign them later after you have created them.
Select All	Checks the check boxes of all listed projects.
Deselect All	Un-checks the check boxes of all listed projects.

Working with Projects

This topic describes the conceptual background of projects in Performance Manager.

Projects are a prerequisite for beginning work with Performance Manager. Projects serve as containers for related sets of tasks and results. Resources such as project managers and analysts are allocated to projects by assigning them to user groups, which have access rights to certain projects.

Adding Projects

To create a project:

1. In the menu, click **Administration** > **Projects** . The **Projects** page displays, listing all existing projects.
2. Click **New Project**. The **Project Settings** page displays.
3. Type a **Project name** and **Description**.
4. Select the **Project Owner**.
5. The **Groups** section includes a list of registered user groups. Check the **Assigned** check boxes of the user groups that will work with this project. If no user groups exist, you may assign them later after you have created them. You can also configure the group/project assignment on the **Group Settings** page. Privileges vary based on user roles. For information about user privileges, see *User Roles and Permissions*.
6. A list of locations is located at the bottom of the page. Select the location(s) from which this project's tasks are to be executed. Click **Select All** to assign all locations to the project, or click **Deselect All** to select no locations. If no locations exist, you may assign them later after you have created them. You can also configure the location/project assignment on the **Location Settings** page. For detailed information, see *Managing Locations*.
7. Click **Save** to save your settings. You are returned to the **Projects** page where the new project is listed.

Editing Projects

To edit an existing project:

1. In the menu, click **Administration** > **Projects** . The **Projects** page displays, listing all existing projects.
2. Click the project name of the project you want to edit.

   Note: The project must be inactive.
3. Edit the **Project name** and **Description** as required.
4. Change the **Project Owner** as required.
5. Check the **Active** check box to activate the project.
6. The **Groups** section includes a list of registered user groups. Check the **Assigned** check boxes of the user groups that will work with this project. If no user groups exist, you may assign them later after you have created them. You can also configure the group/project assignment on the **Group Settings** page. Privileges vary based on user roles. For information about user privileges, see *User Roles and Permissions*.
7. A list of locations is located at the bottom of the page. Select the location(s) from which this project's tasks are to be executed. Click **Select All** to assign all locations to the project, or click **Deselect All** to select no locations. If no locations exist, you may assign them later after you have created them. You can also configure the location/project assignment on the **Location Settings** page. For detailed information, see *Managing Locations*.
8. Click **Save** to save your settings. You are returned to the **Projects** page.

Activating or Deactivating Projects

Note: You can also activate or deactivate an existing project from the **Projects** page. For additional infomation, see *Editing Projects*.

To activate or deactivate an existing project:

1. In the menu, click **Administration** > **Projects** . The **Projects** page displays, listing all existing projects.
2. Click **Active/Inactive** in the **Status** column of the project you want to activate or deactivate. A confirmation dialog box displays, asking you if you are sure about the activation or deactivation.
3. Confirm to toggle the project status to `Active` or `Inactive`.

Deleting Projects

Caution: When you delete a project you permanently remove all related results from the repository. You also destroy all content associated with the project. If you want to keep results, we recommend that you set a project to inactive rather than delete it. For information on deactivating projects, see *Activating or Deactivating Projects*.

To delete a project:

1. In the menu, click **Administration** > **Projects** . The **Projects** page displays, listing all existing projects.
2. Click ✕ in the **Actions** column of the project you want to remove.

   Note: The project must be inactive.

   A confirmation dialog box displays, asking you to confirm the deletion.
3. Click **Yes** to remove the project; or click **No** to abort the operation. If you choose **Yes**, you will be returned to projects list, where the deleted project is no longer listed.

Project Settings Page

Administration > **Projects** > **New Project**

Use the **Project Settings** page to configure projects. The page displays the following items:

Item	Description
Project Name	Specifies the name of the project as it should appear in the GUI and in reports.
Description	A description of the project. You can enter any text for the description.
Project Owner	Specifies the owner of the project. The selected user account does not have any special privileges; this setting is purely informative.
Active	Check this check box to activate the project. Inactive projects are not visible in your application.
Groups	The **Groups** section includes a list of registered user groups. Check the **Assigned** check boxes of the user groups that will work with this project. If no user groups exist, you may assign them later after you have created them. You can also configure the group/project assignment on the **Group Settings** page. Privileges vary based on user roles. For information about user privileges, see *User Roles and Permissions*.
Location	A list of locations is located at the bottom of the page. Select the location(s) from which this project's tasks are to be executed. Click **Select All** to assign all locations to the project, or click **Deselect All** to select no locations. If no locations exist, you may assign them later after you have created them. You can also configure the location/project assignment on the **Location Settings** page. For detailed information, see *Managing Locations*.

Managing Locations

Locations are logical containers for execution servers. For information on setting up execution servers, see *Setting Up Execution Servers*. Since Performance Manager supports worldwide distribution of Points of Presence (PoP) — the distribution of execution servers — it is desirable to group execution servers into locations. Locations are not required to be physical locations though, they can simply be used to group your execution servers into manageable units.

Note: Performance Manager automatically creates a default location called `Local`.

Adding Locations

To add a new location:

1. In the menu, click **Administration** > **Locations**.
2. Click **New Location**.

   The **Add New Location** page displays.
3. Type a **Location Name**.
4. If you have specified the location of a proxy server, select **Use System Proxy** by checking the respective check box.

   For more information, see *Configuring a System Proxy*.
5. In the **Location Proxy** section, you can define a proxy server through which the execution servers of this location will communicate with the application server.

6. In the **Host** field, type the name of the computer hosting the proxy service.
7. In the **Port** field, type the port number of the proxy host.
8. If the proxy server requires a username/password authentication, type the valid credentials in the **User** and **Password** fields.
9. The **Projects** section includes a list of existing projects. Check the **Assigned** check boxes of the projects that you want to assign to this location.
10. Click **OK** to add the new location.

Editing Locations

Describes how to edit a location.

To edit a location:

1. In the menu, click **Administration** > **Locations**.
2. Select the location that you want to modify and click  .

   The **Location Settings** page displays.
3. Modify the **Location Name** as required.
4. If you have specified the location of a proxy server, select **Use System Proxy** by checking the respective check box.

   For more information, see *Configuring a System Proxy*.
5. In the **Location Proxy** section, you can define a proxy server through which the execution servers of this location will communicate with the application server.
6. In the **Host** field, type the name of the computer hosting the proxy service.
7. In the **Port** field, type the port number of the proxy host.
8. If the proxy server requires a username/password authentication, type the valid credentials in the **User** and **Password** fields.
9. The **Projects** section includes a list of existing projects. Check the **Assigned** check boxes of the projects that you want to assign to this location.
10. Click **OK**.

Deleting Locations

Tip: Before you can delete a location, you must first remove all assigned execution servers from the location. For more information, see *Deleting Execution Servers*.

To delete a location:

1. In the menu, click **Administration** > **Locations**.
2. Select the location that you want to remove and click  . A confirmation dialog box displays, asking you to confirm the deletion.
3. Click **Yes** if you want to remove the location, or click **No** to abort the operation.

Location Settings Page

Administration > **Location** > **New Location**

Use the **Location Settings** page to configure locations.

Item	Description
Location Name	Specifies the name of the location as it should appear in the GUI and in reports.

Item	Description
Use system proxy	Enabling this setting will force all execution servers of this location to communicate with the application server through the defined system proxy. If this setting is not enabled, the application server will communicate directly with the execution servers, unless you define a location proxy. This check box is disabled if no system proxy is defined.
Location proxy	Use this area to define a proxy server through which the execution servers of this location will communicate with the application server. Leave the fields empty if you want the execution servers of this location to communicate directly with the application server, or if you checked the **Use system proxy** option. You can also define a system proxy and a location proxy, in which case the communication will be tunneled through both proxies. You may only define a location proxy that supports Secure Sockets Layer (SSL). All execution servers must use the SSL port of the proxy. For detailed information about execution server settings, see *Setting Up Execution Servers*.
Host	The name of the computer hosting the proxy service.
Port	The port number of the proxy host. Default is port 443.
User	If the proxy server requires a username/password authentication, enter a valid username.
Password	If the proxy server requires a username/password authentication, enter a valid password for the user specified in the **User** field.
Projects	Lists all existing projects. Check the check box next to a project to assign the project to the location. If no projects exist, you can assign them later after you have created them. For more information, see *Adding Projects*. Selected projects will have access to the execution servers at this location.
Select All	Checks the check boxes of all listed projects.
Deselect All	Un-checks the check boxes of all listed projects.

Setting Up Execution Servers

Performance Manager execution servers are responsible for executing monitors, for example Silk Test Classic and Silk Performer STM scripts. Silk Test Classic must be installed on the same computer on which a Performance Manager execution server is installed. Silk Performer STM components are installed with the Performance Manager execution server setup.

When executing Silk Performer STM scripts against multibyte applications or Web pages, review the *Multibyte Support* section in the *Silk Performer STM Help*.

For information regarding Silk Test Classic and Silk Performer STM, refer to the respective product documentation.

Execution Server Service

By default, the execution server will run as Windows system service. For Silk Test Classic, Citrix, and SAP test executions it is recommended to run the execution server as Windows process however. For detailed information, see *Starting the Performance Manager Execution Server as a Windows Process*.

Load Balancing of Execution Servers

Performance Manager uses a static approach to balance the load between execution servers within the same location. This approach implies that load balancing takes place only upon user operations, except when an execution server is no longer available and the failover system triggers. Whenever a monitor is scheduled to be moved to another execution server, the server with the lowest number of tasks is selected.

Server selection takes place whenever one of the following operations happens:

- Creating a new scheduled monitor
- Defining a schedule for a previously not scheduled monitor
- Adding a new location to a schedule
- Deactivating an execution server - monitors are shifted to remaining execution servers in the location
- Activating an execution server - the new server adopts monitors from existing execution servers
- Failover of an execution server - operates equally as deactivating a server

Activating or deactivating a project or monitor does not trigger a new server selection.

Editing Execution Servers

Tip: To prevent data inconsistency, you need to deactivate an execution server before you can edit it. For additional information, see *Activating or Deactivating Execution Servers*.

To edit an existing execution server:

1. On the **Administration** > **Locations** page, click the name of the location to which the execution server is assigned. A list of execution servers assigned to the selected location displays.
2. Click the name of the execution server you want to edit. The **Execution Server Settings** page displays.
3. In the **Execution server name** text box, change the name for the execution server as required.
4. Specify the name of the host or the IP-address and the port of the computer on which the execution server is installed.
5. Select **Use SSL** if you want the application server to connect to the execution server through Secure Sockets Layer (SSL).

   Tip: To connect to the execution server through a non-standard SSL port, see *Configuring a Non-Standard SSL Port for Execution Servers*.

   If you selected to use a proxy server for the location to which this execution server is assigned, **Use SSL** is automatically checked with **Port** 443.

   Note: Only port 443 works, and no other applications on this execution server may use port 443. Additionally, you must configure port 443 in the `SccExecServerBootConf.xml` file.

   For additional information, see *Configuring the SSL Port for a Location Proxy*.
6. Select a Usage for the execution server, specifying whether scheduling or alerting scripts are to be executed.

   For additional information, see *Execution Server Settings Page*.
7. Type a description for the execution server and set its status to active, then click **Check** to establish a test connection to the execution server.
8. If the test connection is successful, click **Save**. You are returned to the list of execution servers, with a confirmation message stating that the update was successful.

Adding Execution Servers

To add an execution server:

1. In the menu, click **Administration** > **Locations**.
2. Click the name of the location to which you want to add an execution server. A list of execution servers assigned to the selected location displays. If you are selecting a location for the first time, the list will be empty.
3. Click **New Execution Server**. The **Execution Server Settings** page displays.
4. In the **Execution server name** text box, define a name for the execution server.

5. Specify the name of the host or the IP-address and the port of the computer on which the execution server is installed.
6. Select **Use SSL** if you want the application server to connect to the execution server through Secure Sockets Layer (SSL).

   Tip: To connect to the execution server through a non-standard SSL port, see *Configuring Non-Standard SSL Port for Execution Server*.
7. If you selected to use a proxy server for the location to which this execution server is assigned, see *Configuring the SSL Port for a Location Proxy*.
8. Select a **Usage** for the execution server, specifying whether scheduling or alerting scripts are to be executed.

   For additional information, see *Execution Server Settings Page*.
9. Enter a description for the execution server and set its status to active, then click **Check** to establish a test connection to the execution server.
10. If the test connection is successful, click **Save**. You are returned to the updated list of execution servers, where the new execution server is listed.

Configuring the SSL Port for a Location Proxy

If you selected to use a proxy server for the location to which this execution server is assigned, **Use SSL** is automatically checked with **Port** `443`.

Note: Only port `443` works, and that no other applications on this execution server may use port 443. Additionally, you must configure port `443` in the `SccExecServerBootConf.xml` file.

To configure the SSL port for a location proxy:

1. Stop the execution server.

   For additional information, see *Starting or Stopping Individual Performance Manager Services*.
2. Open the `SccExecServerBootConf.xml` file with a text editor.

   This file is located in the `/conf/execserver` folder of the Performance Manager directory on the execution server.
3. Locate the `RmiProxy\TunnelingSSLPort` XML tag.
4. To enable SSL communication with the proxy, set the `<TunnelingSSLPort>0</TunnelingSSLPort>` tag to `443`.
5. Save the file and close the editor.
6. You need to restart the execution server to activate your changes.

   For additional information, see *Starting or Stopping Individual Performance Manager Services*.

Activating or Deactivating Execution Servers

1. In the menu, click **Administration** > **Locations**.
2. Select a location to access the list of defined execution servers for that location.
3. In the **Status** column of the execution server you want to activate or deactivate, click **Inactive**/**Active**.

   Important: Because the installation of an execution server requires administrative privileges, the automatic upgrade of an execution server fails if UAC is enabled. Disable UAC on all computers that host an execution server.

Deleting Execution Servers

Tip: To prevent data inconsistency, you need to deactivate an execution server before you can delete it. For additional information, see *Activating or Deactivating Execution Servers*.

Note: Deleting an execution server does not remove the actual software installation. Deletion simply disconnects the execution server. You can add a previously deleted execution server again.

1. In the menu, click **Administration** > **Locations**.
2. Select a location to access the list of defined execution servers for that location.
3. In the **Actions** column of the execution server you want to remove, click ✕.

Configuring a Non-Standard SSL Port for Execution Servers

The default SSL port through which the application server communicates with execution servers is `19125`.

Note: This procedure needs to be performed for each execution server that you want to connect to through a non-standard SSL port.

To configure a non-standard SSL port for an execution server:

1. Deactivate the execution server for which you want to configure a non-standard SSL port.
2. Stop the execution server.
3. Open the `SccExecServerBootConf.xml` file with a text editor.

   This file is located in the `/conf/execserver` folder of the Performance Manager directory on the execution server.
4. Locate the `<SSLPort>` XML tag. By default, the tag is set to `<19125>`.

   Set the value to the port number that you want to use for SSL communication.
5. Save and close the XML file.
6. In Performance Manager, set the SSL port of the execution server to the value that you have specified in the XML file.
7. Restart the execution server.
8. Reactivate the execution server.

Replacing the Security Certificate for Execution Server and Application Server Communication

The default communication between execution servers and the application server uses a default security certificate. You can set up your own security configuration for the communication between execution servers and the application server by replacing the default keystores with your own. The keystores contain the security certificates and keys to enable secure SSL communication between execution servers and the application server. For security reasons, both the keystore and the key passwords must be encrypted. The **SSL Password Encrypter** tool enables you to encrypt a custom password. The Performance Manager application server and execution servers need to use this encrypted password so that the communication with the custom keystore can be enabled.

Important: You need to be knowledgeable about how SSL communication works and how to create and configure keys and certificates.

Tip: For testing purposes we strongly recommend that you perform this task with a single execution server before updating all your execution servers. The cipher algorithm needs to be RSA and we recommend to use at least SHA256 for signatures.

1. Stop the application server and all execution server services.
2. Replace the default keystores with your own on the application server and all execution servers. The default location of the keystore files is `<Silk Performance Manager installation folder>\conf\execserver\SccExecServerKS` on the execution server and `<Silk Performance Manager installation folder>\conf\appserver\SccAppServerKS` on the application server.
3. Connect to the computer where Performance Manager is installed and select **Start** > **Programs** > **Silk** > **Silk Performance Manager 19.0** > **Tools** > **SSL Password Encrypter**. The **SSL Password Encrypter** dialog box opens.
4. Enter your custom keystore password in the **Keystore password** field, then click **Encrypt** to encrypt the password. Copy and save the encrypted password for later use.
5. Enter your custom key password in the **Keystore password** field, then click **Encrypt** to encrypt the password. Copy and save the encrypted password for later use.
6. Copy the encrypted passwords that you saved in the steps before and paste them into the `<KeyPassword>` tag and `<KeyStorePassword>` tag, respectively. These tags are located in the `SccExecServerBootConf.xml` and `SccAppServerBootConf.xml` files. This replacement needs to be done on all execution servers and on the application server.

   Important: The defined passwords for the execution servers and the application server must match, otherwise the servers are unable to communicate with each other. Non-matching passwords result in the application server not being able to connect to any execution servers, which means that the **Locations** list in Performance Manager would be empty.

Restart all execution servers and the application server when you are done.

Execution Server Settings Page

Administration > **Locations** > **<Location>** > **New/Edit Execution Server**

Use the **Execution Server Settings** page to configure execution servers within a location.

Item	Description
Execution server name	Defines a name for the execution server. This name will appear in all tables and result reports for executions from this specific computer. You can enter up to 100 characters.
Host or IP-address	Specifies the name of the host or the IP-address of the computer on which the execution server is installed. Some networks may only find the execution server if you specify the full name of the host, including the name of the domain, for example `MyHost.MyDomain`.
Port	Specifies the port of the computer defined in the **Host or IP-address** text box on which the execution server listens.
Use SSL	Check this check box if you want the application server to connect to the execution server through Secure Sockets Layer (SSL). If you selected to use a proxy server for the location to which this execution server is assigned, you must check **Use SSL** with port `443`.
Usage	Specifies which kind of scripts the execution server is able to execute.
Alerting	Select this option if you want the execution server to execute alerting Essential. Alerting execution servers should be on the same LAN as the application server. Alternately, it

Item	Description
	makes sense to configure an alerting execution server on the same computer on which the application server is installed.
Silk Performance Manager	Select **Silk Performance Manager** if you want the execution server to execute monitors. If you select this option, the following settings can be specified: **Client Side Monitoring (Business Transactions)** — Enables the execution server to execute client side monitors, like Silk Performer STM monitors and Silk Test monitors. **Server Side Monitoring (PDCE, IIOP, OCI, ...)** — Enables the execution server to execute server side (infrastructure) monitors, which monitor the state and health of systems. **Supports Silk Test Execution** — Enables the execution server to execute Silk Test monitors. Make sure that Silk Test is installed on the execution server.  **Important:** If **Supports Silk Test Execution** is selected, you must also select **Client Side Monitoring**. If you select this option, we recommend to enable the usage of Terminal Services/Remote Desktop Services sessions. **Use Terminal Services** — Enables the execution of Silk Test monitors in Terminal Services/Remote Desktop Services sessions, allowing parallel execution of multiple monitors on a single execution server. If this option is enabled, you need to specify the following settings: **Terminal Services Username** — Specifies a valid Terminal Services/Remote Desktop Services user. **Terminal Services Password** — Valid password for the specified Terminal Services/Remote Desktop Services user. **Terminal Services Max Number of Sessions** — Specifies the maximum amount of parallel Terminal Services/ Remote Desktop Services sessions running Silk Test monitors. **Terminal Services Connection Timeout (s)** — Time in seconds after which the monitor execution aborts if a Terminal Services/Remote Desktop Services connection was not successfully established.
Responsiveness timeout [s]	Enter a responsiveness timeout in seconds. The responsiveness timeout is the period of time after which the application server will time out if the execution server does not respond. After 2/3 of the time defined here, the administrator will be warned through email that the execution server is no longer available. For detailed information, see *Failover System*.
Max. bandwidth [KBit/s]	Enter the maximum bandwidth in KBit/s. If the network traffic of all scheduled test executions exceeds this number, the execution server will queue any additionally scheduled executions.
Description	A description of the execution server. You can enter any text for the description.
Status	Check this check box to activate the execution server. If you do not activate the execution server, it will not be available for monitor executions.
Check	Click this button to establish a test connection to the execution server. You will receive a message stating that the execution server has successfully been connected. If you receive

Item	Description
	an error message, ensure that your settings are correct, the network is configured properly, and that the required software is installed on the execution server you are setting up.

Failover System

The failover system is designed to shift monitors from one execution server to another and, if there has been a failure, for example a hardware damage, to deactivate a failed server. The system does not however shift or deactivate servers if the network at the location is slow or experiencing problems. To determine if a detected failure is due to a specific execution server or the server's local network, at least two execution servers must be run at each location within the same local area network. Otherwise, if only one server runs on a network, network outages and server hardware outages cannot be distinguished and therefore automatic server deactivation for failures cannot be enabled.

How quickly a failover system reacts to a failure is defined with the **Responsiveness timeout [s]** setting of the execution server.

The failover phases are as follows:

1. After 2/3 of the defined time, the administrator is warned through email that the execution server is unavailable.
2. If the server is still inaccessible after the full timeout has expired, failover analysis is initiated.
3. It is determined if the functioning servers can accept additional load. If they can handle additional load, monitors are shifted to other servers that provide the required resources, for example client/server, Silk Test support, and others. The failed server is then set to `Inactive` mode and is no longer used by monitors. Completed failover is indicated by an email to the administrator stating that the execution server is in the state of `Inaccessible`.
4. Once the previous step is complete, the system attempts to connect to the failed execution server every 30 seconds to add it back to the location. If this procedure is successful, the state of the server is set to `Active` and monitors will be deployed via load balancing again.

Managing Report Templates

Performance Manager offers a variety of pre-installed reports that let you quickly and easily transform data into presentation-quality information for analysis. The default reports can be customized with either Microsoft Excel or BIRT, an Eclipse-based, open source reporting tool for Web applications. You can also use these tools to create entirely new reports.

Performance Manager reports do not support bitmap (.bmp) image file format. For proper display, images must be in JPEG, GIF, or PNG format.

Managing Custom Report Templates with BIRT

Performance Manager is tightly integrated with Business Intelligence and Reporting Tools (BIRT) Report Designer to make it easy for you to generate reports for your monitoring data.

After downloading a copy of BIRT Report Designer, you can customize the core Performance Manager reports and add your own reports. For information about running and customizing reports, please refer to the application's Help.

For additional information on BIRT Report Designer, refer to BIRT Report Designer’s online help system. You can find further information, examples, and demonstrations for BIRT Report Designer at *http://www.eclipse.org/birt*. An active newsgroup (news.eclipse.org) is also available.

The software prerequisites to work with BIRT custom reports are:

- BIRT Report Designer
- Access to Performance Manager with administrator privileges

Note: Performance Manager reports do not support bitmap (.bmp) image file format. For proper display, images must be in JPEG, GIF, or PNG format.

Installing BIRT from Performance Manager

This procedure explains how to install BIRT Report Designer from your Performance Manager installation. By installing BIRT this way, all necessary configurations for Performance Manager are done automatically.

To install BIRT from Performance Manager:

1. Ensure that your system uses a 64bit Java Development Kit (JDK) or Java Runtime Environment (JRE). The BIRT Report Designer will not work on a system that uses a 32bit JDK or JRE.
2. Navigate to **Help** > **Tools** .
3. Click the **BIRT RCP Report Designer** link.
4. After downloading the compressed installer package to your local system, extract the compressed files to a directory on your system, for example `C:\BIRT`.

   Note: If you encounter an error when extracting the installer files using Windows compressed folder functionality, use an extraction tool instead, for example WinZip or WinRAR, to extract the files.
5. Start `BIRT.exe` from the directory you extracted the files to.

Configuring BIRT for Performance Manager

If BIRT is already installed on your computer, or you are installing BIRT from another location, for example from the Eclipse homepage, you need to configure BIRT for use with Performance Manager after the installation. If you have installed BIRT from Performance Manager as described in *Installing BIRT from Performance Manager*, you do not need to perform the steps outlined in this procedure.

To configure BIRT RCP Designer for use with Performance Manager:

1. Copy the `jtds-1.2.jar` file, available in the `\lib` directory of your Performance Manager front-end server installation folder, to the `plugins \org.eclipse.birt.report.data.oda.jdbc_<version>\drivers` directory of your BIRT installation.

   This will allow JDBC access to your Performance Manager installation.
2. In the BIRT Report Designer, select the **Windows** > **Preferences** menu, then select **Report Design** > **Classpath** in the menu tree. Add the `scc.jar` file, available in the `\lib` directory of your Performance Manager front-end server installation folder, to the classpath by clicking **Add External JARs**.
3. Create a directory to store the reports you intend to create, for example `C:\MyBirtReports`. Create a subdirectory called `conf` within the newly created directory.
4. Within the `conf` directory, create a directory called `birt`. You should now have a directory structure that resembles the following: `C:\MyBirtReports\conf\birt`.
5. Copy the file `library.rptlibrary`, available in the `\conf\Birt` directory of your Performance Manager front-end server installation folder, to the `\conf\birt` directory that you created in the previous step.
6. Launch BIRT by executing the `BIRT.exe` file, located in the local directory where you extracted the application's compressed files.
7. From within BIRT RCP Designer, select **Preferences** from the **Window** menu.
8. In the **Preferences** window, select **Report Design** > **Resource** in the directory tree in the left-hand pane.
9. In the **Resource folder** text box, enter the directory that you created.

For example `C:\MyBirtReports\conf\birt`.

10. Click **Apply**, then click **OK**.

Establishing Database Access For a New Report Template

Before you can create a new report template with BIRT Report Designer, you need to establish database access to the Performance Manager repository you want to query.

To establish database access for a new report template:

1. From within BIRT Report Designer, select the menu **File** > **New** > **New Report** .
2. Follow the steps in the **New Report** wizard.
3. Open the **Resource Explorer**.
4. In the **Resource Explorer**, click **Shared Resources** > **conf** > **birt** > **library.rptlibrary** > **Data Sources** > **Data Source** and drag the required data source into your report's `Data Sources` directory, which is located in the **Outline** window.
5. In the **Resource Explorer**, click **Shared Resources** > **conf** > **birt** > **library.rptlibrary** > **Report Parameters** and drag the four report parameters `sourceUser`, `sourcePassword`, `sourceURL`, and `sourceDriver` into your report's `Report Parameters` directory, which is located in the **Outline** window.
6. Double-click the newly imported data source to open the **Edit Data Source** dialog box.
7. Type a valid **Driver Class** and **Database URL**.

   For additional information, see **BIRT Data Source Settings** topic.
8. Click **Test Connection** to test your settings. If the database connection has been established, you can proceed with designing your new report template.
9. Click **OK**.

BIRT Data Source Settings

Use the BIRT **New JDBC Data Source Profile** dialog box to establish database access to an existing Performance Manager repository. To access the **New JDBC Data Source Profile** dialog box, right-click **Data Sources** in the **Outline** pane, click **New Data Source**, select **JDBC Data Source**, and click **Next >**.

To connect to a MS SQL Server or a MS SQL Server Express database, use the following credentials:

Item	String	
Driver Class	`net.sourceforge.jtds.jdbc.Driver`	
Driver URL	**MS SQL Server**	`jdbc:jtds:sqlserver://<HOST>:<PORT>/<DATABASE>`
	MS SQL Server Express	`jdbc:jtds:sqlserver://<HOST>:<PORT>/<DATABASE>;instance=<INSTANCENAME>`
	HOST	Host name or IP-address of the computer hosting the database server.
	PORT	Port number of the database management system. Default is 1433.
	DATABASE	The name of the database.
	INSTANCENAME	Only for MS SQL Server Express. Instance name of the database instance. The default MS SQL Server Express instance is `localhost\SQLExpress`.

Adapting Existing Report Templates

Performance Manager allows you to download and adapt BIRT report templates that contain all the information you need to create custom report templates for use with Performance Manager modules.

Note: Performance Manager reports do not support bitmap (.bmp) image file format. For proper display, images must be in JPEG, GIF, or PNG format.

To create a report based on a Performance Manager template:

1. In the menu, click **Administration** > **Reports** .
2. Click in the **Actions** column.
3. Save the template file `<filename>.rptdesign` to your local system.
4. Open the downloaded template file in BIRT Report Designer.
5. Redesign the report as necessary.

   For instructions on report design, refer to BIRT Report Designer's online help system.
6. To preview your report, choose **View Report** > **As HTML** from the **Run** menu.

   The browser in which you want to preview the report can be specified as follows:

   - Click **Window** > **Preferences** > **Web Browser**, select **Use external web browser** and choose a browser.
   - Click **Window** > **Preferences** > **Report Design** > **Preview** and check the **Always use external browsers** check box.
7. If you preview the report for the first time, the **Enter Parameters** dialog box opens, where you need to specify a valid session ID. To generate a session ID, execute the following URL in a web browser.

   `http://<HOST>:<PORT>/services/sccsystem?method=logonUser&userName=<USERNAME>&plainPasswd=<PASSWORD>`.

Parameter	Description
HOST	Host name or IP-address of the computer hosting Performance Manager.
PORT	Port number of the Performance Manager front-end server. Default is `19120` if you access Performance Manager through a standalone Web server, and `80` if you access Performance Manager through IIS.
USERNAME/ PASSWORD	Valid credentials of a Performance Manager user.

   Note: The order of the valid credentials USERNAME and PASSWORD is very important.
8. If at some point your edited report does not return any data, the likely cause is that the session ID has timed out (timeout is 10 minutes). Close the browser window and choose **View Report** > **As HTML** from the **Run** menu again. To generate a new session ID, repeat the previous step.

Editing Report Template Properties

Once you have created a new custom report template using BIRT Report Designer or Excel and uploaded it to Performance Manager, you can edit the template's properties like its name, description, or for which modules the template can be used.

1. In the menu, click **Administration** > **Reports** .
2. Click the name of the report template for which you would like to edit or set permissions and associations. The **Edit Report Template** dialog box displays.
3. Use the **Name**, **File name** and **Description** fields to edit the template properties.

4. You can change a report's permission settings by modifying the selections in the **Projects** and **Modules** list boxes. This will determine which users have access to the selected report template.
5. Once you are done editing, click **OK** to save your changes to the report template.

   The edits you have made are applied immediately. Users will see changes the next time they access or refresh the report list.

Downloading Report Templates

The report template of the selected report, including the layout, is downloaded. Downloading Performance Manager report templates to your local system enables you to edit them. After you download and edit a report, you can upload it to make it available to other users. For more information, see *Uploading Report Templates*.

To download a Performance Manager report template:

1. In the menu, click **Administration** > **Reports** .
2. Click the **Report Templates** tab. The **Report Templates** page displays, listing all of the report templates that have been uploaded.
3. Click in the **Action** column of the report you want to download. The **File Download** dialog box displays.
4. Click **Save** and download the report file to your local system, depending on the report type that you are downloading.
5. Now edit the report based on your needs using either BIRT Report Designer for `rptdesign` files, or Excel for `xls/xlsx` files.

Uploading Report Templates

Uploading Performance Manager report templates makes them available for others to use. You may want to upload a report template after you have edited it with BIRT Report Designer or Microsoft Excel. You can only run a report if you have access to the project and module to which the report is associated.

Tip: Templates must be configured with additional information so that they can be identified once they are uploaded to Performance Manager.

Note: Performance Manager reports do not support bitmap (.bmp) image file format. For proper display, images must be in JPEG, GIF, or PNG format.

To upload a customized template as a new report:

1. In the menu, click **Administration** > **Reports** .
2. Click **Upload** at the bottom of the page. The **Upload Report Template** dialog box displays.
3. Type a **Name** for the report.
4. *Optional:* Type a **Description** of the report.
5. From the **Projects** list box, select the projects with which the report is to be associated.

   Hold down the **Ctrl** key to select multiple projects.
6. From the **Modules** list box, select the modules with which the report is to be associated.

   Hold down the **Ctrl** key to select multiple modules.
7. Click **Browse** next to the **File** field.
8. Browse to and select the template file that is to serve as the basis for the report template.

   The file you select must have the `rptdesign` or `xls` file extension.
9. Click **OK** to upload the report template for use in Performance Manager.

Updating Report Sources

Updating an existing Performance Manager report template allows you to move a report you have customized with BIRT Report Designer or Microsoft Excel into Performance Manager and make it available to other users.

Caution: Report templates that ship with Performance Manager are automatically patched when you upgrade to a new version. It is therefore important that you save your customized report templates in a dedicated custom folder, or that you upload customized report templates as new templates. For more information, see **Uploading Report Templates**.

To update a report template with a modified template file:

1. In the menu, click **Administration** > **Reports** .
2. Click in the **Action** column of the report you want to update.
3. Click **Browse** on the **Update Report Template** dialog box to browse to and select the template file that is to overwrite the existing template file.

   The file you select must have the `rptdesign` or `xls` file extension.
4. Click **OK** to upload the file, and thereby overwrite the file that the report template was previously based on.

Deleting Report Templates

You can remove a Performance Manager report from the list of available reports.

To delete a Performance Manager report:

1. In the menu, click **Administration** > **Reports** .
2. Click in the **Action** column of the report you want to remove. A confirmation dialog box displays.
3. Click **Yes** to remove the report from the list.

Report Templates Page

Administration > **Reports** > **Report Templates**

Use the **Report Templates** page to manage the report templates which you want to make available to Performance Manager for reporting.

Click **Upload** to upload a new report template from your hard disk or a UNC to Performance Manager.

For each listed report, the page displays the following columns:

Column	Description
Title	The name of the report template as it displays in the application's GUI.
File Name	The physical file name of the report template.
Uploaded On	Date when the report template was uploaded to Performance Manager.
Uploaded By	The user who uploaded the report template to Performance Manager.
Project	The project to which the report template is associated. Only the specified project can use that template for reporting purposes. If a template is assigned to *All Projects*, then any project can use it.
Module	The Performance Manager application which may access the reporting template. If a template is assigned to no module, then any application can use it.

Column	Description	
Actions	This column contains action icons which allow the user to perform the following actions on a report template:	
	Update	Replaces the currently uploaded template with a new one.
	Download	Downloads the template to your local computer.
	Delete	Deletes the template permanently.

Audit Log

Administration > **Reports** > **Audit Log**

The audit log allows administrators to view all recorded Performance Manager user activity. The log file stores all login and logout information, as well as all changes to the Performance Manager database, for example projects, monitors, and schedules.

To be able to view audit logs, ensure you have the **View audit logs** permission.

You can manage the listed log entries to suit your information needs by using the available features.

Sorting Data by Column

Clicking a column header sorts all listed data by that column. Clicking the same column header multiple times toggles the sort order between ascending and descending.

Selecting a Range From the Calendar

Click the displayed time range to expand the calendar. The **From** and **To** rows of the calendar allow you to specify start and end times for the period of time for which you want to view data. After specifying **From** and **To** times with the list boxes, click **Update** to update the audit log based on the new time range.

The **day**, **week**, **month**, **quarter**, **[last 7 days]**, **[last 31 days]** links allow you to bypass the calendar and instead view information for set time periods.

You can also use the **Forward** and **Backward** arrows to increase and decrease the selected time range by the following intervals:

- one day
- one week
- one month
- one quarter

Use and for increasing and decreasing the range of time covered by the audit log. Clicking one time enlarges the period of time by 50%. Clicking one time reduces the period of time by 50%.

When the calendar displays a custom interval, for example after zooming in or out, you can use the left-most arrows, **Earlier** and **Later**, to move the selected period of time forward or backward in time by half of the selected interval.

Tip: After specifying a new time period, click **Update** to update the report.

Filtering Data

Filter options enable you to better target the audit log information you want to analyze.

You can filter listed data by:

Login	Displays the actions of a specified user login.
Object	Displays actions taken on a specified database item, for example project or location.
Operation	Displays selected operations, for example login, logoff, create, or delete.

Accessing and Viewing the Audit Log

To view the audit log:

1. Ensure that you have the **View audit logs** permission.
2. In the menu, click **Administration** > **Log Files**.
3. Click the **Audit Log** tab.
4. Select a calendar range to limit the listed log entries.
5. Use the filter options to better target the audit log information you want to analyze.

Audit Log Page

Administration > **Reports** > **Audit Log**

Use the **Audit Log** page to view all recorded Performance Manager user activity.

To be able to view audit logs, ensure you have the **View audit logs** permission.

Item	Description
Calendar area	Select a calendar range to limit the listed log entries.
Filter area	Use the filter options to better target the audit log information you want to analyze. Click **Update** to refresh the list according to your filter settings.
Result area	This section displays the logged information. Use the page numbers to move between pages. Click the column headers to sort by the defined column.

For detailed information about the calendar and filtering options, see *Audit Log*.

Server Log Files

The front-end server, the application server, and the execution server write log files. These files provide valuable information for error analysis. Performance Manager allows administrators to view, search, and download these files directly from its Web interface.

Downloading Server Log Files

You can download a server log file to your local computer in CSV format to allow for further data analysis, for example in Microsoft Excel.

To download a server log file:

1. In the menu, click **Administration** > **Reports**.
2. Click the tab of the server to which the log file belongs.
   - **Front-end Server Log**
   - **Application Server Log**
   - **Execution Server Log**

A list of log files is displayed in chronological order. Log file names are made up of server component name and a suffix with a timestamp. The current log files are named `FrontendServer.log`, `AppServer.log`, and `ExecServer.log`.

Note: To locate an execution server log file, navigate to the respective execution server through its location.

3. In the **Actions** column of the log file, click .

   Alternative: To view the contents of the log file before downloading it, click the name of the log file you want to download. The selected log file displays, along with chronologically sorted log entries. Click **Download as CSV** at the bottom of the page.
4. To view the data in a spreadsheet program, select **Open** on the subsequent dialog box. To save the data on your hard drive, select **Save** on the subsequent dialog box.

Analyzing Server Log Files

To analyze a server log file:

1. In the menu, click **Administration** > **Reports**.
2. Click the tab of the server to which the log file belongs.

   - **Front-end Server Log**
   - **Application Server Log**
   - **Execution Server Log**

   A list of log files is displayed in chronological order. Log file names are made up of server component name and a suffix with a timestamp. The current log files are named `FrontendServer.log`, `AppServer.log`, and `ExecServer.log`.

   Note: To locate an execution server log file, navigate to the respective execution server through its location.
3. Click the name of the log file you want to view. The selected log file is displayed, along with chronologically sorted log entries.
4. Filter options allow you to page recorded log information.

   You can filter listed data by:

   Severity Displays events of a selected severity.

   Log level Displays events that match a selected log level. More detailed log information can only be displayed when the log level is set accordingly on the server. For more information about configuring a server's log level, see *Changing Log Levels of the Performance Manager Servers*.

   Module Displays log information for a selected module. Log entries can only be displayed when the respective products (modules) are installed and connected to the front-end server that is being accessed.

Deleting Server Log Files

Caution: Deleting a log file permanently removes the file from the server. You will not be able to view log data from the deleted file anymore.

To delete a server log file:

1. In the menu, click **Administration** > **Reports**.
2. Click the tab of the server to which the log file belongs.

   - **Front-end Server Log**

- **Application Server Log**
- **Execution Server Log**

A list of log files is displayed in chronological order. Log file names are made up of server component name and a suffix with a timestamp. The current log files are named `FrontendServer.log`, `AppServer.log`, and `ExecServer.log`.

Note: To locate an execution server log file, navigate to the respective execution server through its location.

3. In the **Actions** column of the log file you want to delete, click ✕. A confirmation dialog box displays.
4. Click **No** to avoid deleting the log file; or click **Yes** to remove the log file from the list.

   If you choose **Yes**, the list of log files redisplays, with the deleted log file no longer listed.

Log File Management

Each of the Performance Manager servers writes its activities to log files. For more information about Performance Manager servers, see *Architecture*. When application errors or system failures occur, these log files provide valuable information regarding the root causes of problems. You can customize the level of detail that is written to server log files and the log file retention period.

The log files for the Performance Manager servers are accessible through **Administration** > **Reports**.

Changing Log Levels of the Performance Manager Servers

The following servers generate log files:

- Front-end server
- Application server (including logs for rules and incidents)
- Execution server

To change the log level of a Performance Manager server:

1. Stop the server for which you want to change the log level.
2. Open the appropriate file with a text editor, depending on the server or component for which you want to change the log level:

Front-end server	`SccFrontendBootConf.xml`, located in the `/conf/frontendserver` folder of the Performance Manager directory on the front-end server.
Application server, rules and incidents	`SccAppServerBootConf.xml`, located in the `/conf/appserver` folder of the Performance Manager directory on the application server.
Execution server	`SccExecServerBootConf.xml`, located in the `/conf/execserver` folder of the Performance Manager directory on the execution server(s).

3. Locate the `<LogLevel>` XML tag in the `<Log>` section of the file. For the application server log file, locate the `<LogLevel>` XML tag in the `<AppLog>` section of the file, and for the rules and condition log files in the `<RuleLog>` section.
4. Set the value to the log level at which you want the server to write information. The following log levels are available:

Value	Log level	Description
0	Overview	The server writes only the most important information to the log files. This is the default setting.
1	Detailed	The server writes additional information to the log files: **Front-end server** Connection- and event-dispatcher information.

Value	Log level	Description	
		Application server	Result-writer and result-fetcher activities.Additionally, the rule log file includes rule evaluation and incident information.
		Execution server	Transaction-execution activities.
2	Verbose	The server writes additional information to the log files:	
		Front-end server	User administration information, for example cookie management.
		Application server	Detailed result-writer and result-fetcher information.Additionally, the rule log file includes detailed rule evaluation and incident information.
		Execution server	Detailed transaction-execution and bandwidth information.
3	Debug	This is the most detailed log level and should only be used for debugging severe issues.	

5. Save and close the XML file, then restart the server.

Changing Log File Retention Periods

Retention periods can be configured to specify how long log information is stored. After the defined period, log files that exceed the retention period can either be moved to an archive location or be deleted automatically. File retention can also be configured based on total file size, so that the oldest files are either deleted or moved to an archive location until the total size of all log files is lower than a specified limit. The log files are checked/moved/deleted every full hour.

1. Open the appropriate file with a text editor, depending on the server or component for which you want to change the log file retention period:

Front-end server	`SccFrontendBootConf.xml`, located in the `/conf/frontendserver` folder of the Performance Manager directory on the front-end server.
Application server, rules and incidents	`SccAppServerBootConf.xml`, located in the `/conf/appserver` folder of the Performance Manager directory on the application server.
Execution server	`SccExecServerBootConf.xml`, located in the `/conf/execserver` folder of the Performance Manager directory on the execution server(s).
Chart server	`SccChartServerBootConf.xml`, located in the `/conf/chartserver` folder of the Performance Manager directory on the chart server(s).

2. Locate the `Log` XML tag. For the application server log file, locate the `<AppLog>` XML tag, and for the rules and condition log files the `<RuleLog>` tag.
3. The following general log file settings can be configured:

XML tag	Description
`<SystemLog>`	Name of the log file, for example `AppServer.log`.
`<LogPath>`	Folder path where the log files are written to. This can be a relative or absolute path.
`<LogLevel>`	Level of detail of the information that is logged. For more information, see *Changing Log Levels of the Servers* .
`<LogSize>`	Size in bytes after which a new log file is created. The minimum configurable size is 512000 byte. If you enter a smaller value, the value is ignored.

4. The following log retention settings can be configured:

XML tag	Description
`<MaxAge>`	Time in days after which log files are either moved or deleted. Enter `0` to disable this setting.
`<MaxTotalSize>`	Total size in megabytes of the log file after which the oldest files are either moved or deleted. Enter `0` to disable this setting.
`<Compress>`	`True` to compress log files before moving them to the archive, `False` to move them as they are.
`<ArchiveLocation>`	Local or remote path where archived files are to be stored. If empty, log files are being deleted instead of moved after they exceed the specified age or total size.

5. Save and close the XML file.

Example

```
  <AppLog>
    <SystemLog>AppServer.log</SystemLog>
    <LogPath>applog</LogPath>
    <LogLevel>3</LogLevel>
    <LogSize>512000</LogSize>
    <JdbcLogConf>conf/AppServer/JdbcLoggingConf.xml</
JdbcLogConf>
    <Archive>
      <MaxAge>2</MaxAge>
      <MaxTotalSize>512</MaxTotalSize>
      <Compress>True</Compress>
      <ArchiveLocation>D:\temp\logArchiver\appserver\</
ArchiveLocation>
    </Archive>
  </AppLog>
```

Front-End Server Log Page

Administration > **Reports** > **Front-end Server Log**

Use this page to view logging information from the Performance Manager front-end server service.

For each log file, the page displays the following columns:

Column	Description
Actions	Click the buttons and to **Delete** or **Download** log files.
Name	The name of the log file.
Size	The physical size of the log file.
Date	Date when the log file was last physically saved.

Administration > **Reports** > **Front-end Server Log** > **Front-end server log file name** .

When clicking on the name of a log file, the logging details list displays. The list includes the following items:

Item	Description	
Filter area	Use the filter options to filter the log list information by `severity`, `log level`, and `module`. Click **Update** to refresh the list according to your filter settings.	
Table area	Displays the following logging information:	
	Severity	Severity of the event: • Info • Warning • Error
	Log Level	Log level of the event: • `OV` = Overview • `DT` = Detailed • `VB` = Verbose • `DB` = Debug

Click **Back** to return to the **Front-end Server Log** page. Click **Download as CSV** to download the log file as a CSV file to your local computer.

Application Server Log Page

Administration > **Reports** > **Application Server Log**

Use this page to view logging information from the Performance Manager application server service.

For each log file, the page displays the following columns:

Column	Description
Actions	Click the buttons  and  to **Delete** or **Download** log files.
Name	The name of the log file.
Size	The physical size of the log file.
Date	Date when the log file was last physically saved.

Administration > **Reports** > **Application Server Log** > **Application server log file name** .

When clicking on the name of a log file, the logging details list displays. The list includes the following items:

Item	Description	
Filter area	Use the filter options to filter the log list information by `severity`, `log level`, and `module`. Click **Update** to refresh the list according to your filter settings.	
Table area	Displays the following logging information:	
	Severity	Severity of the event: • Info • Warning • Error
	Log Level	Log level of the event:

Item	Description
	• OV = Overview • DT = Detailed • VB = Verbose • DB = Debug

Click **Back** to return to the **Application Server Log** page. Click **Download as CSV** to download the log file as a CSV file to your local computer.

Execution Server Log Page

Administration > **Reports** > **Execution Server Log**

Use this page to view logging information from the Performance Manager execution server service.

For each location, the page displays the following columns:

Column	Description
Location	Displays all available locations.
Execution Servers	Displays the amount of execution servers per location.
Status	Displays a summary status of the execution servers in the location.

Administration > **Reports** > **Execution Server Log** > **Location name**

When clicking on the name of a location, the list of execution servers in the selected location displays. The list displays the following columns for each execution server.

Column	Description
Execution Server Name	The name of the execution server.
Host	The name of the computer hosting the execution server.
Type	The Performance Manager application that the execution server is configured for. For Performance Manager, the type is always *Performance Manager*.
Assigned Tasks	The amount of tasks that are currently scheduled on the execution server.
Status	The status of the execution server. `Active` or `Inactive`.

Click **Back** to return to the list of locations.

Administration > **Reports** > **Execution Server Log** > **Location name** > **Execution server name**

When clicking on the name of an execution server, the list of log files for the selected execution server displays. For each log file, the page displays the following columns:

Column	Description
Actions	Click the buttons  and  to **Delete** or **Download** log files.
Name	The name of the log file.
Size	The physical size of the log file.
Date	Date when the log file was last physically saved.

Click **Back** to return to the list of execution servers.

Administration > **Reports** > **Execution Server Log** > **Location name** > **Execution server name** > **Execution server log file name**

When clicking on the name of a log file, the logging details list displays. The list includes the following items:

Item	Description	
Filter area	Use the filter options to filter the log list information by `severity`, `log level`, and `module`. Click **Update** to refresh the list according to your filter settings.	
Table area	Displays the following logging information:	
	Severity	Severity of the event: • Info • Warning • Error
	Log Level	Log level of the event: • `OV` = Overview • `DT` = Detailed • `VB` = Verbose • `DB` = Debug

Click **Back** to return to the **Execution Server Log** page. Click **Download as CSV** to download the log file as a CSV file to your local computer.

System Health

The **System Health** page provides a compact overview of the current Performance Manager system load status, displaying the overall measure writing performance and the data load per project.

A measure is a value that is generated by a specific monitor execution in a location, for example the `PageTime of monitor XY on location ABC = 1` measure.

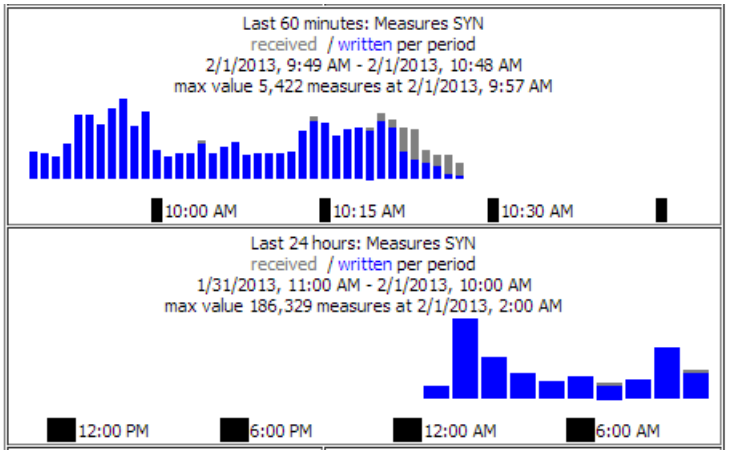
System Health Page

Administration > **System Health**

Use the **System Health** page to view the current health status of your Performance Manager system.

Note: To download the information on this page in XML-file format, click **Download**. This is especially useful when requesting assistance from customer support.

The **System Health** section displays the following information:

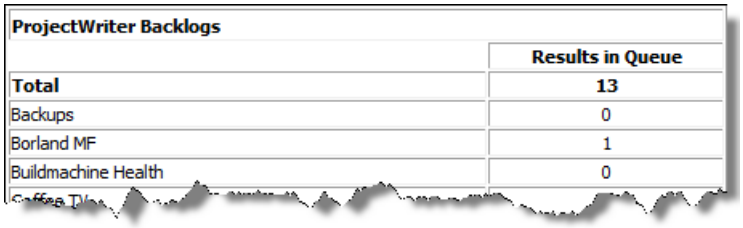


Item	Description
MeasureCache size	Number of measures per monitor/location combination that are currently cached in the system's RAM. The displayed hit ratio should eventually reach 100%. If the hit ratio goes down or never reaches 100%, this is an indicator that Performance Manager's caching system does not work as expected. Requesting assistance from customer support is recommended in such a case.
MeasureCache measSize	Number of records for raw data that are sent to the database in an SQL batch job.
MeasureCache lastSize	Number of records for aggregated data that are sent to the database in an SQL batch job.
HealthCache size	Number of project-wide measures that are currently cached in the system's RAM. The displayed hit ratio should eventually reach 100%. If the hit ratio goes down or never reaches 100%, this is an indicator that Performance Manager's caching system does not work as expected. Requesting assistance from customer support is recommended in such a case.
MeasureCount SYN	Number of measures that are generated by the system per hour from synthetic monitors. `active monitors` x `measures per monitor` x `active locations` x `monitor runs` where `monitor runs` = scheduled executions per hour.
MeasureWriteTime (limit)	The maximum time that the system may use to write one measure to the database, based on calculated estimates. See **Measures received / written per period** for actual numbers.
MeasureWriteTime (avg)	The average time that the system actually uses to write one measure to the database. If this value is higher than **MeasureWriteTime (limit)**, the system is overloaded. See also *Customizing the Displayed Information on the System Health Page*.
Measures received / written per period	The **Measures received / written per period** graph displays the amount of measures that the application

Item	Description
	server has received from all execution servers in a specific period of time. The upper graph displays the numbers for each minute over the last 60 minutes, the lower graph the numbers for each hour over the last 24 hours. Received measures are displayed as gray bars, which should ideally turn to blue bars (written measures) at the end of a period, as all received measures have been written to the database. If you see a stacked bar (blue / gray), this indicates that the system was not able to write the full amount of received measures to the database in the specific period. System overload? Stacked bars (blue / gray), which indicate that the system was not able to write the full amount of received measures to the database in a specific period, do not necessarily mean that your system is not able to handle the load anymore -- it is possible that during certain background activities (for example database backup, index rebuilds, or data deletion jobs), the system may be overloaded for some time, while it may very well be able to recover again after such activities have been completed. Examine the trend in the chart to interpret the load on your system: If gray bars eventually turn blue, this means that the system was able to catch up again. However if the frequency and duration of gray bars increases over time or if you observe a constant overload (gray bars), you may want to reduce the volume of measures being written. Ultimately these only become a concern if the total backlog continues to grow. This graph is intended to give you an early warning of how much and how frequently you have input exceeding output so you can address it before measure volumes become unmanageable. There are several suggested ways to reduce the volume of measures including: **1.** Reduce the number of active monitors. **2.** Increase the scheduled time between monitor runs. **3.** By default, script recordings will create several measures for each individual web page accessed in a script in addition to the overall transaction time. If you don't need the multiple measures for each web page in a script (e.g. measures for total end to end, server busy, document upload, ...), replace the name of the web page measure in the script's function calls with an empty string " ". **4.** Replace one or more page timer measure names commented out as above, if desired with a custom timer which results in only one measure. **5.** Reduce the number of locations running a monitor to only those necessary.  **Note:** The amount of written measures is usually slightly higher than the amount of received measures, as application server-specific

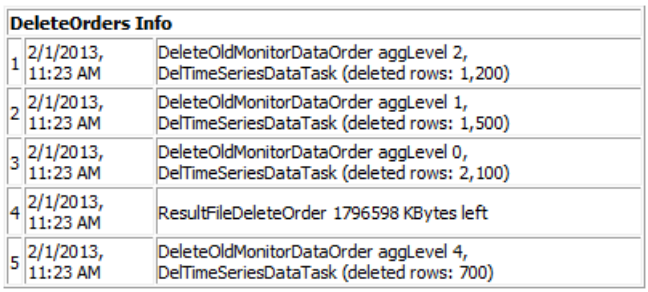
Item	Description
	measures (for example overall health and performance) are counted towards the amount of written measures, however they are not calculated as received measures as they do not come from the execution servers.

The **ProjectWriter Backlogs** section displays the number of results in the queue, displayed for each project. These are measures that are delivered by the execution server, but are not yet saved to the database.



ProjectWriter Backlogs	
	Results in Queue
Total	**13**
Backups	0
Borland MF	1
Buildmachine Health	0

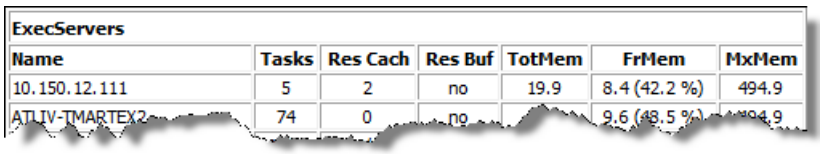
The **DeleteOrders Info** section is only visible if data storage reduction processes are currently running. It displays the running `DataDelete` jobs, where each `DataDelete` job actually creates a job per project plus an additional job for the result files.



DeleteOrders Info		
1	2/1/2013, 11:23 AM	DeleteOldMonitorDataOrder aggLevel 2, DelTimeSeriesDataTask (deleted rows: 1,200)
2	2/1/2013, 11:23 AM	DeleteOldMonitorDataOrder aggLevel 1, DelTimeSeriesDataTask (deleted rows: 1,500)
3	2/1/2013, 11:23 AM	DeleteOldMonitorDataOrder aggLevel 0, DelTimeSeriesDataTask (deleted rows: 2,100)
4	2/1/2013, 11:23 AM	ResultFileDeleteOrder 1796598 KBytes left
5	2/1/2013, 11:23 AM	DeleteOldMonitorDataOrder aggLevel 4, DelTimeSeriesDataTask (deleted rows: 700)

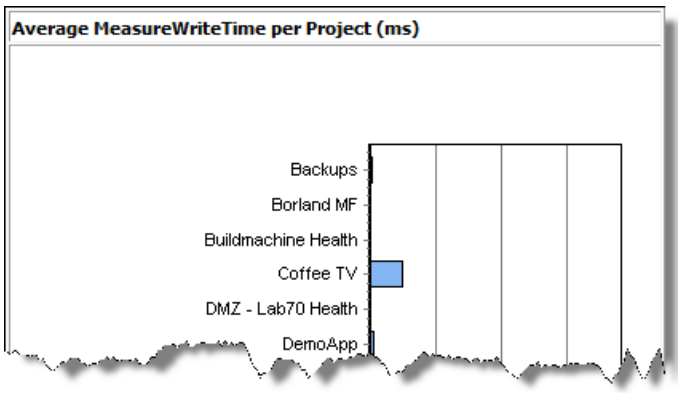
The **ExecServers** section (see *Customizing the Displayed Information on the System Health Page*) displays all execution servers and certain statistical information for each of them:

- Tasks: Amount of monitors scheduled on the execution server.
- Res Cach: Amount of results that have not yet been received by the application server. This value should ideally be zero.
- Res Buf: Displays whether persistent result data is enabled or not on the execution server.
- TotMem: Java heap size that is currently allocated.
- FrMem: Java heap size that is still available.
- MxMem: Maximum Java heap size.



ExecServers						
Name	**Tasks**	**Res Cach**	**Res Buf**	**TotMem**	**FrMem**	**MxMem**
10.150.12.111	5	2	no	19.9	8.4 (42.2 %)	494.9
ATLIV-TMARTEX2	74	0	no		9.6 (48.5 %)	494.9

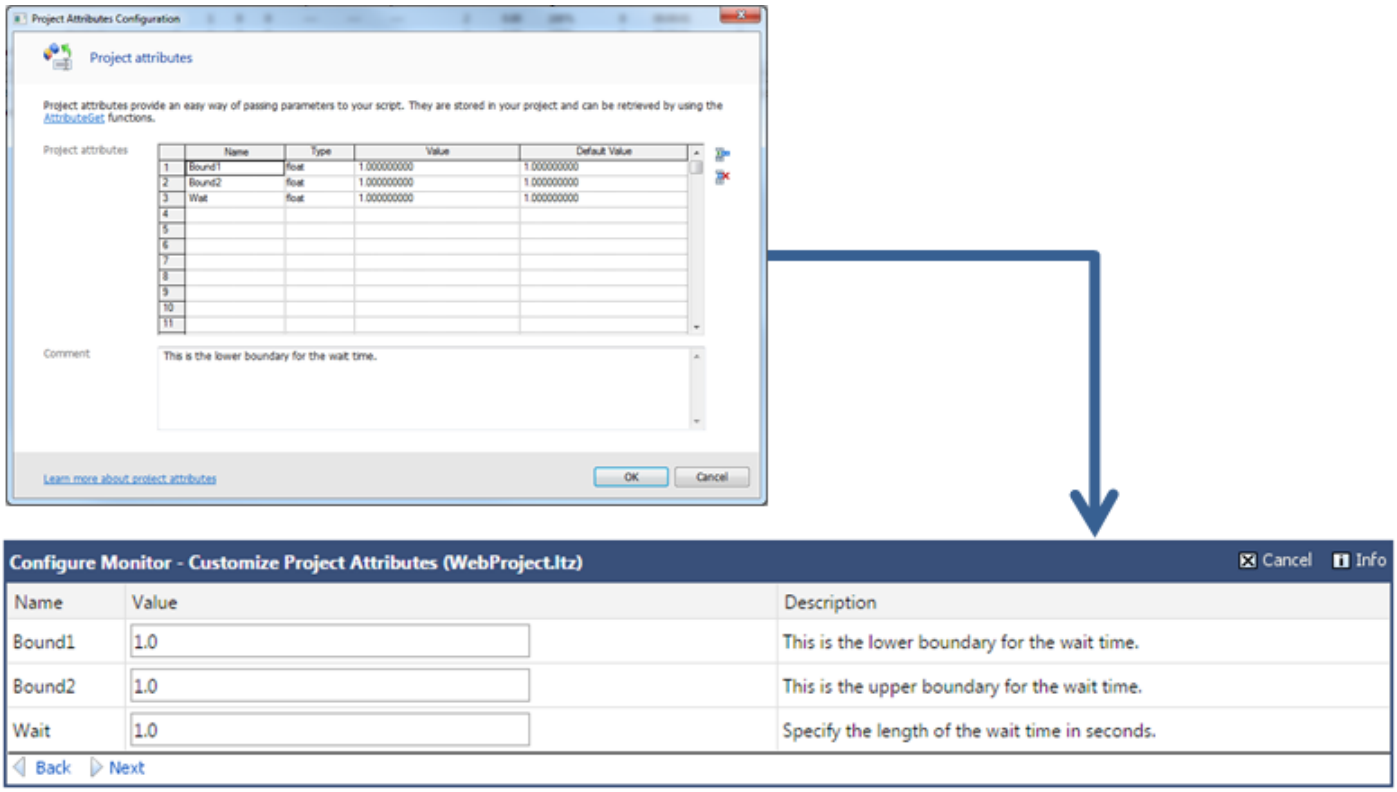
The **Average MeasureWriteTime per Project (ms)** section displays the average time that the system actually uses to write one measure to the database, for each project.



Essentials

Silk Performer Monitor Workbench (Silk Performer) provides a GUI that allows for the specification of name-value pairs that enable the testing of script parameterization. Such scripts can be uploaded directly to applications such as Performance Manager to instantiate new business transaction monitors. This capability provides immediate use of script parameterization and lets users reuse uploaded projects with different input values.

Silk Performer projects can be uploaded to Performance Manager and saved as Essential. Such projects become available as business transaction monitors for all Performance Manager projects — and Silk Performer project attributes act as customizable variables.



With the functionality of Silk Performer — and the ability to reuse, customize, and integrate projects with Performance Manager — Essentials offer a wide range of possibilities, allowing you to:

- Monitor applications, servers, systems, and networks.
- Scan for security problems.
- Take corrective actions on remote (server) systems:
  - Restart systems and processes.
  - Manipulate directories, files, and services. For example BDL, VBScript, Shell (Rexec, secureshell), FTP, LDAP, and others.
- Send notifications:
  - Activate pagers through a proprietary HTTP based pager service.
  - Forward alerts to enterprise management systems.
  - Send custom emails with attachments.
- Spawn and control other programs.
- Collect business metrics:
  - Integrate with ERP systems, for example gathering revenue numbers.
- Perform verifications:
  - Web business transaction verification.
  - End-to-end monitoring.
  - Usability checks.
  - Complex service target validation.
  - HTML syntax conformance.
- Perform root-cause analysis:
  - Special “on-demand” tasks, for example after receiving a Performance Manager alert, an administrator may wish to run HTTP traceroute to check network connectivity.
- And more...

Managing the File Pool

The file pool is an upload and download area on the Performance Manager Web server, which is called the front-end server. SuperUsers and Administrators can upload files to this area and make them available for the creation of new monitors.

You can upload a file from your hard disk or UNC path through the browser interface.

Note: Creating a monitor from an uploaded file does not remove that file from the file pool; it creates an independent instance. To remove files from the file pool, navigate to **Administration** > **Files** and click the **Delete** icon of the file you want to remove.

Uploading Files from a Browser

To upload a file from a browser:

1. In the menu, click **Administration** > **Files** .
2. Click the **File Pool** tab. The **File Pool** page displays, listing the files that have been uploaded to the file pool.
3. Click **Upload From Browser** to open the **Upload file to file pool** page.
4. Type a **Description** for the file you want to upload.
5. To make the uploaded file available only to a specific project, select the project name from the **Project** list box. If the file is to be accessible by all projects, select `No specific project`.

6. Optionally, you can assign an **Owner** to the uploaded file.

   This enables users to filter the file pool based on the owners of files.
7. In the **Select file for upload** text box you can manually enter a valid local path or a UNC path to the file you want to upload. Alternately, you can browse for the file using **Browse**.

   Performance Manager only allows .sep, .stp, .zip, and .ltz files for monitor creation.
8. Click **Upload** to upload the file to the Performance Manager file pool. You are be returned to the **File Pool** page where the file you uploaded is listed. The file is now available for the creation of new monitors in Performance Manager.

File Pool Page

Administration > **Files**

Use the **File Pool** page to upload files to the file pool and to download files from the file pool.

Filter options enable you to better target the uploaded files you want to access. The page allows you to set the following filter items:

Filter Item	Description
Uploaded By	Displays files uploaded by the selected user, or files uploaded by any user.
Project	Displays files associated to the selected project. Selecting `Any Project` will display all uploaded files, while selecting `No specific project` will display only files that are not associated to any project.
Owner	Displays files associated to the selected owner. Selecting `Any Owner` will display all uploaded files, while selecting `No Owner` will display only files that are not associated to an owner.
Update	Updates the list of displayed files according to your filter settings.

For each listed file, the page displays the following columns:

Table Item	Description
Actions	This column contains action icons which allow the user to perform the following actions on a file:  Deletes a file permanently from the file pool.  Downloads a file to your local computer.
File	The filename of a file.
File Size	The size of the file.
Uploaded On	Date when the file was uploaded.
Uploaded By	The user who uploaded the file.
Project	The project to which the file is associated. Files can also be associated to no specific project, indicating that they can be used by any project.
Owner	The user who owns the file. If a file has no owner, any user with permission to access the file pool can access or modify this file.

Upload Buttons	Description
Upload From Browser	Uploads a file from your hard disk or a UNC path through the browser interface.
Upload From Silk Performer STM	Provides information on how to upload a project from Silk Performer STM.

Time Zones

Performance Manager is designed to execute monitors over a network of execution servers. Because the Internet enables such networks to be spread worldwide across multiple time zones, it is important to understand time-zone handling in Performance Manager.

All date and time values are saved in GMT to the database. The presentation of values is set based on the **Time zone** setting specified in the user settings. This needs to be considered especially when you create globally usable schedules. For example, if an administrator who is located in New York creates a global schedule that runs every day at 6 PM, it runs at midnight for a user located in Paris, who applies this schedule to his execution plan. It is good practice to include the time zone in the name, for example "Daily at 6 PM EST", so that users know when it actually runs.

For information on time zone settings, see *Adding User Accounts*.

The following requirements apply:

- The application server and front-end server should be in the same time zone. Separating these servers locally within a WAN does not make sense because the application server communicates closely with one or several front-end servers. Also, front-end servers as well as the application server have direct database access.
- Execution servers may be in different time zones, separated both from the application server and from other execution servers.

Script-Execution Blackout Periods

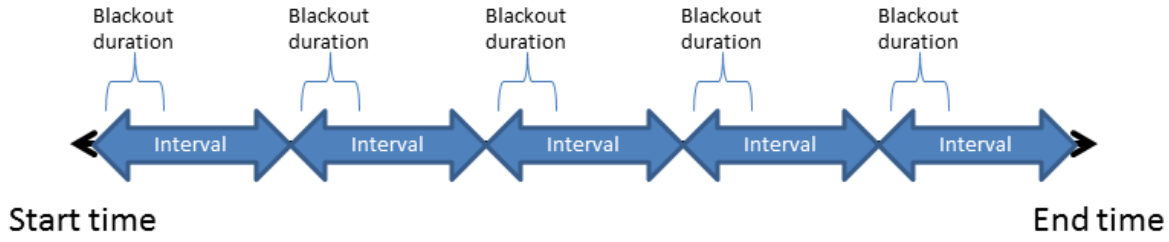
Blackout periods are designated maintenance periods during which script execution ceases. Alerts and alarms are not generated during blackout periods. Blackout periods are scheduled in advance and are configurable for each project. The Performance Manager GUI provides functionality for adding, editing, deleting, and sorting blackout definitions. Optionally you can configure blackout periods so that script execution and data collection continue while only alerts and alarms are suppressed. Additionally, you can configure monitors to automatically reinitialize their runtime environments when executions resume following blackout periods.

Note: After upgrading Performance Manager, all blackouts are set to the time zone of the application server. If a user who set up a blackout is not in the same time zone as the application server, they would need to simply open and save that blackout again so that the time zone of the user will be interpreted correctly.

Blackout Properties

Blackout period schedules are defined by the following properties:

- Start time
- Duration
- Recurrence interval
- End time



Note: To allow for enough time to undeploy / redeploy affected monitors, blackout periods actually start 20 seconds before the scheduled start time and end 20 seconds before the end of the duration. This functionality is also relevant when activating or deactivating blackouts.

Blackout Period Status

You can see whether an active project currently is in a blackout status in **Performance Manager** > **Projects** > **Overview** . Projects that have active blackouts that temporarily disable the project have `with blackout period` appended to their `Active` status message. By placing your cursor over a project's status message, you can view a tooltip that shows the name of the associated blackout definition and the blackout type.

Note: No matter how many of a project's locations are currently disabled, project status will always be shown as only partially disabled if the associated blackout period time type is `Location local time`.

Adding Blackout Periods

Note: For detailed information on the individual settings, refer to *Blackout Periods Page*.

To add a new blackout period:

1. In the menu, click **Administration** > **Projects** . The **Projects** page displays, listing all existing projects.
2. Click the **Blackout Periods** tab.
3. Click **New Blackout Period**. The **Add Blackout Period** page displays.
4. Type a meaningful name for the blackout in the **Blackout Period Name** text box.
5. Select a **Time type**.
   - **One global time**
   - **Location local time**
6. Specify when the blackout period is to begin with the **Start Time** list boxes.
7. Specify how long each blackout will be with the **Duration** list boxes.
8. Specify the amount of time that should transpire between blackouts with the **Interval** list boxes.
9. Specify when the blackout period is to end with the **Scheduled Until** list boxes.
10. Select a **Blackout type**.
    - **Remove monitors from execution servers**
    - **Run monitors, but do not report errors**
11. In the **Projects** area, check the check boxes that correspond to the projects you want to associate with this blackout period.

    Note: Click **Select All** to select all projects, or click **Deselect All** to deselect all projects.
12. Click **Save** to save your blackout settings.

Editing Blackout Periods

To edit an existing blackout period definition:

1. In the menu, click **Administration** > **Projects** . The **Projects** page displays, listing all existing projects.
2. Click the **Blackout Periods** tab.
3. Click the status of the blackout period you want to edit in the **Status** column to toggle the `Active`/`Inactive` status. The blackout period must be set to `Inactive` before you can edit it.

   Note: If a blackout period is deactivated while it is currently running (monitors are not reporting incidents), the blackout is stopped and all affected monitors will run again and report incidents, if encountered.
4. Click the name of the blackout period you want to edit in the **Blackout Period Name** column. The **Edit Blackout Period** page displays.
5. Edit the settings of the blackout period.

   For additional information, see *Adding Blackout Periods*.
6. Click **Save** to confirm your changes.
7. Back on the **Blackout Periods** list, click the status of the updated blackout period in the **Status** column to toggle the status back to `Active`.

Deleting Blackout Periods

Note: Blackout periods can only be deleted if they are deactivated.

To delete a blackout period definition:

1. In the menu, click **Administration** > **Projects** . The **Projects** page displays, listing all existing projects.
2. Click the **Blackout Periods** tab.
3. Click the status of the blackout period you want to delete in the **Status** column to toggle the `Active`/`Inactive` status. The blackout period must be set to `Inactive` before you can delete it.
4. In the **Actions** column of the blackout period that you want to delete, click ✕.
5. Click **Yes** on the subsequent confirmation dialog to delete the blackout period definition.

Blackout Periods Add/Edit Page

Administration > **Projects** > **Blackout Periods**

Use this page to configure script-execution blackout periods for Monitoring Console.

Note: The execution log records an entry each time a blackout period is activated, for both entire projects and individual locations.

For each listed blackout period, the details page displays the following information:

Column	Description
Blackout Period Name	Name defined for the blackout period. For example, `Two-Hour Duration Test, One-Day Interval`.
Time Type	For the dates given in the schedule of the blackout period, two different time type options are available: **One global time (all associated projects** The global time type setting indicates that all associated

Column	Description
	are disabled simultaneously) projects are disabled at exactly the time indicated as the **Start Time**, based on your local time zone, on all locations simultaneously. **Location local time (each of the associated project's locations is disabled according to the location's local time)** Indicates that associated project locations will be disabled based on their local time-zone settings. The active intervals for a single blackout period may differ from location to location. This setting assumes that all execution servers for a single location are located in the same time zone.
Start Time	Time at which the blackout period is to become active.
Duration	Length of time that projects are to be disabled while a blackout is active.
Interval	Interval at which the blackout periods should reoccur. The amount of time that is to transpire between blackouts. Active intervals for blackout periods exclude the start time, but include the end time.  **Note:** Blackout periods cannot overlap. Monitoring Console will not allow you to define overlapping blackout periods.
Scheduled Until	Time at which the blackout period is to end. If the specified **Duration** would call for a blackout to remain active once the **Scheduled Until** time is reached, all associated projects remain disabled until the **Duration** has ended.
Blackout Type	Determines how associated projects are disabled. There are two types of disablement: **Remove monitors from execution servers** The monitors of the associated projects are removed from the execution servers, and therefore do not deliver any results or trigger any incidents. Monitors are distributed again once the blackout period is over. **Run monitors, but do not report errors** The monitors of the associated projects continue to run, their results are still recorded and affect health, availability, accuracy and performance values as usual, but rules and conditions are not evaluated, so no Incidents are raised. Evaluation resumes once the blackout period is over.

Column	Description	
Projects	**Name**	Lists all projects that are available in the system.
	Assigned	Check to assign a blackout to a project.

GUI-Level Testing Support

When to Use GUI-Level Testing

Suppose you have an application that implements a traditional client/server architecture. An example would be a proprietary time-tracking system that stores the working hours of employees on a server. However, you cannot use any of the existing Silk Performer application types for testing, because the application uses an exotic protocol to communicate between client and server. In such instances, you may want to use GUI-level testing.

How GUI-Level Testing Works

When you start a test, the Silk Performer Controller connects to an agent running on a Microsoft Windows Server operating system and has *Remote Desktop Service* (formerly known as *Terminal Services*) running. Silk Test then performs the previously recorded steps on the application, or in other words: Silk Test drives the application.

Setting Up a GUI-Level Testing Environment

1. Install Silk Performer.
2. Install Silk Test.
3. Install your client application.
4. Use Silk Test to model one or more test cases using the application.
5. Create a Silk Performer GUI-level testing project that uses the Silk Test project to run the defined test cases against the system under test.

Once you have performed all these steps, you can start the test in Silk Performer.

Note: You can use the following Silk Test clients for GUI-level testing: Silk Test Classic, Silk4J, and Silk4NET. Make sure that you meet all requirements when you use Silk4J and Silk4NET for GUI-level testing. See *Requirements for GUI-Level Testing with Silk4J and Silk4NET* for details.

Why is it Called *GUI-Level Testing*?

Silk Test performs testing directly on the graphical user interface, or in other words, on the GUI-level. With this approach you can watch how Silk Test performs the recorded test steps, for example mouse clicks and keyboard entries, if you connected to one of the sessions on the agent machine.

GUI-Level Testing Functions

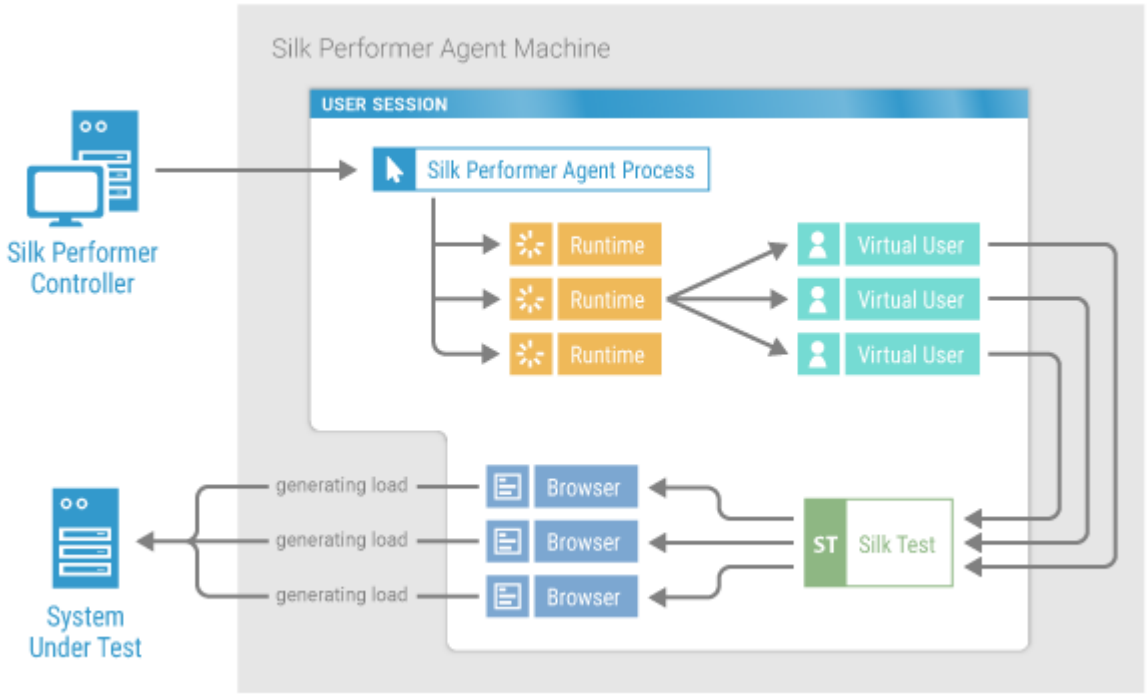
Refer to the Silk Performer BDL Reference for full details on the BDL functions that are offered by Silk Performer.

Note: Silk Test can be started in local host mode. With this approach, virtual users use a console session rather than a separate Windows session.

Single Session GUI-Level Testing

For tests against web applications using Google Chrome, Mozilla Firefox, or PhantomJS, Silk Performer allows you to run all virtual users within a single Windows session. The benefits are that no remote

Desktop licenses are required and that resource consumption per virtual user is considerably lower compared to the conventional GUI-level testing approach.



Configuring Windows for GUI-Level Testing

Before you can execute GUI-level tests, you must configure your Windows operating system. Additionally, Silk Test needs to be installed on the agent computer (refer to the Silk Test Help for details).

Configuring Windows 2003 for GUI-Level Testing

1. Enable Remote Desktop Protocol (RDP).

   RDP is disabled by default.

   Note: A complete installation of Terminal Server is required to enable GUI-level testing on Windows 2003 machines, as opposed to the default two-user RDP trial version.

   a) Open Windows **System Properties**.
   b) Click the **Remote** tab.
   c) Check the checkbox **Enable Remote Desktop on this computer**.
   d) Click **OK**.
2. Allow RDP users to run multiple sessions.
   a) Navigate to **Administrative Tools** > **Terminal Services Configuration** > **Server Settings**.
   b) Double-click **Restrict each user to one session**. The **Single session per user** dialog box displays.
   c) Uncheck the checkbox **Restrict each user to one session**.
   d) Click **OK**.
3. Configure Remote Desktop settings.
   a) Navigate to **Administrative Tools** > **Terminal Services Configuration** .
   b) Right-click the **Remote Desktop Protocol-TCP (RDP-Tcp)** icon and click **Properties**.
   c) Click the **Logon Settings** tab and make sure that **Always prompt for password** is disabled.

d) Click the **Sessions** tab and make sure that **Override user settings** is selected and that **End a disconnected session** is set to `1 minute`. Make sure that all other settings are disabled or left blank.
e) Click the **Environment** tab and make sure that **Run initial program specified by user profile and Remote Desktop Connection or Terminal Services client** is enabled.
f) Click the **Remote Control** tab and make sure that **Use remote control with default user settings** is enabled.
g) Click the **Client Settings** tab and make sure that all connection settings in the **Connection** section are enabled.
h) Click the **Network Adapter** tab and make sure that **All Network adapters configured with this protocol** is selected in the **Network adapter** list.
i) Click **OK**.

4. Using the Windows user and group administration functionality, select the local users that can execute GUI-level tests. Ensure that this user is a member of the `Administrators` and/or `Remote Desktop Users` group.

Configuring Windows 2008 for GUI-Level Testing

Before you can perform this task, make sure that **TS RemoteApp Manager** is installed. If **TS RemoteApp Manager** is not installed, visit *Microsoft Download Center* for information on downloading and installing **TS RemoteApp Manager**.

1. Enable Remote Desktop Protocol (RDP).
   RDP is disabled by default.

   Note: A complete installation of Terminal Server is required to enable GUI-level testing on Windows 2008 machines, as opposed to the default two-user RDP trial version.

   a) Open Windows **Control Panel** > **System**.
   b) Click the **Remote Settings** link.
   c) Check the checkbox **Allow connections from computers running any version of Remote Desktop (less secure)**.
   d) Click **OK**.
2. Allow RDP users to launch applications remotely.
   a) Navigate to **Administrative Tools** > **Terminal Services** > **TS RemoteApp Manager**.
   b) Click **Change** next to **Terminal Server Settings**.
   c) In the **Access to unlisted programs** group box, check the checkbox **Allow users to start both listed and unlisted programs on initial connection**.
   d) Click **OK**.
3. Allow RDP users to run multiple sessions.
   a) Navigate to **Administrative Tools** > **Terminal Services** > **Terminal Services Configuration**.
   b) Double-click **Restrict each user to a single session**. The **Properties** dialog box displays.
   c) Uncheck the checkbox **Restrict each user to a single session**.
   d) Click **OK**.
4. Configure Remote Desktop settings.
   a) Navigate to **Administrative Tools** > **Terminal Services** > **Terminal Services Configuration**.
   b) Right-click **Remote Desktop Protocol-TCP (RDP-Tcp)** in the **Connections** list and click **Properties**.
   c) Click the **Log on Settings** tab and make sure that **Always prompt for password** is disabled.
   d) Click the **Sessions** tab and make sure that **Override user settings** is selected and that **End a disconnected session** is set to `1 minute`. Make sure that all other settings are disabled or left blank.
   e) Click the **Environment** tab and make sure that **Run initial program specified by user profile and Remote Desktop Connection or client** is enabled.

f) Click the **Remote Control** tab and make sure that **Use remote control with default user settings** is enabled.
g) Click the **Network Adapter** tab and make sure that **All Network adapters configured with this protocol** is selected in the **Network adapter** list.
h) Click **OK**.

5. User Account Control (UAC) is enabled by default, but is not required for GUI-level testing. If you want to leave UAC turned on, the agent must run under a user account.

   To turn UAC on or off:

   a) Navigate to **Control Panel** > **User Accounts** > **Turn User Account Control on or off**.
   b) Check or uncheck the checkbox **Use User Account Control (UAC) to help protect your computer**.
   c) Click **OK**.

6. Using the Windows user and group administration functionality, select the local users that can execute GUI-level tests. Ensure that this user is a member of the `Administrators` and/or `Remote Desktop Users` group.

Configuring Windows 2008 R2 for GUI-Level Testing

Before you can perform this task, make sure that the **Remote Desktop Services** server role is installed.

1. Enable Remote Desktop Protocol (RDP).

   RDP is disabled by default.

   a) Open Windows **Control Panel** > **System and Security** > **System**.
   b) Click the **Remote Settings** link.
   c) Check the checkbox **Allow connections from computers running any version of Remote Desktop (less secure)**.
   d) Click **OK**.

2. Allow RDP users to launch applications remotely.

   a) Navigate to **Administrative Tools** > **Remote Desktop Services** > **RemoteApp Manager**.
   b) Click **Change** next to **RD Session Host Server Settings**.
   c) In the **Access to unlisted programs** group box, check the checkbox **Allow users to start both listed and unlisted programs on initial connection**.
   d) Click **OK**.

3. Allow RDP users to run multiple sessions.

   a) Navigate to **Administrative Tools** > **Remote Desktop Services** > **Remote Desktop Session Host Configuration**.
   b) Double-click **Restrict each user to a single session**. The **Properties** dialog box displays.
   c) Uncheck the checkbox **Restrict each user to a single session**.
   d) Click **OK**.

4. Configure Remote Desktop settings.

   a) Navigate to **Administrative Tools** > **Remote Desktop Services** > **Remote Desktop Session Host Configuration**.
   b) Right-click **Remote Desktop Protocol-TCP (RDP-Tcp)** in the **Connections** list and click **Properties**.
   c) Click the **Log on Settings** tab and make sure that **Always prompt for password** is disabled.
   d) Click the **Sessions** tab and make sure that **Override user settings** is selected and that **End a disconnected session** is set to `1 minute`. Make sure that all other settings are disabled or left blank.
   e) Click the **Environment** tab and make sure that **Run initial program specified by user profile and Remote Desktop Connection or client** is enabled.
   f) Click the **Remote Control** tab and make sure that **Use remote control with default user settings** is enabled.

g) Click the **Network Adapter** tab and make sure that **All Network adapters configured with this protocol** is selected in the **Network adapter** list.
h) Click **OK**.

5. User Account Control (UAC) is enabled by default, but is not required for GUI-level testing. If you want to leave UAC turned on, the agent must run under a user account.

   To configure UAC settings:

   a) Navigate to **Control Panel** > **User Accounts** > **User Accounts** > **Change User Account Control Settings**.
   b) Modify the UAC notification level as desired.
   c) Click **OK**.

6. Using the Windows user and group administration functionality, select the local users that can execute GUI-level tests. Ensure that this user is a member of the `Administrators` and/or `Remote Desktop Users` group.

Configuring Windows 2012 for GUI-Level Testing

Before you can perform this task, make sure that **Remote Desktop Services** is enabled.

1. End disconnected sessions.
   a) Start the Windows **Server Manager** and navigate to **Remote Desktop Services** > **Collections** > **<name of the collection>**. In the **Properties** area, select **Edit Properties** from the **Tasks** menu.
   b) On the **Session Collection** dialog, select **Session**.
   c) In the **End a disconnected session** list, select **1 minute**.
   d) Click **OK**.
2. Allow RDP users to run multiple sessions and launch all programs.
   a) Start the Windows **Local Group Policy Editor** and navigate to **Local Computer Policy** > **Computer Configuration** > **Administrative Templates** > **Windows Components** > **Remote Desktop Services** > **Remote Desktop Session Host** > **Connections**.
   b) Double-click **Restrict Remote Desktop Services users to a single Remote Desktop Services session**.
   c) Click the **Disabled** option.
   d) Click **OK**.
   e) Double-click **Allow remote start of unlisted programs**.
   f) Click the **Enabled** option.
   g) Click **OK**.
3. User Account Control (UAC) is enabled by default, but is not required for GUI-level testing. If you want to leave UAC turned on, the agent must run under a user account.

   To configure UAC settings:

   a) Navigate to **Control Panel** > **User Accounts** > **User Accounts** > **Change User Account Control Settings**.
   b) Modify the UAC notification level as desired.
   c) Click **OK**.
4. Using the Windows user and group administration functionality, select the local users that can execute GUI-level tests. Ensure that this user is a member of the `Administrators` and/or `Remote Desktop Users` group.

GUI-Level Test Execution

Modeling GUI-Level Tests - Silk Test Classic

1. Click **File** in the menu and click **New Project**. In the tree, click **GUI-Level Testing** and **Silk Test**. Enter a **Name** and a **Description** and click **Next**.
2. In the **File** field, specify the Silk Test asset you want to use for a performance test. Silk Performer automatically detects the file type and enables the appropriate button below.
3. Click **Import Silk Test Classic test**.
4. If the test case file you want to import is located within a Silk Test package file (.stp), select **Open a Silk Test package file** and specify the file in the **Silk Test Package** field.
5. If you want to import a test case file, select **Open a Silk Test script file** and specify the file in the **Script File** field.
6. Select a specific **Testcase** from the list.
7. *(optional)* You can add Silk Test Classic test data to the selected test case, if required. Enter test data into the **Test Data** field using the format `"<test case name>",<test data>` (For example, `"test", 10`).
8. Click **Add**. The selected test case appears below in the **Testcase** field.
9. Add more test cases to your project as required by repeating this procedure.
10. Select a **Web Browser** from the drop-down list. This list is only enabled when the file that is to be imported is based on a Silk Test web project. Silk Test web projects can make use of the single-session concept for GUI-level testing.
11. Enable **Use project attributes for session login** to let Silk Performer use credentials from the **Project Attributes** to login into sessions. To edit the project attributes, click **Project** > **Project Attributes** . The credentials will be added to the `TInit` transaction of your script. The check box **Use project attributes for session login** is only available when the file that is to be imported is based on a Silk Test web project. Silk Test web projects can make use of the single-session concept for GUI-level testing.
12. Click **OK** and save the .bdf file.

Silk Performer imports the test assets and generates an appropriate .bdl stub.

Modeling GUI-Level Tests - Silk4J

1. Click **File** in the menu and click **New Project**. In the tree, click **GUI-Level Testing** and **Silk Test**. Enter a **Name** and a **Description** and click **Next**.
2. In the **File** field, specify the Silk Test asset you want to use for a performance test. Silk Performer automatically detects the file type and enables the appropriate button below.
3. Click **Import Silk4J test**.
4. In the **File** field, specify the archive that is to be tested. The archive is automatically added to the profile classpath. The available classes are then retrieved and displayed, sorted alphabetically in the **Class** field.
5. From the **Class** list, select one of the available classes for testing.

   When you do not specify a specific archive for testing, the wizard enables you to specify a class that is available in the profile classpath. Type the fully qualified class name into the **Class** field, for example `java.lang.String`.

   The available constructors and methods are automatically retrieved and displayed.
6. In the **Methods** area, select the methods that you want to call.
7. To filter the methods that are shown in the **Methods** area, perform the following steps:
   a) Click the **Advanced Settings** button (the funnel icon above the **Methods** area).
   b) Once you have customized filter settings, click **OK** to update the **Methods** area.
8. To change general Java settings including the Java version, Java home directory, or JVM DLL, click the **Active Profile Settings** link. The **Profile Settings** dialog opens to the **Java/General** page for Java projects (JUnit project type).

Note: Changes made to these settings (for example Java Classpath) may lead to different results. Selections made in the **Class**, **Constructor**, and **Methods** fields will be updated with the new results.

Note: If you change the Java version, Java home directory, or JVM DLL, you must restart Silk Performer for the changes to take effect.

9. Select a **Web Browser** from the drop-down list. This list is only enabled when the file that is to be imported is based on a Silk Test web project. Silk Test web projects can make use of the single-session concept for GUI-level testing.
10. Enable **Use project attributes for session login** to let Silk Performer use credentials from the **Project Attributes** to login into sessions. To edit the project attributes, click **Project** > **Project Attributes** . The credentials will be added to the `TInit` transaction of your script. The check box **Use project attributes for session login** is only available when the file that is to be imported is based on a Silk Test web project. Silk Test web projects can make use of the single-session concept for GUI-level testing.
11. Click **OK** and save the .bdf file.

Silk Performer imports the test assets and generates an appropriate .bdl stub.

Modeling GUI-Level Tests - Silk4NET

1. Click **File** in the menu and click **New Project**. In the tree, click **GUI-Level Testing** and **Silk Test**. Enter a **Name** and a **Description** and click **Next**.
2. In the **File** field, specify the Silk Test asset you want to use for a performance test. Silk Performer automatically detects the file type and enables the appropriate button below.
3. Click **Import Silk4NET test**.
4. In the **File** field, specify the archive that is to be tested. The available classes are retrieved and displayed, sorted alphabetically in the **Class** field.
5. From the **Class** list, select one of the available classes for testing. Type the fully qualified class name into the **Class** field. The available methods are automatically retrieved and displayed.
6. In the **Methods** area, select the methods that you want to call.
7. To filter the methods that are shown in the **Methods** area, perform the following steps:
   a) Click the **Advanced Settings** button (the funnel icon above the **Methods** area).
   b) Once you have customized filter settings, click **OK** to update the **Methods** area.
8. To change general .NET settings, click the **Active Profile Settings** link. The **Profile Settings** dialog opens to the **.NET/General** page.
9. Select a **Web Browser** from the drop-down list. This list is only enabled when the file that is to be imported is based on a Silk Test web project. Silk Test web projects can make use of the single-session concept for GUI-level testing.
10. Enable **Use project attributes for session login** to let Silk Performer use credentials from the **Project Attributes** to login into sessions. To edit the project attributes, click **Project** > **Project Attributes** . The credentials will be added to the `TInit` transaction of your script. The check box **Use project attributes for session login** is only available when the file that is to be imported is based on a Silk Test web project. Silk Test web projects can make use of the single-session concept for GUI-level testing.
11. Click **OK** and save the .bdf file.

Silk Performer imports the test assets and generates an appropriate .bdl stub.

User Credentials for GUI-Level Testing

User credentials for GUI-level testing can be specified in the following areas:

- Profile settings
- Project attributes (username and password project attributes are automatically defined when you create a GUI-level testing project)

- Plain text specified in the BDL script
- Imported from data files

Note: Ensure that the user accounts used for GUI-level testing are members of the Remote Desktop Users Windows group on the remote agent.

If you want each VUser to connect using different login credentials, specify the credentials using project attributes or use script customization through data files.

If you want each VUser to connect with identical login credentials, specify the credentials using profile settings or with plain text in the BDL script.

Note: User credentials specified in profile settings are used only when the other options listed above are not used. When no user credentials are specified in any of the areas listed above, Silk Performer connects to the console session without using the remote desktop protocol.

Timers in GUI-Level Testing

Timers are central to GUI-level testing. You can add timers to your Silk Test Classic, Silk4J, and Silk4NET scripts which will be reported to Silk Performer's test results. Refer to the Silk Test Help for detailed information about creating timers within Silk Test scripts.

Silk Performer automatically generates names for Silk Test timers that do not have names.

When executing keyword-driven tests, the execution time for each keyword is logged automatically.

GUI-Level Testing Result Files

You can find the most recent Try Script TrueLog files in the `RecentTryScriptTest` directory within your Silk Performer project directory. During GUI-level testing, temporary Silk Test TrueLog files with the extension `.xlgs` are written. After each Silk Test test case execution, the results of the Silk Test `.xlgs` and the results of the Silk Performer `.xlgs` files are merged into the Silk Performer `.xlgs` files (per VUser) and the temporary `.xlgs` files are deleted.

The `RecentTryScriptTest` directory within your Silk Performer project directory also includes Silk Test `.xlgs` result files. These are the files that are displayed in Silk Test when you initiate the **Explore** Silk Test **results** command.

Exploring Silk Test Results

1. Within Silk Performer, right-click a virtual user profile.
2. Select **Explore** Silk Test **Results** from the context menu. Silk Test launches, allowing you to analyze the corresponding Silk Test `.res` result file.

   You can also select **Explore TrueLog** from the context menu to view a Try Script's TrueLog in TrueLog Explorer.

   Click the **Results** tab to view test results directly in Silk Performer.

Requirements for GUI-Level Testing with Silk4J and Silk4NET

Make sure to meet the following requirement when you use Silk4J for GUI-Level testing:

- You must have Silk Test 15.0 or higher installed.

Make sure to meet the following requirements when you use Silk4NET for GUI-Level testing:

- You must have Silk Test 15.0 or higher installed.
- You must have Test Agent from the .NET Framework installed.
- You need the same version of MSTest that was used to build the test file.

Note: Silk Performer will always use the latest MSTest version that is installed on the test machine. If the version you used for building the test file differs from the latest version that is installed on the test machine, the Silk4NET information in the TrueLog file will be missing.

Troubleshooting GUI-Level Testing Issues

When troubleshooting GUI-Level issues it is important to note that there are three separate components (Silk Performer, Silk Test, and Windows/Terminal Services/Remote Desktop Services) that play integrated roles during the execution of GUI-Level tests; each of these components should be considered when attempting to isolate the root causes of errors.

Step 1: Windows test-environment configuration

Note: For resolutions to issues outlined in this section, please visit the *Micro Focus Knowledge Base* and enter the referenced **Resolution ID**.

The first thing to consider is that Silk Performer can only execute multiple GUI-level virtual users on Microsoft Windows operating systems that have Terminal Services/Remote Desktop Services installed, licensed and configured. If you attempt to execute more than one GUI-level virtual user from a Microsoft Windows machine you will encounter the following error message: `StInitSession(GUI-Level Testing Replay: 10 - Virtual user information, Silk Test Connection timeout reached.`

Resolution ID: `17256`, `17231`

The next, and perhaps most important, step is to configure Windows Terminal Services/Remote Desktop Services to allow each Silk Performer virtual user to execute a Silk Test test case within a separate terminal session. Therefore it is of the vital importance that each of the settings below be configured exactly as specified in the resolution listed below.

Resolution ID: `17255`

Please note that failure to configure Windows Terminal Services/Remote Desktop Services as recommended above can result in error messages such as `GUI-Level Testing Replay: 10 - Virtual user information, RDP not connected`.

Resolution ID: `20117`

Once you have configured Terminal Services/Remote Desktop Services, the final configuration check is to ensure that you are using the correct version of Silk Test (for test case generation) and that you have the correct Silk Performer licenses available for a GUI-level testing.

Resolution ID: `17168`, `17148`

Step 2: Proxy Server Configuration

In some situations, when recording a Silk Performer script via the Silk Test interface, the resulting BDF file contains no Silk Performer functions. To resolve this issue, perform the following:

1. Launch Internet Explorer and navigate to **Tools** > **Internet Options**.
2. Select the **Connections** tab.
3. Click **LAN settings**. The **Local Area Network (LAN) Settings** dialog box opens.
4. Check the **Use a proxy server for your LAN** check box.
5. In the **Address** field, type `localhost`.
6. In the **Port** field, type `8080`.
7. Click **OK**.

Step 3: Silk Test configuration and test-case generation

Note: For resolutions to issues outlined in this section, please visit the *Micro Focus Knowledge Base* and enter the referenced **Resolution ID**.

When using Silk Test to generate a test case for execution in Silk Performer it is important that you consider that the test case will eventually be executed by Silk Performer within a Terminal Services/Remote Desktop Services/Remote Desktop Services environment. This means that certain considerations need to be made, such as ensuring that a full version of Silk Test is installed on the Silk Performer Agent otherwise Silk Performer will report the error message `GUI-Level Testing Replay: 7 - Application could not be launched`.

Resolution ID: `17181`

Ensure that any directory paths that have been configured for Silk Test are still available when the Silk Test project is exported to Silk Performer; otherwise the Silk Performer runtime engine may be unable to can locate the directory path used to launch the application under test. Failure to set a global path can result in an error message such as `Error: Directory XXXX does not exist"`.

Resolution ID: `17204`

Finally, before exporting the Silk Test project to Silk Performer it is imperative that you export the project using the correct settings. Otherwise you may see the following error: `GUI-Level Testing Replay:11 SilkTest reported. Project failed to open`. The resolution below describes both the consequences of not doing this and the correct way to export a project from Silk Test.

Resolution ID: `17200`

Step 4: Silk Performer configuration and common GUI-level replay errors

Note: For resolutions to issues outlined in this section, please visit the *Micro Focus Knowledge Base* and enter the referenced **Resolution ID**.

The final component to look at when troubleshooting GUI-level issues is Silk Performer. The first thing an end user should consider before they replay a GUI-level BDF script in Silk Performer is that there are major differences between executing a Silk Test testcase within Silk Performer using a normal *console session* and executing a Silk Test test case using a *terminal server session*. The major differences between running a BDF script as a console session and terminal server session are detailed in the following resolution.

Resolution ID: `17258`

Failure to understand the differences between the types of sessions that can be executed in Silk Performer and failure to instruct Silk Performer that you wish to execute a terminal server session can lead to the common replay error `GUI-Level Testing Replay: 10 - Virtual user information, More than 1 user per Session is not allowed`. Refer to the resolution listed below to learn how to avoid this error during replay in Silk Performer.

Resolution ID: `17257`

Other errors that commonly occur during replay are related to the Terminal Services/Remote Desktop Services session in which the Silk Test test case runs. For example is it important to consider that when a Silk Test test case is initially recorded it is often within an operating system environment that uses different user credentials than the environments in which the Silk Test test case will be executed within the terminal server environment. This can result in unexpected windows being generated during replay within the terminal server session and as a result the Silk Test agent will report an error message during replay within Silk Performer such as `Log Error: *** Error: Window 'window name' was not found`. The following resolution provides a good example of one such error and explains how you can avoid it.

Resolution ID: `17236`

Before you execute an actual GUI-level test it is important to consider that there are limitations in regards to the number of virtual users that can be executed within a Terminal Server environment. The resolution

below outlines the typical number of GUI-level virtual users that can be executed from a single Silk Performer installation.

Resolution ID: 17202

Configuring Advanced Settings

This section describes how to configure advanced settings to customize your Performance Manager system.

Login Options

The following two enhanced login configurations are available:

Remember Login

Changing the default setting for the **Remember login** option on the Performance Manager login page.

Each user may enable or disable the **Remember login** option as required; the administrator can however set the default setting.

Cookie Duration

Each time a user accesses Performance Manager, a cookie containing encoded login information is created. These cookies are destroyed when users log out, or when sessions time out. When the **Remember login** option is enabled however, cookies are not destroyed when sessions time-out. Instead, they remain active for a set duration of time. This enables users to continue working with Performance Manager without re-entering login information after each session time-out. By default, cookies remain active for 30 days. The duration setting can be adjusted by the administrator.

Configuring the Remember Login Option

To enable or disable the remember login option:

1. Stop the front-end server.
2. Open the `SccFrontendBootConf.xml` file with a text editor.

   The default path for this file is `C:\Program Files (x86)\Silk\Silk Performance Manager <version>/conf/frontendserver` on the front-end server.
3. Locate the `BootConf\Options\Login\RememberLogin` XML tag.

   By default, the tag is set to `<RememberLogin>true</RememberLogin>`.
4. Set the value to `false` to have the login page open with an unchecked **Remember Login** check box by default. Set the value to `true` to have the login page open with a checked **Remember Login** check box by default.
5. Save and close the XML file.
6. Re-start the front-end server.

Adjusting the Cookie Duration

To set the duration of login cookies:

1. Stop the front-end server.
2. Open the `SccFrontendBootConf.xml` file with a text editor.

   The default path for this file is `C:\Program Files (x86)\Silk\Silk Performance Manager <version>/conf/frontendserver` on the front-end server.

3. Locate the `BootConf\Options\Login\MaxCookieAge` XML tag.

   By default, the tag is set to `<MaxCookieAge>30</MaxCookieAge>`.
4. Set the value to the number of days you want login cookies to remain active on user computers.
5. Save and close the XML file.
6. Re-start the front-end server.

Using the Performance Manager Service Manager

The Performance Manager Service Manager is a tool that is used to manage the Performance Manager services and to view their log files. The following services are available:

- Execution server
- Front-end server
- Application server
- Chart server

Log Files

Performance Manager servers write their activities to log files. When application errors or system failures occur, these log files provide valuable information regarding the root causes of problems.

Performance Manager Services

Setup automatically installs the Service Manager when any of the four services are installed. You can access the Service Manager either from the Performance Manager program group, or from its Windows task bar tray icon. The Windows services, which are viewable in the Windows Services window, are called *<Service name> Server*, for example *Application Server*.

Note: The Service Manager does not work out-of-the box on Windows platforms that use User Account Control (UAC), like for example Microsoft Windows Vista, Microsoft Windows 7, or Microsoft Windows Server 2008. To enable the Service Manager to work on these platforms, you either need to disable UAC or stop the Service Manager and start it again with the option **Run as administrator**.

All four services must be running to enable operation of Performance Manager. The services can be distributed over different computers or run on a single machine. For information about installing services, refer to the *Performance Manager Installation and Configuration Guide*.

Tip: Stopping and restarting services is an administrative task that only needs to be done when a system is not operating as intended, or when maintenance tasks are required.

Performance Manager Execution Server

The Performance Manager execution server can be run as both a Windows system service and as a Windows process.

By default, Performance Manager launches an execution server as Windows system service. Do not change this default setting without good reason. For the work with Silk Test the execution server has to run in process mode.

While a Windows process is launched with the credentials of the currently logged in user, a system service is launched with the local system account, by default the Windows system account. A system service remains active even after the user logs off; thus the Performance Manager execution server is available until the computer is turned off completely.

To execute and monitor Silk Test Classic, Citrix, and SAP scripts you must launch the Performance Manager execution server as a Windows process, with valid user credentials.

Managing Which Performance Manager Services Shall Be Running At System Start

Performance Manager services are services that will start automatically when the system is started. You can change this behavior if you want to deactivate a service, or if you want to switch an execution server permanently from service mode to process mode.

To manage which individual Performance Manager services shall be running at system start:

1. Double-click the **Silk Performance Manager Service Manager** tray icon in the Windows task bar. The *Silk Performance Manager Service Manager* displays, with up to five tabs visible, depending on the services that are installed on this computer.
2. Click the tab that corresponds to the service you want to access:
   - Execution Server
   - Execution Server (Process)
   - Front-End Server
   - Application Server
   - Chart Server
3. Check the **Run at start-up** check box if you want the selected service to start automatically.
4. Click **OK** to finish managing the servers. The *Silk Performance Manager Service Manager* closes, but remains active in the system tray.

Note: The **Execution Server (Process)** will only start after a logon to the Windows server.

Starting or Stopping All Performance Manager Services

Caution: Performance Manager will not operate properly when the four services are not running.

To start or stop all Performance Manager services at once:

1. Right-click the **Silk Performance Manager Service Manager** tray icon in the Windows task bar.
2. Click one of the following:

Start all Services	All Performance Manager services currently installed on the computer begin running.
Stop all Services	All Performance Manager services installed on the computer are stopped.

3. To start or stop individual services, see *Starting or Stopping Individual Services*.

Starting or Stopping a Local Execution Server Service

Use the **Silk Performance Manager Service Manager** to start or stop a locally installed execution server service.

1. Double-click the **Silk Performance Manager Service Manager** tray icon in the Windows task bar. The **Silk Performance Manager Service Manager** dialog appears.
2. Click **Start** or **Stop** to start or stop the execution server service.
3. Click **Query Status** to check the current status of the service.
4. If you wish to monitor real-time activity, launch the Performance Manager execution server with a console window:

1. Check the **Start with console** check box.
2. Click **Stop**.
3. Click **Start**.

5. Click the **Execution Server Logfile** link to view the log file. The log file opens in the registered text editor.
6. Click **OK** to finish managing the execution server service. The Service Manager closes, but remains active in the system tray.

Starting the Execution Server as Windows Process

Start the execution server service as a Windows process if your monitor needs to run using the credentials of the currently logged in user.

Monitors run in Windows Terminal Services sessions by default. Note that multiple Terminal Services sessions are only supported by Windows Server operating systems. Other Windows operating systems like Home or Professional editions support only limited Terminal Services sessions.

The execution server can be run either as a Windows service or a Windows process. In most instances this is preferable since it is active even when a user logs off, which means the execution server is always available, unless the computer is powered off. However, the Windows service is launched using the default system account and this may not always be suitable-for example, launching certain executables within a monitor may require particular users' credentials. In such instances it may be necessary for the execution server to be launched as a Windows process-this uses the credentials of the currently logged in user.

To start the Performance Manager execution server as a Windows process:

1. Double-click the **Silk Performance Manager Service Manager** tray icon in the Windows task bar. The *Silk Performance Manager Service Manager* displays, with up to five tabs visible, depending on the services that are installed on this computer.
2. Click the **Execution Server** tab.

   This tab represents the Performance Manager execution server, running as a Windows system service.
3. Click **Stop** to stop the execution server system service.
4. Click **Query Status** to check the service's status.

   Make sure that the service status is `stopped`.
5. Uncheck **Run at start-up** to prevent that the service is started after computer re-boot.
6. Click the **Execution Server (Process)** tab.

   This tab represents the Performance Manager execution server, running as a Windows process.

   Note: The Windows process is launched with the credentials of the user who is currently logged in. Make sure that this user has sufficient privileges to accomplish the tasks you are planning to execute with Performance Manager.
7. Click **Start** to start the execution server as a Windows process.
8. Check **Run at start-up** so that the process is started after computer re-boot and re-login.
9. Click **OK** to finish managing the execution server. The **Service Manager** closes, but remains active in the system tray.

Viewing Log Files from the Performance Manager Service Manager Console

To view Performance Manager log files from the Performance Manager Service Manager console:

1. Double-click the **Silk Performance Manager Service Manager** tray icon in the Windows task bar. The *Silk Performance Manager Service Manager* displays, with up to five tabs visible, depending on the services that are installed on this computer.

2. Select the tab representing the server of which you want to view the log file.
3. Click the **Logfile** link of the server.

   The log file opens in the registered text editor. Microsoft Notepad by default.
4. On the Performance Manager Service Manager, click **OK** or **Cancel** to close the Service Manager. The Service Manager closes, but remains active in the system tray.

Date and Time Formats

Performance Manager offers user-defined date and time format settings. Each Performance Manager user can change their user settings, which include options for displaying custom date formats in the form of long or short date formats. For additional information, see *Editing User Accounts*.

Performance Manager presents lists of predefined date and time formats from which users may choose. Performance Manager administrators can populate these lists with customized formats.

Pattern Definition

Date and time formats are specified by date and time pattern strings. Within date and time pattern strings, unquoted letters from "A" to "Z" and from "a" to "z" are interpreted as pattern letters representing the components of a date or time string. Text can be quoted using single quotes (') to avoid interpretation. "''" represents a single quote. All other characters are not interpreted; they are simply copied into the output string during formatting or matched against the input string during parsing.

The following pattern letters are defined. All other characters from "A" to "Z" and from "a" to "z" are reserved:

Letter	Date or Time Component	Presentation	Examples
G	Era designator	Text	AD
y	Year	Year	1996; 96
M	Month in year	Month	July; Jul; 07
w	Week in year	Number	27
W	Week in month	Number	2
D	Day in year	Number	189
d	Day in month	Number	10
F	Day of week in month	Number	2
E	Day in week	Text	Tuesday; Tue
a	Am/pm marker	Text	PM
H	Hour in day (0-23)	Number	0
k	Hour in day (1-24)	Number	24
K	Hour in am/pm (0-11)	Number	0
h	Hour in am/pm (1-12)	Number	12
m	Minute in hour	Number	30
s	Second in minute	Number	55
S	Millisecond	Number	978
z	Time zone	General time zone	Pacific Standard Time; PST; GMT-08:00

Letter	Date or Time Component	Presentation	Examples
Z	Time zone	RFC 822 time zone	-0800

Pattern letters are usually repeated, as their number determines the exact presentation.

The following list explains the items in the **Presentation** column in the table above:

Item	Description
Text	For formatting, when the number of pattern letters is 4 or more, the full form is used; otherwise an abbreviated form is used, when available. For parsing, both forms are accepted, independent of the number of pattern letters.
Number	For formatting, the number of pattern letters is the minimum number of digits, and shorter numbers are zero-padded to this amount. For parsing, the number of pattern letters is ignored unless it is needed to separate two adjacent fields.
Year	For formatting, when the number of pattern letters is 2, the year is truncated to 2 digits; otherwise it is interpreted as a *Number*.
Month	When the number of pattern letters is 3 or more, the month is interpreted as *Text*; otherwise, it is interpreted as a *Number*.
General time zone	Time zones are interpreted as *Text* when they have names. When the number of pattern letters is less than 4, the time zone abbreviation is displayed, for example PST. When the number of pattern letters is 4 or more, the full name is displayed, for example Pacific Standard Time.
RFC 822 time zone	The RFC 822 4-digit time zone format is used, for example -0800.

Examples

The following examples show how date and time patterns are interpreted in the U.S. The given date and time are 2001-07-04 12:08:56 local time, Pacific Standard Time zone.

Date and Time Pattern	Result
"yyyy.MM.dd G 'at' HH:mm:ss z"	2001.07.04 AD at 12:08:56 PDT
"EEE, MMM d, "yy"	Wed, Jul 4, '01
"h:mm a"	12:08 PM
"hh 'o''clock' a, zzzz"	12 o'clock PM, Pacific Daylight Time
"K:mm a, z"	0:08 PM, PDT
"yyyyy.MMMMM.dd GGG hh:mm aaa"	02001.July.04 AD 12:08 PM
"EEE, d MMM yyyy HH:mm:ss Z"	Wed, 4 Jul 2001 12:08:56 -0700
"yyMMddHHmmssZ"	010704120856-0700

Customizing Date and Time Formats

To customize date and time formats:

1. Stop the front-end server.

2. Open the `SccFrontendBootConf.xml` file with a text editor.

   The default path for this file is `C:\Program Files (x86)\Silk\Silk Performance Manager <version>/conf/frontendserver` on the front-end server.
3. Locate the `DateFormats` XML tag.

   The XML tags `<LongDateFormats>` and `<ShortDateFormats>` show the date formats that are available by default. You can add or remove any formats you want to make available or unavailable to users.
4. Type time formats as described in *Date and Time Formats*.
5. Save and close the XML file.
6. Re-start the front-end server.

HTML Response Compression

The Performance Manager front-end server offers an option for automatically sending gzip-compressed responses. Enabling this feature speeds up load times of Performance Manager HTML pages, but results in a slight increase of load on the front-end server, depending on the amount of HTML requests, which is the number of concurrent Performance Manager users, that you expect.

HTML response compression only works when the Web browsers of the users support HTML response compression.

For the current list of supported browsers, refer to the release notes.

Enabling or Disabling HTML Response Compression

To enable or disable HTML response compression:

1. Stop the front-end server.
2. Open the `Server.xml` file with a text editor.

   This file is located in the `/conf/frontendserver` folder of the Performance Manager directory on the front-end server.
3. Locate the `Connector` XML tag.
4. Add `compression="on"` and `compressableMimeType="text/html,text/xml,text/plain,text/css,text/javascript,application/xml"` to the connectors.

   The servlet will compress any response with gzip. Gzip is taken from Apache Tomcat Native.
5. Save and close the XML file.
6. Re-start the front-end server.

User Interface Settings

Certain areas of the Performance Manager user interface can be customized by modifying the `SccFrontendBootConf.xml` file on the front-end server.

Displaying or Hiding the Host Name in the Tab Name of Your Web Browser

To display or hide the host name in the tab name of your Web browser:

1. Stop the front-end server.

2. Open the `SccFrontendBootConf.xml` file with a text editor.

   The default path for this file is `C:\Program Files (x86)\Silk\Silk Performance Manager <version>/conf/frontendserver` on the front-end server.
3. Locate the `DisplayHostNameInTitleBar` XML tag in the `Options` section of the file.
4. If you set the value to `true`, the host name of the front-end server will be displayed in the tab name of Web browsers when accessing Performance Manager. If you set the value to `false`, which is the default value, no host name will be displayed, and if you set the value to any other string, the specified string will be displayed. The currently selected unit in Performance Manager is always displayed.

   For example, when the XML tag is set to `true`, the browser displays: `HOSTNAME - Micro Focus - <unit>`.

   When the tag is set to `false`, the browser displays: `Micro Focus - <unit>`.

   When custom text is entered, for example `MyCustomText`, the browser displays: `MyCustomText - Micro Focus - <unit>`.

   When the tag is left empty, the browser displays: `Micro Focus - <unit>`.
5. Save and close the XML file.
6. Re-start the front-end server.

Customizing the Displayed Information on the System Health Page

The **System Health** page displays information about the Performance Manager servers and projects. Per default, detailed information about the execution servers is not displayed, but this information can be turned on by modifying the `SccFrontendBootConf.xml` file. Likewise, the displayed average measure write time can be divided by the number of project result writer threads to display the real throughput. This may give a better view on your system's actual measure writing performance.

To modify the displayed information on the **System Health**:

1. Stop the front-end server.
2. Open the `SccFrontendBootConf.xml` file with a text editor.

   The default path for this file is `C:\Program Files (x86)\Silk\Silk Performance Manager <version>/conf/frontendserver` on the front-end server.
3. Locate the `SystemHealthShowExecServerDetails` XML tag in the `Options` section of the file. If you set the value to `true`, detailed information about each execution server will be displayed on the **System Health** page. If you set the value to `false`, which is the default, this information will not be displayed.
4. Locate the `SystemHealthDivideMeasureWriteTime` XML tag in the `Options` section of the file. If you set the value to `true`, the displayed average measure write time is divided by the number of project result writer threads. If you set the value to `false`, which is the default, the displayed average measure write time is the cumulated measure write time of all project result writer threads. This influences how good your measure writing performance is, from a display perspective. Setting the value to `true` will display a much better measure writing performance.
5. Save and close the XML file.
6. Re-start the front-end server.

Displaying the Servlet Busy Time

You can configure Performance Manager to show how long the server needed to calculate the contents of each Performance Manager page and how long it took to assemble the HTML page. Enabling this setting will display the information on the top right-hand side of the toolbar.

To display the servlet busy time:

1. Stop the front-end server.
2. Open the `SccFrontendBootConf.xml` file with a text editor.

   The default path for this file is `C:\Program Files (x86)\Silk\Silk Performance Manager <version>/conf/frontendserver` on the front-end server.
3. Locate the `DisplayServletBusyTime` XML tag in the `Options` section of the file. If you set the value to `true`, servlet busy time and page assembly time is displayed on the top right-hand side of the toolbar on every page in Performance Manager. If you set the value to `false`, which is the default, this information will not be displayed.
4. Save and close the XML file.
5. Re-start the front-end server.

Displaying Different Measure Writing Performance Graphs on the System Health Page

Choose whether to display the measures received / written per period graph on the **System Health** page that displays actual measures written versus measures that have been received (default), or a graph that tries to predict the system's load (red/amber/green) based on a background calculation.

Note that a calculated prediction may include false assumptions based on estimates of both load and parallel processing and thus sometimes misinterprets the actual system load. This behavior can be seen for example when the graph displays the system as being overloaded, but the backlog of unwritten measures is not actually growing over time. For this reason, it is recommended to use the actual measures received / written per period graph, which gives a better picture of indicating whether or how well the Performance Manager application server is keeping up with its workload over time. This actual graph is the default setting and no action is required to display it on the **System Health** page.

To change the display to the original, older graph, which shows calculated estimates, proceed as follows:

1. Open the `SvAppServerHomeConf.xml` file with a text editor.

   The default path for this file is `C:\Program Files (x86)\Silk\Silk Performance Manager <version>/conf/appserver` on the application server.
2. Locate the `<UseSystemhealthHistory>` XML tag. If it does not exist, add it manually.
3. Set the value to `true` (default) to display a graph that displays actual measures written versus measures that have been put in a backlog to be written later due to system overload. Set the value to `false` to display a graph that displays a predicted system load (red/amber/green). Example: `<UseSystemhealthHistory>true</UseSystemhealthHistory>`.
4. Save and close the XML file.
5. Refresh the **System Health** page to see the changes.

Restricting Access to Database Tables

When submitting advanced reports with SQL queries like for example `SELECT * FROM SCC_Roles`, users with access to reports basically have unrestricted access to the information stored in the Performance Manager database. To restrict this access, you can configure which user roles may not access which database tables. If a user tries to create an advanced report using one of the restricted tables, an information message is displayed.

1. Stop the front-end server.
2. Open the `SVFrontendBootConf.xml` file with a text editor.

   This file is located in the `/conf/frontendserver` folder of the Performance Manager directory on the front-end server.

3. Locate the `<LockedTables>` XML tag. The list within this tag specifies the prohibited database table(s) as comma separated list for each user role with access to the reports section:

XML tag	Restricted tables
`<SuperUser>SCC_Users,SCC_UserGroups,dual</SuperUser>`	Restricts the SuperUser role's access to the SCC_Users and SCC_UserGroups tables.
`<Reporter>SCC_Users,SCC_UserGroups,dual</Reporter>`	Restricts the Reporter role's access to the SCC_Users and SCC_UserGroups tables.

4. Save and close the XML file.
5. Re-start the front-end server.

Example

```
<Reports>
  <LockedTables>
    <SuperUser>SCC_Users,SCC_UserGroups,dual</SuperUser>
    <Reporter>SCC_Users,SCC_UserGroups,dual</Reporter>
  </LockedTables>
</Reports>
```

Storage Reduction and Performance Stabilization

Storage Reduction

Monitoring Console stores all monitor execution results and all result files, like TrueLog files, .wrt files, and others, in the repository. If you run multiple monitors over a long period of time, you may want to save space on the hard drive of your database server. This feature is only supported by Monitoring Console. Monitoring Console offers the following two options for storage reduction:

Reducing storage by removing old result files (TrueLog files, .wrt files, etc.) from the repository	Result files are stored as BLOBs in the repository. You might, for example, set up storage reduction so that when result files in the repository reach a size of 20 GB (GigaBytes), the oldest result files are removed as new result files are written to the repository.
Reducing storage by aggregating monitoring results	While Monitoring Console saves raw monitoring values by default, you may not need such a level of detail for older results. You can advise Monitoring Console to aggregate results after defined time intervals into units of 15 minutes, 1 hour, 1 day, or 1 week. You might for example, with data older than 1 month, reduce the detail level of results to an aggregated value of 15 minutes intervals. For data older than 6 months, you could reduce the detail level of results to an aggregated value of 1 hour intervals. For data older than 1 year, you might reduce the detail level of results to an aggregated value of 1 day intervals. For data older than 2 years, you could reduce the detail level of results to an aggregated value of 1 week intervals.

Performance Stabilization

By default, the history of the project health is not being re-calculated after deleting a monitor. This guarantees that database performance is consistent. However, if you want to have the historical project health data be re-calculated to reflect the missing monitor, you can turn this on in the `SvAppServerHomeConf.xml` file. Be aware that if you turn this on, the database takes a severe performance hit every time a monitor is being deleted.

Reducing Repository Size and Stabilizing Performance on the Database Server

Older result data for which you no longer need the full level of detail can be aggregated, thus saving space in the repository.

To reduce the repository size on the database server:

1. Stop the application server.
2. Open the `SvAppServerHomeConf.xml` file with a text editor.

   The default path for this file is `C:\Program Files (x86)\Silk\Silk Performance Manager <version>/conf/appserver` on the application server.
3. Locate the `<KeepOldData>` XML tag.
4. Define the interval when Monitoring Console should perform the data reduction process by setting the tag `<ScheduleDayPeriod>`. Set the value to the number of days after which the data reduction process should be performed.

   For example, to start removing old result files and aggregating old results every week, enter the following settings:

   ```
   <ScheduleDayPeriod>7</ScheduleDayPeriod>
   ```
5. If you defined a weekly interval in the `<ScheduleDayPeriod>` tag, define the starting day of the interval by setting the tag `<ScheduleDay>` to the respective day of the week. Set the value to one the following numbers, depending on the day you want the process to run:

Value	Weekday
0	Sunday
1	Monday
2	Tuesday
3	Wednesday
4	Thursday
5	Friday
6	Saturday

   For example, to start removing old result files and aggregating old results every week on Friday, enter the following settings:

   ```
   <ScheduleDayPeriod>7</ScheduleDayPeriod>
   <ScheduleDay>5</ScheduleDay>
   ```
6. If your interval in the `<ScheduleDayPeriod>` tag is not set to `7` (weekly), set the `<ScheduleDay>` value to `0`.

   Caution: Setting the `<ScheduleDay>` value to a higher value than the one specified in the `<ScheduleDayPeriod>` tag will disable the data reduction process.
7. Define a time of the day when Monitoring Console should perform the data reduction process by setting the hour and minutes in the tags `<ScheduleTimeHour>` and `<ScheduleTimeMinute>`. Set the hour within an interval of 0 to 23 and the minutes within an interval of 0 to 59.

   Note: This time has to be specified in the local time zone of the application server. When the local time zone of the application server is changed, this only takes effect after a restart of the application server. This is also the case when daylight saving time changes.

For example, to start removing old result files and aggregating old results at 1:15 AM, enter the following settings:

```
<ScheduleTimeHour>1</ScheduleTimeHour>
<ScheduleTimeMinute>15</ScheduleTimeMinute>
```

8. Define how Monitoring Console should remove old result data by setting the tags `<RawValues>`, `<I15min>`, `<I60min>`, `<I1440min>`, `<I10080min>`, and `<Incidents>`.

   These settings allow you to define how far in the past old results must be before they get removed. Enter a value in days, or enter 0 (zero) if you do not want Monitoring Console to remove old data.

   Note: Aggregated values remain in the repository. Data aggregation is a background job that consistently aggregates data as it qualifies.

   The following table displays a few examples on the usage of the settings:

Settings	What this does
<RawValues>31</RawValues>	Removes raw values for data older than 31 days.
<I15min>182</I15min>	Removes 15 minute interval values for data older than half a year.
<I60min>365</I60min>	Removes 1 hour interval values for data older than one year.
<I1440min>730</I1440min>	Removes 1 day interval values for data older than two years.
<I10080min>1095</I10080min>	Removes 1 week interval values for data older than 3 years.
<Incidents>35</Incidents>	Removes incidents that are older than 35 days.

9. Define the maximum amount of space that result files, like TrueLog files, .wrt files, and others, may take up in the repository in Megabytes.

   Once this size is reached, the oldest result files will be removed as newer files enter the repository. Thus the amount of space that result files use will grow up to this setting and then remain at that setting. To set the result file size, enter a number in Megabytes in the `<ResultFileSize>` tag. The default setting is 10000 Megabytes.

   For example, to limit the space allocated to result files in the repository to 5 GB:

   ```
   <ResultFileSize>5000</ResultFileSize>
   ```

10. The `<ProjectHealthUpdate>` tag defines whether project health should be re-calculated after deleting a monitor. By default, the history of the project health is not being re-calculated after deleting a monitor. This guarantees that database performance is consistent. However, if you want to have the historical project health data be re-calculated to reflect the missing monitor, you can turn this on in the `SvAppServerHomeConf.xml` file. Be aware that if you turn this on, the database takes a severe performance hit every time a monitor is being deleted. To turn on re-calculation, set `<ProjectHealthUpdate>true</ProjectHealthUpdate>` (not recommended).
11. Save and close the XML file.
12. Restart the application server.

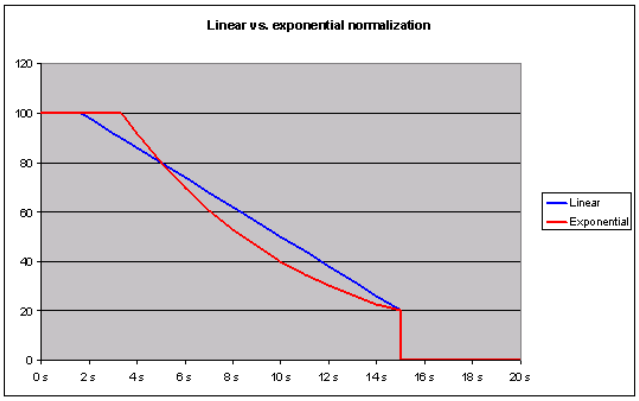
Normalization Settings

You can use the following two options to convert individual measurements into rates ranging from 0 to 100:

Exponentially normalized	Between a lower and upper boundary
Linearly normalized	Between a lower and upper boundary

There is no difference between calculating performance rates for timers and calculating performance rates for counters. Both are treated the same, thereby enabling health rate comparisons. The default setting for

Monitoring Console is exponential normalization, but you can change this setting to linear normalization. This setting is used for all health calculations in Monitoring Console. This feature is only supported by Monitoring Console. The following graph illustrates linear in comparison to exponential normalization. For this chart, times are measured in seconds. A lower bound of 15 s is used with a rating of 20%, and an upper bound of 5 s is used with a rating of 80%.



Changing Normalization Settings

Note: This procedure explains how to go from exponential normalization, the default, to linear normalization. Reverse the code-change instructions to go from linear normalization to exponential normalization.

To change from exponential normalization to linear normalization:

1. Stop the application server.
2. Open the `SvAppServerHomeConf.xml` file with a text editor.

   The default path for this file is `C:\Program Files (x86)\Silk\Silk Performance Manager <version>/conf/appserver` on the application server.
3. Locate the `<MeasureNormalization>` XML tab, which contains the `<Class>` tag.

   The `<Class>` tag is set to `<Class>com.segue.vision.appserver.result.ExponentialNormalization</Class>` by default.
4. Comment the `<Class>` tag by entering `<!--` before the tag and `-->` after the tag.
5. Uncomment the `<!--<Class>com.segue.vision.appserver.result.LinearNormalization</Class>-->` tag, by removing the `<!--` before the tag and `-->` after the tag.
6. Save the file and close the editor.
7. Restart the application server.

Monitoring Console now has linear normalization.

Maximum Threads on Execution Server

To make sure that an execution server delivers accurate monitoring results, you must ensure that the network connection to the execution server is not overloaded with Performance Manager internal traffic. The maximum number of monitors to be executed simultaneously on an execution server can be customized through an XML-file, thus ensuring controllable network traffic.

Setting Maximum Threads on an Execution Server

To make sure that an execution server delivers accurate monitoring results, you must ensure that the network connection is not overloaded with internal traffic.

To set the maximum threads on an execution server:

1. Stop the execution server.

   For additional information, see *Starting or Stopping Individual Performance Manager Services*.
2. Open the `SccExecServerBootConf.xml` file with a text editor.

   This file is located in the `/conf/execserver` folder of the Performance Manager directory on an execution server.
3. Locate the `<MaxThreads>` tag in the `<Scheduler>` section of the file.
4. Set the value to the maximum number of monitors you want the execution server to handle simultaneously.

   If the execution server receives more than the defined number of monitors, they will be queued to be executed as soon as resources become available.
5. Save the file and restart the execution server service.

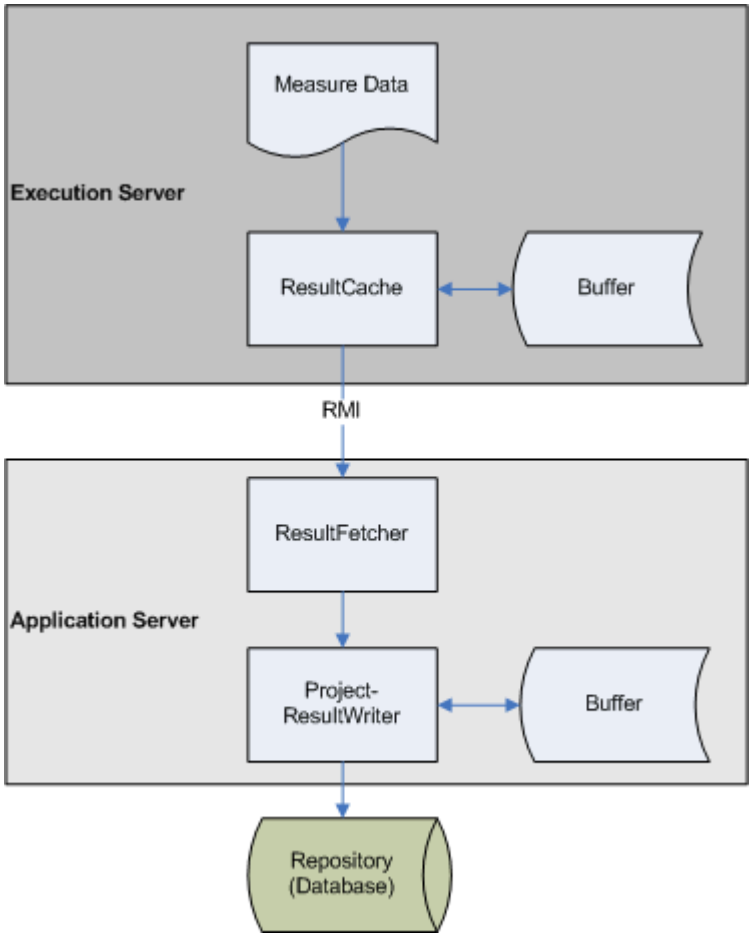
   For additional information, see *Starting or Stopping Individual Performance Manager Services*.

Persistent Result Data

Monitor executions on the execution server generate result and measure data. This data passes several stages before it is stored persistently in the repository (database). By default, these stages include only volatile storage (RAM). This leads to data loss if a server crashes or hangs, or if network problems lead to a cache overflow.

Result Data Flow

The flow of result data starts with incoming results from the monitor execution. These results are stored in the system memory by the *ResultCache* service which waits for the *ResultFetcher* service to pull data to the application server. As soon as the transmission completes successfully, the data is removed from the *ResultCache*. The application server caches the data in the *ProjectResultWriter* service, which then cycles through the projects and writes data in portions (round-robin) to the repository.



Loss of Result Data

The *ResultCache* service on the execution server stores incoming result data until it is collected by the application server. In case of network outage or the application server being down for a longer period, the memory of the execution server limits the amount of data that can be cached. If the limit is reached, any incoming result data will be dropped and is then lost.

The application server pulls data from the execution server and caches it in the *ProjectResultWriter* service, from where it is written to the repository in a round-robin cycle, project by project. If data arrives faster than the database is able to store it, the cache will grow until the memory limit is reached, at which point the *ProjectResultWriter* will cease pulling data from the execution servers, which ultimately leads to cache overflows on the execution servers. If a system crashes while an amount of data is being cached, those results will be lost.

Enabling Persistent Result Data

To avoid the loss of data on the execution servers and on the application server, Performance Manager provides the option to enable transactional file-based intermediate result data storage.

Enabling Persistent Result Data on the Application Server

To enable persistent result data on the application server:

1. Open the `SccAppServerBootConf.xml` file with a text editor.

This file is located in the `/conf/appserver` folder of the Performance Manager directory on the application server.

2. Create the `ResultBuffer` XML tag in the `SccPath` section of the file if it does not yet exist.
3. Specify the path to where result data shall be stored before it moves to the next stage in the data flow.

   You can specify a relative or an absolute path:

   Relative path example Creates a `resultBuffer` directory in the`Application Data` directory, which is normally at `C:\Users\<username>\AppData\Local\Silk\Silk Performance Manager 19.0`.

   ```
   <SccPath>
   ...
           <ResultBuffer>resultBuffer</ResultBuffer>
   ...
   </SccPath>
   ```

   Absolute path example Creates the directory as specified.

   ```
   <SccPath>
   ...
           <ResultBuffer>c:\temp\resultBuffer</ResultBuffer>
   ...
   </SccPath>
   ```

   Beneath the specified path, a subdirectory for each project is created to divide the number of files and therefore speed up the file system.
4. Save and close the XML file.

Enabling Persistent Result Data on the Execution Server

The following procedure needs to be performed on each execution server where you want to enable persistent result data storage.

To enable persistent result data on the execution server:

1. Open the `SccExecServerBootConf.xml` file with a text editor.

   This file is located in the `/conf/execserver` folder of the Performance Manager directory on the execution server.
2. Create the `ResultBuffer` XML tag in the `SccPath` section of the file if it does not yet exist.
3. Specify the path to where result data shall be stored before it moves to the next stage in the data flow.

   You can specify a relative or an absolute path:

   Relative path example Creates a `resultBuffer` directory in the `Application Data` directory, which is normally at `C:\Users\<username>\AppData\Local\Silk\Silk Performance Manager 19.0`.

   ```
   <SccPath>
   ...
           <ResultBuffer>resultBuffer</ResultBuffer>
   ...
   </SccPath>
   ```

   Absolute path example Creates the directory as specified.

   ```
   <SccPath>
   ...
   ```

```
        <ResultBuffer>c:\temp\resultBuffer</ResultBuffer>
...
</SccPath>
```

Beneath the specified path, a subdirectory for each project is created to divide the number of files and therefore speed up the file system.

4. Save and close the XML file.

Execution Server Host Name Resolution

An execution server may no longer be recognized by the application server if the execution server's IP address has changed. Re-starting the application server means the execution server should be recognized again.

Java uses a cache to store the host name resolution to guard against DNS spoofing attacks. In Performance Manager the result of positive host name resolutions are cached forever, but this can be changed by editing the file `java.security` on the application server. This enables the application server to recognize execution servers even if their IP address has changed.

For more information on this Java setting, visit the *Networking Properties* page.

Disabling the Caching of Host Name Resolutions

To specify that host name resolutions are never cached:

1. Stop the application server.
2. Open the `java.security` file with a text editor.

   The default path for this file is `C:\Program Files (x86)\Silk\Silk Performance Manager <version>\lib\jre\lib\security` on the application server.
3. Locate the line `#networkaddress.cache.ttl=-1` and change it to `networkaddress.cache.ttl=0`.

   Note: The "#" character needs to be removed to uncomment this line.

   Caution: This change should be discussed with your network administrator, as there may be security concerns in doing this.
4. Save and close the file.
5. Restart the application server.

Security Settings

Explains security configurations for Performance Manager.

Disabling Unused Ports on Execution Servers

Depending on whether you use SSL or insecure communication between the application server and the execution servers, you may want to disable the respective unused port. You can also disable the default Tomcat port, which is never used by Performance Manager.

The following procedure needs to be performed on each execution server where you want to disable the unused port.

To disable unused ports on the execution server:

1. Stop the execution server.
2. Open the `SccExecServerBootConf.xml` file with a text editor.

   The default path for this file is `C:\Program Files (x86)\Silk\Silk Performance Manager <version>/conf/execserver` on the execution server.
3. Locate the `InsecurePort` and `SSLPort` XML tags in the `RmiProxy` section of the file.
4. Depending on whether you use SSL or insecure communication between application server and execution server, proceed as follows:

SSL communication	Set the value of `InsecurePort` to `0`.
Insecure communication	Set the value of `SSLPort` to `0`.

5. Save and close the XML file.
6. Restart the execution server.

Disabling Unused Ports on Front-End Servers

To disable the unused Tomcat port:

1. Stop the front-end server.
2. Open the `server.xml` file with a text editor.

   This file is located in the `/conf/frontendserver/conf` folder of the Performance Manager directory on the front-end server.
3. Change the port setting in the first line of the file from `<Server port="19132" shutdown="SHUTDOWN">` to `<Server port="0" shutdown="SHUTDOWN">`.
4. Save and close the XML file.
5. Re-start the front-end server.

Disabling the JMX RMI Interface

Due to a minor security issue, unauthenticated access to the JMX RMI interface used in Performance Manager is possible. No sensitive information is accessible or exposed due to this issue. To ensure that this type of access is not possible you can disable JMX for Performance Manager. If JMX is disabled it will not be possible to use Performance Manager's System Health monitor or monitor the application server via JMX; no other functionality will be affected by making this change.

To disable JMX:

1. Open the Registry Editor.
2. Remove the following from the "Options" registry key for each service:

   - -Dcom.sun.management.jmxremote.ssl=false
   - -Dcom.sun.management.jmxremote.authenticate=false
   - -Dcom.sun.management.jmxremote.port=1914x

   Perform this step on each computer that hosts Performance Manager services in the following registry key paths:

   - Application server: `HKEY_LOCAL_MACHINE\SOFTWARE\Apache Software Foundation \Procrun 2.0\SPMAppServer<version>\Parameters\Java`
   - Chart server: `HKEY_LOCAL_MACHINE\SOFTWARE\Apache Software Foundation\Procrun 2.0\SPMChartServer<version>\Parameters\Java`
   - Execution servers: `HKEY_LOCAL_MACHINE\SOFTWARE\Apache Software Foundation \Procrun 2.0\SPMExecServer<version>\Parameters\Java`
   - Front-end server: `HKEY_LOCAL_MACHINE\SOFTWARE\Apache Software Foundation \Procrun 2.0\SPMFrontendServer<version>\Parameters\Java`

Note: On 64-bit operating systems, the registry paths must include `Wow6432Node` after `SOFTWARE`, for example

`HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software Foundation\Procrun 2.0\SPMAppServer<version>\Parameters\Java`.

Memory Settings for Performance Manager Servers

This section describes how you can change the memory settings of the Performance Manager servers when out-of-memory errors occur.

The Java heap size of the Performance Manager front-end and application servers is set by default to 512 MB. If you are experiencing out-of-memory errors, try to increase the heap size on the front-end or application server.

Increasing the Java Heap Size on a Performance Manager Server

Increase the Java heap size on a Performance Manager server when you receive out-of-memory errors.

To increase the Java heap size on a front-end or application server:

1. Stop all Performance Manager services.
2. Click **Start** > **Run**.
3. In the **Run** dialog box, type `regedit` into the **Open** field.
4. Click **OK**. The **Registry Editor** opens.
5. In the menu tree, choose one of the following locations, depending on your operating system and the server type:

Performance Manager server	Location
Front-end server	`HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software Foundation\Procrun 2.0\SPMFrontendServer190\Parameters\Java`
Application server	`HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software Foundation\Procrun 2.0\SPMAppServer190\Parameters\Java`
Chart server	`HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software Foundation\Procrun 2.0\SPMChartServer190\Parameters\Java`

6. Double-click **JvmMx**. The **Edit DWORD Value** dialog box opens.
7. In the **Base** section of the dialog box, click the **Decimal** option button.
8. In the **Value data** field, type the new memory size, for example `1024`.

Note: The value of the Java heap size cannot exceed the available physical RAM on the front-end server machine and enough memory should be left available for other necessary processes. For example, if 2 GB of RAM are available, you can increase the Java heap size to a value of 1.5 GB, which corresponds to a value of 1536 in the **Value data** field, depending on what other processes are running. If you enter a value that is too big, the server may not start anymore.

9. Click **OK**.
10. Restart all Performance Manager services.

Configuring Result Writer Alerts

If the result writer experiences timing issues, you can configure how Performance Manager behaves.

1. Open the `SvAppServerHomeConf.xml` file with a text editor.

   The default path for this file is `C:\Program Files (x86)\Silk\Silk Performance Manager <version>/conf/appserver` on the application server.
2. Locate the `<ResultWriteWatcher>` XML tag.
3. Define how Performance Manager behaves when the result writer experiences timing issues:

XML tag	Action
`<AlertMaxResultWriteTime>`	If the result write time exceeds the specified value (in milliseconds), a warning is logged. If the value is set to zero, the watcher is deactivated.
`<NotificationUponMaxResultWriteTimeExceeded>`	If set to `true`, sends a notification to the Performance Manager administrator if an alert is triggered.
`<AppServerRestartUponMaxResultWriteTimeExceeded>`	If set to `true`, immediately restarts the application server service if an alert is triggered.

4. Save and close the XML file.

Caching Measure Results

Set the maximum number of measurement items that are cached in memory.

1. Open the `SvAppServerHomeConf.xml` file with a text editor.

   The default path for this file is `C:\Program Files (x86)\Silk\Silk Performance Manager <version>/conf/appserver` on the application server.
2. Locate the `<MaxMeasureCacheSize>` XML tag.
3. Set the maximum number of items that are cached in memory for faster retrieval of measure details during the measure writing process, for example `<MaxMeasureCacheSize>100000</MaxMeasureCacheSize>`.
4. Save and close the XML file.

Configuring Automatic Monitor Deployment

Set whether to re-deploy monitors to all execution servers on application server service restart.

Monitor deployment on execution servers usually does not need to be performed upon every restart of the application server service. You will only want to turn this setting on if execution servers experience an inconsistency with their assigned monitors. Depending on the amount of monitors, an automatic re-deployment can take very long. We recommend that you only turn this setting on if some monitors are no longer deployed where they should be.

1. Open the `SvAppServerHomeConf.xml` file with a text editor.

   The default path for this file is `C:\Program Files (x86)\Silk\Silk Performance Manager <version>/conf/appserver` on the application server.

2. Locate the `<RedeployMonitors>` XML tag.
3. Set the value to `true` to re-deploy monitors to all execution servers when the application server service is restarted.
4. Save and close the XML file.

Index

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

R

S

T

U

V

W