MICRO FOCUS

Silk Central 20.5

Installation and System Configuration Help

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

© Copyright 2004-2019 Micro Focus or one of its affiliates.

MICRO FOCUS, the Micro Focus logo and Silk Central are trademarks or registered trademarks of Micro Focus or one of its affiliates.

All other marks are the property of their respective owners.

2019-11-21

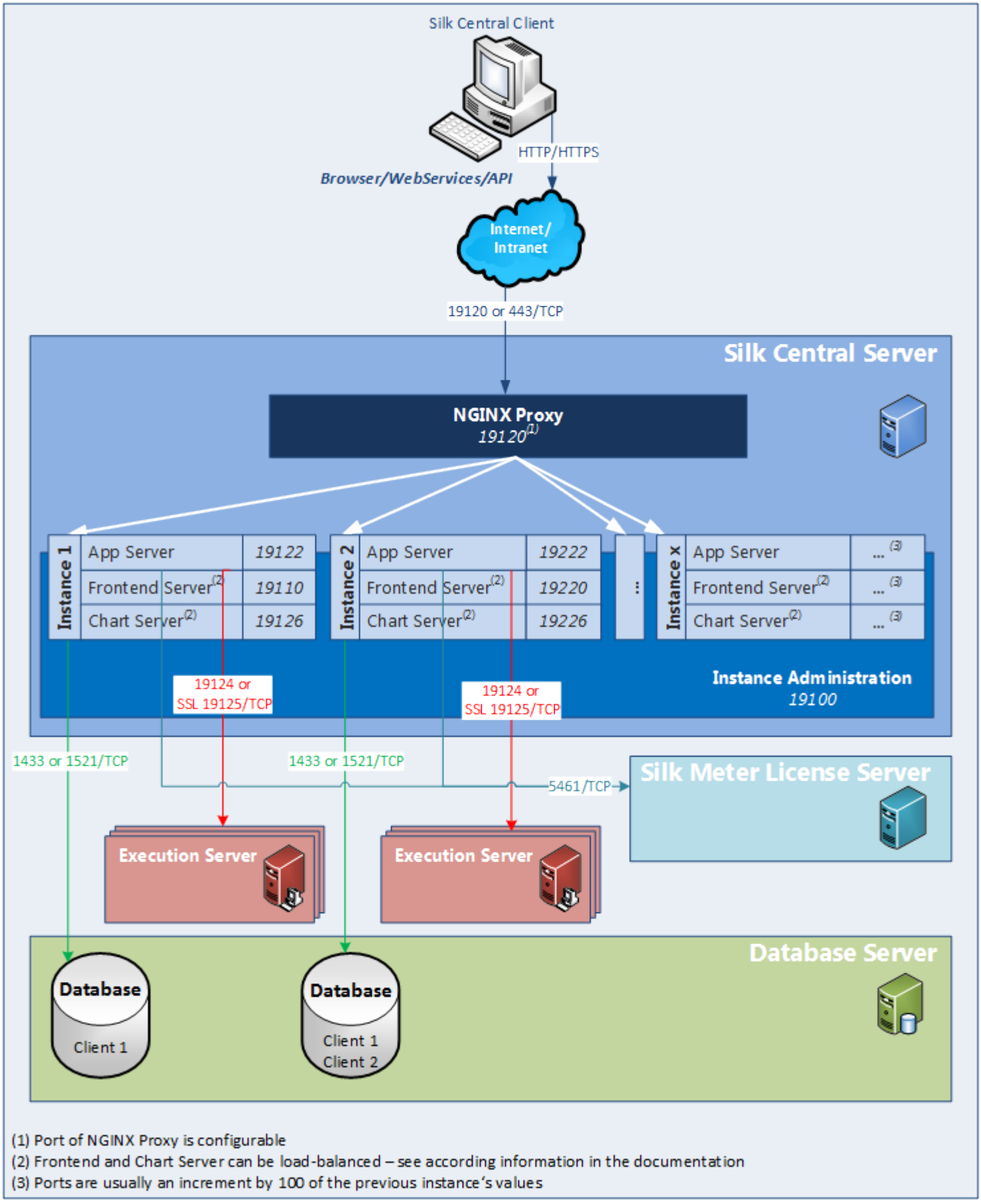
Contents

Silk Central Architecture 5
Installing Silk Central 10
System Requirements and Prerequisites 10
Choosing the Appropriate Components for Your Operating System 11
Installing Silk Central for Evaluation 12
Installing Silk Central 12
Installing a Windows Execution Server 15
Installing a Windows Execution Server in Silent Mode 15
Installing a Linux Execution Server 16
Installing a Command-Line-Driven Execution Server 17
Installing a Hotfix 18
Upgrading to Silk Central 20.5 18
Silk Central Licensing 19
License Handling 19
Generating a Silk Central License Policy 20
Finding the Host ID 20
Silk Meter Installation 21
Silk Meter License Server Configuration 21
Modifying Your License Server Configuration 22
Tested and Supported Software 22
Configuring and Managing the Infrastructure 25
Setting up a Secure Silk Central System 25
General Guidelines 25
Enabling Secure Web Server Connections with SSL 25
Enabling BIRT Reports in SSL Environments 26
Configuring a Non-Standard SSL Port for Execution Servers 27
Disabling Unused Ports on Execution Servers 27
Communicating with an External System Over SSL 28
Managing Instances 28
Installing a Hotfix 30
Starting or Stopping a Local Execution Server Service 30
Front-End Server Load Balancing 31
Managing Clients 32
System Administrator 32
Databases 32
Clients 38
Infrastructure 42
System Diagnostics 51
Configuring Advanced Settings 52
Login Options 52
Suspicious Execution Duration 53
Disable Updating of External Issue Statistics 54
Date and Time Formats 54
Host Name Display 56
Storing Attachments and Result Files on the File System 57
Configuring the LQM Reporting Updater 58
Scheduling Automatic LDAP Group Synchronization 59
Data Caching in Tests 59
Configuring JMX Settings 61
Execution Server Host Name Resolution 65
Configuring the Silk Central Location in Issue Manager 66

Disabling Unused Ports on Execution Servers 67
Setting the Maximum Number of MRU Reports 67
Memory Settings for Silk Central Servers 67
Setting the Maximum Size of Result Files from Manual Tests 68
Setting the Maximum Size of Result Files from Automated Tests 68
Storing Percentile Marker Data for Silk Performer Results 69

Silk Central Architecture

This section provides an overview of Silk Central's architecture.



(1) Port of NGINX Proxy is configurable
(2) Frontend and Chart Server can be load-balanced – see according information in the documentation
(3) Ports are usually an increment by 100 of the previous instance's values

Silk Central Server

The server on which the Silk Central Setup was executed.

Instance Administration

Instances and their Silk Central services are managed through a common user interface called **Instance Administration**, which you can access only on the server where Silk Central is installed, using the URL `http://localhost:19100`.

Instances

An instance is an independent set of Silk Central services (application server (AS), front-end server (FE) and chart server (CS)), with their own database and execution server (ES) connections. By default, Silk Central creates a single instance called *silk* for you. The default URL is `http://<computer name>:19120/login` (no port information required if Silk Central runs on IIS). Create additional instances if you need to physically separate test data and processes of your various clients for increased data security and reduced influence of independent user groups on each other (for example departments). With the help of clients you can further logically separate the data of one instance within one database.

Proxy

A proxy service is installed on the Silk Central server to control the access to the different instances. The services of each instance run on dedicated ports, but for security and increased flexibility reasons, the proxy routes the instance name to the actual URL in the form of `http://<Silk Central server>:19120/<instance name>`.

Application Server (AS)

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. The application server uses port 19122 for the default instance. For every additional instance, this value is incremented by 100.

Front-End Server (FE)

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, Firefox and Chrome. 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. The front-end server uses port 19110 for the default instance. The second instance uses port 19220 and for every additional instance, this value is incremented by 100. For secure connections with SSL, the server also uses port 443. The front-end server can be accessed through the URL `http://<Silk Central server>:19120/<instance name>` (no instance name required for default instance).

Chart Server (CS)

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. The chart server uses port 19126 for the default instance. For every additional instance, this value is incremented by 100.

Execution Server (ES)

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. The execution server uses port 19124 for the default instance. For secure connections with SSL, the server also uses port 19125.

Agent Computers:

Silk Performer and Silk Test Classic agent computers are assigned to particular Silk Performer or Silk Test Classic projects from the pool of agent computers that are available to the controller computer. In combination with Silk Central, the controller computer acts as an execution server.

Silk Performer Agents	Silk Performer agent computers host the virtual users that are run during load tests. As many agent computers as necessary can be added to a Silk Performer project so that the required quantity of virtual users can be run. Configuration of agents is done through Silk Performer. Refer to the Silk Performer documentation for details on configuring agents.
Silk Test Classic Agents	The same rules that apply to Silk Performer agents apply to Silk Test Classic agents, except Silk Test Classic agents host Silk Test Classic tests.

Database Server (DB)

System persistency is implemented using a RDBMS (Relational Database Management System). The database server uses ports 1433 (SQL Server) or 1521 (Oracle).

Silk Meter License Server

Silk Meter, the licensing software that accompanies Silk products, determines the Silk Central-application functionality that you may access. For more information on licensing, refer to the installation guide of the respective product. Silk Meter uses port 5461.

Clients

Clients are distinct units within a Silk Central instance. A client can for example be a *customer* or a *division* within a company. Clients enhance security, but in contrast to instances, they share the same database and Silk Central services. Each client consists of the following main entities:

- User roles and permissions
- User groups and user accounts
- Projects
- Locations, execution servers and agent computers
- Products with components, versions and builds
- Global schedules

Projects

Projects in Silk Central usually reflect a software project in your company, respectively the work of a development team, with a common release date, a common source control system, common requirements, etc. Each project consists of the following main entities:

- Filters
- Attributes
- Requirement properties
- Step properties
- Notifications
- Integrated requirements and issue tracking tools

- Integrated source control system
- Data sources
- Status reasons

Important File Locations

- Instance administration and execution server log files: `C:\ProgramData\SilkCentral\log`
- Application-, front-end- and chart server log files: `C:\ProgramData\SilkCentral\instance_<instance number>_<instance name>\log`
- Location for hotfixes: `C:\Program Files (x86)\Silk\Silk Central 20.5\hotfixes`
- Configuration files: `C:\Program Files (x86)\Silk\Silk Central 20.5\instance_<instance number>_<instance name>\Conf`
- Plugins: `C:\Program Files (x86)\Silk\Silk Central 20.5\instance_<instance number>_<instance name>\Plugins`
- Office import mapping files: `C:\ProgramData\SilkCentral\instance_<instance number>_<instance name>\OfficeImportMappingFiles`

Installing Silk Central

The Silk Central installation DVD and setup program enable you to install all Silk Central software components.

To install Silk Central, your computer system must meet the minimum requirements. The installation program checks your system and optionally installs any required software.

Note: You must have administrative rights on the computer to install Silk Central.

System Requirements and Prerequisites

For optimal performance of Silk Central, we recommend the configuration outlined in this section.

Server System Requirements

System Area	Requirement
CPU	2 cores, Intel Core i5 or better
Memory	8 GB minimum
Free disc space	30 GB minimum, except for the database server
Network	100 Mbit
Operating system, database management system, Web server	See *Tested and Supported Software*.
Power Supply	Uninterruptible power supply (UPS) for all environments to reduce risks of power outages

For each additional instance that you add, at least 10 GB of additional disk space are required, and the following initial minimal memory:

- Front-end server: 500 MB
- Application server: 300 MB
- Chart server: 200 MB

Depending on your workload, these values may need to be higher.

For more information on the optimal configuration of Silk Central contact technical support or your technical account team.

Execution Server Requirements

The actual requirements and prerequisites for execution servers depend on the application under test (AUT) and the type of testing.

For load testing, refer to the environment requirements of Silk Performer. Running load tests with the minimal configuration can result in inaccurate results.

For functional testing, refer to the environment requirements of Silk Test. We recommend a minimum of 2048 MB main memory for intensive testing, such as Web browser replay.

The Linux execution server requires the latest version of Java Runtime Environment 1.8.

Proxy Server Requirements

If you plan to use Microsoft IIS for Silk Central, install the following IIS extensions before you install Silk Central:

- Application Request Routing (ARR)
- URL Rewrite

You can download the latest versions of these extensions on the *IIS Downloads* page.

Virtualization

Silk Central is tested to run on the virtual infrastructure environment VMware vSphere server.

Client-Side System Requirements

System Area	Requirement
Processor	Intel Core i3 or better
Memory	2 GB
Web browser	• Google Chrome • Internet Explorer 11 or later (no compatibility mode) • Mozilla Firefox • Microsoft Edge

The manual testing UI requires the latest version of Java Runtime Environment 1.8. For manual testing with Internet Explorer 11, a 32bit version of Java is required to be installed on the client.

Choosing the Appropriate Components for Your Operating System

Silk Central 19.5 or later internally uses the libraries of the AdoptOpenJDK instead of the Oracle JRE. This change affects all servers, which means the application server, the front-end servers, the chart server, and the execution server, as well as the communication and interaction between all servers.

There is no dependency between any installed JRE and the internally used JRE libraries, except if you require an execution server to run in 32bit mode. To start the execution server in this case, you need to use the **Execution Server Launcher** or the **Execution Server Package** and your own installed 32bit JRE. By default, execution servers are running in 64bit mode.

For the front-end server, the chart server, and the application server, the following rules apply with Silk Central 19.5 or later:

- New instances of these servers are always 64bit.
- The default instance (silk) that is created with a new installation of Silk Central is always 64bit.
- As long as an existing 32bit instance is not upgraded, it remains a 32bit instance.
- Applying a hotfix to an existing 32bit instance does not change the bitness to 64bit. The instance remains a 32bit instance.
- Upgrading an existing 32bit instance to Silk Central 19.5 or later automatically converts it to a 64bit instance.

The following rules apply for the execution of Silk Performer 19.5 or later with Silk Central 19.5 or later:

- Silk Performer 19.5 or later includes a separate JRE for the Silk Performer execution.

- To execute Silk Performer by using a different JRE than the one that is shipped with Silk Performer, add the path to the JRE as a *JREPath* tag to the `SccLtcVersionsConf.xml` file. For example:

  ```
  <JREPath>C:\Program Files (x86)\Java\MyJre8.0</JREPath>
  ```

  Note: The JRE specified in the *JREPath* tag must be a 32bit JRE.
- The full path of the *JREPath* tag in the `SccLtcVersionsConf.xml` file is `CoreVersions > Entry > JREPath`.
- When using the **Execution Server Launcher** for Silk Performer execution, Silk Performer 19.5 must be installed in the default directory `C:\Program Files (x86)\Silk\Silk Performer 19.5`. Changes to the `SccLtcVersionsConf.xml` file are overwritten by the **Execution Server Launcher** on each execution server restart.

Installing Silk Central for Evaluation

Before you start, download the Silk Central executable file or insert the Silk Central DVD into the drive.

Note: Because the installation of Microsoft SQL Server Express requires administrative privileges, the installation will fail if UAC is enabled. Disable UAC on the computer on which you want to install Silk Central for evaluation.

Set up a standalone installation with all features installed on a single machine. Standalone installations do not provide the full performance of Silk Central. Use this installation type for evaluation or demonstration purposes only.

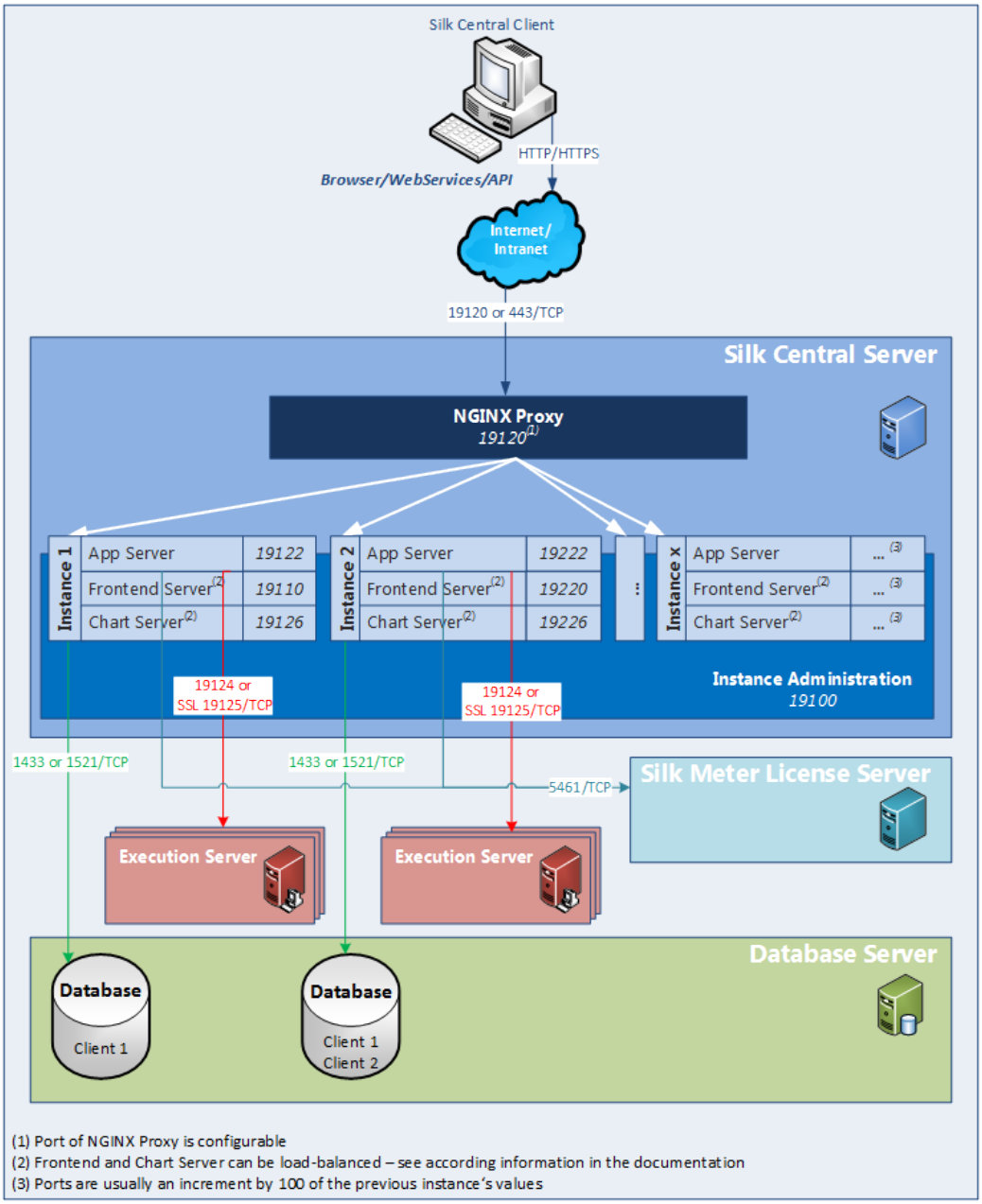
Note: The .NET Framework 3.5 SP1 setup cannot be executed during the installation of Silk Central on Microsoft Windows Server 2008 R2, Microsoft Windows Server 2008 R2 SP1, or Microsoft Windows Server 2012. If .NET Framework 3.5 SP1 is not installed on your system, and your operating system is Microsoft Windows Server 2008 R2, Microsoft Windows Server 2008 R2 SP1, or Microsoft Windows Server 2012 and you want to install the evaluation version of Silk Central , install .NET Framework 3.5 SP1 on your system with the Windows Server Manager before you install Silk Central.

1. Locate and double-click the Silk Central executable file. The InstallShield wizard opens.
2. Follow the setup wizard and confirm all default settings by clicking either **Next** or **OK** on each dialog.
3. On the **Select Licensing Mode** dialog, keep the default setting (**Evaluation**).

   Silk Central requires a database repository. For the purpose of evaluation we recommend you use Microsoft SQL Server Express, which is installed as part of Silk Central. Make sure the **Install Microsoft SQL Server 2008 Express SP1** checkbox is checked.
4. Complete the installation by clicking **Next**.

Installing Silk Central

Before you start, download the Silk Central executable file or insert the Silk Central DVD into the drive. Make sure that your system meets the *System Requirements and Prerequisites*.



1. Locate and double-click the Silk Central executable file.

   If you have a Silk Central DVD, insert your DVD. If the setup program does not start automatically, manually start the Silk Central setup program by choosing **Start** > **Run** and entering `<DVD drive>:\setup.exe`.

   The InstallShield wizard opens.
2. The welcome page of the wizard opens. The wizard guides you through the setup procedure. Click **Next** to continue.
3. Select the language that you want to use, and then click **Next**. The **License Agreement** opens.
4. Read the license agreement carefully. If you accept the terms of the agreement, click **I accept the terms of the license agreement**. The **Setup Type** page opens.
5. To install the Silk Central Execution Server, check the **Install Execution Server** check box. To use Microsoft Internet Information Services (IIS), check the **Use Microsoft Internet Information Services** check box.

The default installation destination is displayed in the **Destination path** section of the **Setup Type** page. To change the default installation directory, perform the following steps:

a) Click **Browse**. The **Choose Folder** dialog box opens.
b) Specify the folder in which you want to install Silk Central, and then click **OK** to return to the **Setup Type** page.

Note: Silk Central must be installed on a local drive. An error message appears if you specify an invalid installation destination.

6. Click **Next** to continue. The **Installation Options Summary** page lists the settings that you selected.
7. Review the provided information and perform one of the following steps:

   - To change any settings, click **Back** to return to the appropriate page.
   - If you are satisfied with the settings, click **Next** to start the installation process.

   The status bar on the **Setup Status** page provides information about the installation process. Upon completion, the **Select licensing mode** page opens.
8. Click one of the following option buttons:

   - **Evaluation** – Installs an evaluation version of Silk Central, which grants you full product functionality for 45 days. The usage is limited to 10 Silk Central users and 10 Issue Manager users. To upgrade to a full version at a later point in time, contact your sales representative. Check the **Install Microsoft SQL Server 2008 Express SP1** check box to additionally install Microsoft SQL Server 2008 Express SP1.
   - **Licensed** – Installs an unrestricted version of Silk Central, which requires a license.
9. Click **Next**.

   Depending on the components you have selected for installation, the licensing page opens. If you have not installed any of the components that require licensing and the page does not open, proceed to the next step.

   To install the license file, perform the following steps:

   a) Click **OK** to specify the location of your license file.

      The license utility checks your local system for the existence of Silk Meter license server configuration files. If the files are found, the configuration and type of license server are displayed and used for licensing. If no configuration data is found, the **Select Silk Meter License Server** page is displayed with the default settings.

      This page provides generic information about Silk Meter licensing. For detailed information on Silk Meter licensing, click **Open Silk Meter ReadMe**. This action opens the Silk Meter documentation in your default browser.

      Note: Open Silk Meter ReadMe is not available if the document is not available in the installation source directory. This document is typically unavailable when installing a Silk Central Web package.

   b) From the **Application** list box, select **Silk Central** as the application you are licensing.
   c) Click one of the following option buttons:

      Using local or remote server

      In the **License Server Host** field, type the name of the computer on which Silk Meter is installed. Do not change the default port number, `5461`, unless your network administrator has defined a different port. Click **Apply** to generate your license server configuration. Click **Test Connection** to verify that a Silk Meter server is accessible on the specified host and port. Testing the connection to the license server might fail during installation as required system libraries, which are installed later with the software package, might not yet be available.

      Note: In some cases, specifying the simple name of the license server in the **License Server Host** field, such as `licenseserver`, might not work. A message box stating `there is no license server running on`

`the hostname you specified` opens. To resolve this issue, specify the hostname by using a fully qualified name, such as `licenseserver.mycompany.com`.

Not using server (standalone)	Runs Silk Meter standalone. You are prompted to import a Silk Meter license file. Click **Yes** and specify the location of your license file.

d) Click **Close** to return to the InstallShield wizard.

10. Click **Finish** to complete the installation.

Note: If the InstallShield wizard fails to update a file during the installation because a system library is locked by Windows, or if the InstallShield wizard detects that the system must be restarted, you are prompted to restart your computer. If you do not restart your computer, you might experience problems when accessing Silk Central.

The **Instance Administration** page appears, which enables you to configure your Silk Central installation. For additional information, see *Managing Instances*.

Installing a Windows Execution Server

Install an execution server on each point of presence (POP) that you want to use as a remote Silk Central execution server. The execution server executes Silk Central tests on remote computers.

1. In the Silk Central menu, click **Help** > **Tools** > **Windows Execution Server** and download the Windows execution server package.
2. Locate and double-click the Silk Central executable file. The InstallShield wizard opens.
3. Follow the instructions on the Installation Wizard.
4. Click **Finish** to complete the installation.

Note: If the InstallShield wizard fails to update a file during the installation because a system library is locked by Windows, or if the InstallShield wizard detects that the system must be restarted, you are prompted to restart your computer. If you do not restart your computer, you might experience problems when accessing Silk Central.

Installing a Windows Execution Server in Silent Mode

Before you start, download the Silk Central executable file or insert the Silk Central DVD into the drive.

Install an execution server on each point of presence (POP) that you want to use as a remote Silk Central execution server. The execution server executes Silk Central tests on remote computers.

To install a Windows execution server in silent mode, enter the following command from a DOS shell or batch file: `WindowsExecServer.exe -s -c -f"<PATH_TO_EXTRACTED_FILES>" -a /s /f1"<PATH_TO_EXTRACTED_FILES>\Install.iss" /v"/qn PROP_SILENTMODE=1 PROP_LANGUAGE=<LOCALE>"`.

Set the parameter *PROP_SILENTMODE* to 1 to install the execution server in silent mode. Choose the appropriate of the following values for the parameter *PROP_LANGUAGE* to define the language of the installation:

Value	Description
EN	English
DE	German

Value	Description
FR	French
JA	Japanese
ZH	Chinese (Simplified)

For example, the following command installs an execution server in English:

```
 WindowsExecServer.exe -s -c -f"c:\temp\SilkCentralExecSrv" -a /s /f1"c:\temp
\SilkCentralExecSrv\Install.iss"
/v"/qn PROP_SILENTMODE=1 PROP_LANGUAGE=EN"
```

Installing a Linux Execution Server

This task addresses Silk Central users who use Linux or Unix.

Install an execution server on each point of presence (POP) that you want to use as a remote Silk Central execution server. The execution server executes Silk Central tests on remote computers.

1. In the Silk Central menu, click **Help** > **Tools** > **Execution Server Package** and download the Linux execution server package.

   You could also use CURL to download the package:

   ```
   curl http://schost:port/silkroot/tools/SilkCentralExecServer.tar.gz --
   output SilkCentralExecServer.tar.gz
   ```

   Note: The Linux execution server package does not include a Java Runtime Environment (JRE). Ensure that you have the latest version of JRE 1.8 installed. You can download the JRE from *AdoptOpenJDK*.
2. Unpack the `tar.gz` package using the following command:

   ```
   tar xfz SilkCentralExecServer.tar.gz
   ```
3. Use the following command to navigate to the directory where the package file was extracted:

   ```
   cd SilkCentralExecServer
   ```
4. Start the execution server using the following command:

   ```
   ./startExecServer.sh
   ```

   Note: Cache information and log files are stored in the sub-folder `ExecServerData` of the current directory. The `ExecServer.log` log file is also accessible through the Silk Central web interface.

Note: The source control systems currently supported for Linux execution servers are Subversion, Git and the Apache Commons virtual file system (VFS).

Tests created with the following technologies are not supported for execution on a Linux execution server:

- Silk Test technologies that are not supported by Silk Test for execution on Linux.
- .NET Explorer.
- Unified Functional Testing.
- MSTest.
- NUnit.
- Silk Performer.
- TestPartner.
- Windows Script Host.

These test types are platform-specific for the Microsoft Windows operating system.

Installing a Command-Line-Driven Execution Server

Install a command-line-driven execution server to execute tests from a virtual infrastructure where execution servers are started and stopped on demand.

From Silk Central, you can download an executable JAR that starts a new execution server.

1. In the Silk Central menu, click **Help** > **Tools** > **Execution Server Launcher** to download the executable JAR that starts a new execution server.

   Note: The latest version of Java 1.8 needs to be installed on the machine from which you want to start the execution server. The Silk Central application server needs permission to access the execution server port.

   The launcher works for both Linux and Windows machines.
2. Locate the `sc-execserverlauncher.jar` and use a command-line call to start an execution server.

   Specify the following parameters.

Parameter Name	Long Parameter Name	Description
-u	--sc.url	The URL to the Silk Central server, in the format *http://host:port[/instance]*. The execution server machine needs access to the specified URL.
-t	--sc.token	The Silk Central web-service token, used for user authentication.
-l	--sc.location	The name of the server group (location) to which the execution server will be added.
-h	--sc.externalhost	*Optional:* The host name used by Silk Central to connect to this execution server. For example, if the execution server is started in Docker, specify the host where the container is accessible.
-p	--sc.externalport	*Optional:* The port used by Silk Central to connect to this execution server. The default port is 19124. For example, if the execution server is started in Docker, specify the published port of port 19124. The Silk Central application server needs permission to access this port.
-k	--sc.keywords	*Optional:* A comma-separated list of keywords that describe this execution server.
-n	--sc.execservername	*Optional:* The name the execution server should be registered with.
-rt	--sc.responsivenesstimeout	*Optional:* The timeout in seconds after which Silk Central sends an email to the Silk Central administrator if the execution server does not respond. If you do not want Silk Central to send emails in such a case, set the timeout to 0.
-sr	--sc.skipselfregistration	*Optional:* Suppress self-registration of the execution server. The options --sc.token and --sc.location are not required when this option is used.
-ssl	--sc.usessl	*Optional:* Whether to connect to the execution server through SSL. Boolean.
-ut	--sc.uptime	*Optional:* The time in hours after which the execution server is shut down and deregistered from Silk Central. If the server is executing some job at this time, the shutdown waits for the execution to finish first. The default value is 0, meaning that the execution server is never shut down and deregistered from Silk Central.
-esp	--sc.execserverport	*Optional:* The port on which the execution server listens for connections from the application server. The default port is port 19124 for non-SSL connections and port 19125 for SSL connections.

Parameter Name	Long Parameter Name	Description
		Specify this parameter if multiple execution servers should run on the same machine in parallel. In that case, a different port must be used for each execution server. This parameter might be useful if the execution servers are used by different Silk Central instances or installations, or with different operating system permissions. **Note:** Micro Focus recommends not to run more than one execution server for the same instance. Instead of running multiple servers, disable the **Exclusive Execution** option for the execution plans to enable parallel execution on the same execution server.

For example, such a call might look like:

```
java -jar sc-execserverlauncher.jar -u http://sc-host:19120 -t
d28930f4-9c77-4fc7-bc1d-aac4cd235d3 -l Local -ssl true
```

After upgrading to a newer version of Silk Central, the launcher automatically downloads the new execution server version and restarts the execution server. Additionally, whenever the execution server is terminated, for example because of a crash, the launcher will attempt to restart the execution server.

Installing a Hotfix

When a hotfix becomes available, update your instances to the latest hotfix.

1. On the computer where Silk Central is installed, locate and double-click the setup file.
2. Follow the instructions on the Installation Wizard.
3. When the installation has completed, open a browser and navigate to the URL `http://localhost:19100/` (if it doesn't open automatically).

   Note: You cannot access the **Instance Administration** page from a remote computer.

   The **Instance Administration** page appears. At this point you should reset your browser cache, otherwise fixes in JavaScript and style sheets may not get activated.
4. In the **Version** column, click the **Install Hotfix <version>** link to start the upgrade. A dialog appears to activate maintenance mode.
5. Enter a notification text that users will see when they try to access Silk Central, for example: `Silk Central is currently unavailable as we're performing updates. The system will be back online again shortly.` Click **Yes** to activate maintenance mode and start the upgrade.
6. Once the update has completed, click ▶ to start the instance again.

Repeat the **Instance Administration** steps for each instance that you want to update.

Tip: Remind your users to reset their browser cache, otherwise fixes in JavaScript and style sheets may not get activated.

Upgrading to Silk Central 20.5

The Silk Central 20.5 setup program automatically removes the existing installation before upgrading to Silk Central 20.5. Do not use the Windows **Add or remove programs** feature to remove the previous Silk Central installation, as this would delete your customized configuration files.

1. Make a backup copy of your Silk Central database before you start upgrading to a new version.
2. If you have enabled SSL, make a backup copy of your certificate file. Re-import the certificate into the keystore `C:\Program Files (x86)\Silk\Silk Central 20.5\instance_<instance number>_<instance name>\lib\jre64\lib\security\cacerts`.

   For additional information, see *Enabling Secure Web Server Connections with SSL*.
3. Install Silk Central. This will install the NGINX proxy and the **Instance Administration**.

   To install an execution server on the same computer as one of the previously mentioned components, install the execution server together with the other components.

   The database settings are automatically updated. For detailed information about advanced settings in the configuration files, see *Configuring Advanced Settings*.

   Note: For large databases, a small database transaction log size may result in an error during the update. To prevent the error, set the size of the database transaction log to 5 GB.
4. When the installation has completed, open a browser and navigate to the URL `http://localhost:19100/` (if it doesn't open automatically).

   Note: You cannot access the **Instance Administration** page from a remote computer.

   The **Instance Administration** page appears. At this point you should reset your browser cache, otherwise fixes in JavaScript and style sheets may not get activated.
5. In the **Version** column, click the **Upgrade to <version>** link start the upgrade. A dialog appears to activate maintenance mode.
6. Enter a notification text that users will see when they try to access Silk Central, for example: `Silk Central is currently unavailable as we're performing updates. The system will be back online again shortly.` Click **Yes** to activate maintenance mode and start the update.
7. Once the update has completed, click ▶ to start the instance again.

Repeat the **Instance Administration** steps for each instance that you want to update.

Tip: Remind your users to reset their browser cache, otherwise fixes in JavaScript and style sheets may not get activated.

Silk Central Licensing

This section describes how to obtain a license policy for Silk Central and how to install Silk Meter. You must have administrator privileges to install Silk Meter.

Note: Silk Central requires Silk Meter version 2008 or later as well as a Silk Central license policy.

Install Silk Meter once per license server. If you have multiple license servers, you need multiple license policy files, each one tied to a particular license server. A single Silk Meter license server can administer license policies for multiple products.

If you have received a Silk Central license policy, install the license policy on your license server. If you have not received a license policy, generate a license policy.

License Handling

Silk Central provides different types of licenses.

Per-User Licenses

These licenses are checked out from the license server as soon as a user enters a certain area of Silk Central:

License Type	Area
Test Manager	This license is checked out when you access a test management area for the first time after your login. Silk Central test management areas are: **Requirements**, **Tests**, **Execution Planning**, **Tracking**, **Issues** (excluding the Issue Manager area), and **Reports**.
Manual Testing	This license is checked out when you open the **Manual Testing** window. A **Manual Testing** license is checked out when a test is downloaded for offline execution. The license is checked back in when results are uploaded.
Issue Tracking	This license is checked out when you access Issue Manager.

Note the following:

- When you click **Log out** (**User** > **Log out**), the licenses are checked in to the license server again, except checked out manual testing licenses for offline testing.
- If you do not log out (and just close the browser window), the license will only be checked in when the session expires.

The **About** page (**Help** > **About**) displays how many licenses are currently used and how many licenses are available for the client you are currently logged in to.

Site Licenses

These licenses enable a specific feature set for all users, without limitations:

License Type	Area
Mobile Testing	This license enables testing on mobile devices (physical devices, emulators and simulators) for manual, automated, and configuration testing.

Generating a Silk Central License Policy

To run Silk Central, you need a valid license. If you have purchased Silk Central, you can use our online license generator to generate a license policy file. The online license generator requires an SSL-capable browser, such as Firefox or Internet Explorer. You will receive an email with instructions on how to generate your license policy file. If you did not receive these instructions, contact customer care at *http://support.microfocus.com*.

Finding the Host ID

To obtain a license policy file, you need to know the host ID of the machine on which you want to install the licenses. For floating licenses this is a license server with Silk Meter installed. For node-locked licenses this is typically the controller machine.

1. On the machine, open a command prompt and enter the command `ipconfig/all`. The network adapters and additional information is listed.
2. Note the host ID, which is the `MAC Address` or `Physical Address` of your LAN card, for example `00-BF-00-1C-D3-3D`.

   Tip: Depending on your system setup, including virtual machines and VPN connections, your computer might have several network adapters with different MAC addresses. Be sure to note the host ID of your physical LAN card.

Silk Meter Installation

If you already have a Silk Central license policy file, you can install it when you install Silk Meter. If you do not have a valid Silk Central license, access the online License Generator to generate a license policy file.

To install and run Silk Meter on your license server, no license policy file is required. However, you must import a license policy file before you can run Silk Central. You can import a license policy file using the Silk Meter **Policy Administrator**.

If you have multiple license servers, you need multiple license policy files, each one tied to a particular license server. A single Silk Meter license server can administer license policy files for multiple products.

Silk Meter License Server Requirements

Before installing Silk Meter, refer to the *Release Notes* to ensure that the license server meets the requirements.

Uninstalling a Previous Version of Silk Meter

If a previous version of Silk Meter is installed on your license server, you must uninstall it before the latest version of Silk Meter can be installed.

1. Choose **Start** > **Programs** > **Silk** > **Silk Meter** > **Uninstall** .
2. Click **Yes** to uninstall Silk Meter. The **Remove Settings** dialog box opens.
3. Click **No** to keep your Silk Meter settings.

   Attention: You must click **No** to preserve license policies that currently exist on your Silk Meter license server.
4. Reboot your computer.

Silk Meter is now uninstalled, and you can install the latest version of Silk Meter.

Installing Silk Meter on Your License Server

Before installing Silk Meter, verify the following information:

- Your user account possesses administrator privileges.
- An instance of Silk Meter is not installed on your license server.

1. Visit the *product updates site* and search for Silk Meter.
2. Download and save the latest **Silk Meter Installation Files**.
3. Navigate to the location where you saved the .exe file and double-click it. For a standard installation, follow the Silk Meter installation wizard by using the default options.

   Important: If setup prompts you to restart the computer, make sure to do so.

Silk Meter License Server Configuration

To run any version of Silk Central, Silk Meter must be installed and configured on a computer within your network.

The communication process between Silk Central and Silk Meter relies on the following files and variables:

- *SILK_CONFIG_PATH* environment variable
- `CosLicensingService.ref` file
- `CosPropertyService.ref` file
- `ls_segue.ref` file

- `silkmeter.cfg` file

Important: Do not delete these files.

The Silk Central setup program creates these objects based on the values you enter in the fields of the **Select Silk Meter License Server** utility.

Modifying Your License Server Configuration

Use the **Select Silk Meter License Server** utility to modify or repair your license server configuration. This utility is installed with your Silk Central installation.

1. Choose **Start** > **Programs** > **Silk** > **Silk Central 20.5** > **Administration Tools** > **Change your License Server Configuration** . The **Select Silk Meter License Server** utility opens.
2. In the **Application** list box, select the product for which you want to configure the license server.
3. Click the **Using local or remote server** option button to configure a Silk Meter license server.
4. In the **License Server Host** field, type the computer name of the Silk Meter license server.
   Unless your network administrator has defined a different port, do not change the **Port Number**.
5. Click **Apply** to activate the license server configuration.
6. Click **Test Connection** to verify that a Silk Meter server is accessible on the specified host and port. If the connection is successful, the **Status** field displays a SUCCESS message.

   Note: In some cases, specifying the simple name of the license server in the **License server host** field, such as `licenseserver`, might not work. A message box stating `Connection to Silk Meter license server failed` opens. To resolve this issue, specify the hostname by using a fully qualified name, such as `licenseserver.mycompany.com`.
7. Click **Close** to complete the license server configuration.

Tested and Supported Software

This section lists the software with which Silk Central 20.5 has been tested as well as the software that Silk Central supports.

Operating System Support

- Microsoft Windows Server 2012
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2016
- Microsoft Windows Server 2019
- Microsoft Windows 8.1 32-bit/64-bit (execution server)
- Microsoft Windows 10 32-bit/64-bit (execution server)
- Android 5.x, 6.x, 7.x, 8.x, 9.x, 10.x (mobile device testing)
- iOS 10.x, 11.x, 12.x, 13.x (mobile device testing)

Important: *Update for Universal C Runtime in Windows* is required for all Microsoft Windows operating systems. For Microsoft Windows Server 2016 or later, the installation option **Windows Server (Server with Desktop Experience)** is required.

Linux Operating System Support

Silk Central supports Linux operating systems only for the execution server.

- Debian

- Red Hat Enterprise Linux
- SUSE Linux
- Ubuntu

Web Browser Support

- Google Chrome
- Internet Explorer 11 or later (no compatibility mode)
- Mozilla Firefox
- Microsoft Edge

Web Server Support

- IIS 8 32 bit/64 bit
- IIS 10 32 bit/64 bit

Database Management System Support

- Microsoft SQL Server 2014 Service Pack 3
- Microsoft SQL Server 2016 Service Pack 2
- Microsoft SQL Server 2017
- Oracle 11g (version 11.2.0.4). Oracle RAC is not supported.
- Oracle 12c (version 12.2.0.1). Oracle RAC is not supported.

Integrated Micro Focus Software Support

- AccuRev 7.2
- Caliber 11.4, 11.5
- Mobile Center 2.51 or later
- Silk Performer 20.5
- Silk Test 20.5
- StarTeam 15.x, 16.x, 17.0
- Silk TestPartner 6.3
- Unified Functional Testing (UFT) 14.0

Integrated Third-Party Software Support

- Apache Commons Virtual File System (VFS)
- Atlassian JIRA 6, 7, 8 (versions 6 and 7 are supported but not tested)
- Atlassian JIRA Agile 6, 7, 8 (versions 6 and 7 are supported but not tested)
- Bugzilla 4.4.13, 5.0.4
- CA Agile Central
- Git 2.20.1
- IBM Rational ClearQuest 8.0
- IBM Rational DOORS 9.5, 9.6
- IBM Rational DOORS Next Generation 6.0
- JUnit 4.x, 5.x
- The latest version of Java Runtime Environment 1.8
- Microsoft Office Excel (.xlsx) for importing tests and requirements
- Microsoft Office Word (.doc, .docx) for importing requirements
- Microsoft Visual Studio/Visual Studio Test Agent 2015
- NUnit 2.6.4, NUnit Console and Engine 3.8
- SAP Solution Manager 7.2

- Subversion 1.9
- Team Foundation Server 2015, 2017
- VersionOne Enterprise Edition
- VMware vCloud Director 5.5

Configuring and Managing the Infrastructure

An instance is an independent set of Silk Central services (application server (AS), front-end server (FE) and chart server (CS)), with their own database and execution server (ES) connections. By default, Silk Central creates a single instance called *silk* for you. The default URL is `http://<computer name>:19120/login` (no port information required if Silk Central runs on IIS).

Setting up a Secure Silk Central System

This section explains how to set up a secure Silk Central system.

General Guidelines

After having installed Silk Central, you should consider the following guidelines to set up Silk Central in a secure environment.

- First of all, change the default password of the `sysadmin` user. For detailed information, see *System Administrator*.
- Configure LDAP authentication to enable Silk Central logins through an LDAP server. For detailed information, see *LDAP Authentication*.
- If multiple groups will be working with Silk Central, ensure that your users can only access the data they are supposed to see by creating instances or clients. For detailed information, see *Managing Instances* and *Managing Clients*.
- To ensure that running reports with advanced queries will not change any data in the database, consider creating and using a read-only database user. For detailed information, see *Database Page*.
- Configure your firewall so that only the ports that are required by Silk Central are open. For detailed information on which ports Silk Central uses, see *Silk Central Architecture*.
- Backup your database regularly.
- Use the most current and supported operating system versions and ensure that updates are being applied regularly.
- Use the latest versions and hotfixes of Silk Central. Register to Micro Focus SupportLine at *http://supportline.microfocus.com* for up-to-date support news and access to other support information.

Enabling Secure Web Server Connections with SSL

If you intend to let users only access Silk Central through secured connections (SSL), enable Silk Central to use Secure Sockets Layer (SSL).

For additional information, see also *Communicating with an External System Over SSL*, *Enabling BIRT Reports in SSL Environments* and *Configuring a Non-Standard SSL Port for Execution Servers*.

1. Copy your certificate and key files to the front-end server computer.
2. Open the file `nginx.conf.template` in `C:\ProgramData\SilkCentral\InstanceAdministration\nginx\conf` with a text editor.
3. Uncomment the following lines by removing the #:

```
#listen   443 ssl;
#ssl_protocols TLSv1.2 TLSv1.1 TLSv1;
#ssl_certificate    "C:/.../ssl/host.cert";
#ssl_certificate_key    "C:/.../ssl/host.key";
```

```
#add_header Strict-Transport-Security "max-age=31536000; includeSubDomains"
always;
```

4. Set the path for `ssl_certificate` and `ssl_certificate_key` to where you copied your certificate and key files. Specify the path using slashes instead of backslashes.
5. If you want to allow only SSL connections, comment the line `listen 19120;` by adding a #.
6. *Optional:* To configure a redirection from the non-secure port to the secure one, add a new `server` section with the following syntax:

```
server {
  listen <non-secure port>;
  server_name localhost;
  return 301 https://$host$request_uri;
  }
```

7. To apply your changes:
   a) Open a browser window.
   b) Type *localhost:19100* into the address bar.
   c) Stop and restart one of the Silk Central instances.

Enabling BIRT Reports in SSL Environments

After you have configured Silk Central to use a secure web server connection with SSL, enable BIRT reports to work in this environment.

1. Stop the chart server service of the instance you want to configure, using the **Instance Administration** page.
2. Use OpenSSL to create a PKCS #12 key store with the following command line: `openssl pkcs12 -export -in ./host.cert -inkey ./host.key > ./host.p12`
   Example:

```
openssl pkcs12 -export -in C:/ProgramData/SilkCentral/ssl/host.cert -inkey
C:/ProgramData/SilkCentral/ssl/host.key > C:/ProgramData/SilkCentral/ssl/
host.p12
```

3. Convert the keystore `host.p12` into a Java key store with the following command line: `keytool.exe -importkeystore -srckeystore ./host.p12 -destkeystore ./host.jks -srcstoretype pkcs12`
   Example:

```
"C:\Program Files (x86)\Silk\Silk Central
20.5\instance_1_silk\lib\jre\bin\keytool.exe"
-importkeystore -srckeystore C:/ProgramData/SilkCentral/ssl/host.p12 -
destkeystore
C:/ProgramData/SilkCentral/ssl/host.jks -srcstoretype pkcs12
```

4. Add the following lines to the chart server's process configuration file `sc_ChartServer.processconfig`, located at `C:\Program Files (x86)\Silk\Silk Central 20.5\instance_<instance number>_<instance name>\Conf`:

```
<Service>
  <SystemProperties>
          ...
             <SystemProperty name="javax.net.ssl.trustStore" value="<path
to host.jks file>" />
             <SystemProperty name="javax.net.ssl.trustStorePassword"
value="<password>" />
       </SystemProperties>
</Service>
```

   Example:

```
<Service>
  <SystemProperties>
          ...
```

```
            <SystemProperty name="javax.net.ssl.trustStore" value="C:/
ProgramData/SilkCentral/ssl/host.jks" />
            <SystemProperty name="javax.net.ssl.trustStorePassword"
value="changeit" />
        </SystemProperties>
</Service>
```

5. Restart the chart server service.

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 Silk Central 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 Silk Central, 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.

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 Silk Central.

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 Central 20.5 Execution Server\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.

Communicating with an External System Over SSL

If the certificate of the host you want to connect to is self signed, you may receive the following error message:
sun.security.provider.certpath.SunCertPathBuilderException: unable to find valid certification path to requested target

Note: This error message does not display for valid certificates, which are certificates that are signed by Certificate Authorities.

To use a server with a self-signed certificate, you need to perform the following steps:

1. Download the SSL certificate from the server.

   Use a browser to view the certificate and export it. For example, in Mozilla Firefox, navigate to **Tools** > **Page Info** > **Security** > **View Certificate** > **Details** > **Export**.
2. Start the key- and certificate-management tool *Keytool*.

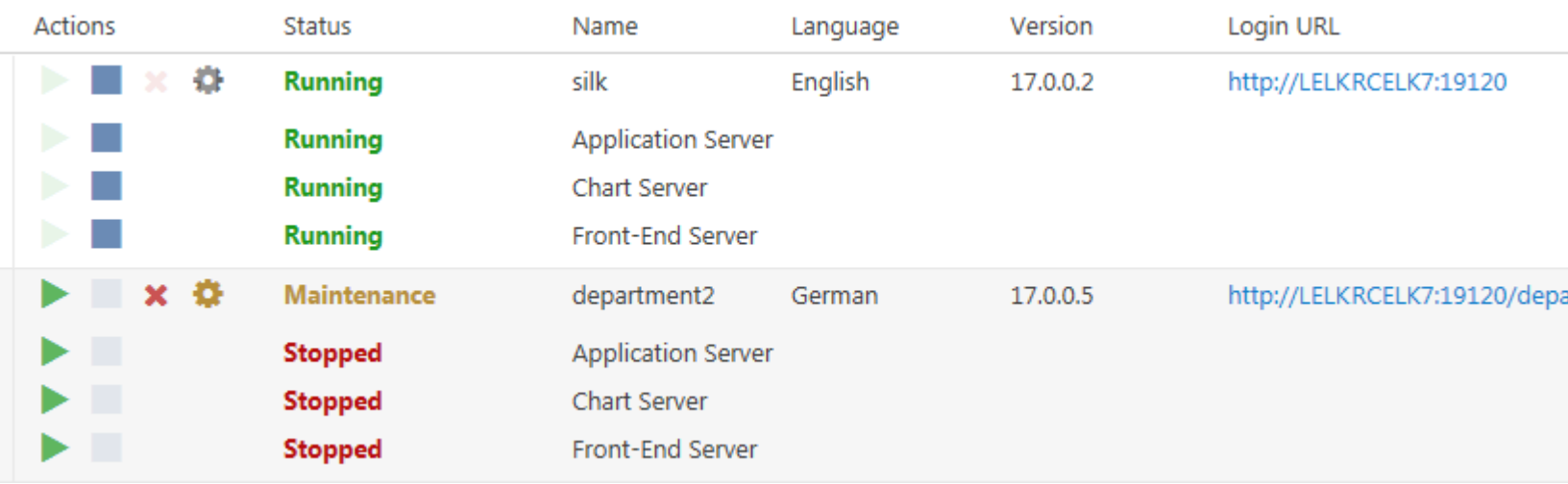
   Keytool is part of your JRE installation, and is located in your JRE installation folder, for example `C:\Program Files (x86)\Silk\Silk Central <version>\ instance_<instance number>_<instance name>\lib\jre64\bin`. For additional information on Keytool, refer to the *Java SE Technical Documentation*.
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 Central <version>
   \instance_<instance number>_<instance name>\lib\jre64\lib\security\cacerts"
   ```

   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.

Managing Instances

Create additional instances if you need to physically separate test data and processes of your various clients for increased data security and reduced influence of independent user groups on each other (for example departments). With the help of clients you can further logically separate the data of one instance within one database.



Actions	Status	Name	Language	Version	Login URL
	Running	silk	English	17.0.0.2	http://LELKRCELK7:19120
	Running	Application Server			
	Running	Chart Server			
	Running	Front-End Server			
	Maintenance	department2	German	17.0.0.5	http://LELKRCELK7:19120/depa
	Stopped	Application Server			
	Stopped	Chart Server			
	Stopped	Front-End Server			

Managing Instances

Instances and their Silk Central services are managed through a common user interface called **Instance Administration**, which you can access only on the server where Silk Central is installed, using the URL `http://localhost:19100`. You cannot access the **Instance Administration** page from a remote computer. You can perform the following actions on an instance or the individual services:

- Click or to stop or start services individually. If you stop or start an instance, all services of the instance are stopped or started, respectively.
- Click to delete an instance. Use this option only if you are sure that an instance is not required anymore! This action does not remove the data in the database.

  Note: To assign an execution server to a different application server, you need to delete the following file on the computer where the execution server is installed: `C:\ProgramData\SilkCentral\AgentBase\ItemObjects.ser`.
- Click to configure instance settings.

Maintenance Mode

Before you perform instance maintenance during which a Silk Central instance is no longer accessible to users, for example when installing a new hotfix or adjusting the settings of a service, you can notify your Silk Central users that the instance is under maintenance:

1. On the **Instance Administration** page, click to open the **Settings** dialog.
2. On the **Maintenance** tab, check the **Activate maintenance mode** check box.
3. Enter a notification text that users will see when they try to access Silk Central, for example: `Silk Central is currently unavailable as we're performing updates. The system will be back online again shortly.`
4. Click **OK**.
5. When you are done with the maintenance and all services are running again, deactivate the maintenance mode to allow your users to access Silk Central again.

JMX Measures

To access information or perform operations through JMX, you need the JMX connection string. Click to open the **Settings** dialog. On the **Servers** tab, select the required server and copy the **JMX connection** string. For additional information, see *Configuring JMX Settings*.

Creating a New Instance

Click **New Instance** to create an additional instance. Make sure you give the instance a meaningful name, as this name will be used to identify the instance's services and files, and it is part of the URL that users use to access the instance.

For each additional instance that you add, at least 10 GB of additional disk space are required, and the following initial minimal memory:

- Front-end server: 500 MB
- Application server: 300 MB
- Chart server: 200 MB

Depending on your workload, these values may need to be higher.

For more information on the optimal configuration of Silk Central contact technical support or your technical account team.

Installing a Hotfix

When a hotfix becomes available, update your instances to the latest hotfix.

1. On the computer where Silk Central is installed, locate and double-click the setup file.
2. Follow the instructions on the Installation Wizard.
3. When the installation has completed, open a browser and navigate to the URL `http://localhost:19100/` (if it doesn't open automatically).

   Note: You cannot access the **Instance Administration** page from a remote computer.

   The **Instance Administration** page appears. At this point you should reset your browser cache, otherwise fixes in JavaScript and style sheets may not get activated.
4. In the **Version** column, click the **Install Hotfix <version>** link to start the upgrade. A dialog appears to activate maintenance mode.
5. Enter a notification text that users will see when they try to access Silk Central, for example: `Silk Central is currently unavailable as we're performing updates. The system will be back online again shortly.` Click **Yes** to activate maintenance mode and start the upgrade.
6. Once the update has completed, click to start the instance again.

Repeat the **Instance Administration** steps for each instance that you want to update.

Tip: Remind your users to reset their browser cache, otherwise fixes in JavaScript and style sheets may not get activated.

Starting or Stopping a Local Execution Server Service

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

1. Double-click the **Silk Central Service Manager** tray icon in the Windows task bar. The **Silk Central 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 Silk Central 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.

Front-End Server Load Balancing

You can use load balancing to spread the load (website traffic) between several machines that are hosting a front-end server.

While it used to be a common practice to address performance issues with front-end server load-balancing to distribute the load (website traffic) between several front-end servers installed on separate machines, the switch to 64-bit JVM and the advancement of the architecture, in the direction of smaller self-contained units (instances), make this practice - even for larger installations - rather unnecessary.

It is more beneficial to focus on the performance of the machine that is hosting the database server and the database in general. For large testing environments, Micro Focus recommends increasing the amount of independent Silk Central instances, where each instance has a dedicated database.

Configuring Load Balancing for Front-End Servers

If you have a running Silk Central instance and experience issues with insufficient memory that cannot be further increased, you can set up additional front-end servers to distribute user sessions and consumed memory across multiple machines.

Note: When using load-balancing architectures, multiple front-end servers will still be used through a single NGINX proxy and will still access the same application server and database. There is no reduction of load from that perspective.

To set up and configure additional front-end servers for load-balancing:

1. If you have installed Silk Central on a server, enable access to the application server on this server from any host:
   a) Stop the application server on this server.
   b) In the installation directory of the Silk Central instance, navigate to the configuration file `conf\SccAppServerBootConf.xml`.
   c) Remove the entry `<RegistryHost>127.0.0.1 </RegistryHost>` and save the configuration file.
   d) Re-start the application server.
2. Use the Silk Central setup to install Silk Central on all machines that you want to add as front-end servers for load-balancing.
3. When setup is completed, navigate to the **Instance Administration** (`http://localhost:19100`) on the machine.
4. As you just need a front-end server, stop the application server and the chart server of the instance you want to use for load balancing.
5. Click to open the **Settings** dialog of this instance. On the **Servers** tab, select the front-end server and copy the **front-end server port**.
6. Switch to the machine that is used as the application server and navigate to the **Instance Administration** (`http://localhost:19100`).
7. Click to open the **Settings** dialog of your performance lacking instance and activate the maintenance mode.
8. On the file system, open the NGINX custom properties file (`C:\ProgramData\SilkCentral\InstanceAdministration\nginx\conf\nginxCustom.properties`) and add the URL of the front-end server on *Server B* (`<SERVER_NAME>:<PORT>`), using the copied **front-end server port**.

   Notation: `frontendservers.<INSTANCE_NAME>=<FE_URL1>{,<FE_URL2>,...,<FE_URLX>}`

For example: `frontendservers.silk=localhost:19110,silkserver2:19320`

Attention: Because of NGINX restrictions it is not possible to use port `19120` of a front-end server. Always get the port from the settings dialog as described in step 4.

9. Go back to the **Instance Administration** page and click to open the **Settings** dialog of your performance lacking instance. On the **Servers** tab, select the application server and copy the **application server port**.
10. To establish the connection between the front-end server and the application server, open a web browser and navigate directly to the machine that hosts the front-end server by using `http://<Server B>:<front-end server port>`. Make sure you use the port from the settings dialog, not `19120`!
11. On the application server connection page, enter the **Host or IP-address** and the copied **application server port** of the machine that hosts the application server.
12. Go back to the **Instance Administration** page and deactivate the maintenance mode. This will update the NGINX configuration.

When your users now access the instance using the same URL as before, they are automatically balanced between the front-end server on the initial machine, which also hosts the application server, and the new front-end server machine.

Managing Clients

Use the **System Administration** area to configure the clients of Silk Central. Configuring clients includes the following activities:

- Creating, connecting, and disconnecting databases.
- Creating and managing clients.
- Configuring the infrastructure of the Silk Central client (chart server, email server, and proxy connections).
- Maintaining system services by analyzing diagnostic information and system log files.

System Administrator

The System Administrator is the only user who can access the **System Administration** area and the System Administrator can access only this area. This user has no access to the actual Silk Central user interface.

Access the **System Administration** area by logging in with the following credentials:

- username: `sysadmin`
- password: `sysadmin`

Important: Change this default password as soon as possible. We recommend doing this after you have connected to a Silk Central database for the first time. To change the password, click **Change Your Password** in the menu of the **System Administration** area (on the top right). The username cannot be changed.

If no database is connected, the System Administrator will automatically be directed to the **System Administration** area.

Databases

Silk Central uses databases to store, maintain, and analyze data. You must establish a connection to a database before you can work with Silk Central. You can establish multiple databases, but only one database at a time can be connected. To connect to a new database, you must first disconnect from the current one.

To configure database connections, go to the **Database** page in the **System Administration** area. Only the System Administrator can access this page. For more information see *System Administrator*.

Any administrative tasks that require the database to be disconnected should be performed during off-hours. Make sure to inform the users about the unavailability and its duration. For additional information on configuring your database, please contact SupportLine. If you are using Microsoft SQL Server, we recommend that you read *Silk Central MSSQL Server Recommendations*.

Choosing a Relational Database Management System

Install and setup Oracle or Microsoft's SQL Server as described in your relational database management system (RDBMS) documentation.

Silk Central supports the following database management systems:

- Microsoft SQL Server 2014 Service Pack 3
- Microsoft SQL Server 2016 Service Pack 2
- Microsoft SQL Server 2017
- Oracle 11g (version 11.2.0.4). Oracle RAC is not supported.
- Oracle 12c (version 12.2.0.1). Oracle RAC is not supported.

The following table describes the requirements for each database type.

RDBMS	Have ready
Oracle	• Oracle tablespace. • Server host name and port number, or *Single Client Access Name* (SCAN). The default port is 1521. • Name of the Oracle instance (`$ORACLE_SID`). • Name and password of your Silk Central database user. The user must possess quotas and sufficient permissions. Ask your Oracle administrator for assistance if necessary. **Note:** Oracle does not create databases but rather schemes that are assigned to specific user names. Therefore, database names are not assigned to Oracle databases but instead to user names. Silk Central refers to such user names as *database names*.
Microsoft SQL Server	• Server host name and port number. • MS SQL Server system user name and password. • Name for your Silk Central database. • Name and password of your Silk Central database user. **Note:** Silk Central supports only *Microsoft SQL Server* servers that are set up to be case-insensitive and accent sensitive. Silk Central does not support changing the collation after the database was connected for the first time as this might cause collation conflicts. Do not use *Microsoft SQL Server Express* for production environments, because it has limited capabilities compared to a full database server installation.

Database User Privileges

Because of the security risks, we recommend that you do not use the database administrator user for maintaining your Silk Central database. This topic lists the database roles that can be used for specific tasks, as follows:

Microsoft SQL Server

If Microsoft SQL Server is your DBMS for Silk Central, the following database user roles/privileges are required for your Silk Central database:

Either:	Or:
• db_owner • db_ddladmin • VIEW SERVER STATE	• db_datareader • db_datawriter • db_ddladmin • EXECUTE • VIEW SERVER STATE

These roles/privileges allow creating and configuring database tables, working with a previously created database, and installing and upgrading the software.

Note: The Silk Central database user requires these roles/privileges. Otherwise, errors occur.

Oracle

If Oracle is your DBMS for Silk Central, set the following Oracle database user privileges to work with Silk Central:

- CREATE SESSION
- CREATE PROCEDURE
- CREATE SEQUENCE
- CREATE TABLE
- CREATE TRIGGER
- CREATE VIEW

Note: The Silk Central database user requires all the preceding privileges. Otherwise, errors occur. To get all database-related analysis data in system diagnostics, it is also recommended to assign the `SELECT_CATALOG_ROLE` to your database user.

Note: The Oracle user must have sufficient quotas to work with Silk Central.

When setting up an Oracle DBMS for Silk Central, ensure that the Oracle environment meets the following requirements:

- At least 2 GB of temporary tablespace is available.
- Sufficient disk space is available to handle the size of the temporary tablespace.

Creating Databases

If Silk Central is currently connected to a database, you must disconnect the database before you can create a new one.

Note: If you installed Silk Central using the evaluation setup package, a demo database with the name `demodb` is automatically created and connected. In this case, you do not have to process the following steps.

To create a new database:

1. If you have already set up your Silk Central application server, the **Database** page will display in a browser window, and you can proceed with step 3.

Tip: Alternatively, you can browse to your Silk Central site with a Web browser. The default URL is `http://<computer name>:19120/login` (no port information required if Silk Central runs on IIS). When you use the *Standard Setup* option for installing Silk Central, the **Database** page displays immediately after you connect to the application. On the computer where the front-end server is installed, you can also select **Start** > **Programs** > **Silk** > **Silk Central** > **Silk Central 20.5** > **Silk Central Home Page** .

2. Log in to Silk Central as System Administrator.

   For more information see *System Administrator*.
3. In the menu, click **Databases**.
4. Configure the settings for the new database.

   For more information see *Database Page*.

   You can create a database on the locally installed Microsoft SQL Server 2008 Express SP1, a locally installed Microsoft SQL Server or Oracle installation, or on a network server that has MS SQL Server or Oracle installed. Silk Central supports:

   - Microsoft SQL Server 2014 Service Pack 3
   - Microsoft SQL Server 2016 Service Pack 2
   - Microsoft SQL Server 2017
   - Oracle 11g (version 11.2.0.4). Oracle RAC is not supported.
   - Oracle 12c (version 12.2.0.1). Oracle RAC is not supported.
5. Click **Connect Database** and click **Yes**. The **Create New Database** dialog box appears.
6. Type in the database administrator credentials and click **OK**.

   Tip: If you are creating a local or network Microsoft SQL Server or Oracle database, enter the login information provided to you by your database administrator.

   The **Create ALM Repository ID** dialog box appears.
7. Type in a unique **ALM repository ID** and click **OK**.
8. You will be notified that the repository has been created successfully. Click **OK**. The login page displays.

The database is created and connected. Now you can log in to Silk Central with your username and password.

Connecting to a Database

To connect to a database:

1. Browse to the Silk Central site with a web browser.

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

   Note: If currently no database is connected, you are automatically directed to the **System Administration** area.
2. Log in to Silk Central as System Administrator.

   For more information see *System Administrator*.
3. In the menu, click **Databases**.
4. Click **Disconnect Database** to disconnect the current database. You are directed to the **Database** page.
5. Change the settings as required.

   For more information see *Database Page*.
6. Click **Connect Database**.

Establishing the database connection may take from several minutes up to some hours. When the connection is established, a dialog box appears. Click **OK**. The Silk Central login page displays.

Disconnecting from a Database

To disconnect from a database:

1. Browse to your Silk Central site with a Web browser.

   The default URL is `http://<computer name>:19120/login` (no port information required if Silk Central runs on IIS).
2. Log in to Silk Central as System Administrator.

   For more information see *System Administrator*.
3. In the menu, click **Databases**.
4. Click **Disconnect Database** to disconnect the current database. You are directed to the **Database** page.

ALM Repository IDs

Each Silk Central database must have a unique repository ID. This ID is used in ALM URIs to uniquely identify Silk Central requirements and tests across multiple Silk Central repositories. The repository ID must be unique within your company's Silk Central installations. The supplied repository ID will be part of the ALM URI. For additional information on ALM URIs, see *ALM URIs*. It is good practice to use a descriptive ID, for example `USCA01`, for USA, California, repository #01 or `GEBE02`, for Germany, Berlin, repository #02. Allowed characters are letters, numbers, period (.), and minus (-). IDs must have a length of 1 to 20 characters.

Caution: Once a repository ID has been set, it cannot be changed.

ALM URIs

Repository IDs are incorporated into Application Lifecycle Management Uniform Resource Identifiers (ALM URIs). ALM URIs offer a means of addressing elements across ALM Server platform and the ability to distinguish and track elements between applications. Among other things, ALM URIs are used to uniquely identify Silk Central requirements and tests across multiple Silk Central repositories.

The ALM element URI syntax is as follows:

```
<ALM URI> = alm://<source project>/<source element path>[?<source version>]
 <source project> = <source type>!<project identity>
```

For Silk Central, `<source type> = sctm`. For Issue Manager, `<source type> = scim`.

Project identity is built as follows:

```
<project identity> = <repository ID>_<project ID>
```

`<repository ID>` is a unique identifier for each Silk Central and Issue Manager repository. Each repository generates a unique identifier that is stored inside the repository. Uniqueness is guaranteed across all repositories that you may have installed. `<project ID>` is an identifier for a Silk Central or Issue Manager project. This identifier is unique in the context of each repository.

Source Element Path:

For Silk Central and Issue Manager, the following syntax for referencing artifacts is used:

Silk Central native requirements, which are requirements that are not linked with an external requirement management system, use the following syntax:

```
<source element path> = /<requirement ID>;ns=requirement
```

Silk Central tests use the following syntax:

```
<source element path> = /<test ID>;ns=test
```

Silk Central and Issue Manager issues use the following syntax:

```
<source element path> = /<issue ID>;ns=issue
```

Example ALM URI:

```
alm://sctm!USCA01_23/602;ns=test
```

Silk Central repository `USCA01`, project ID `23`, element ID `602`, element type `test`.

Database Page

On the **Database** page you can connect a database with Silk Central and disconnect the database again.

If no database is connected, you will automatically be directed to the **Database** page.

If a database is connected, you have to log in as System Administrator and click **Database** to access the **Database** page. For more information see *System Administrator*.

Configure the database connection with the following UI controls:

Item	Description
DBMS hostname or IP address	The name of the computer hosting the DBMS (database management system). Type in the name 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. **Oracle Server** — `<computer name>` or *Single Client Access Name (SCAN)*. For example: `MyDBMSHost`. If you plan on creating custom reports with direct database access, define a **DBMS hostname** that is available throughout the network.
DBMS type	The type of DBMS you want to access, `MS SQL Server` or `Oracle`.
Port	The port on which the DBMS listens. The default port for Microsoft SQL Server, including Express, is `1433`. The default port for Oracle is `1521`.
Database / SID	MS SQL Server database name or Oracle SID provided by your Oracle administrator. To connect to an Oracle RAC environment, precede the SID with a slash (*/*). *For Oracle database administrators:* Configure the Oracle SID to use the UTF-8 character set.
Username / **Password**	**Microsoft SQL Server, including Express** — Database user with sufficient credentials, or a valid Windows domain user (`domain\username`). When using Windows authentication, the database server must support LMv2 and NTLMv2. Single sign-on without specifying a user is not supported. **Note:** If you are evaluating Silk Central, the default credentials are `sa` / `SilkCentral12!34`. **Oracle Server** — Database user with sufficient credentials, provided by your Oracle administrator.

Item	Description
	Important: For Oracle Servers, the database username must not contain periods (.).
Read-only username	An optional database user with read-only rights on all tables and views in the specified database. This user is used for actions where only read rights are required, for example 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. Accessing the database with a read-only user also has a positive impact on performance. If your DBMS is Microsoft SQL Server, Silk Central automatically creates this user if you specify a name and password. If your DBMS is Oracle, your database administrator needs to create the user in Oracle and your Silk Central administrator needs to add that user to Silk Central.
Read-only password	Valid password for the specified **Read-only Username**.
DBMS version info	Displays DBMS and operating system version information.
ALM repository ID	Displays the ALM URI of the repository.
Connect Database / **Disconnect Database**	Click this button to connect to or disconnect from a DBMS.

Note: If the version of the execution server is an invalid older version, but later than version *SilkCentral Test Manager 2009 SP1*, the execution server is automatically upgraded to the current Silk Central version. Silk Central shows a message concerning the upgrade in the **Information** column in the list of execution servers. As long as the upgrade procedure is not complete, the upgrading execution server is not used.

Clients

Clients are distinct units within a Silk Central instance. A client can for example be a *customer* or a *division* within a company. Clients enhance security, but in contrast to instances, they share the same database and Silk Central services.

The **System Administration** area allows you to generate clients. You can configure various client settings which will affect the projects that are assigned to that client. From the total pool of available licenses, you can specify the maximum limit of licenses that can be used per client. You can only access the data of a client if you are logged in to that client. Within a client, all assets are then accessible across the projects.

When you install Silk Central, a default client is created automatically. When you upgrade Silk Central from an older version, all existing projects and users are assigned to this default client. A Super User is created for each client. For more information, see *Super User* . You can delete all clients, but you need at least one client to be able to create projects and users and to work with Silk Central.

Super User

The Super User has all permissions within a client. By contrast, the System Administrator can just manage the various clients of a Silk Central installation but has no access to the actual Silk Central UI.

When the System Administrator creates a new client, a Super User is automatically created for that client.

Log in as Super User with the following default credentials:

- username: `admin`
- password: `admin`

Important: Change this default password as soon as possible. To change the password, click **Administration** > **User Management** in the menu, click the **Accounts** tab, and click **admin** in the grid. The username cannot be changed.

For a list of all available user roles and permissions, see *User Roles and Permissions*.

Creating Clients

To create a client:

1. Log in to Silk Central as System Administrator.
   For more information see *System Administrator*.
2. In the menu, click **Clients**.
3. Click **New Client**. The **New Client** dialog box appears.
4. Enter the **Client Name** and a **Description**.
5. In the **License Limits** section, specify the maximum amount of licenses that can be in use concurrently for this client. Once the specified amount of licenses is in use, no more users will be able to acquire a license on the selected client. This is especially useful if you want to ensure that a more important client has enough available licenses, while less important clients can be restricted.
   The following rules apply:
   - No value: No license limit is applied, the client can make use of the total amount of available licenses.
   - `0` (zero): No licenses can be consumed by the client, which essentially deactivates all related features of the selected license.
   - Any number: The amount of licenses that can be consumed by the client. If the number is higher than the total amount of available licenses, the client can make use of the total amount of available licenses.

   Tip: The total amount of available licenses is displayed at the bottom of the **Clients** page.
6. Click **OK**.

Log in to the client as Super User to perform client-specific administration tasks. For more information, see *Super User*.

Editing Clients

To edit the settings of a client:

1. Log in to Silk Central as System Administrator.
   For more information see *System Administrator*.
2. In the menu, click **Clients**.
3. Click (**Edit**) in the **Actions** column. The **Edit Client** dialog box appears.
4. Edit the **Client Name** and the **Description**.
5. In the **License Limits** section, specify the maximum amount of licenses that can be in use concurrently for this client. Once the specified amount of licenses is in use, no more users will be able to acquire a license on the selected client. This is especially useful if you want to ensure that a more important client has enough available licenses, while less important clients can be restricted.
   The following rules apply:
   - No value: No license limit is applied, the client can make use of the total amount of available licenses.
   - `0` (zero): No licenses can be consumed by the client, which essentially deactivates all related features of the selected license.

- Any number: The amount of licenses that can be consumed by the client. If the number is higher than the total amount of available licenses, the client can make use of the total amount of available licenses.

Tip: The total amount of available licenses is displayed at the bottom of the **Clients** page.

6. Click **OK**.

Note: Notify the Silk Central users if you change the **Client name**. Silk Central users need to enter the correct client name on the login page.

Log in to the client as Super User to perform client-specific administration tasks. For more information, see *Super User*.

Removing Clients

To remove a client:

1. Log in to Silk Central as System Administrator.
   For more information see *System Administrator*.
2. In the menu, click **Clients**.
3. Click (**Delete**) in the **Actions** column.
4. Click **Yes** to confirm.

Default Client

When you install Silk Central, a client (with the name `Default`) is created automatically and the status of this client is set to default. To define which client has the default status, log in to Silk Central as System Administrator and click **Clients**. For more information, see *System Administrator*.

To set a client as default, click **Set as Default**. To unset the default status, click **Unset Default**. The icon shows, which client is currently the default client. It is also possible that there is no default client defined, but only one client at a time can have the default status.

The purpose of the default client is to simplify the login: When you login to Silk Central with a user of the default client, you can omit the client name. Just enter your username. This is especially useful for Silk Central installations with only one client. When you upgrade Silk Central from an older version, the login behaviour is the same as it was before.

License Handling

Silk Central provides different types of licenses.

Per-User Licenses

These licenses are checked out from the license server as soon as a user enters a certain area of Silk Central:

License Type	Area
Test Manager	This license is checked out when you access a test management area for the first time after your login. Silk Central test management areas are: **Requirements**, **Tests**, **Execution Planning**, **Tracking**, **Issues** (excluding the Issue Manager area), and **Reports**.
Manual Testing	This license is checked out when you open the **Manual Testing** window. A **Manual Testing** license is checked

License Type	Area
	out when a test is downloaded for offline execution. The license is checked back in when results are uploaded.
Issue Tracking	This license is checked out when you access Issue Manager.

Note the following:

- When you click **Log out** (**User** > **Log out**), the licenses are checked in to the license server again, except checked out manual testing licenses for offline testing.
- If you do not log out (and just close the browser window), the license will only be checked in when the session expires.

The **About** page (**Help** > **About**) displays how many licenses are currently used and how many licenses are available for the client you are currently logged in to.

Site Licenses

These licenses enable a specific feature set for all users, without limitations:

License Type	Area
Mobile Testing	This license enables testing on mobile devices (physical devices, emulators and simulators) for manual, automated, and configuration testing.

Clients Page

To access this page, log in to Silk Central as System Administrator and click **Clients**. For more information see *System Administrator*.

Use this page to create and manage your clients. Click **New Client** to create a new client. Click **Set as Default** or **Unset Default** to change the default status of the client. The icon shows, which client is currently the default client.

The grid on the page contains the following columns:

Column	Description
Actions	Click the buttons and to **Delete** or **Edit** clients.
ID	The Identifier of the client.
Name	The name of the client. Click to **Edit** the name. Notify the Silk Central users if you change the client name. Silk Central users need to enter the correct client name on the login page.
Description	Describes the client in more detail. Click to **Edit** the description.
Test Manager	The maximum amount of **Test Manager** licenses that can be in use concurrently.
Manual Testing	The maximum amount of **Manual Testing** licenses that can be in use concurrently.
Issue Tracking	The maximum amount of **Issue Tracking** licenses that can be in use concurrently.
Automated Testing	The maximum amount of **Automated Testing** licenses that can be in use concurrently.
Created On	Date when the client was created.
Created By	The user who created the client.

Column	Description
Changed On	Date when the client was modified.
Changed By	The user who modified the client.

Client Permissions

Use this page to modify system settings and permissions for clients.

Item	Description
Show front-end server and application server log views for client users.	When checked, shows the front-end server and application server log tabs in the UI (logs may contain client specific data).
Allow advanced reports for client users.	When checked, enables reports with advanced queries. If not checked, you can still execute them but you cannot create new ones or edit.
Allow report template management for client users.	When checked, enables uploading, editing, updating, and deleting report templates. Report templates may contain arbitrary SQL and read data of other clients.

Infrastructure

Contains settings for chart servers, email servers, and the system proxy.

Chart Servers

A chart server is a service that computes data and produces graphs. These graphs are displayed within the Silk Central application. The service can be installed with the Silk Central setup on a computer of your choice. You must configure a chart server connection to display graphs.

Note: You can configure as many chart server connections as you want. Silk Central automatically implements a load balancing mechanism for chart generation.

Configuring Chart Server Connections

To configure a chart server connection:

1. In the menu, click **Infrastructure** > **Chart Servers**
2. If a chart server was installed with the application server on the same computer, a chart server connection to `localhost` is configured automatically.
3. *Optional:* If your chart servers should communicate with the front-end server through a different URL than the one that users use to access the Web user interface, click **Configure Web Service URL** and type this URL into the text field. This is required for example when users access the Web user interface through a proxy, while your chart servers need the internal URL or IP address of the front-end server.
4. Click **New Chart Server**. The **New Chart Server** dialog box appears.
5. Enter the **Hostname or IP address**, the **Port**, and the **URL** where the chart service is installed. The default port is `19126`, 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 **Close**. If the test connection was successful, check the **Active** check box and click **OK**.

You can configure as many chart server connections as you want. Silk Central automatically implements a load balancing mechanism for chart generation.

Note: You can only configure a chart server connection if the *chart server service* is installed on the target computer. For more information, see the installation instructions of your Silk Central application.

Editing Chart Server Connections

To edit a chart server connection:

1. In the menu, click **Infrastructure** > **Chart Servers**
2. *Optional:* If your chart servers should communicate with the front-end server through a different URL than the one that users use to access the Web user interface, click **Configure Web Service URL** and type this URL into the text field. This is required for example when users access the Web user interface through a proxy, while your chart servers need the internal URL or IP address of the front-end server.
3. Click (**Edit**) in the **Actions** column. The **Edit Chart Server** dialog box displays.
4. Edit the **Hostname or IP address**, the **Port**, or the **URL** where the chart service was installed. The default port is `19126`, the default URL is `ChartServer`.
5. Check/uncheck the **Active** check box to activate/deactivate the server.
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 **Close** and click **OK**.

Removing Chart Server Connections

To remove a chart server connection:

1. In the menu, click **Infrastructure** > **Chart Servers**
2. Click (**Edit**) in the **Actions** column. The **Edit Chart Server** dialog box displays.
3. Uncheck the **Active** check box and click **OK**.
4. Click (**Delete**) in the **Actions** column.
5. Click **Yes** to confirm.

Note: This removes the connection to the server. It does not remove the server itself.

Chart Servers Page

To access this page, log in to Silk Central as System Administrator and click **Infrastructure** > **Chart Servers**. For more information see *System Administrator*.

Use this page to manage the connections to your chart servers. Click **New Chart Server** to configure a new chart server connection. **Configure Web Service URL** allows you to configure an alternate URL with which your chart servers connect to the front-end server. The grid on the page contains the following columns:

Column	Description
Actions	Click the buttons and to **Delete** or **Edit** chart server connections. You must deactivate a connection before you can delete it.
Chart Server URL	Shows the URL of the chart server. Syntax: `http://<computer name or IP address>:<port>/ChartServer`. The default port is `19126`. Click to **Edit** the URL.

Column	Description
Status	Shows if the connection to the chart server is active or inactive. Click (**Edit**) to change the status of a connection.
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.

Email Server

When you configure an email server, Silk Central can notify you about results from your application.

Configuring Email Servers

To configure up to three email servers:

1. Log in to Silk Central as System Administrator.
   For more information see *System Administrator*.
2. Click **Infrastructure** > **Email Server**.
3. Enter an email address in the field **Email address of system administrator**.
   Silk Central will send the notifications to this address.
4. Enter an email address in the field **'From' address to use for emails**.
   This address will display as sender in the notifications.
5. Enter the host name or the IP address of your email servers in the **Server** fields.
   You can configure up to three email servers.
6. If the servers require credentials, enter them in the **Username** and **Password** fields.
7. Click **Check** to test the connection to the servers. Silk Central sends a test email to the email address you entered in step three.
8. If an error message displays, or if you do not receive an email, review your email settings. Ensure that the host name of your email server is correct and that the SMTP protocol is running on that computer.

   Note: SMTP with TLS is currently not supported.
9. If you receive the test email, the test was successful. Click **Save**.

Email Server Page

To access this page, log in to Silk Central as System Administrator and click **Infrastructure** > **Email Server**. For more information see *System Administrator*.

Use this page to configure up to three email servers. The page displays the following items:

Item	Description
Email address of system administrator	Specifies the email address of the Silk Central System Administrator.
'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`.

Item	Description
Server 1 **Server 2** **Server 3**	Specify the host names or IP addresses of the servers that send your email. For many companies, this server is simply called `mail`. If your email server uses SMTP authentication (LOGIN PLAIN), you must enter a valid user and password for the email 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 field **Email address of system administrator**.
Save	Saves your settings.
Reset	Clears all values in the fields.

System Proxy

Execution servers of a certain location can communicate with the application server through a proxy. Once you (as System Administrator) have configured a proxy server, the clients can enable the proxy. To do so, the clients have to click **Administration** > **Execution Servers** in the menu, click (**Edit**) in the **Actions** column and check the **Use system proxy** check box.

Configuring a System Proxy

To configure a system proxy:

1. Log in to Silk Central as System Administrator.
   For more information see *System Administrator*.
2. Click **Infrastructure** > **System Proxy**.
3. Enter the **Host** and the **Port** of the proxy server.
4. Enter the **Username** and the **Password** if required.
5. Click **Check** to test the connection to the proxy server. A dialog box shows you the result of the test.
6. If the connection could not be established, make sure your settings are correct.
7. If the connection could be established, click **Save**. The system proxy is ready for use.

System Proxy Page

To access this page, log in to Silk Central as System Administrator and click **Infrastructure** > **System Proxy**. For more information, see *System Administrator*.

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

Item	Description
Host	The host name 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 (optional)	Enter a valid user name if the proxy server requires login credentials.
Password (optional)	Enter a valid password for the user name.
Check	Tests the connection to the proxy with the credentials you provided.

Item	Description
Save	Saves your settings.
Reset	Clears all items on this page.

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 Silk Central, you need to specify the location of the application server.

Specifying a Location for the Application Server

When connecting to the default Silk Central instance, 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 Silk Central software, connect to Silk Central using a Web browser.

   Tip: The default URL is `http://<computer name>:19120/login` (no port information required if Silk Central 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 Silk Central'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.

LDAP Authentication

Configure LDAP authentication to enable Silk Central 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.

Silk Central LDAP Integration

The most important aspect of LDAP integration in Silk Central 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.

Silk Central 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 user name exists in the Silk Central 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 user name 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 user name 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.

Adding LDAP Servers

To configure an LDAP server for usage with Silk Central:

1. In the menu, click **Administration** > **System Settings** .
2. Click the **LDAP Servers** tab.
3. Click **New LDAP Server**. The **New 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 Silk Central. If unchecked, the LDAP server's services are not available to Silk Central.
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:* Specify a **Domain** if your users should log in to Silk Central with the pattern `<domain>\<username>`. Leave this field empty if your users should log in to Silk Central without entering a domain name. If your Silk Central installation consists of multiple clients, make sure that the specified LDAP domain name does not conflict with any of your client names, as the login pattern `<domain>\<username>` is also used for logging in to specific clients.
9. *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.
10. Type the **Password** of the user defined by **Bind DN**. This is not required when anonymous access is allowed.
11. Type the **Base DN** root for LDAP queries. For example `DC=yourcompany,DC=com`.
12. *Optional:* Type the **User Filter** that is to be used for querying LDAP.

    Example: `(memberOf=CN=Development,CN=Users,DC=yourcompany,DC=com)`

    This example queries the LDAP server for the logged in Silk Central 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 Silk Central to create accounts only for members of a certain LDAP group.
13. *Optional:* To filter your LDAP query by specific groups for the **Import LDAP Group** functionality, specify a **Group Filter**. The syntax is identical to the syntax used for the **User Filter** field.

14. Click **Configure LDAP Properties** to map your LDAP attributes to Silk Central's user and group settings. This is essential if you plan to import users from your LDAP server into Silk Central.
15. *Optional:* You can let Silk Central automatically create a Silk Central user account when a user logs in to Silk Central for the first time. If the user account with the entered login name does not exist in Silk Central, the entered credentials are authenticated against the LDAP server. If this succeeds, a new account with the supplied login name and password is created in Silk Central. Newly created accounts initially copy the general settings, including the dashboard settings, from the selected Silk Central user, which acts as a template. First name, last name and email address are queried from the LDAP values. To do this, click **Configure** next to **User account creation**. On the **User Account Creation** dialog box, select a **Silk Central user** from the list. Depending on your LDAP configuration, you may need to adapt the LDAP values for first name, last name and email address.
16. Click **Test** to perform a test connection to the LDAP server.

    For more information, see *Testing LDAP Servers*.
17. Click **OK** to save your settings.
18. 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 Settings** .
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 Silk Central. If unchecked, the LDAP server's services are not available to Silk Central.
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:* Specify a **Domain** if your users should log in to Silk Central with the pattern `<domain>\<username>`. Leave this field empty if your users should log in to Silk Central without entering a domain name. If your Silk Central installation consists of multiple clients, make sure that the specified LDAP domain name does not conflict with any of your client names, as the login pattern `<domain>\<username>` is also used for logging in to specific clients.
9. *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.
10. Type the **Password** of the user defined by **Bind DN**. This is not required when anonymous access is allowed.
11. Type the **Base DN** root for LDAP queries. For example `DC=yourcompany,DC=com`.
12. *Optional:* Type the **User Filter** that is to be used for querying LDAP.

    Example: `(memberOf=CN=Development,CN=Users,DC=yourcompany,DC=com)`

    This example queries the LDAP server for the logged in Silk Central 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 Silk Central to create accounts only for members of a certain LDAP group.
13. *Optional:* To filter your LDAP query by specific groups for the **Import LDAP Group** functionality, specify a **Group Filter**. The syntax is identical to the syntax used for the **User Filter** field.

14. Click **Configure LDAP Properties** to map your LDAP attributes to Silk Central's user and group settings. This is essential if you plan to import users from your LDAP server into Silk Central.
15. *Optional:* You can let Silk Central automatically create a Silk Central user account when a user logs in to Silk Central for the first time. If the user account with the entered login name does not exist in Silk Central, the entered credentials are authenticated against the LDAP server. If this succeeds, a new account with the supplied login name and password is created in Silk Central. Newly created accounts initially copy the general settings, including the dashboard settings, from the selected Silk Central user, which acts as a template. First name, last name and email address are queried from the LDAP values. To do this, click **Configure** next to **User account creation**. On the **User Account Creation** dialog box, select a **Silk Central user** from the list. Depending on your LDAP configuration, you may need to adapt the LDAP values for first name, last name and email address.
16. Click **Test** to perform a test connection to the LDAP server.

    For more information, see *Testing LDAP Servers*.
17. 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 Silk Central, 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 Settings** .
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).

Silk Performer Load-Test Agent Clusters

In addition to assigning workload to individual agents, you have the option of assigning Silk Performer workload to clusters of agents with defined capabilities. Silk Performer's dynamic workload-assignment functionality matches specific load-test requirements to the replay capabilities of available agent computers at execution time. The capabilities that are defined for test agents in Silk Performer are used to optimize workload-to-agent assignment. For example, if a test requires a workload that only an agent computer with a SAPGUI client can deliver, then dynamic workload-assignment functionality can ensure that the test's workload is assigned only to available agents with SAPGUI clients. Additionally, the percentage of required workload or virtual users that can be allocated to each agent can be configured, thereby ensuring that agents are not pushed beyond their capacities.

Upon execution of a Silk Performer test, a Silk Central load-test agent-clusters XML file is checked out of the appropriate execution server and used for dynamic workload assignment during execution. You must specify the location of your project's load-test agent-clusters XML file by way of **Administration** > **System** settings.

An advantage of dynamic assignment of workload to load-test agent clusters is that successful execution of tests is not contingent on maintaining a static test-execution environment. Silk Performer can dynamically assign an unavailable agent's workload to an available agent in the same cluster that has the same capabilities. This feature is of particular value when Silk Performer load tests are managed and executed based on predefined schedules in Silk Central. The manner in which workload is balanced across agents and the health of individual agents are not issues to consider from the Silk Central perspective.

For details regarding dynamic workload assignment, refer to the *Silk Performer Help*.

Uploading Load Test Agent Cluster Files

Describes how to add or change your project's load-test agent-clusters file in support of Silk Performer dynamic workload assignment.

To change your project's agent-clusters file definition:

1. In the menu, click **Administration** > **System Settings** .
2. Click the **Load Test Agent Clusters** tab.
3. Click **Upload**.
4. On the **Upload Agent Clusters File** dialog box, browse to the location of the agent-cluster file on your local disk.

   When you upload the file, it is displayed in the **Load Test Agent Clusters** page.
5. Click **OK** to confirm your selection.

Deleting Load Test Agent Clusters Files

Delete a load-test agent clusters file to remove it from the application server.

To delete a load-test agent clusters file:

1. In the menu, click **Administration** > **System Settings** .
2. Click the **Load Test Agent Clusters** tab.
3. Click **Delete**.
4. Click **Yes** to confirm.

Editing Load Test Agent Cluster Files

To edit your project's agent-clusters file definition:

1. In the menu, click **Administration** > **System Settings** .
2. Click the **Load Test Agent Clusters** tab.
3. Click the name of the load-test agent-clusters file that you want to change.
4. Download the file.
5. Edit the file in an editor.
6. Upload the file.

   For more information, see *Uploading Load Test Agent Cluster Files*.

Load Test Agent Clusters Page

Administration > **System Settings** > **Load Test Agent Clusters**

The **Load Test Agent Clusters** page shows the currently configured load-test agent-clusters XML file. Use this page to manage Silk Performer load-test agent-cluster files in support of dynamic workload assignment.

From this page you can perform the following actions:

- Click **Upload** to upload a load-test agent-clusters XML file.
- Click **Delete** to remove an existing load-test agent-clusters XML file.
- Click the name of the load-test agent-cluster file to download and edit the file.

System Diagnostics

Use the **System Diagnostics** tab to retrieve diagnostic information and to retrieve system log files.

System Diagnostics

The **System Diagnostics** page provides a way to retrieve the following system information:

- Product version.
- Version and type of database.
- Used integrations.
- System environment information and system properties.
- JDBC information.
- Database statistics: number of projects, test types, indices, triggers, constraints.
- Application server, front-end server, and nginx access logs.

The page can be zipped and downloaded to the local file-system by clicking the **Download** button. You can select the server logs that should be downloaded by selecting them via the check boxes.

1. You can access the **System Diagnostics** page remotely or, if you can no longer login to the system, locally on the computer where the front-end server is running.
   - For remote access:
     1. Login as System Administrator.
     2. Click **System Diagnostics** > **System Diagnostics**.
     3. Click **Open System Diagnostics**.
   - If remote access does not work:
     1. Navigate to `http://localhost:19120/systemdiagnostics` or `http://127.0.0.1:19120/systemdiagnostics` on the computer where the front-end server is running (do not use the host name or the server's external IP address).
2. Select the Silk Central server logs that should be downloaded by selecting them via the check-boxes.
3. Click **Download** to zip and download the data to the local file-system.

Front-End Server Logs

To access this page, log in as System Administrator and click **System Diagnostics** > **Front-end Server Logs**. For more information see System Administrator.

Use this page to view logging information from the Silk Central 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.

Application Server Logs

To access this page, log in as System Administrator and click **System Diagnostics** > **Application Server Logs**. For more information see System Administrator.

Use this page to view logging information from the Silk Central 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.

Configuring Advanced Settings

This section describes how to configure advanced settings to customize your Silk Central system.

Login Options

The following two enhanced login configurations are available:

Remember Login

Changing the default setting for the **Remember login** option on the Silk Central login page.

Normally when users work with multiple browser windows, each browser session checks out a unique license. Enabling **Remember login** allows individual users to work with multiple browser sessions on a single computer while checking out only a single license.

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 Silk Central, 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 Silk Central 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. On the **Instance Administration** page, stop the front-end server of the instance that you want to modify.
2. Open the `TMFrontendBootConf.xml` file with a text editor.

   The default path for this file is `C:\Program Files (x86)\Silk\Silk Central 20.5\instance_<instance number>_<instance name>\Conf\FontendServer` 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. On the **Instance Administration** page, stop the front-end server of the instance that you want to modify.
2. Open the `TMFrontendBootConf.xml` file with a text editor.

   The default path for this file is `C:\Program Files (x86)\Silk\Silk Central 20.5\instance_<instance number>_<instance name>\Conf\FontendServer` 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.

Suspicious Execution Duration

The execution durations of tests vary, however if an execution takes too long, the user that made the last change to the execution plan can get notified by email.

Silk Central sends a notification when test execution takes longer than a certain amount of time. The user can define how long a test execution may take before an email is sent.

Note: You can also set a timeout for each specific test by setting the **Execution Time-Out [s]** property in the **Success Conditions** section of the **Tests** area.

Setting the Suspicious Execution Duration

To set the suspicious execution duration:

1. On the **Instance Administration** page, stop the application server of the instance that you want to modify.
2. Open the `TMAppServerHomeConf.xml` file with a text editor.

   The default path for this file is `C:\Program Files (x86)\Silk\Silk Central 20.5\instance_<instance number>_<instance name>\Conf\AppServer` on the application server.
3. Locate the `Config\ExecutionTracking\SuspicousDuration` XML tag.

   By default, the tag is set to `<SuspicousDuration>360</SuspicousDuration>`.
4. Set the duration value to the number of minutes after which Silk Central should notify the administrator about test executions that take too long.
5. Save and close the XML file.
6. Restart the application server.

Disable Updating of External Issue Statistics

Updating the issue statistics of external issue tracking profiles may use much memory. This may also slow down performance. To disable updating:

1. On the **Instance Administration** page, stop the application server of the instance that you want to modify.
2. Open the `TMAppServerHomeConf.xml` file with a text editor.

   The default path for this file is `C:\Program Files (x86)\Silk\Silk Central 20.5\instance_<instance number>_<instance name>\Conf\AppServer` on the application server.
3. Locate the `Config/IssueStateUpdate/UpdateIssueUnitStatistics` XML tag.

   By default, the tag is set to `true`.
4. Set the value to `false` to disable updating.
5. Save and close the XML file.
6. Restart the application server.

Date and Time Formats

Silk Central offers user-defined date and time format settings. Each Silk Central 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*.

Silk Central presents lists of predefined date and time formats from which users may choose. Silk Central 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

Letter	Date or Time Component	Presentation	Examples
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
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. On the **Instance Administration** page, stop the front-end server of the instance that you want to modify.
2. Open the `TMFrontendBootConf.xml` file with a text editor.

   The default path for this file is `C:\Program Files (x86)\Silk\Silk Central 20.5\instance_<instance number>_<instance name>\Conf\FontendServer` 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.

Host Name Display

When you are working with Web applications on multiple front-end servers, it can be useful to know which host you are working on. Silk Central offers a setting that displays the host name of the front-end server in the title bar of your Web browser.

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. On the **Instance Administration** page, stop the front-end server of the instance that you want to modify.
2. Open the `TMFrontendBootConf.xml` file with a text editor.

The default path for this file is `C:\Program Files (x86)\Silk\Silk Central 20.5\instance_<instance number>_<instance name>\Conf\FontendServer` 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 Silk Central. 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 Silk Central is always displayed.

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

   When the tag is set to `false`, the browser displays: `<unit> | Silk Central`.

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

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

Storing Attachments and Result Files on the File System

Per default, Silk Central stores all attachments and result files in the database, but you can configure Silk Central to store these files on the file system of the application server.

Although it is not recommended to save attachments and result files separated from the other data, you may have reasonable arguments to prefer this approach (e.g. cost for database space). A disadvantage of this approach is that you have to maintain your data twice, meaning that you have to make a backup of your database and also of your file system. When restoring a database backup, you also need to restore the file system.

Caution: If you enable the option to save files to the file system, make sure to never change the structure or directly move, update, or delete files in this location. Only the Silk Central services and the system you use for backup and restore should have write permissions in the specified **File store root directory**.

1. On the **Instance Administration** page, activate the maintenance mode on the instance that you want to modify. For additional information, see *Maintenance Mode*.
2. Log in to your instance as System Administrator and disconnect the database. For additional information, see *Disconnecting from a Database*.
3. On the **Instance Administration** page, stop the instance that you want to modify.
4. Open the `TMAppServerHomeConf.xml` file with a text editor.

   The default path for this file is `C:\Program Files (x86)\Silk\Silk Central 20.5\instance_<instance number>_<instance name>\Conf\AppServer` on the application server.
5. Locate the `<StoreFilesOnFileSystem>` XML tag in the `<Config>/<RdbmsSpecifics>` section of the file. Set the value for this tag to `true`.
6. Save and close the XML file.
7. On the **Instance Administration** page, restart the instance.
8. Log in to your instance as System Administrator again. On the **Database** page you will see a new field called **File store root directory** where you have to define a local path (e.g. "`c:/sc_files/testdb`") which will be used for storing attachments and result files. This path needs to exist already and the front-end and application server services require full permissions on this folder.

9. Click **Connect Database**.

All attachments and result files will now be saved in the specified location. Attachments and result files that are already stored in the connected database will gradually be moved to the file system. In case the file system is not available, Silk Central will store the files in the database blob tables and move them to the file system at a later time when the file system is available again.

Be aware that there is currently no automatic way to move the files back to the database again. Enable this option only if you permanently plan to store your files to the file system.

Configuring the LQM Reporting Updater

Describes how to configure the interval and other settings of the thread that updates the LQM Reporting tables (LQM Reporting Updater). For detailed information about the LQM Reporting tables, refer to the *Database Model Schema*.

To configure the LQM Reporting Updater settings:

1. On the **Instance Administration** page, stop the application server of the instance that you want to modify.
2. Open the `TMAppServerHomeConf.xml` file with a text editor.

   The default path for this file is `C:\Program Files (x86)\Silk\Silk Central 20.5\instance_<instance number>_<instance name>\Conf\AppServer` on the application server.
3. Locate the `LQMReporting` XML tag.

   You can modify the following settings:

UpdateInterval	Defines the interval in seconds when the LQM Reporting tables are updated with the most current data.
MSSqlUpdateBatchSize	Number of test tables processed at once. The batch size determines how much memory and processor resources are used on the application server for the update process. This setting only affects MS SQL Server databases.
OracleUpdateBatchsize	Same as *MSSqlUpdateBatchSize*, but for Oracle databases.
QueryTimeout	Specifies the time-out in seconds after which queries in the LQM Reporting update process are aborted. 0 or a negative value specifies that the queries never time out.
OracleCheckForUpdateStrategy	Determines how the update process reads from the source tables. Allowed values are `NOWAIT` and `WAIT`. • `NOWAIT`: When the update process wants to read from the source tables and another process is currently writing to these tables, the update process terminates and retries the next time it is called. • `WAIT`: The update process grabs a table lock and waits until other processes have finished accessing the tables, then reads from the source tables. The advantage is that the process always executes because it doesn't have to wait until a table is unlocked. The disadvantage is that all other processes that try to access a table after the LQM update process are blocked and have to wait until the process releases the table lock.

4. Save and close the XML file.
5. Restart the application server.

Scheduling Automatic LDAP Group Synchronization

If you have imported user groups from LDAP servers in your Silk Central system, you can specify a schedule to automatically synchronize your Silk Central groups with changes that were made on the LDAP servers.

To define a schedule for synchronizing Silk Central groups with changes that were made on the LDAP servers:

1. On the **Instance Administration** page, stop the application server of the instance that you want to modify.
2. Open the `TMAppServerHomeConf.xml` file with a text editor.

   The default path for this file is `C:\Program Files (x86)\Silk\Silk Central 20.5\instance_<instance number>_<instance name>\Conf\AppServer` on the application server.
3. Locate the `LdapUpdate` XML tag.

   You can modify the following settings:

ScheduledTime	Timestamp (hh:mm, 24h clock) when the data from LDAP is updated the first time. ScheduledTime is interpreted with the timezone of the application server system environment. Leave this setting empty to disable automatic synchronization.
UpdateIntervalInMinutes	This interval (in minutes) specifies how often LDAP groups and users are synchronized, starting relatively from `ScheduledTime`. Minimum value is 1.

4. Save and close the XML file.
5. Restart the application server.

Data Caching in Tests

Silk Central uses caching in **Tests** to improve the scalability of the front-end server and to reduce database load when multiple users work on the same project simultaneously. The **Tests** tree and test filters have significant impact on the front-end and database servers. Because information from the **Tests** tree and filters for specific projects can be shared among users, these areas are well suited to caching.

Tests Tree Caching

The **Tests** tree cache retains all tree information for projects that are currently in use in memory and regularly checks the database for changes to the tree. Administrators can influence the behavior of the cache by setting `Cache/TestPlanTree/CheckForChangesInterval` in the `TMFrontendBootConf.xml` configuration file. This is the maximum interval in seconds that tree information may remain outdated. Regardless of this setting, if a change occurs to a test, folder, or container on the same front-end server, the cache will be immediately updated with the change. The `Cache/TestPlanTree/CheckForChangesInterval` setting is only relevant when a change occurs on a different front-end server. When a project is not used by a user for more than an hour, the entire project tree cache is cleared and the project is reloaded the next time a user accesses it.

Test Filter Caching

With filter caching, the IDs of tests that match the criteria of specific filters are cached for a specified period of time, based on the minimum cache time setting and the execution time of each filter. Administrators can influence this behavior by setting two properties at `Cache/FilterCache/` in the `TMFrontendBootConf.xml` configuration file.

The first property, `MinimalLifeTime`, defines the minimum time in seconds before a filter result can be removed from the cache. The second property, `LifeTimeMultiplier`, makes this minimum setting

dependent on the time it takes to execute the filter query. For example, if you define a multiplier of `> 0`, the maximum time that a result can remain in the cache is `MinimalLifeTime`, or the query execution time, multiplied by the `LifeTimeMultiplier`. So, if you have a filter query that takes 1 second to execute, and you use the default values, both `30`, for `MinimalLifeTime` and `LifeTimeMultiplier`, then the filter result will be cached for 30 seconds. If the filter query takes half a second to execute, then the filter result will still be cached for 30 seconds. If however the filter query takes 2 seconds to execute, then the filter result will be cached for 60 seconds.

Recommendation Engine Caching

When you add keywords to a keyword-driven test or a keyword sequence in the **Keyword-Driven Test Editor**, Silk Central recommends existing keywords which you might want to use as the next keyword in your test. The recommended keywords are listed on top of the keywords list, and are indicated by a bar graph, with the filled-out portion of the graph corresponding to how much Silk Central recommends the keyword.

Administrators can influence the interval at which the recommendation cache is refreshed by setting the `RecommendationCache/ExpireAfterWrite` property in the `TMFrontendBootConf.xml` configuration file.

JMX Measures for Caching

Silk Central offers JMX read measures to monitor underlying Java processes and other process-specific measures. JMX information for the **Tests** tree cache and the test filter cache can be found in the JMX measures tree at `borland.com/Frontend/TM`.

Note: Silk Performance Explorer and other tools can be used to track these and other measures.

JMX Measures for Caching in Tests

JMX information for the **Tests** tree cache and the filter cache can be found on your front-end server in the JMX measures tree at `borland.com/Frontend/TM`.

Tests Tree Cache Measures

Two primary measures are available for the **Tests** tree cache. `TestPlanTreeCache` only delivers a measure, *NumberOfCachedProjects*, on how many projects are currently cached. All details of the cache of the project are available from the second measure, *TestPlanTreeCache_<number>*. This measure is actually made out of the following measures:

Measure	Description
Hits	The number of times the cache was used, and database requests were not required.
LastUpdateCheckDurationInMillis	The duration in milliseconds the last update took, see *LastUpdateCheckTime*, to check for updates in the database.
LastUpdateCheckTime	The time when the last update check occurred.
LastUpdateDurationInMillis	The duration in milliseconds the last update took, see *LastUpdateTime*, to update the cache after a change occurred.
LastUpdateTime	The time when the last update to the cache occurred due to a change in the **Tests** tree.

Measure	Description
TreeInitializationTimeInMillis	The duration in milliseconds it took to load the whole project tree into the cache. This value will not change as long as the project cache is loaded.
TreeSize	The number of test nodes, which are test containers, test folders, and tests, in the project.
UpdateChecks	The number of checks for changes of the **Tests** tree for this project since the project tree cache was initialized.
Updates	The number of updates of the cached tree due to changes in the **Tests** tree.

Test Filter Cache Measures

The *TestPlanFilterCache* measure is comprised of the following three measures:

Measure	Description
Hits	The number of times the cache was used and no separate execution of the filter on the database was necessary.
Misses	The number of times the filter cache was not used, but the filter was executed against the database.
Size	The current number of cached filter results.

Configuring JMX Settings

Silk Central offers a set of default ports for the configuration of JMX settings.

Available Locations for Configuring JMX Settings

The communication on the default ports is by default unencrypted, meaning no SSL is running.

Important: Micro Focus does not take responsibility for your JMX security settings. Please make sure that your IT department configures JMX security accordingly.

Setting	Description
com.sun.management.jmxremote.ssl	The SSL is set to `false` by default.
com.sun.management.jmxremote.authenticate	The authentication is set to `false` by default.
com.sun.management.jmxremote.host	With the default value `localhost`, connections to the JMX port are only possible from the local machine. There is no remote access to the JMX port. To enable remote access, remove this setting as well as the setting `java.rmi.server.hostname`.

You can modify these settings in the `processconfig` files in `C:\Program Files (x86)\Silk\Silk Central 20.5\instance_<instance number>_<instance name>\Conf`. Note that the JMX connection is not secure as long as either of the two settings is set to `false`.

To access information or perform operations through JMX, you need the JMX connection string. Click to open the **Settings** dialog. On the **Servers** tab, select the required server and copy the **JMX connection** string. For additional information, see *Managing Instances*.

JMX Measures for Caching in Tests

JMX information for the **Tests** tree cache and the filter cache can be found on your front-end server in the JMX measures tree at `borland.com/Frontend/TM`.

Tests Tree Cache Measures

Two primary measures are available for the **Tests** tree cache. `TestPlanTreeCache` only delivers a measure, *NumberOfCachedProjects*, on how many projects are currently cached. All details of the cache of the project are available from the second measure, *TestPlanTreeCache_<number>*. This measure is actually made out of the following measures:

Measure	Description
Hits	The number of times the cache was used, and database requests were not required.
LastUpdateCheckDurationInMillis	The duration in milliseconds the last update took, see *LastUpdateCheckTime*, to check for updates in the database.
LastUpdateCheckTime	The time when the last update check occurred.
LastUpdateDurationInMillis	The duration in milliseconds the last update took, see *LastUpdateTime*, to update the cache after a change occurred.
LastUpdateTime	The time when the last update to the cache occurred due to a change in the **Tests** tree.
TreeInitializationTimeInMillis	The duration in milliseconds it took to load the whole project tree into the cache. This value will not change as long as the project cache is loaded.
TreeSize	The number of test nodes, which are test containers, test folders, and tests, in the project.
UpdateChecks	The number of checks for changes of the **Tests** tree for this project since the project tree cache was initialized.
Updates	The number of updates of the cached tree due to changes in the **Tests** tree.

Test Filter Cache Measures

The *TestPlanFilterCache* measure is comprised of the following three measures:

Measure	Description
Hits	The number of times the cache was used and no separate execution of the filter on the database was necessary.
Misses	The number of times the filter cache was not used, but the filter was executed against the database.
Size	The current number of cached filter results.

JMX Measures for Monitoring the LQM Reporting Updater

LQM Reporting Updater Measures

The following measures are available:

Measure	Description
LastDataLoadResetTime	Gives the time when the last reset of the LQM reporting tables was performed. If this attribute is null, then no reset was performed during the lifetime of the process.
LastDeleteDurationInMillis	Time used to remove deleted nodes from the LQM Reporting tables.
LastDeleteTestsCnt	Number of tests deleted in the last run.
LastInsertLQMTestsDuration	Time used to insert new tests in the `LQM_Tests` table.
LastInsertLQMTestPDAsDuration	Time used to insert new tests in the `LQM_TestPDAs` table.
LastInsertLQMTestUDAsDuration	Time used to insert new tests in the `LQM_TestUDAs` table.
LastRunFromDate	Gives the start of the time span processed for the current update cycle.
LastRunToDate	Gives the end of the time span processed for the current update cycle.
LastSelectChangedDataIterateDurationInMillis	Time used for iterating changed data.
LastSelectChangedDataQueryDurationInMillis	Time used for querying changed data.
LastTotalUpdateDurationInMillis	Total time used for the last update run.
LastUpdateFixedAttributesDurationInMillis	Duration of the last update of fixed attributes.
LastUpdatePDAttributesDurationInMillis	Duration of the last update of the `LQM_TestPDAs` table.
LastUpdatesNeededCheckDurationInMillis	The duration (in milliseconds) of the last check for new or changed data.
LastUpdatesNeededCheckOracleWaitForTableLocksDuration	Oracle requires special handling when checking for updated tests. It may be necessary to wait for other processes to finish their transactions on test tables. The time waited for these transactions is measured by this attribute.
LastUpdateTestsDurationInMillis	Duration of the last update of properties in the `LQM_Tests` table.
LastUpdateUDAttributesDurationInMillis	Duration of the last update of `LQM_TestUDAs` table.

JMX Measures for Data Mart

Data Mart Updater Measures

JMX information on the Data Mart Updater can be found on your application server in the JMX measures tree at `borland.com/DataMart/TM`:

Measure	Description
AverageCheckDurationInMilliseconds	Average time in milliseconds used to check for updated rows
AverageUpdateDurationInMilliseconds	Average time in milliseconds used to update rows
FailedCheckCount	Number of failed checks for updates

Measure	Description
FailedUpdateCount	Number of failed updates
FastestCheckInMilliseconds	Shortest time in milliseconds used to check for updated rows
FastestUpdateInMilliseconds	Shortest time in milliseconds used to update rows
Id	ID of Data Mart Updater
IntervalInMilliseconds	Interval in milliseconds which defines how often the Data Mart Updater runs
LastBlockedRunDate	Time when the execution was blocked the last time (wait for exclusive access failed)
LastFailedRunDate	Time when the execution failed the last time
LastSuccessfulRunDate	Time when the execution completed successfully the last time
LatestDataLoadInfo	Information about the latest data load
SlowestCheckInMilliseconds	Longest time in milliseconds used to check for updated rows
SlowestUpdateInMilliseconds	Longest time in milliseconds used to update rows
SlowestWaitForExclusiveAccessInMilliseconds	Longest time in milliseconds used to wait for exclusive access
StartupDate	Time when the Data Mart Updater was initialized
SuccessfulCheckCount	Number of successful checks for updates
SuccessfulUpdateCount	Number of successful updates

Data Mart Service Measures

JMX information on the Data Mart service can be found on your application server in the JMX measures tree at `borland.com/DataMart/Service`:

Measure/Operation	Description
Enabled	Shows whether the Data Mart service is enabled or disabled.
disable()	Disables the Data Mart service.
enable()	Enables the Data Mart service.
isEnabled()	Queries whether the Data Mart service is enabled or disabled.

JMX Measures for LDAP Synchronization

JMX information on the LDAP synchronization can be found on your application server in the JMX measures tree at `borland.com/LdapUpdater`.

Measure/Operation	Description
Enabled	Shows whether automatic LDAP synchronization is enabled or disabled.
LastDurationInMillis	Duration of the last LDAP synchronization in milliseconds.
enable()	Enables the automatic LDAP synchronization.

Measure/Operation	Description
disable()	Disables the automatic LDAP synchronization.

JMX Measures for Limiting Usage of REST Services

If you want to limit the usage of REST API services, you can find the relevant JMX measures under `borland.com/RestService/LimitingFilter` in the JMX measures tree on your front-end server.

Set the *Overdraft* measure for a session token to specify the limit for a burst usage of the REST service and set the *RefillPerMinute* measure to specify the permanent usage-limit-per-minute. Handling usage bursts in such a way is known as the token-bucket algorithm. Exceeding the limit will result in a `429 - Too Many Requests` response to a service call and the user will be asked to try again later.

LoginPasswordAuthentication Measures

Here you can set the request limits for a user to obtain a session ID through basic authentication using username and password.

Note: Micro Focus recommends authentication through a web-service token.

Measure	Description
FilterEnabled	Whether limiting usage is enabled or not. True or false.
Overdraft	The maximum number of login requests that can happen in a burst scenario.
RefillPerMinute	The average number of login requests that is allowed.
MinimumRemainingTokens	The number of tokens in the bucket with the fewest tokens since the service was started or since the *Overdraft* and the *RefillPerMinute* were set.
MinimumRemainingTokensBucket	The login of the user with the bucket that has the fewest available tokens.

SessionIdAuthentication Measures

Here you can set the request limits for each web-service token or each session ID.

Measure	Description
FilterEnabled	Whether limiting usage is enabled or not. True or false.
Overdraft	The maximum number of requests that can happen in a burst scenario with a specific web-service token or with a specific session ID.
RefillPerMinute	The average number of requests that is allowed with a specific web-service token or with a specific session ID.
MinimumRemainingTokens	The number of tokens in the bucket with the fewest tokens since the service was started or since the *Overdraft* and the *RefillPerMinute* were set.
MinimumRemainingTokensBucket	The web-service token or the session ID with the fewest available tokens.

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 Silk Central 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. On the **Instance Administration** page, stop the application server of the instance that you want to modify.
2. Open the `java.security` file with a text editor.

   The default path for this file is `C:\Program Files (x86)\Silk\Silk Central 20.5\instance_<instance number>_<instance name>\lib\jre\lib\security` on the application server. If your application server runs in 64-bit mode, use the `jre64\lib\security` folder instead.
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.

Configuring the Silk Central Location in Issue Manager

Describes how to configure the location of your Silk Central installation in Issue Manager. This enables the traceability from issues in Issue Manager to related tests in Silk Central. For additional information on using the traceability feature, refer to the Issue Manager documentation.

To configure the Silk Central location in Issue Manager:

1. On the **Instance Administration** page, stop the front-end server of the instance that you want to modify.
2. Open the `SRFrontendBootConf.xml` file with a text editor.

   The default path for this file is `C:\Program Files (x86)\Silk\Silk Central 20.5\instance_<instance number>_<instance name>\Conf\FontendServer` on the front-end server.
3. Locate the `Alm\ElementServiceEndpoint` and `Alm\LinkServiceEndpoint` XML tags.
4. Replace the default values `localhost:19120` with the host and port information of your Silk Central installation in both tags.

   If your Silk Central installation uses the same front-end server as your Issue Manager installation, and you use Tomcat Web server with the default port, then you can leave the default values.
5. Save and close the XML file.
6. If you do not use the default port, edit the file `configuration.xml`, located in `\instance_<instance number>_<instance name>\wwwroot\AlmServices1.0`. Locate the `connectString` XML tag and set the correct ports.

   Example:

```
<properties>
   <name>connectString</name>
   <!-- value>com.borland.tm.system.endpoint=http://gershwin:19120/services/
sccsystem;
      com.borland.tm.spi.endpoint=http://gershwin:19120/services/
```

```
SpiService</value  -->
   <value>com.borland.tm.system.endpoint=http://MyHost:8555/services/
sccsystem;
      com.borland.tm.spi.endpoint=http://MyHost:8555/services/SpiService</
value>
</properties>
```

7. Re-start the front-end server.

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 Silk Central.

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 Central 20.5 Execution Server\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.

Setting the Maximum Number of MRU Reports

To set the maximum number of MRU reports that displays in the **Last Used Reports** list box:

1. On the **Instance Administration** page, stop the front-end server of the instance that you want to modify.
2. Open the `TMFrontendBootConf.xml` file with a text editor.

   The default path for this file is `C:\Program Files (x86)\Silk\Silk Central 20.5\instance_<instance number>_<instance name>\Conf\FontendServer` on the front-end server.
3. Locate the `<MRUListSize>` XML tag in the `<Report>` section of the file.

   The default value for this tag is `10`.
4. Set the value to the maximum number of reports that you want to have displayed in the **Last Used Reports** list box.
5. Save and close the XML file.
6. Re-start the front-end server.

Memory Settings for Silk Central Servers

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

The Java heap size of the Silk Central front-end and application servers is set by default to 512 MB (2048 MB for 64-bit front-end server). If you are experiencing out-of-memory errors, for example while copying a project in Silk Central, try to increase the heap size on the front-end or application server.

The following error is an indicator that the Java heap size is to small: `java.lang.RuntimeException: java.lang.OutOfMemoryError: Java heap space`. This error is reported in the logfile of the front-end server or the application server. Another indicator is the error message `The system is now working close to capacity. For security reasons no more users will be permitted to login`, which displays when you try to login to Silk Central.

Increasing the Java Heap Size on a Silk Central Server

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

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

1. On the **Instance Administration** page, stop the instance that you want to modify.
2. Open the `sc_<server>.processconfig` file of the server for which you want to change the memory settings with a text editor. The default path for these files is `C:\Program Files (x86)\Silk\Silk Central 20.5\instance_<instance number>_<instance name>\Conf`.
3. Set the value in the `<JvmOption name="-Xmx"` tag under `<JvmOptions>`.
4. Save and close the XML file.
5. Start the instance again.

Setting the Maximum Size of Result Files from Manual Tests

Limit the size of result files that are uploaded to the front-end server from the Manual Testing window, by using the REST API, or by using the test planning web service.

1. On the **Instance Administration** page, stop the front-end server of the instance that you want to modify.
2. Open the `TMFrontendBootConf.xml` file with a text editor.

   The default path for this file is `C:\Program Files (x86)\Silk\Silk Central 20.5\instance_<instance number>_<instance name>\Conf\FontendServer` on the front-end server.
3. Locate the `<MaximumResultFileSizeInBytes>` XML tag.
4. Set the value to the maximum file size you want to allow. Enter the file size in bytes.
5. Save and close the XML file.
6. Re-start the front-end server.

To limit the file size of result files that are generated by automated tests on the execution servers, see *Setting the Maximum Size of Result Files from Automated Tests*.

Setting the Maximum Size of Result Files from Automated Tests

Limit the file size of result files that are generated by automated tests on the execution servers.

1. On the **Instance Administration** page, stop the application server of the instance that you want to modify.
2. Open the `TMAppServerHomeConf.xml` file with a text editor.

The default path for this file is `C:\Program Files (x86)\Silk\Silk Central 20.5\instance_<instance number>_<instance name>\Conf\AppServer` on the application server.

3. Locate the `<MaximumESResultFileSizeInBytes>` XML tag.
4. Set the value to the maximum file size you want to allow. Enter the file size in bytes.
5. Save and close the XML file.
6. Re-start the application server.

To limit the file size of result files that are uploaded to the front-end server from the Manual Testing window, by using the REST API, or by using the test planning web service, see *Setting the Maximum Size of Result Files from Manual Tests*.

Storing Percentile Marker Data for Silk Performer Results

Silk Performer results contain a high amount of percentile marker data that would consume a lot of space in the database (table `TM_PerfReportPercentileMarker`). Therefore, storing this information is disabled by default. To enable the storing of percentile marker data whenever Silk Performer results are stored, proceed as follows:

1. On the **Instance Administration** page, stop the application server of the instance that you want to modify.
2. Open the `TMAppServerHomeConf.xml` file with a text editor.

   The default path for this file is `C:\Program Files (x86)\Silk\Silk Central 20.5\instance_<instance number>_<instance name>\Conf\AppServer` on the application server.
3. Locate the `Config/SilkPerformerResultStorage/StorePercentileMarkerData` XML tag. By default, the tag is set to `false`.
4. Set the value to `true`.
5. Save and close the XML file.
6. Restart the application server.

Index

32bit
    setup type 11
64bit
    setup type 11

A

accessing
    databases 35
accounts
    system administrator 38
adding
    chart servers 42
    instances 28
    LDAP servers 47
adjusting
    cookie duration 53
advanced settings
    configuring 52
application server
    location 46
    specifying location 46
application server logs
    page for system administrator 52
application servers
    installing 12
architecture
    overview 5
attachments
    storing on file system 57
automatic user account creation
    LDAP 47

B

BIRT
    enabling SSL connections 26

C

caching
    JMX measures in tests 60, 62
chart servers
    adding 42
    editing 43
    installing 12
    locations 42
    page 43
    removing connections 43
clients
    about 38
    creating 39
    default 40
    editing 39
    page 41
    permissions 42
    removing 40
configuring
    advanced settings 52
    JMX settings 61
    LQM reporting updater 58
    non-standard SSL ports for execution servers 27
    remeber login option 53
    Silk Central location 66
connection
    JMX 28
cookie duration
    adjusting 53
creating
    databases 34
customizing
    date and time formats 56

D

data caching
    tests 59
databases
    accessing 35
    ALM URIs 36
    creating 34
    database page 37
    disconnecting 36
    IDs 36
    overview 32
    roles 34
    user privileges 34
date and time
    user-defined settings 54
date formats
    customizing 56
DBMS 33
deleting
    instances 28
    LDAP servers 49
disabling
    caching of host name resolutions 66
    unused ports on execution servers 27, 67
disconnecting
    databases 36
displaying
    host name on Web browsers 56

E

Edit LDAP Server
    dialog box 47
editing
    chart servers 43
    LDAP servers 48
email server
    about 44
    configuring 44
    page 44
evaluation

installation 12
execution duration
suspicious 53
execution servers
configuring non-standard SSL ports 27
disabling unused ports 27, 67
host name resolution 65
installing, Linux 16
installing, virtual infrastructures 17
silent mode 15
external systems
communicating over SSL 28

F

files
location 5
formats
date and time 54
free disk space 34
front-end server
logs 52
front-end servers
configuring load balancing 31
installing 12

G

generating license policies 20
guidelines
secure environment 25

H

hiding
host name on Web browsers 56
host IDs 20
host name
displaying on Web browsers 56
hiding on Web browsers 56
host name display
Web browsers 56
host name resolution
disabling caching 66
hotfix
installing 18, 30

I

increasing
server Java heap sizes 68
infrastructure
managing 25
installing
evaluation version 12
execution servers 15
execution servers, Linux 16
execution servers, virtual infrastructures 17
hotfix 18, 30
process overview 10
production 12
standalone 12
Windows execution servers 15
installing execution servers
silent mode 15
instances
adding 28
deleting 28
maintenance 28
managing 28
overview 25
removing 28

J

Java heap sizes
increasing 68
JMX
connection 28
JMX measures
LDAP synchronization 64
monitoring Data Mart 63
monitoring LQM reporting updater 62
JMX settings
configuring 61

L

LDAP
authentication 46
integration 46
synchronizing groups 59
LDAP authentication
logic 46
mixed mode 46
standard mode 46
LDAP servers
adding 47
automatic user account creation 47
deleting 49
editing 48
page 49
testing connection 49
license policies 20
license servers
modifying configuration 21
requirements 21
license types 19, 40
licenses
checking out and in 19, 40
licensing
overview 19
test connections 22
limiting usage
REST services 65
Linux
execution servers, installing 16
load balancing
configuring for front-end servers 31
overview 31
load test agent cluster files
editing 50
load test agent clusters

page 51
removing 50
Silk Performer 50
uploading 50
load test agent clusters file
adding 50
changing 50
deleting 50
log files
location 5
login
configuring remember login option 53
cookie duration 52
enhanced options 52
remember login 52
login options
adjusting cookie duration 53
configuring remember login option 53
enhanced 52
LQM reporting updater
configuring 58

M

maintenance
instances 28
managing
infrastructure 25
instances 28
maximum size
result files, automated tests 68
result files, manual tests 68
memory settings
servers 67
MRU reports
setting maximum number 67
MS SQL server 33

N

New LDAP Server
dialog box 47
new versions 18

O

Oracle
free disk space 34
temporary tablespace sizes 34
overview
architecture 5
instances 25

P

percentile marker data
Silk Performer results 69
storing 69
ports
disabling unused on execution servers 27, 67
production
installations 12

R

RDBMS 33
removing
instances 28
REST services
JMX measures, limiting usage 65
result files
maximum size, automated tests 68
maximum size, manual tests 68
storing on file system 57

S

secure environment
guidelines 25
servers
increasing Java heap sizes 68
memory settings 67
service manager
starting execution server service 30
stopping execution server service 30
services
starting 28
stopping 28
setting
suspicious execution duration 53
setting maximum number
MRU reports 67
setup type
operating system 11
Silk Central location
configuring in Issue Manager 66
Silk Meter
changing license servers 21
installing 21
installing on license servers 21
modifying configuration 21
testing connections 22
uninstalling 21
Silk Performer
load test agent clusters 50
Silk Performer results
percentile marker data 69
SQL 33
SSL
handling self-signed certificates 28
secure web server connections 25
SSL connections
enabling for BIRT 26
starting
services 28
starting execution server service
service manager 30
stopping
services 28
stopping execution server service
service manager 30
storing
percentile marker data 69

storing on file system
attachments 57
result files 57
suspicious execution duration
setting 53
synchronizing
groups from LDAP 59
system administration
overview 32
system administrator 32
system administrator
accounts 38
system diagnostics
system diagnostics page 51
viewing 51
system proxy
client enablement 45
configuring 45
page 45

T

temporary tablespace sizes 34
testing
connection to LDAP servers 49
tests
data caching 59
JMX measures for caching 60, 62
time formats
customizing 56

U

Unix
execution servers, installing 16
upgrading 18

W

Web browsers
displaying host name 56
hiding host name 56
host name display 56
web server connections
SSL 25
Windows execution servers 15