



Silk Central 18.5

Installations- und
Systemkonfigurationshilfe

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

Copyright © Micro Focus 2004-2017. Alle Rechte vorbehalten.

MICRO FOCUS, das Logo von Micro Focus und Silk Central sind Markenzeichen oder eingetragene Markenzeichen der Micro Focus IP Development Limited oder deren Tochtergesellschaften bzw. Konzerngesellschaften in den Vereinigten Staaten, Großbritannien und anderen Ländern.

Alle anderen Markenzeichen sind Eigentum der jeweiligen Inhaber.

2017-10-23

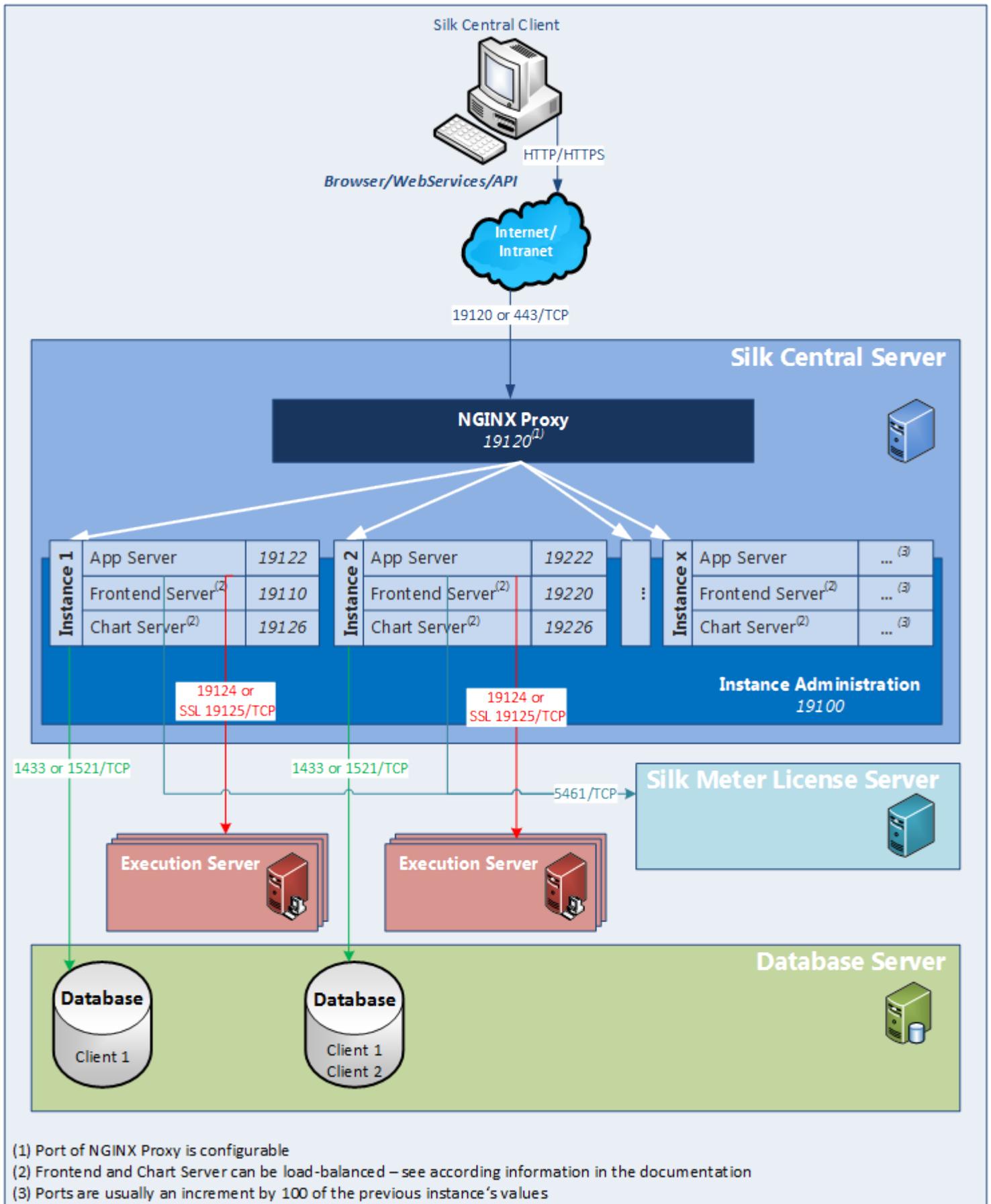
Inhalt

Silk Central-Architektur	5
Installieren von Silk Central	10
Systemanforderungen und Voraussetzungen	10
Installieren von Silk Central zu Evaluationszwecken	11
Installieren von Silk Central	12
Installieren eines Windows-Ausführungsservers	14
Installieren eines Linux-Ausführungsservers	15
Installieren von einem Hotfix	16
Aktualisieren auf Silk Central 18.5	16
Silk Central	17
Lizenzverarbeitung	17
Erzeugen eines Silk Central-Lizenzierungsschemas	18
Ermitteln der Hostkennung	18
Installieren von Silk Meter	19
Silk Meter-Lizenzserverkonfiguration	19
Ändern der Lizenzserverkonfiguration	20
Getestete und unterstützte Software	20
Konfigurieren und Verwalten der Infrastruktur	23
Aufsetzen eines sicheren Silk Central-Systems	23
Allgemeine Richtlinien	23
Sichere Webserververbindungen mit SSL aktivieren	23
BIRT-Berichte in SSL-Umgebungen aktivieren	24
Konfigurieren eines benutzerdefinierten SSL-Ports für Ausführungsserver	25
Deaktivieren nicht verwendeter Ports auf Ausführungsservern	25
Kommunikation mit einem externen System über SSL	26
Verwalten von Instanzen	26
Installieren von einem Hotfix	28
Starten oder Stoppen eines lokalen Ausführungsserverdienstes	29
Lastausgleichsmechanismus für Front-End-Server	29
Verwalten von Mandanten	30
Systemadministrator	30
Datenbanken	31
Mandanten	37
Infrastruktur	41
Systemdiagnose	51
Konfigurieren erweiterter Einstellungen	52
Anmeldeoptionen	52
Verdächtige Ausführungsdauer	54
Deaktivieren der Aktualisierung externer Fehlerstatistiken	54
Datums- und Zeitformate	55
Hostnamensanzeige	57
Speichern von Anhängen und Ergebnisdateien auf dem Dateisystem	57
Konfigurieren von LQM Reporting Updater	58
Ausführungstermine für die automatische LDAP-Synchronisierung planen	59
Zwischenspeicherung von Daten in Tests	60
Konfigurieren der JMX-Einstellungen	62
Hostnamenauflösung des Ausführungsservers	66
Konfigurieren des Silk Central-Standorts in Issue Manager	67
Deaktivieren nicht verwendeter Ports auf Ausführungsservern	67
Festlegen der Anzahl zuletzt angezeigter Berichte	68
Speichereinstellungen für Silk Central-Server	68

Festlegen der maximalen Größe von Testschritt-Ergebnisdateien	69
Speichern von Perzentil-Markierungsdaten für Silk Performer-Testergebnisse	69

Silk Central-Architektur

Dieser Abschnitt enthält einen Überblick über die Architektur von Silk Central.



(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

Der Server auf dem das Silk Central-Setup ausgeführt wurde.

Instanzen-Verwaltung

Instanzen und deren Silk Central-Dienste werden über eine gemeinsame Benutzeroberfläche namens **Instanzen-Verwaltung** verwaltet, auf welche Sie über die URL `http://localhost:19100` auf dem Server wo Silk Central installiert ist zugreifen können.

Instanzen

Eine Instanz ist ein unabhängiges Set von Silk Central-Diensten (Anwendungsserver (AS), Front-End-Server (FE) und Diagrammserver (CS)), mit eigener Datenbank und eigenen Ausführungsservern (ES). Standardmäßig erstellt Silk Central eine einzelne Instanz namens *silk* für Sie. Die Standard-URL ist `http://<Computername>:19120/login` (keine Portinformationen nötig wenn Silk Central auf IIS läuft).

Proxy

Ein Proxy-Dienst wird auf dem Silk Central-Server installiert, um den Zugang zu den verschiedenen Instanzen zu verwalten. Die Dienste der verschiedenen Instanzen laufen auf unabhängigen Ports, aber aus Sicherheitsgründen und für eine größere Flexibilität, leitet der Proxy den Instanznamen auf die eigentlich URL um, und zwar in der folgenden Form: `http://<Silk Central-Server>:19120/<Instanzname>`.

Anwendungsserver (AS)

Der Anwendungsserver synchronisiert Aufgaben, wie etwa die Verteilung der Ausführungspläne, das Steuern der Ausführungsserver und die Verwaltung der Datenbankkonfiguration. Diese Aufgaben erfordern eine zentrale Steuerung, damit die konsistente und zuverlässige Ausführung gewährleistet ist. Außerdem wertet der Anwendungsserver die Ergebnisse aus, speichert diese in der Datenbank und sendet anhand der Erfolgsbedingungen Benachrichtigungen. Der Anwendungsserver verwendet Port 19122 für die Standard-Instanz. Für jede weitere Instanz wird dieser Wert um 100 erhöht.

Front-End-Server (FE)

Der Front-End-Server ist für die grafische Benutzeroberfläche zuständig. Er basiert auf HTML und kann mit einem beliebigen Webbrowser (z.B. Internet Explorer, Chrome und Firefox) aufgerufen werden. Der Benutzer sendet eine entsprechende HTTP-Anforderung an den Front-End-Server, und daraufhin wird eine Anmeldeseite zur Authentifizierung im Browser geöffnet. Nach der erfolgreichen Anmeldung kann der Benutzer auf die Anwendungen und Funktionen zugreifen, für die er über Berechtigungen verfügt. Der Front-End-Server kann als eigenständiger HTTP-Server ausgeführt oder in einen anderen Webserver (z. B. IIS) eingebunden werden. Der Front-End-Server verwendet Port 19110 für die Standard-Instanz. Die zweite Instanz verwendet Port 19220, und für jede weitere Instanz wird dieser Wert um 100 erhöht. Für sichere Verbindungen mit SSL verwendet der Server zudem Port 443. Der Front-End-Server kann über die URL `http://<Silk Central-Server>:19120/<Instanzname>` erreicht werden (die Standard-Instanz benötigt keinen Instanznamen).

Diagrammserver (CS)

Der Diagrammserver erzeugt die in den Berichten verwendeten Diagramme. Das System ermöglicht das Konfigurieren eines Pools von Diagrammservern. Die Verarbeitung wird dann durch einen internen Lastausgleichsmechanismus auf die Server im Pool verteilt. Mit einem Diagrammserver können auch Berichte erzeugt und direkt an den Endbenutzer gesendet werden. Der Diagrammserver verwendet Port 19126 für die Standard-Instanz. Für jede weitere Instanz wird dieser Wert um 100 erhöht.

Ausführungsserver (ES)

Der Ausführungsserver führt automatisierte Tests aus, die von autorisierten Benutzern geplant wurden. Die Benutzer sind für die richtige Konfiguration der Ausführungsserver und der sonstigen für die Ausführung erforderlichen Ressourcen verantwortlich. Es können mehrere Ausführungsserver installiert und konfiguriert werden, die unabhängig voneinander laufen. Der Ausführungsserver verwendet Port 19124 für die Standard-Instanz. Für sichere Verbindungen mit SSL verwendet der Server zudem Port 19125.

Agentencomputer:

- und -Agentencomputer werden aus dem Pool von Agentencomputern, die für den steuernden Computer verfügbar sind, bestimmten - und/oder Silk Performer-Projekten zugewiesen. Der steuernde Computer dient zusammen mit Silk Central als Ausführungsserver.

Silk Performer-Agenten Auf den Silk Performer-Agentencomputern befinden sich die virtuellen Benutzer, die während der Lasttests verwendet werden. Einem Silk Performer-Projekt können so viele Agentencomputer hinzugefügt werden, wie virtuelle Benutzer für die Testausführung erforderlich sind. Die Konfiguration der Agenten wird mit Silk Performer durchgeführt. Nähere Informationen zur Agentenkonfiguration finden Sie in der Dokumentation zu Silk Performer.

Silk Test Classic-Agenten Die -Agenten entsprechen den -Agenten, nur dass auf den -Agentencomputern Silk Performer-Tests ausgeführt werden.

Datenbankserver (DB)

Die dauerhafte Datenspeicherung wird durch ein relationales Datenbankmanagementsystem (RDBMS) implementiert. Der Datenbankserver verwendet die Ports 1433 (SQL Server) oder 1521 (Oracle).

Silk Meter-Lizenzserver

Silk Meter, die im Lieferumfang von Silk-Produkten enthaltene Lizenzierungssoftware, bestimmt, auf welche Funktionen der Anwendung Silk Central Sie zugreifen können. Weitere Informationen zur Lizenzierung finden Sie im Installationshandbuch zum jeweiligen Produkt. Silk Meter verwendet Port 5461.

Mandanten

Mandanten sind getrennte Einheiten innerhalb einer Silk Central-Instanz. Ein Mandant kann z.B. ein *Kunde* oder ein *Geschäftsbereich* eines Unternehmens sein. Mandanten erhöhen die Datensicherheit, aber im Gegensatz zu Instanzen verwenden sie dieselbe Datenbank und dieselben Silk Central-Dienste. Jeder Mandant besteht aus den folgenden Hauptobjekten:

- Benutzerrollen und Berechtigungen
- Benutzergruppen und Benutzerkonten
- Projekte
- Servergruppen, Ausführungsserver und Agentencomputer
- Produkte mit Komponenten, Versionen und Builds
- Allgemeine Ausführungstermine

Projekte

Projekte reflektieren in Silk Central üblicherweise ein Software-Projekt in Ihrer Firma, respektive die Arbeit eines Entwicklungsteams, mit gemeinsamem Release-Datum, Versionsverwaltungssystem, gemeinsamen Anforderungen, usw. Jedes Projekt besteht aus den folgenden Hauptobjekten:

- Filter
- Attribute
- Anforderungseigenschaften
- Testschritteigenschaften

- Benachrichtigungen
- Anforderungs- und Fehlerverwaltungsintegrationen
- Integriertes Versionsverwaltungssystem
- Datenquellen
- Statusursachen

Wichtige Datei-Speicherorte

- Instanzen-Verwaltungs- und Ausführungsserver Logdateien: C:\ProgramData\SilkCentral\log
- Anwendungs-, Front-End- und Diagrammserver Logdateien: C:\ProgramData\SilkCentral\instance_<Instanznummer>_<Instanzname>\log
- Speicherort für Hotfixes: C:\Program Files (x86)\Silk\hotfixes
- Konfigurationsdateien: C:\Program Files (x86)\Silk\instance_<Instanznummer>_<Instanzname>\Conf
- Plug-Ins: C:\Program Files (x86)\Silk\instance_<Instanznummer>_<Instanzname>\Plugins
- Zuordnungsdateien für Office-Import: C:\ProgramData\SilkCentral\instance_<Instanznummer>_<Instanzname>\OfficeImportMappingFiles

Installieren von Silk Central

Die Silk Central Installations-DVD und das Setup Programm ermöglichen Ihnen, sämtliche Silk Central-Softwarekomponenten zu installieren.

Der Computer, auf dem Silk Central installiert werden soll, muss die Systemanforderungen erfüllen. Das Installationsprogramm prüft, ob das System diese Voraussetzungen erfüllt, und ermöglicht dann das Installieren der erforderlichen Software.

 **Hinweis:** Sie müssen auf dem Computer über Administratorrechte verfügen, um Silk Central zu installieren.

Systemanforderungen und Voraussetzungen

Für eine optimale Leistung von Silk Central wird die in diesem Abschnitt erläuterte Konfiguration empfohlen.

Server-Systemvoraussetzungen

Systembereich	Anforderung
Prozessor	Intel Core i5 oder besser
Speicher	Mindestens 8 GB
Freier Festplattenspeicher	Mindestens 30 GB, außer für den Datenbankserver
Netzwerk	100 MBit
Betriebssystem, DBMS, Webserver	Siehe Getestete und unterstützte Software .
Stromversorgung	Um Datenverluste bei einem Stromausfall zu vermeiden, wird für alle Umgebungen eine USV (unterbrechungsfreie Stromversorgung) empfohlen.

Für jede zusätzliche Instanz werden mindestens 10 GB zusätzlicher Festplattenplatz benötigt, sowie mindestens der folgende initiale Systemspeicher:

- Front-End-Server: 500 MB
- Anwendungsserver: 300 MB
- Diagrammserver: 200 MB

Je nach Ihrem Workload könnten diese Werte noch höher sein.

Weitere Informationen zur optimalen Konfiguration von Silk Central erhalten Sie vom technischen Support oder Ihrem Technical Account Team.

Anforderungen an Ausführungsserver

Die tatsächlichen Anforderungen und Voraussetzungen, die ein Anwendungsserver erfüllen muss, richten sich nach der getesteten Anwendung (Application under Test, AUT) und der Art des Tests.

Für einen Lasttest müssen die Umgebungsanforderungen von Silk Performer erfüllt werden. Lasttests mit der Mindestkonfiguration können zu ungenauen Ergebnissen führen.

Beachten Sie bei Funktionstests die Umgebungsanforderungen von Silk Test. Für umfassende Tests (wie Browser-Wiedergaben) wird ein Arbeitsspeicher mit mindestens 2048 MB empfohlen.

Ein Linux Ausführungsserver benötigt Java Runtime Environment (JRE) 8.

Anforderungen an Proxy-Server

Wenn Sie Microsoft IIS für Silk Central verwenden möchten, installieren Sie zuerst die folgenden IIS-Erweiterungen, bevor Sie Silk Central installieren:

- Application Request Routing (ARR)
- URL Rewrite

Die aktuellsten Versionen dieser Erweiterungen können von der Seite [IIS Downloads](#) heruntergeladen werden.

Virtualisierung

Silk Central kann in der virtuellen Infrastrukturmgebung VMware vSphere Server ausgeführt werden.

Client-Systemvoraussetzungen

Systembereich	Anforderung
Prozessor	Intel Core i3 oder besser
Speicher	2 GB
Browser	<ul style="list-style-type: none">• Google Chrome• Internet Explorer 10 oder höher (ohne Kompatibilitätsmodus)• Mozilla Firefox• Microsoft Edge

Die Benutzeroberfläche für manuelles Testen benötigt Java Runtime Environment (JRE) 7 Update 79 oder höher.

Installieren von Silk Central zu Evaluationszwecken

Laden Sie zuerst die ausführbare Datei von Silk Central herunter, oder legen Sie die Silk Central-DVD in das DVD-Laufwerk ein.



Hinweis: Da die Installation von Microsoft SQL Server Express Administratorrechte benötigt, scheitert die Installation wenn die Benutzerkontensteuerung (UAC) eingeschaltet ist. Schalten Sie die Benutzerkontensteuerung (UAC) auf dem Rechner aus, auf dem Sie Silk Central für Evaluationszwecke installieren möchten.

Richten Sie eine Einzelplatzinstallation ein, bei der sämtliche Komponenten auf einem einzigen Computer installiert werden. Beachten Sie, dass bei einer Einzelinstallation nicht die volle Leistung von Silk Central zur Verfügung steht. Dieser Installationstyp ist nur für Evaluations- und Demozwecke geeignet.



Hinweis: Das .NET Framework 3.5 SP1 Setup kann nicht während der Installation von Silk Central unter Microsoft Windows Server 2008 R2, Windows Microsoft Windows Server 2008 R2 SP1 oder Microsoft Windows Server 2012 ausgeführt werden. Wenn .NET Framework 3.5 SP1 nicht in Ihrem System installiert ist, Ihr Betriebssystem Microsoft Windows Server 2008 R2, Windows Microsoft Windows Server 2008 R2 SP1 oder Microsoft Windows Server 2012 ist und Sie die Testversion von installieren möchten, installieren Sie .NET Framework 3.5 SP1 mithilfe von Windows Server Manager in Ihrem System, bevor Sie Silk Central installieren.

1. Suchen Sie die ausführbare Datei von Silk Central, und doppelklicken Sie auf die Datei. Der InstallShield-Assistent wird geöffnet.
2. Folgen Sie den Anweisungen des Installationsassistenten und klicken Sie auf den Dialogen jeweils auf **Next** oder **OK**.

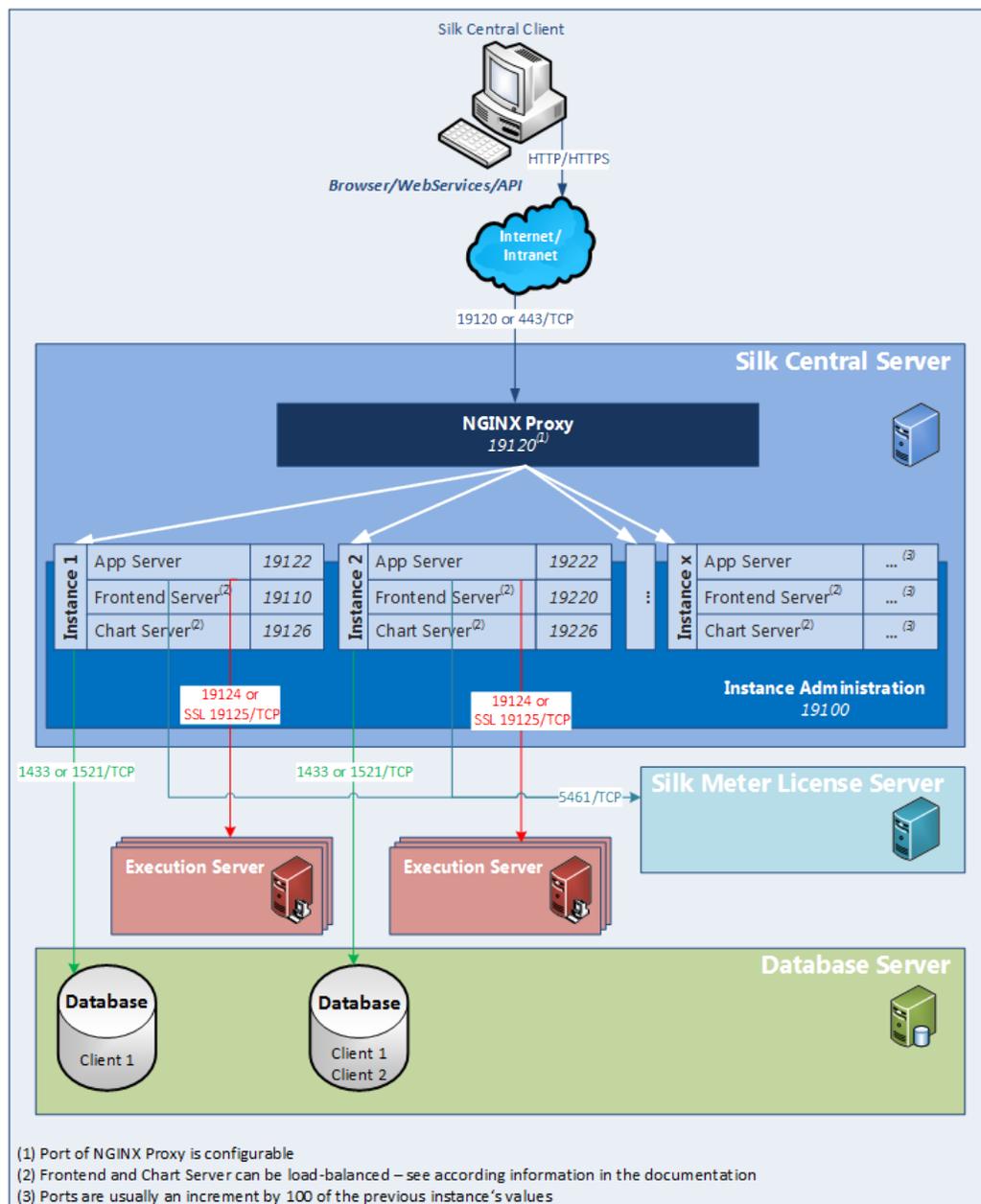
3. Lassen Sie auf dem Dialog **Select Licensing Mode** die Standardeinstellung auf **Evaluation**.

Silk Central benötigt ein Datenbank-Repository. Für Evaluationszwecke empfehlen wir die Verwendung von Microsoft SQL Server Express, welches als Teil von Silk Central installiert werden kann. Stellen Sie sicher, dass das Kontrollkästchen **Install Microsoft SQL Server 2008 Express SP1** aktiviert ist.

4. Klicken Sie auf **Next** um die Installation abzuschließen.

Installieren von Silk Central

Laden Sie zuerst die ausführbare Datei von Silk Central herunter, oder legen Sie die Silk Central-DVD in das DVD-Laufwerk ein. Stellen Sie sicher, dass Ihr System die [Systemanforderungen und Voraussetzungen](#) erfüllt.



1. Suchen Sie die ausführbare Datei von Silk Central, und doppelklicken Sie auf die Datei.
Wenn Sie die Silk Central-DVD verwenden, legen Sie die DVD ein. Wenn das Silk Central-Installationsprogramm nicht automatisch gestartet wird, wählen Sie **Start > Ausführen**, und geben Sie <DVD-Laufwerk>:\setup.exe ein.
Der InstallShield-Assistent wird geöffnet.
2. Der Begrüßungsbildschirm des Assistenten wird geöffnet. Der Assistent führt Sie durch die verschiedenen Installationsschritte. Klicken Sie auf **Weiter**.
3. Wählen Sie die gewünschte Sprache aus, und klicken Sie dann auf **Next**. Das Fenster **License Agreement** wird angezeigt.
4. Lesen Sie die Lizenzvereinbarung sorgfältig durch. Wenn Sie mit den Bestimmungen einverstanden sind, klicken Sie auf **I accept the terms of the license agreement**. Die Seite **Setup Type** wird geöffnet.
5. Um den Silk Central-Ausführungsserver zu installieren, aktivieren Sie das Kontrollkästchen **Install Execution Server**. Um Microsoft Internet Information Services (IIS) zu verwenden, haken Sie das Kontrollkästchen **Use Microsoft Internet Information Services** an.
Das Standardinstallationsziel wird im Bereich **Destination path** des Dialogs **Setup Type** angezeigt. Wenn Sie das Standardinstallationsverzeichnis ändern möchten, führen Sie die folgenden Schritte aus:
 - a) Klicken Sie auf **Durchsuchen**. Der Dialog **Ordner auswählen** wird angezeigt.
 - b) Wählen Sie das Installationsverzeichnis für Silk Central aus, und klicken Sie auf **OK**, um zum Dialogfeld **Setup-Typ** zurückzukehren.

 **Hinweis:** Silk Central muss auf einem lokalen Laufwerk installiert werden. Wenn Sie ein ungültiges Installationsziel auswählen, wird eine Fehlermeldung angezeigt.
6. Klicken Sie auf **Weiter**. Der Dialog **Installation Options Summary** wird mit den ausgewählten Installationsoptionen angezeigt.
7. Überprüfen Sie die Informationen, und führen Sie einen der folgenden Schritte aus:
 - Wenn Sie Einstellungen ändern möchten, klicken Sie auf **Back**, um zum entsprechenden Dialog zurückzukehren.
 - Wenn Sie mit den Einstellungen zufrieden sind, klicken Sie auf **Next**, um mit der Installation zu beginnen.

In der Statusleiste des Dialogs **Setup Status** werden Informationen zum Installationsvorgang angezeigt. Nach Abschluss der Installation wird der Dialog **Select licensing mode** angezeigt.
8. Klicken Sie auf eins der folgenden Optionsfelder:
 - **Evaluation** – Installiert eine Testversion von Silk Central, die für einen Zeitraum von 45 Tagen alle Funktionen des Produkts uneingeschränkt zur Verfügung stellt. Die Verwendung ist auf zehn Silk Central-Benutzer und zehn Issue Manager-Benutzer beschränkt. Wenn Sie später auf die Vollversion upgraden möchten, wenden Sie sich an den Vertriebsbeauftragten. Aktivieren Sie das Kontrollkästchen **Install Microsoft SQL Server 2008 Express SP1** um auch Microsoft SQL Server 2008 Express SP1 zu installieren.
 - **Licensed** – Installiert die Vollversion von Silk Central, für die eine Lizenz benötigt wird.
9. Klicken Sie auf **Weiter**.
Je nach den zur Installation ausgewählten Komponenten wird der Lizenz-Dialog geöffnet. Wenn Sie keine der Komponenten, für die eine Lizenzierung erforderlich ist, installiert haben, und der Dialog nicht geöffnet wird, fahren Sie mit dem nächsten Schritt fort.
Führen Sie zur Installation der Lizenzdatei die folgenden Schritte durch:
 - a) Klicken Sie auf **OK**, um das Verzeichnis mit der Lizenzdatei anzugeben.
Das lokale System wird nach den Konfigurationsdateien für den Silk Meter-Lizenzserver durchsucht. Wenn das Programm die Dateien findet, werden die Konfiguration und der Typ des Lizenzservers angezeigt und für die Lizenzierung verwendet. Werden keine Konfigurationsdaten gefunden, wird der Dialog **Select Silk Meter License Server** mit den Standardeinstellungen geöffnet.

Dieser Dialog enthält allgemeine Informationen zur Silk Meter-Lizenzierung. Detaillierte Informationen zur Silk Meter-Lizenzierung erhalten Sie, wenn Sie auf **Open Silk Meter ReadMe** klicken. Mit dieser Aktion öffnen Sie die Silk Meter-Dokumentation in Ihrem Standardbrowser.



Hinweis: Open Silk Meter ReadMe ist nicht verfügbar, wenn sich das Dokument nicht im Installationsverzeichnis befindet. Dieses Dokument steht nicht zur Verfügung, wenn ein Silk Central-Webpaket installiert wird.

- b) Wählen Sie in dem Listenfeld **Application Silk Central** als zu lizenzierende Anwendung aus.
- c) Klicken Sie auf eins der folgenden Optionsfelder:

Lokalen oder Remote-Server verwenden

Geben Sie in das Feld **License Server Host** den Namen des Computers ein, auf dem Silk Meter installiert ist. Ändern Sie den Standardwert für die Port-Nummer 5461 nur, wenn Ihr Netzwerkadministrator einen anderen Port konfiguriert hat. Klicken Sie auf **Apply**, um die Lizenzserverkonfiguration zu erzeugen. Klicken Sie auf **Test Connection**, um zu überprüfen, ob die Kommunikation mit dem Silk Meter-Server auf dem angegebenen Host über den konfigurierten Port möglich ist. Möglicherweise schlägt der Test der Verbindung mit dem Lizenzserver fehl, da zu diesem Zeitpunkt erforderliche Systembibliotheken noch nicht verfügbar sind. Die Bibliotheken werden erst später installiert.



Hinweis: Manchmal reicht die Angabe des Hostnamens für den Lizenzserver im Feld **License Server Host**, z. B. `Lizenzserver`, nicht aus. In diesem Fall wird gemeldet: `There is no license server running on the hostname you specified`. Geben Sie dann statt des Hostnamens den vollständigen Namen ein, z. B. `licenseserver.mycompany.com`.

Server wird nicht verwendet (Einzelplatz)

Führt Silk Meter als eigenständige Anwendung aus. Sie werden aufgefordert, eine Silk Meter-Lizenz zu importieren. Klicken Sie auf **OK**, und geben Sie das Verzeichnis mit der Lizenzdatei an.

- d) Klicken Sie auf **Schließen**, um wieder zum InstallShield-Assistent zurückzukehren.

10. Klicken Sie auf **Finish**, um die Installation abzuschließen.



Hinweis: Wenn der InstallShield-Assistent eine Datei während der Installation nicht aktualisieren konnte, weil eine Systembibliothek von Windows gesperrt war oder der InstallShield-Assistent feststellt, dass das System neu gestartet werden muss, werden Sie aufgefordert, den Computer neu zu starten. Falls Sie den Computer nicht neu starten, können beim Zugriff auf Silk Central Probleme auftreten.

Der Dialog **Instanzen-Verwaltung** wird angezeigt, mit dem Sie Ihre Silk Central-Installation konfigurieren können. Weitere Information finden Sie unter *Verwalten von Instanzen*.

Installieren eines Windows-Ausführungsservers

Installieren Sie einen Ausführungsserver auf jedem Computer, der als entfernter Silk Central-Ausführungsserver verwendet werden soll. Mit diesem Server werden die Silk Central-Tests auf entfernten Computern ausgeführt.

1. Klicken Sie im Silk Central-Menü auf **Hilfe > Tools > Windows-Ausführungsserver**, und laden Sie das Windows-Ausführungsserverpaket herunter.
2. Suchen Sie die ausführbare Datei von Silk Central, und doppelklicken Sie auf die Datei. Der InstallShield-Assistent wird geöffnet.
3. Folgen Sie der Anleitung des Installationsassistenten.
4. Klicken Sie auf **Finish**, um die Installation abzuschließen.



Hinweis: Wenn der InstallShield-Assistent eine Datei während der Installation nicht aktualisieren konnte, weil eine Systembibliothek von Windows gesperrt war oder der InstallShield-Assistent feststellt, dass das System neu gestartet werden muss, werden Sie aufgefordert, den Computer neu zu starten. Falls Sie den Computer nicht neu starten, können beim Zugriff auf Silk Central Probleme auftreten.

Installieren eines Linux-Ausführungsservers

Diese Anleitung ist für Silk Central-Benutzer gedacht, die Linux verwenden.

Installieren Sie einen Ausführungsserver auf jedem Computer, der als entfernter Silk Central-Ausführungsserver verwendet werden soll. Mit diesem Server werden die Silk Central-Tests auf entfernten Computern ausgeführt.

1. Klicken Sie im Silk Central-Menü auf **Hilfe > Tools > Linux-Ausführungsserver**, und laden Sie das Linux-Ausführungsserverpaket herunter.



Hinweis: Das Linux-Ausführungsserverpaket enthält keine JRE. Stellen Sie sicher, dass Java Runtime Environment (JRE) 8 installiert ist. Sie können JRE unter [Java SE Downloads](#) herunterladen.

2. Entpacken Sie die Datei `tar.gz` mit dem folgenden Befehl:

```
gzip -d <Paket-Dateiname>.tar.gz
```

Entpacken Sie dann die `tar`-Datei mit dem folgenden Befehl:

```
tar xfz <Paket-Dateiname>.tar
```

Der Name der Paketdatei ist `LinuxExecServer-<Version>`.

3. Mit dem folgenden Befehl wechseln Sie in das Verzeichnis, in das die Paket-Datei extrahiert wurde:

```
cd LinuxExecServer
```

4. Starten Sie den Ausführungsserver mit dem folgenden Befehl:

```
./startExecServer.sh
```



Hinweis: Zwischengespeicherte Informationen und Log-Dateien werden in dem verborgenen Ordner `~/LinuxExecServer-<version>` in Ihrem Benutzerverzeichnis gespeichert. Auf die Log-Datei `ExecServer.log` kann auch über die Weboberfläche von Silk Central zugegriffen werden.



Hinweis: Für Linux-Ausführungsserver werden gegenwärtig die Versionsverwaltungssysteme Subversion, Git und das virtuelle Dateisystem (VFS) von Apache Commons unterstützt.

Tests, die mit den folgenden Technologien erstellt wurden, werden bei der Ausführung auf einem Linux-Ausführungsserver nicht unterstützt:

- Alle Silk Test-Technologien
- .NET Explorer
- Unified Functional Testing
- MSTest
- NUnit
- Silk Performer
- TestPartner
- Windows Script Host

Diese Testtypen sind spezifisch für das Betriebssystem Microsoft Windows.

Installieren von einem Hotfix

Aktualisieren Sie Ihre Instanzen auf den aktuellsten Hotfix, wenn ein neuer Hotfix verfügbar ist.

1. Suchen Sie auf dem Computer wo Silk Central installiert ist die ausführbare Datei, und doppelklicken Sie auf die Datei.
2. Folgen Sie der Anleitung des Installationsassistenten.
3. Wenn die Installation abgeschlossen wurde, öffnen Sie einen Browser und gehen Sie zur URL `http://localhost:19100/` (falls sich die Seite nicht automatisch öffnet).



Hinweis: Die Seite **Instanzen-Verwaltung** ist nicht von einem anderen Rechner aus erreichbar.

Die Seite **Instanzen-Verwaltung** wird geöffnet. Nun sollten Sie Ihren Browser-Cache zurücksetzen, sonst könnten Aktualisierungen in JavaScript und in den Stylesheets nicht aktiviert werden.

4. Klicken Sie in der Spalte **Version** auf **Hotfix <Version> installieren** um die Aktualisierung zu starten. Ein Dialog zum Aktivieren des Wartungs-Modus wird angezeigt.
5. Geben Sie einen Text ein, den Anwender sehen sollen wenn Sie versuchen Silk Central zu erreichen, zum Beispiel: *Silk Central ist zur Zeit nicht verfügbar, da wir Wartungsarbeiten durchführen. Das System wird in Kürze wieder verfügbar sein.* Klicken Sie auf **Ja** um den Wartungs-Modus zu aktivieren und die Aktualisierung zu starten.
6. Nachdem die Aktualisierung abgeschlossen wurde, klicken Sie auf  um die Instanz wieder zu starten.

Wiederholen Sie die **Instanzen-Verwaltung**-Schritte für alle Instanzen, die Sie aktualisieren möchten.



Tipp: Erinnern Sie Ihre Benutzer daran, dass sie ihren Browser-Cache zurücksetzen, sonst könnten Aktualisierungen in JavaScript und in den Stylesheets nicht aktiviert werden.

Aktualisieren auf Silk Central 18.5

Das Silk Central 18.5 Setup Programm entfernt automatisch die bestehende Installation, bevor es auf Silk Central 18.5 aktualisiert. Verwenden Sie nicht die Windows-Funktionalität **Programme ändern oder entfernen**, um die bestehende Silk Central-Installation zu entfernen, da sonst Ihre modifizierten Konfigurationsdateien gelöscht werden.

1. Erstellen Sie vor dem Upgrade eine Sicherungskopie der Silk Central-Datenbank.
2. Machen Sie eine Sicherungskopie Ihres Zertifikats, wenn Sie SSL aktiviert haben. Je nachdem in welchem Modus Sie Ihren Front-End-Server betreiben, müssen Sie das Zertifikat erneut in einen der folgenden Keystores importieren:

- Im 64-Bit Modus: `C:\Program Files (x86)\18.5\Silk Central Silk \instance_<Instanznummer>_<Instanzname>\lib\jre64\lib\security\cacerts`
- Im 32-Bit Modus: `C:\Program Files (x86)\18.5\Silk Central Silk \instance_<Instanznummer>_<Instanzname>\lib\jre\lib\security\cacerts`

Weitere Informationen finden Sie unter [Sichere Webserververbindungen mit SSL aktivieren](#).

3. Installieren Sie Silk Central. Dadurch wird der NGINX-Proxy und die **Instanzen-Verwaltung** installiert. Sie können zusammen mit diesen Komponenten auch einen Ausführungsserver auf demselben Computer installieren.

Die Datenbankeinstellungen werden automatisch aktualisiert. Nähere Informationen zu den erweiterten Einstellungen in den Konfigurationsdateien finden Sie unter [Konfigurieren erweiterter Einstellungen](#).

 **Hinweis:** Bei großen Datenbanken kann eine zu kleine Transaktionsprotokolldatei während des Updates zu einem Fehler führen. Sie verhindern dies, indem Sie für die Transaktionsprotokolldatei eine Größe von 5 GB festlegen.

4. Wenn die Installation abgeschlossen wurde, öffnen Sie einen Browser und gehen Sie zur URL `http://localhost:19100/` (falls sich die Seite nicht automatisch öffnet).

 **Hinweis:** Die Seite **Instanzen-Verwaltung** ist nicht von einem anderen Rechner aus erreichbar.

Die Seite **Instanzen-Verwaltung** wird geöffnet. Nun sollten Sie Ihren Browser-Cache zurücksetzen, sonst könnten Aktualisierungen in JavaScript und in den Stylesheets nicht aktiviert werden.

5. Klicken Sie in der Spalte **Version** auf **Upgrade auf <Version>** um die Aktualisierung zu starten. Ein Dialog zum Aktivieren des Wartungs-Modus wird angezeigt.
6. Geben Sie einen Text ein, den Anwender sehen sollen wenn Sie versuchen Silk Central zu erreichen , zum Beispiel: `Silk Central ist zur Zeit nicht verfügbar, da wir Wartungsarbeiten durchführen. Das System wird in Kürze wieder verfügbar sein. Klicken Sie auf Ja um den Wartungs-Modus zu aktivieren und die Aktualisierung zu starten.`
7. Nachdem die Aktualisierung abgeschlossen wurde, klicken Sie auf  um die Instanz wieder zu starten.

Wiederholen Sie die **Instanzen-Verwaltung**-Schritte für alle Instanzen, die Sie aktualisieren möchten.

 **Tipp:** Erinnern Sie Ihre Benutzer daran, dass sie ihren Browser-Cache zurücksetzen, sonst könnten Aktualisierungen in JavaScript und in den Stylesheets nicht aktiviert werden.

Silk Central

In diesem Abschnitt wird beschrieben, wie Sie ein Lizenzierungsschema für Silk Central abrufen und Silk Meter installieren. Sie benötigen zur Installation von Silk Meter Administratorrechte.

 **Hinweis:** Silk Central erfordert Silk Meter-Version 2008 oder höher sowie ein Silk Central-Lizenzierungsschema.

Installieren Sie Silk Meter einmal pro Lizenzserver. Wenn mehrere Lizenzserver vorhanden sind, werden entsprechend viele Lizenzierungsschemadateien benötigt (eine pro Lizenzserver). Ein Silk Meter-Lizenzserver kann Lizenzierungsschemas für mehrere Produkte verwalten.

Wenn Sie bereits ein Silk Central-Lizenzierungsschema erhalten haben, installieren Sie das Lizenzierungsschema auf Ihrem Lizenzserver. Wenn Sie noch kein Lizenzierungsschema erhalten haben, erzeugen Sie ein Lizenzierungsschema.

Lizenzverarbeitung

Silk Central bietet verschiedene Lizenztypen.

Benutzerbasierte Lizenzen

Diese Lizenzen werden vom Lizenzserver ausgecheckt, sobald ein Benutzer in einen bestimmten Bereich von Silk Central gelangt:

Lizenztyp	Bereich
Testmanager	Diese Lizenz wird ausgecheckt, wenn Sie nach Ihrer Anmeldung erstmalig auf einen Testmanagementbereich klicken. Die Silk Central-Testmanagementbereiche sind: Anforderungen, Tests, Ausführungsplanung, Verfolgung, Fehler (mit Ausnahme des Issue Manager-Bereichs) und Berichte .

Lizenztyp	Bereich
Manuelles Testen	Diese Lizenz wird ausgecheckt, wenn Sie das Fenster Manuelles Testen öffnen. Eine Lizenz für manuelles Testen wird ausgecheckt sobald ein Test für die Offline-Ausführung heruntergeladen wird. Die Lizenz wird wieder eingecheckt sobald die Ergebnisse hochgeladen werden.
Fehlerverfolgung	Diese Lizenz wird ausgecheckt, wenn Sie auf Issue Manager zugreifen.

Beachten Sie Folgendes:

- Wenn Sie auf **Abmelden (Benutzer > Abmelden)** klicken, werden die Lizenzen wieder am Lizenzserver eingecheckt, mit Ausnahme der Lizenzen für manuelles Testen, die zur Offline-Testausführung ausgecheckt wurden.
- Wenn Sie sich nicht abmelden (sondern nur das Browserfenster schließen), wird die Lizenz erst bei Ablauf der Sitzung eingecheckt.

Die Seite **Info (Hilfe > Info)** zeigt an, wie viele Lizenzen derzeit verwendet werden und wie viele für den Mandanten verfügbar sind, auf dem Sie gerade eingeloggt sind.

Standort-Lizenzen

Diese Lizenzen schalten eine bestimmte Funktionalität für alle Benutzer frei, ohne Einschränkungen:

Lizenztyp	Bereich
Mobiles Testen	Diese Lizenz ermöglicht das Testen auf mobile Geräten (physische Geräte, Emulatoren und Simulatoren) für manuelles, automatisiertes und Konfigurationstesten.

Erzeugen eines Silk Central-Lizenzierungsschemas

Um Silk Central auszuführen, benötigen Sie eine gültige Lizenz. Wenn Sie Silk Central bereits erworben haben, können Sie mit unserem Online-Lizenzierungsprogramm eine Lizenzierungsschema-Datei generieren. Wenn Sie das Online-Lizenzierungsprogramm verwenden möchten, benötigen Sie einen Browser mit SSL-Unterstützung, wie z. B. Firefox oder Internet Explorer. Sie erhalten E-Mail mit den Anweisungen, wie Sie Ihre Lizenzierungsschema-Datei erzeugen können. Sollten Sie diese Anweisungen nicht erhalten, wenden Sie sich an den Kundendienst unter <http://support.microfocus.com>.

Ermitteln der Hostkennung

Um eine Lizenzierungsschema-Datei zu erhalten, benötigen Sie die Hostkennung des Computers, auf dem Sie die Lizenzen installieren möchten. Für Floating-Lizenzen ist dies ein Rechner, auf dem Silk Meter installiert ist. Für Node-locked-Lizenzen ist es üblicherweise der Controller-Rechner.

1. Öffnen Sie auf dem Rechner ein Befehlsfenster, und geben Sie `ipconfig/all` ein. Die Netzwerkadapter werden aufgelistet, sowie weitere Informationen.
2. Notieren Sie die Hostkennung, die die `MAC-Adresse` oder die `Physische Adresse` Ihrer LAN-Karte ist, wie z. B. `00-BF-00-1C-D3-3D`.



Tipp: Je nachdem, wie Ihr System eingerichtet ist (virtuelle Maschinen, VPN-Verbindungen usw), kann Ihr Computer mehrere Netzwerkadapter mit unterschiedlichen MAC-Adressen haben. Notieren Sie unbedingt die Hostkennung Ihrer physischen LAN-Karte.

Installieren von Silk Meter

Wenn Sie bereits über eine Lizenzierungsschema-Datei für Silk Central verfügen, können Sie sie zusammen mit Silk Meter installieren. Wenn Sie keine gültige Silk Central Lizenz haben, können Sie mit unserem Online-Lizenzierungsprogramm eine Lizenzierungsschema-Datei generieren.

Für die Installation und das Ausführen von Silk Meter auf Ihrem Lizenzserver wird keine Lizenzierungsschema-Datei benötigt. Sie können Silk Central jedoch erst verwenden, nachdem Sie die Lizenzierungsschema-Datei importiert haben. Eine Lizenzierungsschema-Datei kann mit dem Silk Meter **Policy Administrator** importiert werden.

Wenn mehrere Lizenzserver vorhanden sind, werden entsprechend viele Lizenzierungsschemadateien benötigt (eine pro Lizenzserver). Ein Silk Meter-Lizenzserver kann Lizenzierungsschema-Dateien für mehrere Produkte verwalten.

Lizenzserver Voraussetzungen für Silk Meter

Überprüfen Sie vor der Installation von Silk Meter die *Versionshinweise*, um sicherzustellen, dass der Lizenzserver die Anforderungen erfüllt.

Deinstallieren einer vorhergehenden Version von Silk Meter

Falls Silk Meter bereits auf dem Lizenzserver installiert ist, müssen Sie das Programm deinstallieren, bevor Sie die aktuelle Version von Silk Meter installieren.

1. Wählen Sie **Start > Programme > Silk > Silk Meter > Uninstall**.
2. Klicken Sie auf **Ja**, um Silk Meter zu deinstallieren. Das Dialogfeld **Einstellungen entfernen** wird angezeigt.
3. Klicken Sie auf **Nein**, damit Ihre Silk Meter-Einstellungen erhalten bleiben.



Achtung: Klicken Sie auf **Nein**, damit die aktuell auf dem Silk Meter-Lizenzserver vorhandenen Lizenzierungsschemata erhalten bleiben.

4. Starten Sie den Computer neu.

Silk Meter ist deinstalliert. Sie können jetzt die aktuelle Version von Silk Meter installieren.

Installieren von Silk Meter auf dem Lizenzserver

Überprüfen Sie vor der Installation von Silk Meter die folgenden Informationen:

- Ihr Benutzerkonto verfügt über Administratorrechte.
 - Auf Ihrem Lizenzserver ist keine Instanz von Silk Meter installiert.
1. Besuchen Sie die [Product Updates Seite](#) und suchen Sie nach Silk Meter.
 2. Laden Sie die aktuellsten **Silk Meter Installationsdateien** herunter.
 3. Wechseln Sie zu dem Verzeichnis, in dem Sie die .exe-Datei gespeichert haben. Wenn Sie eine Standardinstallation durchführen möchten, folgen Sie einfach den Schritten des Silk Meter-Installationsassistenten und belassen Sie jeweils die Standardeinstellungen.



Wichtig: Starten Sie den Computer neu, sobald Sie dazu aufgefordert werden.

Silk Meter-Lizenzserverkonfiguration

Zur Ausführung jeder Version von Silk Central, muss Silk Meter auf einem Computer im Netzwerk installiert und konfiguriert werden.

Für die Kommunikation zwischen Silk Central und Silk Meter sind folgende Dateien und Variablen erforderlich:

- `SILK_CONFIG_PATH` Umgebungsvariable
- `CosLicensingService.ref` Datei
- `CosPropertyService.ref` Datei
- `ls_segue.ref` Datei
- `silkmeter.cfg` Datei



Wichtig: Löschen Sie diese Dateien auf keinen Fall.

Das Silk Central-Installationsprogramm erstellt diese Objekte anhand der von Ihnen im Dienstprogramm **Select Silk Meter License Server** eingegebenen Werte.

Ändern der Lizenzserverkonfiguration

Mit dem Dienstprogramm **Select Silk Meter License Server** kann die Lizenzserverkonfiguration geändert oder repariert werden. Dieses Werkzeug wird zusammen mit Silk Central installiert.

1. Wählen Sie **Start > Programme > Silk > Silk Central 18.5 > Verwaltungswerkzeuge > Lizenzserverkonfiguration auswählen**. Das Dienstprogramm **Select Silk Meter License Server** wird geöffnet.
2. Wählen Sie im Listenfeld **Anwendung** das Produkt, für das Sie den Lizenzserver konfigurieren möchten.
3. Klicken Sie auf das Optionsfeld **Lokalen oder Remote-Server verwenden**, um einen Silk Meter-Lizenzserver zu konfigurieren.
4. Geben Sie im das Feld **License Server Host** den Namen des Computers des Silk Meter-Lizenzservers ein.
Der Wert im Feld **Port-Nummer** sollte nur geändert werden, wenn Ihr Netzwerkadministrator einen anderen Port konfiguriert hat.
5. Klicken Sie auf **Apply**, um die Lizenzserverkonfiguration zu aktivieren.
6. Klicken Sie auf **Test Connection**, um zu überprüfen, ob die Kommunikation mit dem Silk Meter-Server auf dem angegebenen Host über den konfigurierten Port möglich ist. Wenn die Verbindung hergestellt werden konnte, wird im Feld **Status** eine `SUCCESS`-Meldung angezeigt.



Hinweis: Manchmal reicht die Angabe des Hostnamens für den Lizenzserver im Feld **License server host**, z. B. `Lizenzserver`, nicht aus. Die Meldung `Connection to Silk Meter license server failed` wird angezeigt. Geben Sie dann statt des Hostnamens den vollständigen Namen ein, z. B. `licenseserver.mycompany.com`.

7. Klicken Sie auf **Schließen**, um die Lizenzserverkonfiguration fertig zu stellen.

Getestete und unterstützte Software

Dieser Abschnitt listet die Software auf, mit der Silk Central 18.5 getestet wurde, sowie die Software, die von Silk Central unterstützt wird.

Unterstützte Betriebssysteme

- Microsoft Windows Server 2012
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2016
- Microsoft Windows 7 32-Bit/64-Bit Service Pack 1 (Ausführungsserver)
- Microsoft Windows 8,1 32-Bit/64-Bit (Ausführungsserver)
- Microsoft Windows 10 32-Bit/64-Bit (Ausführungsserver)
- Android 4.4, 5.x, 6.x, 7.x, 8.x (Testen auf mobilen Geräten)

- iOS 9.3, 10.x, 11.x (Testen auf mobilen Geräten)



Wichtig: *Update für universelle C RunTime in Windows* wird für alle Microsoft Windows-Betriebssysteme benötigt. Für Microsoft Windows Server 2016 wird die Installationsoption **Windows Server (Server mit Desktopdarstellung)** benötigt.

Unterstützte Linux-Betriebssysteme

Silk Central unterstützt Linux-Betriebssysteme nur für den Ausführungsserver.

- Debian
- Redhat Enterprise Linux
- Suse Linux
- Ubuntu

Unterstützte Webbrowser

- Google Chrome
- Internet Explorer 10 oder höher (ohne Kompatibilitätsmodus)
- Mozilla Firefox
- Microsoft Edge

Unterstützte Webserver

- IIS 8 32-Bit/64-Bit
- IIS 10 32-Bit/64-Bit

Unterstützte Datenbankmanagementsysteme

- Microsoft SQL Server 2012 Service Pack 3
- Microsoft SQL Server 2014 Service Pack 2
- Microsoft SQL Server 2016
- Oracle 11g (Version 11.2.0.4)
- Oracle 12c (Version 12.1.0.2)

Integrierte Softwareunterstützung für Micro Focus

- AccuRev 6.2
- Caliber 11.4, 11.5
- Mobile Center 2.51 oder höher
- Silk Performer 18.5
- Silk Test 18.5
- StarTeam 15.x, 16.x
- Silk TestPartner 6.3
- Unified Functional Testing (UFT) 14.0

Unterstützte integrierte Software von Drittanbietern

- VFS (Apache Commons Virtual File System)
- Atlassian JIRA 6, 7
- Bugzilla 4.4.12, 5.0.3
- CA Agile Central
- Git 2.14.2
- IBM Rational ClearQuest 8,0
- IBM Rational DOORS 9.5, 9.6

- IBM Rational DOORS Next Generation 6.0
- IBM Rational RequisitePro 7.1.3, 7.1.4
- JUnit 4.11 oder höher
- Microsoft Office Excel (.xlsx) zum Importieren von Tests und Anforderungen
- Microsoft Office Word (.doc, .docx) zum Importieren von Anforderungen
- Microsoft Visual Studio/Visual Studio Test Agent 2012, 2013, 2015
- NUnit 2.6.4, 3.4.1
- SAP Solution Manager 7.1
- Subversion 1,9
- Team Foundation Server 2010, 2012, 2013, 2015
- VersionOne Enterprise Edition
- VMware vCloud Director 5.5

Konfigurieren und Verwalten der Infrastruktur

Eine Instanz ist ein unabhängiges Set von Silk Central-Diensten (Anwendungsserver (AS), Front-End-Server (FE) und Diagrammserver (CS)), mit eigener Datenbank und eigenen Ausführungsservern (ES). Standardmäßig erstellt Silk Central eine einzelne Instanz namens *silk* für Sie. Die Standard-URL ist `http://<Computername>:19120/login` (keine Portinformationen nötig wenn Silk Central auf IIS läuft).

Aufsetzen eines sicheren Silk Central-Systems

Hier wird beschrieben, wie ein sicheres Silk Central-System aufgesetzt wird.

Allgemeine Richtlinien

Nachdem Sie Silk Central installiert haben, sollten Sie folgende Richtlinien beachten, um Silk Central in einer sicheren Umgebung zu betreiben.

- Ändern Sie zuerst das Kennwort des `sysadmin`-Benutzers. Weitere Informationen finden Sie unter [Systemadministrator](#).
- Konfigurieren Sie die LDAP-Authentifizierung, damit sich Benutzer über einen LDAP-Server bei Silk Central anmelden können. Weitere Informationen finden Sie unter [LDAP-Authentifizierung](#).
- Falls mehrere Gruppen mit Silk Central arbeiten werden, stellen Sie sicher, dass Ihre Benutzer nur die Daten sehen können, die sie auch sollen. Richten Sie hierzu Instanzen oder Mandanten ein. Detaillierte Informationen hierzu finden Sie unter [Verwalten von Instanzen](#) und [Verwalten von Mandanten](#).
- Um sicherzustellen, dass Berichte mit erweiterten Abfragen keine Daten in der Datenbank verändern können, ziehen Sie in Betracht einen Datenbank-Benutzer für Lesezugriff zu erstellen und zu verwenden. Weitere Informationen finden Sie unter [Datenbank \(Seite\)](#).
- Konfigurieren Sie Ihre Firewall so, dass nur von Silk Central verwendete Ports offen sind. Informationen über von Silk Central verwendete Ports finden Sie unter [Silk Central-Architektur](#).
- Machen Sie regelmäßig ein Backup Ihrer Datenbank.
- Verwenden Sie die aktuellsten und unterstützten Betriebssystem-Versionen und stellen Sie sicher, dass regelmäßig Aktualisierungen durchgeführt werden.
- Verwenden Sie die aktuellsten Versionen und Hotfixes von Silk Central. Registrieren Sie sich bei Micro Focus SupportLine unter <http://supportline.microfocus.com>, um die aktuellsten Neuigkeiten und andere Supportinformationen zu erfahren.

Sichere Webserververbindungen mit SSL aktivieren

Wenn sich Ihre Benutzer nur über eine sichere Verbindung (SSL) zu Silk Central verbinden können sollen, aktivieren Sie SSL (Secure Sockets Layer) in Silk Central.

Weitere Informationen finden Sie unter [Kommunikation mit einem externen System über SSL](#), [BIRT-Berichte in SSL-Umgebungen aktivieren](#) und [Konfigurieren eines benutzerdefinierten SSL-Ports für Ausführungsserver](#).

1. Kopieren Sie Ihr Zertifikat und die Schlüsseldateien auf den Front-End-Server.
2. Öffnen Sie die Datei `nginx.conf.template` im Ordner `C:\ProgramData\SilkCentral\InstanceAdministration\nginx\conf` mit einem Texteditor.

3. Kommentieren Sie die folgenden Zeilen aus, indem Sie die #-Zeichen entfernen:

```
#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. Setzen Sie die Pfade für `ssl_certificate` und `ssl_certificate_key` auf den Ort wo Sie Ihr Zertifikat und die Schlüsseldateien hin kopiert haben. Geben Sie den entsprechenden Pfad mithilfe von Schrägstrichen statt Backslashes ein.
5. Wenn Sie nur SSL-Verbindungen zulassen möchten, dass , kommentieren Sie die Zeile `listen 19120;` durch Hinzufügen von # aus.
6. *Optional:* Um eine Weiterleitung vom unsicheren zum sicheren Port zu konfigurieren, fügen Sie eine neue `server`-Sektion mit der folgenden Syntax hinzu:

```
server {
    listen <unsicherer Port>;
    server_name localhost;
    return 301 https://$host$request_uri;
}
```

7. Starten Sie den Silk Central Instanzen-Verwaltungsdienst mit dem Windows Dienstmanager neu.

BIRT-Berichte in SSL-Umgebungen aktivieren

Nachdem Sie Silk Central für die Verwendung einer sicheren Webserververbindung mit SSL konfiguriert haben, müssen BIRT-Berichte für diese Umgebung aktiviert werden.

1. Stoppen Sie über die Seite **Instanzen-Verwaltung** den Diagrammserverdienst der Instanz die Sie konfigurieren möchten.
2. Verwenden Sie OpenSSL um mit der folgenden Befehlszeile einen PKCS #12 Keystore zu erstellen:
`openssl pkcs12 -export -in ./host.cert -inkey ./host.key > ./host.p12`
Beispiel:

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

3. Konvertieren Sie den Keystore `host.p12` in einen Java-Keystore mit der folgenden Befehlszeile:
`keytool.exe -importkeystore -srckeystore ./host.p12 -destkeystore ./host.jks -srcstoretype pkcs12`
Beispiel:

```
"C:\Program Files (x86)\Silk\Silk Central
18.5\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. Fügen Sie die folgenden Zeilen zur Konfigurationsdatei `sc_ChartServer.processconfig` des Diagrammservers hinzu, welche sich in `C:\Program Files (x86)\Silk\Silk Central 18.5\instance_<Instanznummer>_<Instanzname>\Conf` befindet:

```
<Service>
  <SystemProperties>
    ...
    <SystemProperty name="javax.net.ssl.trustStore" value="<Pfad
zur host.jks-Datei>" />
    <SystemProperty name="javax.net.ssl.trustStorePassword"
value="<Kennwort>" />
  </SystemProperties>
</Service>
```

Beispiel:

```
<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. Starten Sie den Diagrammserverdienst neu.

Konfigurieren eines benutzerdefinierten SSL-Ports für Ausführungsserver

Standardmäßig kommuniziert der Anwendungsserver über den SSL-Port 19125 mit den Ausführungsservern.



Hinweis: Diese Schritte müssen für jeden Ausführungsserver durchgeführt werden, der über einen Nicht-Standard-SSL-Port angeschlossen werden soll.

So konfigurieren Sie einen benutzerdefinierten SSL-Port für einen Ausführungsserver:

1. Deaktivieren Sie den Ausführungsserver, für den der SSL-Port konfiguriert werden soll.
2. Halten Sie den Ausführungsserver an.
3. Öffnen Sie die Datei `SccExecServerBootConf.xml` mit einem Texteditor.
Diese Datei befindet sich auf dem Ausführungsserver im Ordner `/conf/execserver` des Silk Central-Verzeichnisses.
4. Suchen Sie das XML-Tag `<SSLPort>`. Die Standardeinstellung dieses Tags lautet `<19125>`.
Geben Sie die Portnummer ein, die Sie für die SSL-Kommunikation verwenden möchten.
5. Speichern und schließen Sie die XML-Datei.
6. Weisen Sie in Silk Central dem SSL-Port des Ausführungsservers den Wert zu, den Sie in der XML-Datei angegeben haben.
7. Starten Sie den Ausführungsserver neu.
8. Aktivieren Sie den Ausführungsserver wieder.

Deaktivieren nicht verwendeter Ports auf Ausführungsservern

Je nachdem, ob Sie eine SSL-Verbindung oder eine unsichere Verbindung zwischen dem Anwendungsserver und den Ausführungsservern verwenden, können Sie den jeweils nicht benötigten Port deaktivieren. Außerdem können Sie den Tomcat-Standardport deaktivieren, da dieser von Silk Central nicht genutzt wird.

Die folgenden Schritte müssen auf jedem Ausführungsserver durchgeführt werden, auf dem der nicht verwendete Port deaktiviert werden soll.

So deaktivieren Sie nicht verwendete Ports auf dem Ausführungsserver:

1. Halten Sie den Ausführungsserver an.
2. Öffnen Sie die Datei `SccExecServerBootConf.xml` in einem Texteditor.
Diese Datei befindet sich standardmäßig in `C:\Program Files (x86)\Silk\Silk Central 18.5 Execution Server\conf\execserver` auf dem Ausführungsserver.

- Suchen Sie die XML-Tags `InsecurePort` und `SSLPort` im Abschnitt `RmiProxy` der Datei.
- Das weitere Vorgehen hängt davon ab, ob Sie eine SSL- oder eine unsichere Verbindung zwischen dem Anwendungs- und dem Ausführungsserver eingerichtet haben:

SSL-Verbindung Setzen Sie den `InsecurePort`-Wert auf 0.

Unsichere Verbindung Setzen Sie den `SSLPort`-Wert auf 0.

- Speichern und schließen Sie die XML-Datei.
- Starten Sie den Ausführungsserver neu.

Kommunikation mit einem externen System über SSL

Falls das Zertifikat des Hosts, den Sie verbinden wollen, selbstsigniert ist, erhalten Sie eventuell die folgende Fehlermeldung:

`sun.security.provider.certpath.SunCertPathBuilderException: unable to find valid certification path to requested target`



Hinweis: Diese Fehlermeldung wird nicht für gültige Zertifikate angezeigt. Dies sind alle Zertifikate, die durch Zertifizierungsstellen signiert sind.

Um einen Server mit einem selbstsignierten Zertifikat zu verwenden, müssen Sie die folgenden Schritte vornehmen:

- Laden Sie das SSL-Zertifikat vom Server herunter.
Verwenden Sie einen Browser, um das Zertifikat anzusehen und um es zu exportieren. Gehen Sie bei Mozilla Firefox zu **Extras > Seiteninformationen > Sicherheit > Zertifikat anzeigen > Details > Exportieren**.
- Starten Sie das Schlüssel- und Zertifikats-Managementtool *Keytool*.
Keytool ist Teil Ihrer JRE-Installation und befindet sich in Ihrem JRE-Installationsverzeichnis, z.B. `C:\Program Files (x86)\Silk\Silk Central <Version>\instance_<Instanznummer>_<Instanzname>\lib\jre\bin`. Weitere Informationen über Keytool finden Sie in der [Java SE Technische Dokumentation](#).
- Um ein Zertifikat zu dem standardmäßigen Java-Keystore auf dem Front-End-Server und dem Anwendungsserver hinzuzufügen, geben Sie zum Beispiel den folgenden Befehl in Keytool ein:

```
keytool
-importcert
-file CERTIFICATE.crt
-keystore "C:\Program Files (x86)\Silk\Silk Central <version>\
instance_<instance number>_<instance name>\lib\jre\lib\security\cacerts"
```

Sie werden dann dazu aufgefordert, das Kennwort einzugeben.

- Geben Sie das standardmäßige Keystore-Kennwort ein, `changeit`.
- Starten Sie den Front-End-Server und den Anwendungsserver erneut, um den Keystore neu zu laden.

Verwalten von Instanzen

Erstellen Sie zusätzliche Instanzen, wenn Sie die Testdaten und Testprozesse Ihrer Mandanten physisch trennen möchten. Dadurch wird die Datensicherheit erhöht und der Einfluss unabhängiger Benutzergruppen (z.B. Abteilungen) aufeinander reduziert. Durch Mandanten können Sie die Testdaten innerhalb einer Instanz zusätzlich logisch trennen.

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			

Verwalten von Instanzen

Instanzen und deren Silk Central-Dienste werden über eine gemeinsame Benutzeroberfläche namens **Instanzen-Verwaltung** verwaltet, auf welche Sie über die URL <http://localhost:19100> auf dem Server wo Silk Central installiert ist zugreifen können. Die Seite **Instanzen-Verwaltung** ist nicht von einem anderen Rechner aus erreichbar. Sie können folgende Aktionen für eine Instanz oder deren Dienste ausführen:

- Klicken Sie auf  oder , um einzelne Dienste anzuhalten oder wieder zu starten. Wenn Sie eine Instanz stoppen oder starten, werden sämtliche Dienste der Instanz angehalten/gestartet.
- Klicken Sie auf , um die Instanz zu löschen. Verwenden diese Option nur dann, wenn Sie sich absolut sicher sind, dass die Instanz nicht mehr benötigt wird! Diese Aktion löscht jedoch die Daten in der Datenbank nicht.
 -  **Hinweis:** Um einen Ausführungsserver einem anderen Anwendungsserver zuzuweisen, müssen Sie die folgende Datei auf dem Computer löschen, auf dem der Ausführungsserver installiert ist:
C:\ProgramData\SilkCentral\AgentBase\ItemObjects.ser.
- Klicken sie auf , um die Instanz-Einstellungen zu konfigurieren.

Wartungs-Modus

Bevor Sie an einer Silk Central-Instanz Wartungsarbeiten vornehmen, während denen die Benutzer nicht mehr auf das System zugreifen können, können Sie Ihre Silk Central-Anwender im Voraus darüber informieren. Solche Wartungsarbeiten sind z.B. Die Installation eines Hotfixes oder die Einstellungen eines Dienstes zu ändern.

1. Klicken sie auf der Seite **Instanzen-Verwaltung** auf , um den Dialog **Einstellungen** zu öffnen.
2. Aktivieren Sie auf der Registerkarte **Wartung** das Kontrollkästchen **Wartungs-Modus aktivieren**.
3. Geben Sie einen Text ein, den Anwender sehen sollen wenn Sie versuchen Silk Central zu erreichen , zum Beispiel: *Silk Central ist zur Zeit nicht verfügbar, da wir Wartungsarbeiten durchführen. Das System wird in Kürze wieder verfügbar sein.*
4. Klicken Sie auf **OK**.
5. Wenn Sie mit den Wartungsarbeiten fertig sind und alle Dienste wieder laufen, deaktivieren Sie den Wartungs-Modus so dass Ihre Anwender wieder auf Silk Central zugreifen können.

32-Bit-/64-Bit Modus

1. Klicken sie auf der Seite **Instanzen-Verwaltung** auf , um den Dialog **Einstellungen** zu öffnen.

2. Verwenden Sie die **Modus**-Liste der **Instanz**, um zu bestimmen ob die Front-End-, Anwendungs- und Ausführungsdienste im 32-Bit oder im 64-Bit-Modus laufen sollen. Beachten Sie bitte, dass Dienste nur im 64-Bit-Modus laufen können, wenn Sie auch ein 64-Bit-Betriebssystem verwenden. Wenn der Modus geändert wird, müssen die Instanzen-Dienste neu gestartet werden.
3. Klicken Sie auf **OK**.

JMX-Messdaten

Wenn Sie über JMX auf Informationen zugreifen oder Aktionen ausführen möchten, benötigen Sie die JMX-Verbindung. Klicken Sie auf  um den **Einstellungen**-Dialog zu öffnen. Wählen Sie auf der Registerkarte **Server** den gewünschten Server aus und kopieren Sie die **JMX-Verbindung**. Weitere Informationen finden Sie unter [Konfigurieren der JMX-Einstellungen](#).

Erstellen einer neuen Instanz

Klicken Sie auf **Neue Instanz**, um eine weitere Instanz hinzuzufügen. Geben Sie der Instanz einen aussagekräftigen Namen, da dieser verwendet wird um die Dienste und Dateien der Instanz zu identifizieren. Er wird auch ein Teil der URL sein über die die Anwender auf die Instanz zugreifen.

Für jede zusätzliche Instanz werden mindestens 10 GB zusätzlicher Festplattenplatz benötigt, sowie mindestens der folgende initiale Systemspeicher:

- Front-End-Server: 500 MB
- Anwendungsserver: 300 MB
- Diagrammserver: 200 MB

Je nach Ihrem Workload könnten diese Werte noch höher sein.

Weitere Informationen zur optimalen Konfiguration von Silk Central erhalten Sie vom technischen Support oder Ihrem Technical Account Team.

Installieren von einem Hotfix

Aktualisieren Sie Ihre Instanzen auf den aktuellsten Hotfix, wenn ein neuer Hotfix verfügbar ist.

1. Suchen Sie auf dem Computer wo Silk Central installiert ist die ausführbare Datei, und doppelklicken Sie auf die Datei.
2. Folgen Sie der Anleitung des Installationsassistenten.
3. Wenn die Installation abgeschlossen wurde, öffnen Sie einen Browser und gehen Sie zur URL `http://localhost:19100/` (falls sich die Seite nicht automatisch öffnet).



Hinweis: Die Seite **Instanzen-Verwaltung** ist nicht von einem anderen Rechner aus erreichbar.

Die Seite **Instanzen-Verwaltung** wird geöffnet. Nun sollten Sie Ihren Browser-Cache zurücksetzen, sonst könnten Aktualisierungen in JavaScript und in den Stylesheets nicht aktiviert werden.

4. Klicken Sie in der Spalte **Version** auf **Hotfix <Version> installieren** um die Aktualisierung zu starten. Ein Dialog zum Aktivieren des Wartungs-Modus wird angezeigt.
5. Geben Sie einen Text ein, den Anwender sehen sollen wenn Sie versuchen Silk Central zu erreichen, zum Beispiel: *Silk Central ist zur Zeit nicht verfügbar, da wir Wartungsarbeiten durchführen. Das System wird in Kürze wieder verfügbar sein.* Klicken Sie auf **Ja** um den Wartungs-Modus zu aktivieren und die Aktualisierung zu starten.
6. Nachdem die Aktualisierung abgeschlossen wurde, klicken Sie auf  um die Instanz wieder zu starten.

Wiederholen Sie die **Instanzen-Verwaltung**-Schritte für alle Instanzen, die Sie aktualisieren möchten.



Tipp: Erinnern Sie Ihre Benutzer daran, dass sie ihren Browser-Cache zurücksetzen, sonst könnten Aktualisierungen in JavaScript und in den Stylesheets nicht aktiviert werden.

Starten oder Stoppen eines lokalen Ausführungsserverdienstes

Verwenden Sie den **Silk Central Service Manager** um einen lokal installierten Ausführungsserverdienst zu starten oder zu stoppen.

1. Doppelklicken Sie in der Windows-Taskleiste auf das Symbol **Silk Central Service Manager**. Der Dialog **Silk Central Service Manager** wird angezeigt.
2. Klicken Sie auf **Start** oder **Stop**, um den Ausführungsserverdienst zu starten oder anzuhalten.
3. Klicken Sie auf **Query Status**, um den aktuellen Status des Dienstes zu überprüfen.
4. Wenn Sie Echtzeit-Aktivitäten überwachen möchten, starten Sie den Silk Central-Ausführungsserver mit einem Konsolenfenster:
 1. Aktivieren Sie das Kontrollkästchen **Start with console**.
 2. Klicken Sie auf **Stop**.
 3. Klicken Sie auf **Start**.
5. Klicken Sie auf **Execution Server Logfile** um die Logdatei zu öffnen. Die Protokolldatei wird im registrierten Texteditor geöffnet.
6. Klicken Sie auf **OK**, um die Verwaltung des Ausführungsserverdienstes zu beenden. Der Service Manager wird geschlossen, ist aber in der Taskleiste weiterhin verfügbar.

Lastausgleichsmechanismus für Front-End-Server

Der Lastausgleichsmechanismus wird verwendet um die Last (Datenverkehr auf der Website) auf mehrere Server zu verteilen, wodurch eine Leistungs- und Zuverlässigkeitssteigerung ermöglicht wird.

Um einen Lastausgleichsmechanismus für die Front-End-Server von Silk Central einzurichten, fügen Sie der NGINX Proxy-Konfiguration weitere Front-End-Server hinzu, und NGINX verteilt dann die Last zwischen den Servern.

Konfigurieren des Lastausgleichsmechanismus für Front-End-Server

Wenn Sie eine laufende Silk Central-Instanz haben, und die Anwender dieser Instanz aufgrund erhöhter Last eine Verschlechterung der Systemleistung verspüren, können Sie zusätzliche Front-End-Server einrichten um die Last aufzuteilen.

Ursprüngliche Situation:

- Sie haben Silk Central auf *Server A* installiert.
- Sie haben eine laufende Instanz mit Systemleistungsproblemen.
- Sie wollen einen zusätzlichen Front-End-Server einrichten, um die Last aufzuteilen.

So fügen Sie der Instanz für den Lastausgleichsmechanismus einen Front-End-Server hinzu.

1. Installieren Sie Silk Central mit dem Silk Central-Setup auf *Server B*.
2. Wenn die Installation abgeschlossen ist, gehen Sie auf *Server B* zur **Instanzen-Verwaltung** (<http://localhost:19100>).
3. Da Sie lediglich einen Front-End-Server benötigen, deaktivieren Sie auf der Instanz, die Sie für den Lastausgleichsmechanismus verwenden möchten, den Anwendungs- und den Diagrammserver.
4. Klicken Sie auf  um den **Einstellungen**-Dialog dieser Instanz zu öffnen. Wählen Sie auf der Registerkarte **Server** den Front-End-Server aus und kopieren Sie den **Front-End-Server Port**.
5. Wechseln Sie zu *Server A* und gehen Sie zur **Instanz-Verwaltung** (<http://localhost:19100>).
6. Klicken Sie auf  um den **Einstellungen**-Dialog Ihrer Instanz mit Systemleistungsproblemen zu öffnen und aktivieren Sie den Wartungs-Modus.

7. Öffnen sie im Dateisystem die Datei für benutzerdefinierte NGINX-Eigenschaften (C:\ProgramData\SilkCentral\InstanceAdministration\nginx\conf\nginxCustom.properties) und fügen Sie die URL des Front-End-Servers auf *Server B* hinzu (<SERVERNAME>:<PORT>). Verwenden sie hierfür den zuvor kopierten **Front-End-Server Port**.

Notation: frontendserver.<INSTANZNAME>=<FE_URL1>{,<FE_URL2>,...,<FE_URLX>}

Zum Beispiel: frontendserver.silk=localhost:19110,silkserver2:19320



Achtung: Aufgrund von NGINX-Restriktionen kann der Port 19120 eines Front-End-Servers nicht verwendet werden. Verwenden sie immer die Portnummer vom Einstellungsdialog, wie in Schritt 4 beschrieben.

8. Gehen Sie zurück zur **Instanz-Verwaltung** und klicken Sie auf  um den **Einstellungen**-Dialog Ihrer Instanz mit Systemleistungsproblemen zu öffnen. Wählen Sie auf der Registerkarte **Server** den Anwendungsserver aus und kopieren sie den **Anwendungsserver-Port**.
9. Um eine Verbindung zwischen dem Front-End-Server auf *Server B* und dem Anwendungsserver der Instanz auf *Server A* zu erstellen, öffnen Sie einen Web-Browser und navigieren Sie direkt zum Front-End-Server von *Server B* (http://<Server B>:<Front-End-Server Port>). Stellen Sie sicher, dass Sie den Port vom Einstellungsdialog verwenden, nicht 19120!
10. Geben Sie auf der Anwendungsserververbindungs-Seite **Host oder IP-Adresse** und den kopierten **Anwendungsserver-Port** von *Server A* ein.
11. Gehen Sie zurück zur **Instanzen-Verwaltung** und deaktivieren sie den Wartungs-Modus. Dadurch wird die NGINX-Konfiguration aktualisiert.

Wenn Ihre Anwender nun mit derselben URL wie zuvor die Instanz verwenden, wird ihre Last automatisch zwischen den Front-End-Servern auf *Server A* und *Server B* verteilt.

Verwalten von Mandanten

Im Bereich **Systemverwaltung** können Sie die Mandanten von Silk Central konfigurieren. Die Konfiguration von Mandanten umfasst folgende Tätigkeiten:

- Erstellen, Verbinden und Trennen von Datenbanken.
- Erstellen und Verwalten von Mandanten.
- Konfigurieren der Infrastruktur des Silk Central-Mandanten (Diagrammserver, E-Mail-Server und Proxy-Verbindungen).
- Warten von Systemdiensten durch die Analyse von Diagnosedaten und Systemlogdateien.

Systemadministrator

Der Systemadministrator ist der einzige Benutzer, der Zugriff auf den Bereich **Systemverwaltung** hat. Gleichzeitig hat er nur auf diesen Bereich Zugriff. Er hat keinen Zugriff auf die eigentliche Silk Central-Benutzeroberfläche.

Sie erhalten Zugriff auf den Bereich **Systemverwaltung**, indem Sie sich mit den folgenden Daten anmelden:

- Benutzername: sysadmin
- Kennwort: sysadmin



Wichtig: Ändern Sie dieses Standardkennwort so bald wie möglich. Wir empfehlen eine Änderung des Kennworts, sobald Sie zum ersten Mal eine Verbindung zu einer Silk Central-Datenbank hergestellt haben. Klicken Sie zum Ändern des Kennworts im Menü des Bereichs **Systemverwaltung** (oben rechts) auf **Kennwort ändern**. Der Benutzername kann nicht geändert werden.

Wenn keine Datenbankverbindung vorliegt, wird der Systemadministrator automatisch in den Bereich **Systemverwaltung** weitergeleitet.

Datenbanken

Silk Central verwendet Datenbanken zum Speichern, Pflegen und Analysieren von Daten. Sie müssen eine Datenbankverbindung herstellen, bevor Sie mit Silk Central arbeiten können. Sie können mehrere Datenbanken erstellen, wobei jedoch immer nur eine Datenbank verbunden werden kann. Wenn Sie eine Verbindung mit einer neuen Datenbank herstellen möchten, müssen Sie zunächst die aktuelle Datenbankverbindung trennen.

Wenn Sie Datenbankverbindungen konfigurieren möchten, gehen Sie im Bereich **Systemverwaltung** auf die Seite **Datenbank**. Auf diese Seite kann nur der Systemadministrator zugreifen. Weitere Informationen finden Sie unter [Systemadministrator](#).

Verwaltungsaufgaben, für die die Datenbankverbindung getrennt werden muss, sollten außerhalb der regulären Arbeitszeit durchgeführt werden. Setzen Sie die Benutzer über die Nicht-Verfügbarkeit und dessen Dauer in Kenntnis. Für weitere Informationen zur Konfiguration Ihrer Datenbank, wenden Sie sich bitte an die SupportLine. Wenn Sie Microsoft SQL Server verwenden, empfehlen wir Ihnen den Artikel [Silk Central MSSQL Server Recommendations](#) zu lesen.

Auswählen eines relationalen Datenbankmanagementsystems (RDBMS)

Installieren Sie Oracle oder Microsoft SQL Server entsprechend der mit dem Datenbankmanagementsystem mitgelieferten Dokumentation.

Silk Central unterstützt folgende Datenbankmanagementsysteme:

- Microsoft SQL Server 2012 Service Pack 3
- Microsoft SQL Server 2014 Service Pack 2
- Microsoft SQL Server 2016
- Oracle 11g (Version 11.2.0.4)
- Oracle 12c (Version 12.1.0.2)

In der folgenden Tabelle finden Sie die Voraussetzungen für die verschiedenen Datenbanktypen.

RDBMS	Voraussetzungen
Oracle	<ul style="list-style-type: none">• Oracle-Tablespace.• Hostname des Servers und Portnummer, oder <i>Single Client Access Name</i> (SCAN). Der Standardport ist 1521.• Name der Oracle-Instanz (<code>\$ORACLE_SID</code>).• Benutzername und Kennwort des Silk Central-Datenbankbenutzers. Der Benutzer benötigt Kontingente und ausreichende Berechtigungen. <p>Wenn Sie sich an Ihren Oracle-Administrator, wenn Sie Hilfe benötigen.</p> <p> Hinweis: In Oracle werden keine Datenbanken erstellt, sondern Schemas, die bestimmten Benutzernamen zugeordnet sind. Daher werden die Datenbanknamen nicht Oracle-Datenbanken, sondern Benutzernamen zugewiesen. Silk Central verweist auf solche Benutzernamen als <i>Datenbanknamen</i>.</p>
Microsoft SQL Server	<ul style="list-style-type: none">• Hostname des Servers und Portnummer.• Benutzername und Kennwort für MS SQL Server.• Name für die Silk Central-Datenbank.

RDBMS	Voraussetzungen
	<ul style="list-style-type: none"> • Benutzername und Kennwort des Silk Central-Datenbankbenutzers. <p> Hinweis: Silk Central unterstützt nur <i>Microsoft SQL Server</i>-Server, die ohne Berücksichtigung der Groß-/Kleinschreibung eingerichtet wurden. Verwenden Sie <i>Microsoft SQL Server Express</i> nicht für Produktionsumgebungen, da die Anwendung im Vergleich zu einer vollständigen Datenbank-Serverinstallation nur eingeschränkte Möglichkeiten bietet.</p>

Berechtigungen für den Datenbankzugriff

Aus Sicherheitsgründen wird davon abgeraten, die Silk Central-Datenbank mit dem Datenbankadministrator-Benutzer zu verwalten. Dieses Thema führt die Datenbankrollen auf, die Sie bestimmten Aufgaben zuordnen können:

Microsoft SQL Server Wenn Sie Microsoft SQL Server als DBMS für Silk Central einsetzen, werden für die Silk Central-Datenbank folgende Datenbank-Rollen/-Benutzerberechtigungen benötigt:

Entweder:	Oder:
<ul style="list-style-type: none"> • db_owner • db_ddladmin • VIEW SERVER STATE 	<ul style="list-style-type: none"> • db_datareader • db_datawriter • db_ddladmin • EXECUTE • VIEW SERVER STATE

Benutzer mit diesen Rollen/Berechtigungen können Tabellen in der Datenbank erstellen und konfigurieren, auf bereits vorhandene Datenbanken zugreifen sowie die Software installieren und aktualisieren.

 **Hinweis:** Für den Silk Central-Datenbankbenutzer sind diese Rollen/Berechtigungen erforderlich. Ansonsten treten Fehler auf.

Oracle Wenn Sie Oracle als DBMS für Silk Central einsetzen, müssen für die Verwendung mit Silk Central folgende Benutzerberechtigungen für die Oracle-Datenbank gewährt werden:

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

 **Hinweis:** Der Silk Central-Datenbankbenutzer benötigt alle genannten Berechtigungen. Ansonsten treten Fehler auf. Um für die Systemdiagnose sämtliche datenbankbezogenen Analysedaten zu erhalten, wird empfohlen dem Datenbankbenutzer auch die Rolle `SELECT_CATALOG_ROLE` zuzuordnen.

 **Hinweis:** Der Oracle-Benutzer benötigt für die Arbeit mit Silk Central ausreichend Kontingente.

Wenn Sie Oracle als DBMS für Silk Central einrichten, beachten Sie bitte folgende Punkte in Bezug auf die Oracle-Umgebung:

- Der temporäre Tablespace sollte mindestens 2 GB groß sein.

- Auf der Festplatte muss genügend Speicherplatz für den temporären Tablespace vorhanden sein.

Erstellen von Datenbanken

Wenn Silk Central zurzeit mit einer Datenbank verbunden ist, müssen Sie die Verbindung trennen, bevor Sie eine neue Datenbank erstellen können.



Hinweis: Wenn Sie eine Testversion von Silk Central installiert haben, wird automatisch eine Demo-Datenbank namens `demodb` angelegt und verbunden. In diesem Fall müssen Sie die folgenden Schritte nicht ausführen.

So erstellen Sie eine neue Datenbank:

1. Wenn Sie bereits einen Silk Central-Anwendungsserver eingerichtet haben, wird die Seite für die **Datenbank** in einem Browserfenster angezeigt, und Sie können mit Schritt 3 fortfahren.



Tipp: Alternativ können Sie mit einem Browser zur Silk Central-Site navigieren. Die Standard-URL ist `http://<Computername>:19120/login` (keine Portinformationen nötig wenn Silk Central auf IIS läuft). Wenn Sie bei der Installation von Silk Central die Option *Standard Setup* verwenden, wird die Seite **Datenbank** unmittelbar nachdem Sie die Verbindung zur Anwendung hergestellt haben, angezeigt. Auf dem Computer, auf dem der Front-End-Server installiert ist, können Sie auch **Start > Programme > Silk > Silk Central > Silk Central18.5 > Silk Central Homepage** wählen.

2. Melden Sie sich bei Silk Central als Systemadministrator an.

Weitere Informationen finden Sie unter [Systemadministrator](#).

3. Klicken Sie im Menü auf **Datenbanken**.

4. Konfigurieren Sie die Einstellungen für die neue Datenbank.

Weitere Informationen finden Sie unter [Datenbank \(Seite\)](#).

Sie können eine Datenbank auf einem lokal installierten Microsoft SQL Server 2008 Express SP1, einem lokal installierten Microsoft SQL Server, einem Oracle-Server oder auf einem Netzwerkserver erstellen, auf dem MS SQL Server oder Oracle installiert sind. Silk Central unterstützt:

- Microsoft SQL Server 2012 Service Pack 3
- Microsoft SQL Server 2014 Service Pack 2
- Microsoft SQL Server 2016
- Oracle 11g (Version 11.2.0.4)
- Oracle 12c (Version 12.1.0.2)

5. Klicken Sie auf **Datenbank verbinden** und anschließend auf **Ja**. Der Dialog **Neue Datenbank erstellen** wird angezeigt.

6. Geben Sie die Anmeldedaten des Datenbankadministrators ein, und klicken Sie auf **OK**.



Tipp: Wenn Sie eine lokale oder eine Netzwerk-Datenbank mit Microsoft SQL Server oder Oracle erstellen möchten, geben Sie die Anmeldedaten ein, die Sie von Ihrem Datenbankadministrator erhalten haben.

Das Dialogfeld **ALM Repository-ID anlegen** wird angezeigt.

7. Geben Sie eine eindeutige **ALM Repository-ID** ein, und klicken Sie auf **OK**.

8. Sie werden benachrichtigt, dass das Repository erfolgreich erstellt wurde. Klicken Sie auf **OK**. Die Anmeldeseite wird angezeigt.

Die Datenbank wurde erstellt, und es ist eine Verbindung vorhanden. Nun können Sie sich bei Silk Central mit Ihrem Benutzernamen und Ihrem Kennwort anmelden.

Verbinden mit einer Datenbank

So stellen Sie eine Verbindung zu einer Datenbank her:

1. Wechseln Sie mit einem Webbrowser auf Ihre Silk Central-Seite.

Die Standard-URL ist `http://<Computername>:19120/login` (keine Portinformationen nötig wenn Silk Central auf IIS läuft).



Hinweis: Wenn zurzeit keine Datenbankverbindung vorliegt, werden Sie automatisch in den Bereich **Systemverwaltung** weitergeleitet.

2. Melden Sie sich bei Silk Central als Systemadministrator an.
Weitere Informationen finden Sie unter [Systemadministrator](#).
3. Klicken Sie im Menü auf **Datenbanken**.
4. Klicken Sie auf **Datenbank trennen**, um die aktuelle Datenbankverbindung zu beenden. Sie werden auf die Seite **Datenbank** weitergeleitet.
5. Ändern Sie gegebenenfalls die Einstellungen.
Weitere Informationen finden Sie unter [Datenbank \(Seite\)](#).
6. Klicken Sie auf **Datenbank verbinden**.

Die Herstellung der Datenbankverbindung kann einige Minuten bis mehrere Stunden in Anspruch nehmen. Sobald eine Verbindung hergestellt wurde, wird ein Dialogfeld angezeigt. Klicken Sie auf **OK**. Die Silk Central-Anmeldeseite wird angezeigt.

Trennen der Verbindung zu einer Datenbank

So trennen Sie eine Datenbankverbindung:

1. Navigieren Sie mit einem Webbrowser auf Ihre Silk Central-Site.
Die Standard-URL ist `http://<Computername>:19120/login` (keine Portinformationen nötig wenn Silk Central auf IIS läuft).
2. Melden Sie sich bei Silk Central als Systemadministrator an.
Weitere Informationen finden Sie unter [Systemadministrator](#).
3. Klicken Sie im Menü auf **Datenbanken**.
4. Klicken Sie auf **Datenbank trennen**, um die aktuelle Datenbankverbindung zu beenden. Sie werden auf die Seite **Datenbank** weitergeleitet.

ALM Repository-IDs

Jede Silk Central-Datenbank muss eine eindeutige Repository-ID besitzen. Diese ID wird in ALM URIs verwendet, um Silk Central-Anforderungen und Testläufe bei mehreren Silk Central-Repositorys eindeutig zu identifizieren. Die Repository-ID muss in allen Silk Central-Installationen im Unternehmen eindeutig sein. Die angegebene Repository-ID ist Bestandteil des ALM URIs. Weitere Informationen zu ALM URIs finden Sie unter *ALM URIs*. Verwenden Sie eine aussagekräftige ID, beispielsweise `USCA01` für USA, California, Repository-Nr. 01, oder `GE02` für Germany, Berlin, Repository-Nr. 02. Buchstaben, Zahlen, Punkt (.) und Minus (-) sind zulässige Zeichen. IDs müssen zwischen einem und 20 Zeichen lang sein.



Vorsicht: Wenn eine Repository-ID festgelegt wurde, kann sie nicht mehr geändert werden.

ALM URIs

Repository-IDs werden in Application Lifecycle Management Uniform Resource Identifiers (ALM URIs) aufgenommen. Mit ALM URIs können Elemente auf der gesamten ALM-Serverplattform verwendet, unterschieden und über eine Anwendung hinaus nachverfolgt werden. Unter anderem werden mit ALM URIs Silk Central-Anforderungen und Testläufe in mehreren Silk Central-Repositorys eindeutig identifiziert.

Die Syntax des ALM-Element-URIs lautet folgendermaßen:

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

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

Die Projektidentität setzt sich folgendermaßen zusammen:

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

<repository ID> ist ein eindeutiger Bezeichner für jedes Silk Central- und Issue Manager-Repository. Jedes Repository erzeugt einen eindeutigen Bezeichner, der im Repository gespeichert wird. Die Eindeutigkeit wird über alle installierten Repositories hinweg gewährleistet. <project ID> ist ein Bezeichner für ein Silk Central- oder Issue Manager-Projekt. Dieser Bezeichner ist im Kontext eines Repository eindeutig.

Quellelementpfad:

Silk Central und Issue Manager referenzieren Artefakte mit der folgenden Syntax:

Native Anforderungen von Silk Central, bei denen es sich um Anforderungen handelt, die nicht mit einem externen Anforderungsmanagementsystem verknüpft sind, verwenden folgende Syntax:

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

Für Silk Central-Tests wird folgende Syntax verwendet:

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

Für Silk Central- und Issue Manager-Fehler wird folgende Syntax verwendet:

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

Beispiel eines ALM URIs:

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

Silk Central-Repository USCA01, Projekt-ID 23, Element-ID 602, Elementtyp test.

Datenbank (Seite)

Auf der Seite **Datenbank** können Sie eine Datenbank mit Silk Central verbinden und die Verbindung wieder trennen.

Wenn keine Datenbankverbindung vorliegt, werden Sie automatisch auf die Seite **Datenbank** weitergeleitet.

Wenn eine Datenbankverbindung vorliegt, müssen Sie sich als Systemadministrator anmelden und auf **Datenbank** klicken, um auf die Seite **Datenbank** zu gelangen. Weitere Informationen finden Sie unter *Systemadministrator*.

Konfigurieren Sie die Datenbankverbindung mithilfe der folgenden Steuerelemente der Benutzeroberfläche:

Element	Beschreibung
DBMS-Hostname oder IP-Adresse	Der Name des Computers, der das DBMS (Datenbankmanagementsystem) hostet. Geben Sie den Namen im Format <Computer Name>\<Instanz Name> ein.
Datenbanksystem	Beschreibung für den Hostnamen
Microsoft SQL Server	<Computernamen>\<Instanzname>. Zum Beispiel: localhost.  Hinweis: Ein Instanzname muss nur angegeben werden, wenn das DBMS mit einer Instanz installiert wurde.
Oracle Server	<Computernamen> oder <i>Single Client Access Name (SCAN)</i> . Zum Beispiel: MyDBMSHost. Wenn Sie benutzerdefinierte Berichte mit einem direkten Datenbankzugriff erstellen möchten, definieren Sie einen

Element	Beschreibung
	<p>Datenbanksystem Beschreibung für den Hostnamen</p> <p>DBMS-Hostnamen, der im gesamten Netzwerk verfügbar ist/ sind.</p>
DBMS-Typ	Der Typ des DBMS, auf den zugegriffen werden soll: MS SQL Server oder Oracle.
Port	Der Port, über den das DBMS Daten empfängt. Der Standardport für MS SQL Server, einschließlich Express, ist 1433. Der Standardport für Oracle ist 1521.
Datenbank / SID	<p>Name der MSSQL Server-Datenbank oder Oracle SID, die von Ihrem Oracle-Administrator bereitgestellt wird. Um sich mit einer Oracle RAC Umgebung zu verbinden, geben Sie vor der SID einen Schrägstrich (/) ein.</p> <p><i>Für Oracle-Datenbankadministratoren:</i> Konfigurieren Sie die Oracle SID für die Verwendung des UTF8-Zeichensatzes.</p>
Benutzername / Kennwort	<p>Microsoft SQL Server, einschließlich Express</p> <p>Datenbank-Benutzer mit ausreichendem Zugriff, oder ein gültiger Windows Domänen-Benutzer (Domäne\Benutzername). Wenn Sie die Windows-Authentifizierung verwenden, muss der Datenbank-Server LMv2 und NTLMv2 unterstützen. Single Sign-on ohne einen Benutzer anzugeben wird nicht unterstützt.</p> <p> Hinweis: Wenn Sie Silk Central evaluieren, lauten die Standard-Anmeldeinformationen sa / SilkCentral12!34.</p> <p>Oracle Server</p> <p>Datenbank-Benutzer mit ausreichendem Zugriff, welchen Sie von Ihrem Oracle-Administrator erhalten.</p> <p> Wichtig: Bei Oracle-Servern darf der Name des Datenbankbenutzers keinen Punkt (.) enthalten.</p>
Benutzername für Lesezugriff	<p>Ein optionaler Datenbankbenutzer mit schreibgeschütztem Zugriff auf alle Tabellen und Views der angegebenen Datenbank. Dieser Benutzer wird für die Ausführung von Aktionen verwendet, die nur Lesezugriff benötigen, z.B. die Ausführung von Berichten. Dies gewährleistet, dass die Ausführung von Berichten mit erweiterten Abfragen keine Daten in der Datenbank ändert, da erweiterte Abfragen negative Auswirkungen auf die Daten haben können. Der Zugriff auf die Datenbank mit einem Benutzer, der nur Lesezugriff hat, wirkt sich auch positiv auf die Leistung aus.</p> <p>Wenn Sie als DBMS Microsoft SQL Server verwenden, erstellt Silk Central automatisch diesen Benutzer, wenn Sie einen Namen und ein Kennwort angeben. Wenn Sie als DBMS Oracle verwenden, muss der Benutzer vom Datenbankadministrator in Oracle erstellt und vom Silk Central-Administrator in Silk Central hinzugefügt werden.</p>
Kennwort für Lesezugriff	Gültiges Kennwort für den im Feld Benutzername für Lesezugriff angegebenen Benutzer.
DBMS-Versionsinfo	Zeigt Versionsinformationen zu DBMS und Betriebssystem an.
ALM-Repository-ID	Zeigt die ALM URI des Repositorys an.
Datenbank verbinden / Datenbankverbindung trennen	Klicken Sie auf diese Schaltfläche, um eine DBMS-Verbindung herzustellen oder zu trennen.



Hinweis: Wenn Sie eine ungültige ältere Version, aber höher als Version *SilkCentral Test Manager 2009 SP1*, eines Ausführungsservers verwenden, wird diese automatisch auf die aktuelle Version von Silk Central aktualisiert. Silk Central zeigt in der Ausführungsserverliste in der Spalte **Information** eine Nachricht betreffend der Aktualisierung an. Der zu aktualisierende Ausführungsserver wird erst nach Abschluss des Upgrade-Vorgangs verwendet.

Mandanten

Mandanten sind getrennte Einheiten innerhalb einer Silk Central-Instanz. Ein Mandant kann z.B. ein *Kunde* oder ein *Geschäftsbereich* eines Unternehmens sein. Mandanten erhöhen die Datensicherheit, aber im Gegensatz zu Instanzen verwenden sie dieselbe Datenbank und dieselben Silk Central-Dienste.

Im Bereich **Systemverwaltung** können Sie Mandanten erstellen. Sie können verschiedene Mandanteneinstellungen vornehmen, die für die dem Mandanten zugeordneten Projekte gelten. Sie können die maximal verfügbaren Lizenzen pro Mandant aus den insgesamt verfügbaren Lizenzen festlegen. Sie können nur dann auf die Daten eines Mandanten zugreifen, wenn Sie bei diesem Mandanten angemeldet sind. Innerhalb eines Mandanten sind sämtliche Komponenten projektübergreifend verfügbar.

Wenn Sie Silk Central installieren, wird automatisch ein Standardmandanten erstellt. Wenn Sie für Silk Central ein Upgrade von einer älteren Version durchführen, werden vorhandene Projekte und Benutzer diesem Standardmandanten zugeordnet. Für jeden Mandanten wird ein Super User erstellt. Weitere Informationen finden Sie unter *Super User*. Sie können alle Mandanten löschen, benötigen jedoch mindestens einen Mandanten, um Projekte und Benutzerkonten erstellen und mit Silk Central arbeiten zu können.

Super User

Der Super User verfügt innerhalb eines Mandanten über sämtliche Berechtigungen. Im Gegensatz zum Super User kann der Systemadministrator nur die unterschiedlichen Mandanten einer Silk Central-Installation verwalten und hat keinen Zugriff auf die eigentliche Silk Central-Benutzeroberfläche.

Wenn der Systemadministrator einen neuen Mandanten erstellt, wird für diesen Mandanten automatisch ein Super User erstellt.

Melden Sie sich mit den folgenden Standard-Anmeldedaten als Super User an:

- Benutzername: `admin`
- Kennwort: `admin`



Wichtig: Ändern Sie dieses Standardkennwort so bald wie möglich. Klicken Sie zum Ändern des Kennworts im Menü auf **Verwaltung > Benutzerverwaltung**, dann auf die Registerkarte **Konten** und schließlich in der Tabelle auf **admin**. Der Benutzername kann nicht geändert werden.

Eine Liste sämtlicher Benutzerrollen und Berechtigungen finden Sie unter *Benutzerrollen und Berechtigungen*.

Erstellen von Mandanten

So erstellen Sie einen Mandanten:

1. Melden Sie sich bei Silk Central als Systemadministrator an.
Weitere Informationen finden Sie unter *Systemadministrator*.
2. Klicken Sie im Menü auf **Mandanten**.
3. Klicken Sie auf **Neuer Mandant**. Das Dialogfeld **Neuer Mandant** wird angezeigt.
4. Geben Sie den **Mandantennamen** und eine **Beschreibung** ein.
5. Legen Sie die maximal gleichzeitig verfügbaren Lizenzen für diesen Mandanten im Bereich **Lizenzlimits** fest. Sobald die festgelegte Anzahl von Lizenzen in Verwendung ist, erhalten keine weiteren Benutzer mehr eine Lizenz auf diesem Mandanten. Dies ist vor allem dann hilfreich, wenn Sie

z.B. sicherstellen wollen, dass ein wichtiger Mandant immer genügend Lizenzen zur Verfügung hat, während die Lizenzen für einen nicht so wichtigen Mandanten beschränkt sind.

Die folgenden Regeln werden angewendet:

- **Kein Wert:** Es wird kein Lizenzlimit festgelegt und der Mandant kann von den insgesamt verfügbaren Lizenzen Gebrauch machen.
- **0 (Null):** Der Mandant hat gar keine Lizenzen zur Verfügung, was effektiv sämtliche mit der entsprechenden Lizenz in Verbindung stehende Funktionalität deaktiviert.
- **Eine Zahl:** Die Anzahl der Lizenzen, die dem Mandanten zur Verfügung stehen. Falls die festgelegte Zahl höher ist als die insgesamt verfügbaren Lizenzen, kann der Mandant von den insgesamt verfügbaren Lizenzen Gebrauch machen.



Tipp: Die Anzahl der insgesamt verfügbaren Lizenzen wird unten auf der Seite **Mandanten** angezeigt.

6. Klicken Sie auf **OK**.

Loggen Sie sich auf dem Mandanten als Super User ein, um mandantenspezifische Administrationsaufgaben zu erledigen. Weitere Informationen finden Sie unter *Super User*.

Bearbeiten von Mandanten

So bearbeiten Sie die Einstellungen eines Mandanten:

1. Melden Sie sich bei Silk Central als Systemadministrator an.
Weitere Informationen finden Sie unter [Systemadministrator](#).
2. Klicken Sie im Menü auf **Mandanten**.
3. Klicken Sie in der Spalte **Aktionen** auf  (**Bearbeiten**). Das Dialogfeld **Mandant bearbeiten** wird angezeigt.
4. Bearbeiten Sie den **Mandantenamen** und die **Beschreibung**.
5. Legen Sie die maximal gleichzeitig verfügbaren Lizenzen für diesen Mandanten im Bereich **Lizenzlimits** fest. Sobald die festgelegte Anzahl von Lizenzen in Verwendung ist, erhalten keine weiteren Benutzer mehr eine Lizenz auf diesem Mandanten. Dies ist vor allem dann hilfreich, wenn Sie z.B. sicherstellen wollen, dass ein wichtiger Mandant immer genügend Lizenzen zur Verfügung hat, während die Lizenzen für einen nicht so wichtigen Mandanten beschränkt sind.

Die folgenden Regeln werden angewendet:

- **Kein Wert:** Es wird kein Lizenzlimit festgelegt und der Mandant kann von den insgesamt verfügbaren Lizenzen Gebrauch machen.
- **0 (Null):** Der Mandant hat gar keine Lizenzen zur Verfügung, was effektiv sämtliche mit der entsprechenden Lizenz in Verbindung stehende Funktionalität deaktiviert.
- **Eine Zahl:** Die Anzahl der Lizenzen, die dem Mandanten zur Verfügung stehen. Falls die festgelegte Zahl höher ist als die insgesamt verfügbaren Lizenzen, kann der Mandant von den insgesamt verfügbaren Lizenzen Gebrauch machen.



Tipp: Die Anzahl der insgesamt verfügbaren Lizenzen wird unten auf der Seite **Mandanten** angezeigt.

6. Klicken Sie auf **OK**.



Hinweis: Wenn Sie den **Mandantenamen** ändern, sollten Sie die Silk Central-Benutzer darüber informieren. Silk Central Benutzer müssen den Mandantennamen bei der Anmeldung eingeben.

Loggen Sie sich auf dem Mandanten als Super User ein, um mandantenspezifische Administrationsaufgaben zu erledigen. Weitere Informationen finden Sie unter *Super User*.

Entfernen von Mandanten

So entfernen Sie einen Mandanten:

1. Melden Sie sich bei Silk Central als Systemadministrator an.
Weitere Informationen finden Sie unter [Systemadministrator](#).
2. Klicken Sie im Menü auf **Mandanten**.
3. Klicken Sie in der Spalte **Aktionen** auf **✗ (Löschen)**.
4. Klicken Sie zum Bestätigen auf **Ja**.

Standard-Mandant

Wenn Sie Silk Central installieren, wird automatisch ein Mandant (mit dem Namen `Standard`) erstellt und dieser als Standard-Mandant festgelegt. Wenn Sie den Standard-Mandanten ändern möchten, melden Sie sich bei Silk Central als Systemadministrator an, und klicken Sie auf **Mandanten**. Weitere Informationen finden Sie unter [Systemadministrator](#).

Wenn Sie einen Mandanten als Standard festlegen möchten, klicken Sie auf **Als Standard festlegen**.

Wenn Sie den Standardstatus aufheben möchten, klicken Sie auf **Standard aufheben**. Das Symbol  zeigt an, welcher Mandant zurzeit der Standard-Mandant ist. Es ist möglich, dass kein Standard-Mandant festgelegt ist, aber es kann immer nur ein Mandant den Standardstatus aufweisen.

Der Zweck des Standard-Mandanten besteht darin, die Anmeldung zu vereinfachen: Wenn Sie sich bei Silk Central mit den Benutzerdaten des Standard-Mandanten anmelden, brauchen Sie keinen Mandantennamen anzugeben. Geben Sie nur den Benutzernamen ein. Dies ist vor allem bei Silk Central-Installationen mit nur einem Mandanten hilfreich. Wenn Sie für Silk Central ein Upgrade von einer älteren Version durchführen, bleibt der Anmeldevorgang unverändert.

Lizenzverarbeitung

Silk Central bietet verschiedene Lizenztypen.

Benutzerbasierte Lizenzen

Diese Lizenzen werden vom Lizenzserver ausgecheckt, sobald ein Benutzer in einen bestimmten Bereich von Silk Central gelangt:

Lizenztyp	Bereich
Testmanager	Diese Lizenz wird ausgecheckt, wenn Sie nach Ihrer Anmeldung erstmalig auf einen Testmanagementbereich klicken. Die Silk Central-Testmanagementbereiche sind: Anforderungen, Tests, Ausführungsplanung, Verfolgung, Fehler (mit Ausnahme des Issue Manager-Bereichs) und Berichte .
Manuelles Testen	Diese Lizenz wird ausgecheckt, wenn Sie das Fenster Manuelles Testen öffnen. Eine Lizenz für manuelles Testen wird ausgecheckt sobald ein Test für die Offline-Ausführung heruntergeladen wird. Die Lizenz wird wieder eingecheckt sobald die Ergebnisse hochgeladen werden.
Fehlerverfolgung	Diese Lizenz wird ausgecheckt, wenn Sie auf Issue Manager zugreifen.

Beachten Sie Folgendes:

- Wenn Sie auf **Abmelden (Benutzer > Abmelden)** klicken, werden die Lizenzen wieder am Lizenzserver eingecheckt, mit Ausnahme der Lizenzen für manuelles Testen, die zur Offline-Testausführung ausgecheckt wurden.
- Wenn Sie sich nicht abmelden (sondern nur das Browserfenster schließen), wird die Lizenz erst bei Ablauf der Sitzung eingecheckt.

Die Seite **Info (Hilfe > Info)** zeigt an, wie viele Lizenzen derzeit verwendet werden und wie viele für den Mandanten verfügbar sind, auf dem Sie gerade eingeloggt sind.

Standort-Lizenzen

Diese Lizenzen schalten eine bestimmte Funktionalität für alle Benutzer frei, ohne Einschränkungen:

Lizenztyp	Bereich
Mobiles Testen	Diese Lizenz ermöglicht das Testen auf mobile Geräten (physische Geräte, Emulatoren und Simulatoren) für manuelles, automatisiertes und Konfigurationstesten.

Mandanten (Seite)

Melden Sie sich zum Öffnen dieser Seite bei Silk Central als Systemadministrator an, und klicken Sie auf **Mandanten**. Weitere Informationen finden Sie unter *Systemadministrator*.

Mithilfe dieser Seite können Sie Ihre Mandanten erstellen und verwalten. Klicken Sie auf die Schaltfläche **Neuer Mandant**, um einen neuen Mandanten zu erstellen. Klicken Sie auf die Schaltflächen **Als Standard festlegen** oder **Standard aufheben**, um den Standardstatus des Mandanten zu ändern. Das Symbol  zeigt an, welcher Mandant zurzeit der Standard-Mandant ist.

Die Tabelle enthält die folgenden Spalten:

Spalte	Beschreibung
Aktionen	Klicken Sie auf die Schaltflächen  oder  , um Mandanten zu löschen oder zu bearbeiten .
ID	Die Kennung des Mandanten.
Name	Der Name des Mandanten. Klicken Sie auf  , um den Namen zu bearbeiten . Wenn Sie den Mandantennamen ändern, sollten Sie die Silk Central Benutzer darüber informieren. Silk Central Benutzer müssen den Mandantennamen bei der Anmeldung eingeben.
Beschreibung	Hier wird der Mandant ausführlicher beschrieben. Klicken Sie auf  , um die Beschreibung zu bearbeiten .
Test Manager	Die maximale Anzahl von Test Manager Lizenzen, die gleichzeitig in Verwendung sein können.
Manuelles Testen	Die maximale Anzahl von Manuelles Testen Lizenzen, die gleichzeitig in Verwendung sein können.
Fehlerverfolgung	Die maximale Anzahl von Fehlerverfolgung Lizenzen, die gleichzeitig in Verwendung sein können.
Automatisiertes Testen	Die maximale Anzahl von Automatisiertes Testen Lizenzen, die gleichzeitig in Verwendung sein können.
Erstellt am	Datum, an dem der Mandant erstellt wurde.
Erstellt von	Der Name des Benutzers, der den Mandanten erstellt hat.
Geändert am	Datum, an dem der Mandant geändert wurde.
Geändert von	Der Name des Benutzers, der den Mandanten geändert hat.

Mandantenberechtigungen

Mithilfe dieser Seiten können Sie die Systemeinstellungen und -berechtigungen für Mandanten ändern.

Element	Beschreibung
Mandantenbenutzern Log-Ansichten zu Front-End- und Anwendungsservern anzeigen.	Wenn aktiviert, werden die Log-Registerkarten zu den Front-End- und Anwendungsservern auf der Benutzeroberfläche angezeigt (die Logs können Mandanten-spezifische Daten enthalten).
Erweiterte Berichte für Mandantenbenutzer zulassen.	Wenn aktiviert, sind Berichte mit erweiterten Abfragen möglich. Wenn nicht aktiviert, können die Berichte zwar ausgeführt werden, aber die Erstellung oder Bearbeitung neuer Berichte ist nicht möglich.
Verwalten von Berichtsvorlagen für Benutzer des Mandanten erlauben.	Wenn aktiviert, können Berichtsvorlagen hochgeladen, erstellt, bearbeitet und gelöscht werden. Hochgeladene Berichtsvorlagen können beliebigen SQL-Code enthalten und Daten anderer Mandanten lesen.

Infrastruktur

Enthält Einstellungen für Diagrammserver, E-Mail-Server und den System-Proxy.

Diagrammserver

Ein Diagrammserver ist ein Dienst, der Daten berechnet und Diagramme erzeugt. Diese Diagramme werden mit der Silk Central-Anwendung angezeigt. Dieser Dienst kann im Rahmen der Silk Central-Installation auf einem Computer Ihrer Wahl installiert werden. Für die Anzeige von Diagrammen ist die Konfiguration einer Diagrammserver-Verbindung erforderlich.

 **Hinweis:** Sie können beliebig viele Diagrammserver-Verbindungen konfigurieren. Silk Central implementiert automatisch einen Lastausgleichsmechanismus für die Diagrammerzeugung.

Konfigurieren von Diagrammserver-Verbindungen

So konfigurieren Sie eine Diagrammserver-Verbindung:

1. Klicken Sie im Menü auf **Infrastruktur > Diagrammserver**
2. Wenn ein Diagrammserver zusammen mit dem Anwendungsserver auf demselben Computer installiert wurde, wird automatisch eine Diagrammserver-Verbindung zu `localhost` konfiguriert.
3. *Optional:* Wenn Ihre Diagrammserver mit dem Front-end Server über einen anderen URL kommunizieren sollen als den, mit dem auf die Web Benutzeroberfläche zugegriffen wird, klicken Sie auf **Webdienst-URL konfigurieren** geben Sie diesen URL im Textfeld ein. Dies ist zum Beispiel nötig, wenn Benutzer über einen Proxy auf die Web Benutzeroberfläche zugreifen, während Ihre Diagrammserver den internen URL oder die IP-Adresse des Front-end Servers benötigen.
4. Klicken Sie auf **Neuer Diagrammserver**. Das Dialogfeld **Neuer Diagrammserver** wird angezeigt.
5. Geben Sie den **Hostnamen oder die IP-Adresse**, den **Port** und die **URL** des Ortes ein, an dem der Diagrammdienst installiert ist. Der Standardport ist `19126`, und die Standard-URL lautet `ChartServer`.
6. Klicken Sie auf **Prüfen**, um eine Testverbindung zum Diagrammserver herzustellen. Das Dialogfeld **Diagrammserver-Prüfung** wird angezeigt.

-  **Hinweis:** Wenn der Test erfolgreich ist, wird ein Testbild angezeigt. Wenn der Test fehlschlägt, wird eine Fehlernachricht angezeigt. Überprüfen Sie die eingegebenen Daten und vergewissern Sie sich, dass auf dem Zielcomputer ein Diagrammserver installiert ist.
7. Klicken Sie auf **Schließen**. War die Testverbindung erfolgreich, aktivieren Sie das Kontrollkästchen **Aktiv**, und klicken Sie auf **OK**.

Sie können beliebig viele Diagrammserver definieren. Silk Central implementiert automatisch einen Lastausgleichsmechanismus für die Diagrammerzeugung.

 **Hinweis:** Sie können nur dann eine Diagrammserver-Verbindung konfigurieren, wenn der *Diagrammserverdienst* auf dem Zielcomputer installiert ist. Weitere Informationen finden Sie in den Installationsanweisungen Ihrer Silk Central-Anwendung.

Bearbeiten von Diagrammserver-Verbindungen

So bearbeiten Sie eine Diagrammserver-Verbindung:

1. Klicken Sie im Menü auf **Infrastruktur > Diagrammserver**
2. *Optional:* Wenn Ihre Diagrammserver mit dem Front-end Server über einen anderen URL kommunizieren sollen als den, mit dem auf die Web Benutzeroberfläche zugegriffen wird, klicken Sie auf **Webdienst-URL konfigurieren** geben Sie diesen URL im Textfeld ein. Dies ist zum Beispiel nötig, wenn Benutzer über einen Proxy auf die Web Benutzeroberfläche zugreifen, während Ihre Diagrammserver den internen URL oder die IP-Adresse des Front-end Servers benötigen.
3. Klicken Sie in der Spalte **Aktionen** auf  (**Bearbeiten**). Das Dialogfeld **Diagrammserver bearbeiten** wird angezeigt.
4. Bearbeiten Sie **Hostname oder IP-Adresse**, den **Port** oder die **URL** des Ortes, an der Diagrammdienst installiert ist. Der Standardport ist 19126, und die Standard-URL lautet `ChartServer`.
5. Aktivieren/deaktivieren Sie das Kontrollkästchen **Aktiv**, um den Server zu aktivieren/deaktivieren.
6. Klicken Sie auf **Prüfen**, um eine Testverbindung zum Diagrammserver herzustellen. Das Dialogfeld **Diagrammserver-Prüfung** wird angezeigt.

 **Hinweis:** Wenn der Test erfolgreich ist, wird ein Testbild angezeigt. Wenn der Test fehlschlägt, wird eine Fehlermeldung angezeigt. Überprüfen Sie die eingegebenen Daten und vergewissern Sie sich, dass auf dem Zielcomputer ein Diagrammserver installiert ist.

7. Klicken Sie auf **Schließen** und dann auf **OK**.

Entfernen von Diagrammserver-Verbindungen

So entfernen Sie eine Diagrammserver-Verbindung:

1. Klicken Sie im Menü auf **Infrastruktur > Diagrammserver**
2. Klicken Sie in der Spalte **Aktionen** auf  (**Bearbeiten**). Das Dialogfeld **Diagrammserver bearbeiten** wird angezeigt.
3. Deaktivieren Sie das Kontrollkästchen **Aktiv**, und klicken Sie auf **OK**.
4. Klicken Sie in der Spalte **Aktionen** auf  (**Löschen**).
5. Klicken Sie zum Bestätigen auf **Ja**.

 **Hinweis:** Nun wird die Verbindung zum Server entfernt. Der Server selbst wird nicht entfernt.

Diagrammserver (Seite)

Melden Sie sich zum Öffnen der Seite bei Silk Central als Systemadministrator an, und klicken Sie auf **Infrastruktur > Diagrammserver**. Weitere Informationen finden Sie unter *Systemadministrator*.

Mithilfe dieser Seite können Sie die Verbindungen zu Ihren Diagrammservern verwalten. Klicken Sie auf **Neuer Diagrammserver**, um eine neue Diagrammserver-Verbindung zu konfigurieren. **Webdienst-URL konfigurieren** ermöglicht die Konfiguration einer alternativen URL mit der sich Ihre Diagrammserver zum Front-end Server verbinden können. Die Tabelle enthält die folgenden Spalten:

Spalte	Beschreibung
Aktionen	Klicken Sie auf die Schaltflächen  oder  , um Diagrammserver-Verbindungen zu löschen bzw. zu bearbeiten . Es können nur deaktivierte Verbindungen gelöscht werden.
URL des Diagrammservers	Zeigt die URL des Diagrammservers an. Syntax: <code>http://<Computername oder IP-Adresse>:<Port>/ChartServer</code> . Der Standardport ist 19126. Klicken Sie auf  , um die URL zu bearbeiten .
Status	Zeigt an, ob die Verbindung mit dem Diagrammserver aktiv oder inaktiv ist. Klicken Sie auf  (Bearbeiten), um den Status einer Verbindung zu ändern.
Erstellt am	Datum, an dem die Verbindung mit dem Diagrammserver erstellt wurde.
Erstellt von	Der Benutzer, der die Verbindung mit dem Diagrammserver erstellt hat.
Geändert am	Datum, an dem die Verbindung mit dem Diagrammserver geändert wurde.
Geändert von	Der Benutzer, der die Verbindung mit dem Diagrammserver geändert hat.

E-Mail-Server

Wenn Sie einen E-Mail-Server konfigurieren, kann Silk Central Sie über Ergebnisse Ihrer Anwendung benachrichtigen.

Konfigurieren von E-Mail-Servern

So können Sie bis zu drei E-Mail-Server konfigurieren:

1. Melden Sie sich bei Silk Central als Systemadministrator an.
Weitere Informationen finden Sie unter *Systemadministrator*.
2. Klicken Sie auf **Infrastruktur > E-Mail-Server**.
3. Geben Sie in das Feld **E-Mail-Adresse des Systemadministrators** eine E-Mail-Adresse ein.
Silk Central schickt Benachrichtigungen an diese Adresse.
4. Geben Sie in das Feld **"Von"-Adresse für E-Mails** eine E-Mail-Adresse ein.
Diese Adresse wird bei den Benachrichtigungen als Absender angezeigt.
5. Geben Sie den Hostnamen oder die IP-Adresse des E-Mail-Servers in die Felder **Server** ein.
Sie können bis zu drei E-Mail-Server konfigurieren.
6. Wenn für die Server Anmeldedaten erforderlich sind, geben Sie diese in die Felder **Benutzername** und **Kennwort** ein.
7. Klicken Sie auf **Prüfen**, um die Verbindung zu den Servern zu testen. Silk Central schickt eine Test-E-Mail an die E-Mail-Adresse, die Sie in Schritt 3 eingegeben haben.
8. Wenn eine Fehlermeldung angezeigt wird, oder wenn Sie keine E-Mail erhalten, überprüfen Sie die Mail-Einstellungen. Stellen Sie sicher, dass der Hostname Ihres Mailservers korrekt angegeben wurde, und dass auf diesem Computer das SMTP-Protokoll ausgeführt wird.



Hinweis: SMTP mit TLS wird zur Zeit nicht unterstützt.

9. Wenn Sie die Test-E-Mail erhalten, war der Test erfolgreich. Klicken Sie auf **Speichern**.

E-Mail-Server (Seite)

Melden Sie sich zum Öffnen dieser Seite bei Silk Central als Systemadministrator an, und klicken Sie auf **Infrastruktur > E-Mail-Server**. Weitere Informationen finden Sie unter *Systemadministrator*.

Mithilfe dieser Seite können Sie bis zu drei E-Mail-Server konfigurieren. Die Seite enthält folgende Elemente:

Element	Beschreibung
E-Mail-Adresse des Systemadministrators	Gibt die E-Mail-Adresse des Silk Central-Systemadministrators an.
'Von'-Adresse für E-Mails	Legt fest, welcher Name im Feld Von angezeigt wird, wenn jemand eine E-Mail vom System empfängt. Das kann jede beliebige E-Mail-Adresse sein, z. B. <code>System_Nachricht@meinUnternehmen.com</code> .
Server 1	Geben Sie die Hostnamen oder IP-Adressen der Server an, die Ihre E-Mail schicken. In vielen Unternehmen heißt dieser Server einfach <code>Mail</code> . Wenn Ihr Mailserver die SMTP-Authentifizierung (LOGIN PLAIN) verwendet, müssen Sie für den Mailserver einen gültigen Benutzernamen und ein gültiges Kennwort eingeben. Wenden Sie sich an Ihren Mailserver-Administrator, wenn Sie nicht über die zur Anmeldung erforderlichen Daten verfügen.
Server 2	
Server 3	
Prüfen	Sendet eine Test-E-Mail an den Empfänger, der im Textfeld E-Mail-Adresse des Systemadministrators definiert wurde.
Speichern	Speichert die Einstellungen.
Zurücksetzen	Löscht alle Werte in den Feldern.

System-Proxy

Ausführungsserver eines Standorts können über einen Proxy mit dem Anwendungsserver kommunizieren. Sobald Sie (als Systemadministrator) einen Proxy-Server konfiguriert haben, können die Mandanten den Proxy aktivieren. Dafür müssen die Client-Benutzer im Menü auf **Verwaltung > Ausführungsserver** und dann in der Spalte **Aktionen** auf  (**Bearbeiten**) klicken und das Kontrollkästchen **System-Proxy verwenden** aktivieren.

Konfigurieren eines System-Proxy

So konfigurieren Sie einen System-Proxy:

1. Melden Sie sich bei Silk Central als Systemadministrator an.
Weitere Informationen finden Sie unter *Systemadministrator*.
2. Klicken Sie auf **Infrastruktur > System-Proxy**.
3. Geben Sie den **Host** und den **Port** des Proxy-Servers ein.
4. Falls erforderlich, geben Sie den **Benutzernamen** und das **Kennwort** ein.
5. Klicken Sie auf **Prüfen**, um die Verbindung zum Proxy-Server zu testen. Das Ergebnis des Tests wird in einem Dialogfeld angezeigt.
6. Wenn keine Verbindung hergestellt werden konnte, sollten Sie Ihre Einstellungen überprüfen.
7. Wenn eine Verbindung hergestellt werden konnte, klicken Sie auf **Speichern**. Der System-Proxy steht nun zur Verfügung.

System-Proxy (Seite)

Melden Sie sich zum Öffnen dieser Seite bei Silk Central als Systemadministrator an, und klicken Sie auf **Infrastruktur > System-Proxy**. Weitere Informationen finden Sie unter *Systemadministrator*.

Mithilfe dieser Seite können Sie einen System-Proxy konfigurieren. Die Seite enthält folgende Elemente:

Element	Beschreibung
Host	Der Hostname oder die IP-Adresse des Computers, der als System-Proxy dienen soll.
Port	Die Portnummer, von der der System-Proxy empfängt. Der Standardport ist 8080.
Benutzername (optional)	Geben Sie einen gültigen Benutzernamen ein, wenn der Proxy-Server die Eingabe von Benutzerdaten erfordert.
Kennwort (optional)	Geben Sie ein gültiges Kennwort für den Benutzernamen ein.
Prüfen	Testet die Verbindung mit dem Proxy-Server unter Verwendung der angegebenen Benutzerdaten.
Speichern	Speichert die Einstellungen.
Zurücksetzen	Löscht alle Elemente auf dieser Seite.

Anwendungsservergruppen

Der Anwendungsserver synchronisiert Aufgaben, wie etwa die Verteilung der Ausführungspläne, das Steuern der Ausführungsserver und die Verwaltung der Datenbankkonfiguration. Bevor Sie mit Silk Central arbeiten können, müssen Sie den Anwendungsserverstandort festlegen.

Festlegen des Standorts für den Anwendungsserver

Wenn Sie sich mit der Standard-Silk Central-Instanz verbinden, müssen Sie keinen Anwendungsserver-Standort festlegen. Das Setupprogramm konfiguriert automatisch Localhost als Anwendungsserver. In diesem Fall können Sie diese Anleitung überspringen. Weitere Informationen zu Installationsoptionen finden Sie in den Installationsanweisungen der Anwendung.

So stellen Sie eine Verbindung zum Anwendungsserver her:

1. Sobald Sie die Silk Central-Software installiert haben, stellen Sie mit Ihrem Browser eine Verbindung zu Silk Central her.



Tipp: Die Standard-URL ist `http://<Computername>:19120/login` (keine Portinformationen nötig wenn Silk Central auf IIS läuft).

Die Meldung, dass die Verbindung zum Anwendungsserver noch nicht definiert wurde, wird angezeigt.

2. Geben Sie den **Hostnamen** oder die **IP-Adresse** sowie den **Port** des Anwendungsservers ein.
Der Anwendungsserver ist der Computer, auf dem Sie die Anwendungsserver-Komponente von Silk Central installiert haben. Der Standardport ist 19122.
3. Klicken Sie auf **Anmelden**, um fortzufahren. Wenn Ihre Angaben korrekt sind und auf dem angegebenen Computer die installierte Software ausgeführt wird, werden Sie auf die Anmeldeseite zurückgeleitet.

Die Seite für die **Verwaltung der Datenbank** wird angezeigt.

LDAP-Authentifizierung

Konfigurieren Sie die LDAP-Authentifizierung, damit sich Benutzer über einen LDAP-Server bei Silk Central anmelden können.

LDAP (Lightweight Directory Access Protocol) ist ein offener Netzwerkprotokollstandard für den Zugriff auf Verzeichnisdienste. LDAP stellt einen Mechanismus zum Abfragen und Ändern von Informationen bereit, die sich in einer globalen Informationshierarchie, einem so genannten Directory Information Tree (DIT), befinden. Ein Directory Information Tree enthält normalerweise verschiedene Informationen zu

verschiedenen Arten von Netzwerkobjekten, wie Benutzer, Drucker, Anwendungen und andere Netzwerkressourcen.

Silk Central LDAP-Integration

Der wichtigste Aspekt der LDAP-Integration in Silk Central ist die Benutzerauthentifizierung. Da es in den meisten Verzeichnissen nicht möglich ist, das Kennwort eines Benutzers abzurufen, muss jedes Mal, wenn ein Benutzer authentifiziert werden muss, auf LDAP zugegriffen werden.

Die LDAP-Integration in Silk Central unterstützt unverschlüsselte wie auch SSL-verschlüsselte Authentifizierung. Der Verzeichnisdienst muss entweder anonyme Abfragen zulassen, oder es muss ein Benutzer angegeben werden, der über Leserechte für das Verzeichnis verfügt.

LDAP-Authentifizierungslogik

Authentifizierung im Standardmodus bedeutet, dass sich Benutzer nur über LDAP authentifizieren können, wenn ein LDAP-Server definiert und aktiviert ist. Authentifizierung im gemischten Modus bedeutet, dass sich Benutzer entweder über LDAP oder mit lokalen Benutzerdaten anmelden können. Wenn der Benutzer auf einem LDAP-Server verzeichnet ist, jedoch die falschen Anmeldeinformationen eingegeben hat, wird der Zugriff verweigert.



Hinweis: Für beide Authentifizierungsmodi gilt, dass sich nur Benutzer anmelden können, deren Benutzername in der Silk Central-Datenbank enthalten ist.

Authentifizierung im Standardmodus

Die Authentifizierung im Standardmodus ist verfügbar, wenn mindestens ein LDAP-Server aktiv ist. Jeder definierte LDAP-Server wird überprüft, um festzustellen, ob ein Benutzer (mit einem bestimmten Benutzernamen und Kennwort) authentifiziert werden kann. Der Zugriff wird gewährt, wenn die Authentifizierung auf einem Server erfolgreich durchgeführt wird.

Authentifizierung im gemischten Modus

Wenn kein LDAP-Server definiert ist, können sich die Benutzer nur mit lokalen Benutzerdaten anmelden. Wenn mindestens ein LDAP-Server aktiv ist und ein Benutzerkonto für die Authentifizierung im gemischten Modus konfiguriert ist, wird jeder definierte LDAP-Server überprüft, um zu bestimmen, ob der Benutzer (mit einem bestimmten Benutzernamen und Kennwort) authentifiziert werden kann. Wenn der Benutzer auf keinem der definierten LDAP-Server verzeichnet ist, wird eine Authentifizierung mithilfe der lokalen Datenbank versucht. Der Zugriff wird verweigert, wenn die vom Benutzer eingegebenen Benutzerdaten auch in der lokalen Datenbank nicht enthalten sind. Wenn der Benutzer auf einem LDAP-Server verzeichnet ist, jedoch die falschen Anmeldeinformationen eingegeben hat, wird der Zugriff verweigert.

Hinzufügen von LDAP-Servern

So konfigurieren Sie einen LDAP-Server für Silk Central:

1. Klicken Sie im Menü auf **Verwaltung > Systemeinstellungen**.
2. Klicken Sie auf die Registerkarte **LDAP-Server**.
3. Klicken Sie auf **Neuer LDAP-Server**. Das Dialogfeld **Neuer LDAP-Server** wird geöffnet.
4. Geben Sie einen **Namen** und optional eine **Beschreibung** für den Server ein. Sie können für den LDAP-Server jeden beliebigen Namen festlegen; dieses Feld hat keinen Einfluss auf die tatsächlichen LDAP-Einstellungen.
5. Markieren Sie das Kontrollkästchen **Aktiv**, um den Server für die Verwendung mit Silk Central zu aktivieren. Ist dieses Kontrollkästchen deaktiviert, stehen die Dienste des LDAP-Servers Silk Central nicht zur Verfügung.
6. Geben Sie den **Hostnamen** oder die IP-Adresse des LDAP-Servers und den für den LDAP-Dienst zu verwendenden **Port** an. Der Standardport ist 389. Bei Verwendung von SSL lautet der LDAP-Standardport 636.

7. Aktivieren Sie das Kontrollkästchen **SSL verwenden**, um eine Serververbindung über SSL herzustellen. Dieses Kontrollkästchen steht in engem Zusammenhang mit den im Feld **Port** definierten Einstellungen. Weitere Informationen über das Aufsetzen der Kommunikation über SSL finden Sie unter [Kommunikation mit einem externen System über SSL](#).
8. *Optional:* Geben Sie eine **Domäne** ein, wenn sich Ihre Benutzer mit dem Muster <Domäne>\<Benutzername> auf Silk Central anmelden sollen. Lassen Sie das Feld leer, wenn sich Ihre Benutzer ohne Domännennamen auf Silk Central anmelden sollen. Falls Ihre Silk Central-Installation aus mehreren Mandanten besteht, stellen Sie sicher, dass die angegebene LDAP-Domäne nicht gleich ist wie der Name irgendeines Mandanten, da das Anmeldeformular <Domäne>\<Benutzername> auch zum Anmelden auf die Mandanten verwendet wird.
9. *Optional:* Geben Sie im Feld **DN-Bind** den Domännennamen des Benutzers ein, der zum Binden an den LDAP-Dienst verwendet werden soll. Dieser Benutzer muss über Leseberechtigungen für das Verzeichnis im angegebenen **Basis-DN**-Stamm verfügen. Enthält dieses Textfeld keine Angabe, wird der anonyme Zugriff verwendet. Ausgenommen sind LDAP-Server, die keinen anonymen Zugriff unterstützen.
10. Geben Sie das **Kennwort** des Benutzers ein, der im Feld **DN-Bind** angegeben wurde. Dies ist nicht erforderlich, wenn ein anonymer Zugriff zulässig ist.
11. Geben Sie die Stamm-**Basis-DN** für LDAP-Anfragen ein. Zum Beispiel `DC=IhreFirma,DC=com`.
12. *Optional:* Geben Sie den **Benutzer Filter** ein, der für LDAP-Abfragen verwendet werden soll.
Beispiel: `(memberOf=CN=Development,CN=Users,DC=yourcompany,DC=com)`
In diesem Beispiel wird der eingeloggte Silk Central-Benutzer vom LDAP-Server abgefragt, jedoch nur wenn dieser Benutzer zum `Development`-Team gehört. Dies ist zum Beispiel dann hilfreich, wenn Sie die automatische Benutzerkonten-Erstellung aktivieren, aber sicherstellen möchten, dass Silk Central nur Konten für Mitglieder einer bestimmten LDAP-Gruppe anlegt.
13. *Optional:* Um Ihre LDAP-Abfrage nach bestimmten Gruppen zu filtern, geben Sie einen **Gruppen-Filter** ein. Die Syntax ist gleich wie beim **Benutzer Filter**-Feld.
14. Klicken Sie auf **LDAP-Einstellungen konfigurieren**, um Ihre LDAP-Attribute mit den Benutzer- und Gruppen-Einstellungen von Silk Central abzugleichen. Dies ist erforderlich, wenn Sie vor haben, Ihre Benutzer von einem LDAP-Server in Silk Central zu importieren.
15. *Optional:* Sie können einstellen, dass Silk Central automatisch ein Silk Central-Benutzerkonto erstellt, wenn sich ein Benutzer zum ersten mal bei Silk Central anmeldet. Wenn in Silk Central für den eingegebenen Benutzernamen noch kein Benutzerkonto vorhanden ist, werden die eingegebenen Benutzerdaten vom LDAP-Server authentifiziert. Ist die Authentifizierung erfolgreich, wird ein neues Konto mit dem eingegebenen Benutzernamen und dem Kennwort angelegt. Beim Anlegen eines neuen Kontos werden zunächst die allgemeinen Einstellungen, inklusive Dashboard-Einstellungen, vom ausgewählten Silk Central-Benutzerkonto kopiert, welches als Vorlage dient. Vorname, Nachname und E-Mail-Adresse werden von den entsprechenden LDAP-Werten übernommen. Klicken hierzu neben **Erstellen von Benutzerkonten** auf **Konfigurieren**. Wählen Sie im Dialog **Erstellen von Benutzerkonten** einen **Silk Central-Benutzer** aus der Liste aus. Abhängig davon, wie Ihr LDAP-Server konfiguriert ist, kann es notwendig sein, die LDAP-Werte von Vorname, Nachname und E-Mail-Adresse anzupassen.
16. Klicken Sie auf **Testen**, um die Verbindung zum LDAP-Server zu testen.
Weitere Informationen finden Sie unter *Testen von LDAP-Servern*.
17. Klicken Sie auf **OK**, um die Einstellungen zu speichern.
18. Wenn Sie mehrere LDAP-Server verwenden: Geben Sie bei **Reihenfolge** eine Nummer an, um die Reihenfolge festzulegen, in der die LDAP-Server für die Authentifizierung abgefragt werden.

Bearbeiten von LDAP-Servern

So bearbeiten Sie ein LDAP-Serverprofil:

1. Klicken Sie im Menü auf **Verwaltung > Systemeinstellungen**.

2. Klicken Sie auf die Registerkarte **LDAP-Server**.
3. Klicken Sie auf den Namen des LDAP-Servers, den Sie bearbeiten möchten. Das Dialogfeld **LDAP-Server bearbeiten** wird angezeigt.
4. Geben Sie einen **Namen** und optional eine **Beschreibung** für den Server ein. Sie können für den LDAP-Server jeden beliebigen Namen festlegen; dieses Feld hat keinen Einfluss auf die tatsächlichen LDAP-Einstellungen.
5. Markieren Sie das Kontrollkästchen **Aktiv**, um den Server für die Verwendung mit Silk Central zu aktivieren. Ist dieses Kontrollkästchen deaktiviert, stehen die Dienste des LDAP-Servers Silk Central nicht zur Verfügung.
6. Geben Sie den **Hostnamen** oder die IP-Adresse des LDAP-Servers und den für den LDAP-Dienst zu verwendenden **Port** an. Der Standardport ist 389. Bei Verwendung von SSL lautet der LDAP-Standardport 636.
7. Aktivieren Sie das Kontrollkästchen **SSL verwenden**, um eine Serververbindung über SSL herzustellen. Dieses Kontrollkästchen steht in engem Zusammenhang mit den im Feld **Port** definierten Einstellungen. Weitere Informationen über das Aufsetzen der Kommunikation über SSL finden Sie unter [Kommunikation mit einem externen System über SSL](#).
8. *Optional:* Geben Sie eine **Domäne** ein, wenn sich Ihre Benutzer mit dem Muster <Domäne> \<Benutzername> auf Silk Central anmelden sollen. Lassen Sie das Feld leer, wenn sich Ihre Benutzer ohne Domännennamen auf Silk Central anmelden sollen. Falls Ihre Silk Central-Installation aus mehreren Mandanten besteht, stellen Sie sicher, dass die angegebene LDAP-Domäne nicht gleich ist wie der Name irgendeines Mandanten, da das Anmeldemuster <Domäne> \<Benutzername> auch zum Anmelden auf die Mandanten verwendet wird.
9. *Optional:* Geben Sie im Feld **DN-Bind** den Domännennamen des Benutzers ein, der zum Binden an den LDAP-Dienst verwendet werden soll. Dieser Benutzer muss über Leseberechtigungen für das Verzeichnis im angegebenen **Basis-DN**-Stamm verfügen. Enthält dieses Textfeld keine Angabe, wird der anonyme Zugriff verwendet. Ausgenommen sind LDAP-Server, die keinen anonymen Zugriff unterstützen.
10. Geben Sie das **Kennwort** des Benutzers ein, der im Feld **DN-Bind** angegeben wurde. Dies ist nicht erforderlich, wenn ein anonymen Zugriff zulässig ist.
11. Geben Sie die Stamm-**Basis-DN** für LDAP-Anfragen ein. Zum Beispiel `DC=IhreFirma,DC=com`.
12. *Optional:* Geben Sie den **Benutzer Filter** ein, der für LDAP-Abfragen verwendet werden soll.
 Beispiel: `(memberOf=CN=Development,CN=Users,DC=yourcompany,DC=com)`
 In diesem Beispiel wird der eingeloggte Silk Central-Benutzer vom LDAP-Server abgefragt, jedoch nur wenn dieser Benutzer zum `Development`-Team gehört. Dies ist zum Beispiel dann hilfreich, wenn Sie die automatische Benutzerkonten-Erstellung aktivieren, aber sicherstellen möchten, dass Silk Central nur Konten für Mitglieder einer bestimmten LDAP-Gruppe anlegt.
13. *Optional:* Um Ihre LDAP-Abfrage nach bestimmten Gruppen zu filtern, geben Sie einen **Gruppen-Filter** ein. Die Syntax ist gleich wie beim **Benutzer Filter**-Feld.
14. Klicken Sie auf **LDAP-Einstellungen konfigurieren**, um Ihre LDAP-Attribute mit den Benutzer- und Gruppen-Einstellungen von Silk Central abzugleichen. Dies ist erforderlich, wenn Sie vor haben, Ihre Benutzer von einem LDAP-Server in Silk Central zu importieren.
15. *Optional:* Sie können einstellen, dass Silk Central automatisch ein Silk Central-Benutzerkonto erstellt, wenn sich ein Benutzer zum ersten mal bei Silk Central anmeldet. Wenn in Silk Central für den eingegebenen Benutzernamen noch kein Benutzerkonto vorhanden ist, werden die eingegebenen Benutzerdaten vom LDAP-Server authentifiziert. Ist die Authentifizierung erfolgreich, wird in ein neues Konto mit dem eingegebenen Benutzernamen und dem Kennwort angelegt. Beim Anlegen eines neuen Kontos werden zunächst die allgemeinen Einstellungen, inklusive Dashboard-Einstellungen, vom ausgewählten Silk Central-Benutzerkonto kopiert, welches als Vorlage dient. Vorname, Nachname und E-Mail-Adresse werden von den entsprechenden LDAP-Werten übernommen. Klicken hierzu neben **Erstellen von Benutzerkonten** auf **Konfigurieren**. Wählen Sie im Dialog **Erstellen von Benutzerkonten** einen **Silk Central-Benutzer** aus der Liste aus. Abhängig davon, wie Ihr LDAP-Server

konfiguriert ist, kann es notwendig sein, die LDAP-Werte von Vorname, Nachname und E-Mail-Adresse anzupassen.

16. Klicken Sie auf **Testen**, um die Verbindung zum LDAP-Server zu testen.

Weitere Informationen finden Sie unter *Testen von LDAP-Servern*.

17. Klicken Sie auf **OK**, um die Einstellungen zu speichern.

Testen von LDAP-Servern

So testen Sie die Verbindung zu einem LDAP-Server:

1. Wenn Sie in Silk Central ein LDAP-Serverprofil hinzufügen oder bearbeiten, wird im Dialog **LDAP-Server hinzufügen** bzw. **LDAP-Server bearbeiten** die Schaltfläche **Testen** angezeigt.
2. Klicken Sie auf **Testen**, um den Dialog **LDAP-Konfiguration testen** zu öffnen.
3. Geben Sie im Feld **Benutzername** einen Benutzernamen ein, der für den Test der LDAP-Authentifizierung verwendet werden soll.
4. Geben Sie im Feld **Kennwort** das Kennwort des Benutzers ein, der für den Test der LDAP-Authentifizierung verwendet werden soll.
5. Klicken Sie auf **Testen**, um den Authentifizierungstest durchzuführen.



Hinweis: Wenn Tests fehlschlagen, werden auch LDAP-Fehlercodes angegeben.

Ein Dialog zeigt an, ob der Test erfolgreich war.

6. Klicken Sie auf **Schließen**, um wieder zum Dialog **LDAP-Server hinzufügen** bzw. **LDAP-Server bearbeiten** zurückzukehren. Wenn die Testverbindung nicht erfolgreich war, bearbeiten Sie Ihre Einstellungen und wenden Sie sich an den Systemadministrator. Beginnen Sie anschließend wieder mit Schritt 2.

Löschen von LDAP-Servern

So löschen Sie ein LDAP-Serverprofil:

1. Klicken Sie im Menü auf **Verwaltung > Systemeinstellungen**.
2. Klicken Sie auf die Registerkarte **LDAP-Server**.
3. Wenn der LDAP-Server aktiv ist, müssen Sie ihn zuerst deaktivieren, bevor Sie ihn löschen können. Klicken Sie auf den Namen des LDAP-Servers, den Sie löschen möchten. Das Dialogfeld **LDAP-Server bearbeiten** wird angezeigt.
4. Deaktivieren Sie das Kontrollkästchen **Aktiv**, um den Server zu deaktivieren, und klicken Sie auf **OK**.
5. Klicken Sie in der Spalte **Aktionen** des LDAP-Servers, den Sie löschen möchten, auf **X (Löschen)**.
6. Klicken Sie auf **Ja**, um das Löschen zu bestätigen.

LDAP-Server (Seite)

Verwaltung > System > LDAP-Server

Auf der Seite **LDAP-Server** werden alle konfigurierten LDAP-Server aufgeführt. Mithilfe dieser Seite können Sie LDAP-Server verwalten.

Sie können auf dieser Seite die folgenden Aktionen ausführen:

- Klicken Sie auf **Neuer LDAP-Server**, um einen neuen LDAP-Server zu konfigurieren.
- Geben Sie bei **Reihenfolge** eine Nummer an, um die Reihenfolge festzulegen, in der die LDAP-Server für die Authentifizierung abgefragt werden.
- Wählen Sie einen vorhandenen LDAP-Server in der Liste aus, um die Einstellungen zu bearbeiten.
- Klicken Sie in der Spalte **Aktionen** auf **X (Löschen)**, um den LDAP-Server zu löschen (zuvor müssen Sie den LDAP-Server deaktivieren).

Agenten-Cluster für Silk Performer-Lasttests

Neben der Zuweisung von Lasttest-Szenarien an einzelne Agenten kann in Silk Performer das Lasttest-Szenario auch Agenten-Clustern zugewiesen werden, die über definierte Fähigkeiten verfügen. Die dynamische Zuweisung von Lasttest-Szenarien durch Silk Performer entspricht zur Ausführungszeit bestimmten Lasttestanforderungen an die Wiedergabefähigkeiten der verfügbaren Agentencomputer. Diese in Silk Performer für Testagenten definierten Fähigkeiten werden verwendet, um die Zuweisungen der Lasttest-Szenarien pro Agenten zu optimieren. Wenn beispielsweise ein Test ein Lasttest-Szenario voraussetzt, das nur ein Agentencomputer erfüllen kann, auf dem ein SAPGUI-Mandanten installiert ist, dann kann die dynamische Zuweisung sicherstellen, dass das Lasttest-Szenario nur solchen verfügbaren Agenten zugewiesen wird, auf denen SAPGUI-Mandanten installiert sind. Darüber hinaus kann auch der Prozentsatz der erforderlichen Lasttest-Szenarien oder der virtuellen Benutzer, der jedem Agenten zugewiesen werden soll, konfiguriert werden. Dies stellt sicher, dass Agenten nicht über ihre Kapazitäten hinaus belastet werden.

Infolge der Ausführung eines Silk Performer-Tests wird aus dem entsprechenden Ausführungsserver eine Silk Central-XML-Datei für Agenten-Cluster für Lasttests ausgecheckt. Diese Datei wird während der Ausführung für die dynamische Zuweisung des Lasttest-Szenarios verwendet. Sie müssen in den Einstellungen unter **Verwaltung > System** den Speicherort der einem Agenten-Cluster für Lasttests zugehörigen XML-Datei angeben.

Ein Vorteil der dynamischen Zuweisung von Lasttest-Szenarien an Agenten-Cluster besteht darin, dass die erfolgreiche Ausführung von Tests nicht davon abhängt, dass eine statische Ausführungsumgebung für die Tests aufrechterhalten wird. Silk Performer kann die Last eines nicht verfügbaren Agenten dynamisch einem verfügbaren Agenten im gleichen Cluster zuordnen, der über dieselben Fähigkeiten verfügt. Dies ist besonders dann nützlich, wenn Silk Performer-Lasttests anhand von vordefinierten Ausführungsterminen in Silk Central verwaltet und ausgeführt werden. Silk Central ist nicht für die Verteilung der Lasttest-Szenarien auf die Agenten sowie die Verwaltung des Zustands einzelner Agenten zuständig.

Umfassende Informationen zur dynamischen Zuweisung von Lasttest-Szenarien finden Sie in der *Silk Performer-Hilfe*.

Hochladen von Dateien für Agenten-Cluster für Lasttests

Hier wird beschrieben, wie Agenten-Cluster-Dateien für Lasttests in Ihrem Projekt zur Unterstützung der dynamischen Zuweisungen von Lasttest-Szenarien in Silk Performer hinzugefügt oder geändert werden.

So ändern Sie die Dateidefinition der Agenten-Cluster Ihres Projekts:

1. Klicken Sie im Menü auf **Verwaltung > Systemeinstellungen**.
2. Klicken Sie auf die Registerkarte **Agenten-Cluster für Lasttests**.
3. Klicken Sie auf **Hochladen**.
4. Navigieren Sie im Dialogfeld **Agenten-Cluster-Datei hochladen** zu dem Speicherort auf der lokalen Festplatte, in dem sich die Agenten-Cluster-Datei befindet.
Wenn Sie die Datei hochladen, wird sie auf der Seite **Agenten-Cluster für Lasttests** angezeigt.
5. Klicken Sie auf **OK**, um die Auswahl zu bestätigen.

Löschen von Dateien für Agenten-Cluster für Lasttests

Löschen Sie eine Datei für Agenten-Cluster für Lasttests, um sie vom Anwendungsserver zu entfernen.

So löschen Sie eine Datei für Agenten-Cluster für Lasttests:

1. Klicken Sie im Menü auf **Verwaltung > Systemeinstellungen**.
2. Klicken Sie auf die Registerkarte **Agenten-Cluster für Lasttests**.
3. Klicken Sie auf **Löschen**.
4. Klicken Sie zum Bestätigen auf **Ja**.

Bearbeiten von Dateien für Agenten-Cluster für Lasttests

So bearbeiten Sie die Dateidefinition der Agenten-Cluster Ihres Projekts:

1. Klicken Sie im Menü auf **Verwaltung > Systemeinstellungen**.
2. Klicken Sie auf die Registerkarte **Agenten-Cluster für Lasttests**.
3. Klicken Sie auf den Namen der Agenten-Cluster-Datei für Lasttests, die Sie ändern möchten.
4. Laden Sie die Datei herunter.
5. Bearbeiten Sie die Datei in einem Editor.
6. Laden Sie die Datei hoch.

Weitere Informationen finden Sie unter *Hochladen von Dateien für Agenten-Cluster für Lasttests*.

Agenten-Cluster für Lasttests (Seite)

Verwaltung > Systemeinstellungen > Agenten-Cluster für Lasttests

Auf der Seite **Agenten-Cluster für Lasttests** wird die aktuell konfigurierte XML-Datei für Agenten-Cluster für Lasttests angezeigt. Mithilfe dieser Seite können Sie Silk Performer-Agenten-Cluster für Lasttests zur Unterstützung von dynamischen Lasttest-Szenarienzuweisungen verwalten.

Sie können auf dieser Seite die folgenden Aktionen ausführen:

- Klicken Sie auf die Schaltfläche **Hochladen**, um eine vorhandene XML-Datei für Agenten-Cluster für Lasttests hochzuladen.
- Klicken Sie auf die Schaltfläche **Löschen**, um eine vorhandene XML-Datei für Agenten-Cluster für Lasttests zu entfernen.
- Klicken Sie auf den Namen der Agenten-Cluster-Datei für Lasttests, um die Datei herunterzuladen und zu bearbeiten.

Systemdiagnose

Über die Registerkarte **Systemdiagnose** können Sie Diagnosedaten und Systemlogdateien abrufen.

Systemdiagnose

Über die Seite **Systemdiagnose** können Sie die folgenden Systeminformationen abrufen:

- Produktversion.
- Version und Typ der Datenbank.
- Verwendete Integrationen.
- Informationen zu Systemumgebung und Systemeigenschaften.
- JDBC-Informationen.
- Datenbankstatistiken: Anzahl der Projekte, Testtypen, Indizes, Trigger, Constraints.
- Logdateien für Anwendungsserver und Front-End-Server.

Die Seite kann gezippt und in das lokale Dateisystem heruntergeladen werden. Klicken Sie dazu auf die Schaltfläche **Download**. Über die entsprechenden Kontrollkästchen können Sie die Server-Logdateien auswählen, die heruntergeladen werden sollen.

1. Sie können extern auf die **Systemdiagnose**-Seite zugreifen oder, wenn Sie sich nicht mehr beim System anmelden können, lokal auf dem Computer auf dem der Front-End-Server läuft.
 - Für externen Zugriff:
 1. Melden Sie sich als Systemadministrator an.
 2. Klicken Sie auf **Systemdiagnose > Systemdiagnose**.
 3. Klicken Sie auf **Systemdiagnose öffnen**.

- Wenn externer Zugriff nicht mehr geht:
 1. Navigieren Sie zu `http://localhost:19120/systemdiagnostics` oder `http://127.0.0.1:19120/systemdiagnostics` auf dem Computer, auf dem der Front-End-Server läuft (verwenden Sie nicht den Hostnamen oder die externe IP-Adresse des Servers).
 2. Über die entsprechenden Kontrollkästchen können Sie die Silk Central-Server-Logdateien auswählen, die heruntergeladen werden sollen.
 3. Klicken Sie auf **Download**, um die Daten zu zippen und in das lokale Dateisystem herunterzuladen.

Front-End-Server-Logdateien

Melden Sie sich zum Öffnen dieser Seite als Systemadministrator an, und klicken Sie auf **Systemdiagnose > Front-End-Server-Logdateien**. Weitere Informationen finden Sie unter "Systemadministrator".

Mithilfe dieser Seite können Sie Protokolldaten des Silk Central-Front-End-Serverdienstes anzeigen.

Zu jeder Log-Datei werden folgende Spalten angezeigt:

Spalte	Beschreibung
Aktionen	Klicken Sie auf die Schaltflächen  oder  , um Logdateien zu löschen oder herunterzuladen .
Name	Der Name der Logdatei.
Größe	Die physische Größe der Logdatei.
Datum	Datum, an dem die Logdatei zuletzt gespeichert wurde.

Anwendungsserver-Logs

Melden Sie sich zum Öffnen der Seite als Systemadministrator an, und klicken Sie auf **Systemdiagnose > Anwendungsserver-Logdateien**. Weitere Informationen finden Sie unter "Systemadministrator".

Mithilfe dieser Seite können Sie Protokolldaten des Silk Central-Anwendungsserverdienstes anzeigen.

Zu jeder Log-Datei werden folgende Spalten angezeigt:

Spalte	Beschreibung
Aktionen	Klicken Sie auf die Schaltflächen  oder  , um Logdateien zu löschen oder herunterzuladen .
Name	Der Name der Logdatei.
Größe	Die physische Größe der Logdatei.
Datum	Datum, an dem die Logdatei zuletzt gespeichert wurde.

Konfigurieren erweiterter Einstellungen

In diesem Abschnitt wird beschrieben, wie erweiterte Einstellungen zur Anpassung Ihres Silk Central-Systems konfiguriert werden.

Anmeldeoptionen

Die folgenden beiden erweiterten Anmeldekonfigurationen sind verfügbar:

Benutzerdaten merken

Ändert die Standardeinstellung für die Option **Benutzerdaten merken** auf der Silk Central-Anmeldeseite.

Wenn Benutzer mit mehreren Browserfenster arbeiten, wird normalerweise für jede Browsersitzung eine eigene Lizenz ausgecheckt. Wenn die Option **Benutzerdaten merken** aktiviert ist, können einzelne Benutzer auf einem Computer mit mehreren Browsersitzungen arbeiten, ohne mehrere Lizenzen auszuchecken.

Jeder Benutzer kann bei Bedarf die Option **Benutzerdaten merken** aktivieren oder deaktivieren, nur der Administrator kann jedoch die Standardeinstellung festlegen.

Cookie-Dauer

Jedes Mal, wenn ein Benutzer auf Silk Central zugreift, wird ein Cookie mit kodierten Anmeldeinformationen erstellt. Diese Cookies werden gelöscht, wenn sich der Benutzer abmeldet oder wenn die Sitzung wegen einer Wartezeitüberschreitung beendet wird. Wenn die Option **Benutzerdaten merken** aktiviert ist, werden Cookies bei Wartezeitüberschreitungen von Sitzungen nicht gelöscht. Stattdessen bleiben sie über die angegebene Zeitdauer aktiv. Die Benutzer können dann weiter mit Silk Central arbeiten, statt nach jeder Wartezeitüberschreitung in einer Sitzung die Anmeldeinformationen erneut eingeben zu müssen. Standardmäßig bleiben Cookies 30 Tage lang aktiv. Die Einstellung dieser Gültigkeitsdauer kann vom Administrator angepasst werden.

Konfigurieren der Option "Benutzerdaten merken"

So aktivieren oder deaktivieren Sie die Option "Benutzerdaten merken":

1. Stoppen Sie den Front-End-Server der zu bearbeitenden Instanz auf der Seite **Instanzen-Verwaltung**.
2. Öffnen Sie die Datei `SccFrontendBootConf.xml` in einem Texteditor.
Diese Datei befindet sich standardmäßig in `C:\Program Files (x86)\Silk\Silk Central 18.5\instance_<Instanznummer>_<Instanzname>\Conf\FontendServer` auf dem Front-End-Server.
3. Suchen Sie das XML-Tag `BootConf\Options\Login\RememberLogin`.
Die Standardeinstellung dieses Tags lautet `<RememberLogin>true</RememberLogin>`.
4. Legen Sie den Wert `false` fest, wenn das Kontrollkästchen **Benutzerdaten merken** auf der Anmeldeseite standardmäßig deaktiviert sein soll. Legen Sie den Wert `true` fest, wenn das Kontrollkästchen **Benutzerdaten merken** auf der Anmeldeseite standardmäßig aktiviert sein soll.
5. Speichern und schließen Sie die XML-Datei.
6. Starten Sie den Front-End-Server neu.

Anpassen der Cookie-Dauer

So legen Sie die Gültigkeitsdauer von Anmelde-Cookies fest:

1. Stoppen Sie den Front-End-Server der zu bearbeitenden Instanz auf der Seite **Instanzen-Verwaltung**.
2. Öffnen Sie die Datei `SccFrontendBootConf.xml` in einem Texteditor.
Diese Datei befindet sich standardmäßig in `C:\Program Files (x86)\Silk\Silk Central 18.5\instance_<Instanznummer>_<Instanzname>\Conf\FontendServer` auf dem Front-End-Server.
3. Suchen Sie das XML-Tag `BootConf\Options\Login\MaxCookieAge`.
Die Standardeinstellung dieses Tags lautet `<MaxCookieAge>30</MaxCookieAge>`.
4. Legen Sie als Wert die Anzahl von Tagen fest, die Anmelde-Cookies auf den Computern der Benutzer aktiv bleiben sollen.
5. Speichern und schließen Sie die XML-Datei.

6. Starten Sie den Front-End-Server neu.

Verdächtige Ausführungsdauer

Die Dauer der Test-Ausführung ist unterschiedlich. Wenn eine Ausführung jedoch zu lange dauert, kann der Benutzer, der die letzte Änderung an der Testsuite vorgenommen hat, per E-Mail benachrichtigt werden.

Silk Central sendet eine Benachrichtigung, wenn die Ausführung eines Tests einen längeren Zeitraum als definiert in Anspruch nimmt. Der Benutzer kann festlegen, wie lange die Ausführung eines Tests dauern darf, bevor eine E-Mail-Nachricht gesendet wird.



Hinweis: Sie können auch einen Timeout für die einzelnen Tests einrichten. Geben Sie dazu die Eigenschaft **Testausführungs-Timeout [s]** im Abschnitt **Erfolgsbedingungen** des Bereichs **Tests** an.

Festlegen der verdächtigen Ausführungsdauer

So legen Sie die verdächtige Ausführungsdauer fest:

1. Stoppen Sie den Anwendungsserver der zu bearbeitenden Instanz auf der Seite **Instanzen-Verwaltung**.
2. Öffnen Sie die Datei `TmAppServerHomeConf.xml` mit einem Texteditor.
Diese Datei befindet sich standardmäßig in `C:\Program Files (x86)\Silk\Silk Central 18.5\instance_<Instanznummer>_<Instanzname>\Conf\AppServer auf dem Anwendungsserver`.
3. Suchen Sie den XML-Tag `Config\ExecutionTracking\SuspiciousDuration`.
Die Standardeinstellung für dieses Tag ist `<SuspiciousDuration>360</SuspiciousDuration>`.
4. Legen Sie als Wert die Anzahl von Minuten fest, nach deren Ablauf Silk Central den Administrator über die Tests, die zu lange dauern, benachrichtigen soll.
5. Speichern und schließen Sie die XML-Datei.
6. Starten Sie den Anwendungsserver neu.

Deaktivieren der Aktualisierung externer Fehlerstatistiken

Die Aktualisierung der Fehlerstatistiken externer Fehlerverfolgungsprofile kann sehr speicherintensiv sein. Dadurch kann die Systemleistung beeinträchtigt werden. So deaktivieren Sie die Aktualisierung:

1. Stoppen Sie den Anwendungsserver der zu bearbeitenden Instanz auf der Seite **Instanzen-Verwaltung**.
2. Öffnen Sie die Datei `TmAppServerHomeConf.xml` mit einem Texteditor.
Diese Datei befindet sich standardmäßig in `C:\Program Files (x86)\Silk\Silk Central 18.5\instance_<Instanznummer>_<Instanzname>\Conf\AppServer auf dem Anwendungsserver`.
3. Suchen Sie den XML-Tag `Config/IssueStateUpdate/UpdateIssueUnitStatistics`.
Die Standardeinstellung dieses Tags lautet `true`.
4. Setzen Sie den Wert auf `false`, um die Aktualisierung zu deaktivieren.
5. Speichern und schließen Sie die XML-Datei.
6. Starten Sie den Anwendungsserver neu.

Datums- und Zeitformate

Silk Central ermöglicht benutzerdefinierte Einstellungen für Datums- und Zeitformate. Jeder Silk Central-Benutzer kann seine Benutzereinstellungen ändern. Hierzu zählen auch Optionen für die Anzeige von Datumsformaten in Lang- und Kurzformen. Weitere Informationen finden Sie unter *Bearbeiten von Benutzerkonten*.

Silk Central zeigt Listen mit vordefinierten Datums- und Zeitformaten an, die Benutzer auswählen können. Silk Central-Administratoren können diese Listen mit benutzerdefinierten Formaten füllen.

Formatdefinition

Datums- und Zeitformate werden durch Datums- und Zeitformatstrings festgelegt. In Datums- und Zeitformatstrings werden nicht in Anführungszeichen gesetzte Buchstaben von "A" bis "Z" und von "a" bis "z" als Formatzeichen interpretiert, die die Komponenten einer Datums- oder Zeitangabe darstellen. Textzeichen können in einfache Anführungszeichen (') gesetzt werden, wenn sie nicht interpretiert werden sollen. "" steht für ein einfaches Anführungszeichen. Alle anderen Zeichen werden nicht interpretiert; sie werden beim Formatieren einfach in den Ausgabestring kopiert oder beim Parsen mit dem Eingabestring abgeglichen.

Die folgenden Formatmusterbuchstaben sind definiert. Alle Zeichen von "A" bis "Z" und von "a" bis "z" sind reserviert:

Buchstabe	Datums- oder Zeitkomponente	Darstellung	Beispiele
G	Bezeichner des Zeitalters	Text	AD (Anno Domini, n. Chr.)
y	Jahr	Jahr	1996; 96
M	Monat im Jahr	Monat	Jul; Jul; 07
w	Kalenderwoche	Zahl	27
W	Woche im Monat	Zahl	2
D	Tag im Jahr	Zahl	189
t	Tag im Monat	Zahl	10
F	Wochentag im Monat	Zahl	2
E	Wochentag	Text	Dienstag; Di
ein	AM/PM-Markierung	Text	PM
H	Stunde (0-23)	Zahl	0
k	Stunde (1-24)	Zahl	24
K	Stunde mit AM/PM-Angabe (0-11)	Zahl	0
h	Stunde mit AM/PM-Angabe (1-12)	Zahl	12
m	Minute	Zahl	30
s	Sekunde	Zahl	55
S	Millisekunde	Zahl	978
z	Zeitzone	Allgemeine Zeitzone	Pacific Standard Time; PST; GMT-08:00
Z	Zeitzone	RFC 822-Zeitzone	-0800

Die Buchstaben werden im Formatmuster für gewöhnlich wiederholt, da die genaue Darstellung durch ihre Anzahl festgelegt wird.

Nachfolgend werden die Einträge in der Spalte **Darstellung** der obigen Tabelle erläutert:

Element	Beschreibung
Text	Für das Formatieren gilt: Wenn mehr als 4 Buchstaben angegeben werden, wird das lange Datumsformat verwendet, andernfalls wird das kurze Datumsformat verwendet, sofern verfügbar. Für das Parsen gilt: Beide Formen werden unabhängig von der Anzahl der Buchstaben im Formatmuster akzeptiert.
Zahl	Für das Formatieren gilt: Die Anzahl der Buchstaben im Formatmuster entspricht der kleinsten Anzahl von Stellen, und kürzere Zahlen werden mit Nullen auf diese Anzahl von Stellen aufgefüllt. Für das Parsen gilt: Die Anzahl der Buchstaben im Formatmuster wird ignoriert, sofern sie nicht zum Trennen benachbarter Felder benötigt wird.
Jahr	Für das Formatieren gilt: Wenn 2 Buchstaben angegeben werden, wird die Jahresangabe auf 2 Stellen gekürzt; andernfalls wird sie als <i>Zahl</i> interpretiert.
Monat	Wenn 3 oder mehr Buchstaben angegeben werden, wird die Monatsangabe als <i>Text</i> interpretiert. Andernfalls wird sie als <i>Zahl</i> interpretiert.
Allgemeine Zeitzone	Zeitzone werden als <i>Text</i> interpretiert, wenn sie einen Namen haben. Wenn weniger als 4 Buchstaben im Formatmuster angegeben werden, wird die für die Zeitzone gebräuchliche Abkürzung angezeigt, z. B. PST. Wenn das Formatmuster 4 oder mehr Buchstaben umfasst, wird der volle Name angezeigt, z. B. Pacific Standard Time.
RFC 822-Zeitzone	Das in RFC 822 beschriebene vierstellige Zeitzoneformat wird verwendet, z. B. -0800.

Beispiele	
Die folgenden Beispiele zeigen, wie Datums- und Uhrzeitformatmuster in den USA interpretiert werden. Gegeben sind folgendes Datum und folgende Uhrzeit: 04.07.2001 12:08:56 Ortszeit, Zeitzone Pacific Standard Time.	
Datums- und Zeitformate	Ergebnis
"dd.MM.yyyy. G 'um' HH:mm:ss z"	04.07.2001. AD um 12:08:56 PDT
"EEE, MMM d, 'yy"	Wed, Jul 4, '01
"h:mm a"	12:08 PM
"hh 'Uhr' a, zzzz"	12 Uhr 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

Anpassen von Datums- und Zeitformaten

So passen Sie Datums- und Zeitformate an:

1. Stoppen Sie den Front-End-Server der zu bearbeitenden Instanz auf der Seite **Instanzen-Verwaltung**.
2. Öffnen Sie die Datei `ScFrontendBootConf.xml` in einem Texteditor.

Diese Datei befindet sich standardmäßig in C:\Program Files (x86)\Silk\Silk Central 18.5\instance_<Instanznummer>_<Instanzname>\Conf\FontendServer auf dem Front-End-Server.

3. Suchen Sie das XML-Tag `DateFormats`.

Aus den XML-Tags `<LongDateFormats>` und `<ShortDateFormats>` geht hervor, welche Datumsformate standardmäßig verfügbar sind. Sie können beliebige Formate hinzufügen oder löschen, die den Benutzern zur Verfügung bzw. nicht zur Verfügung stehen sollen.

4. Geben Sie Zeitformate wie unter [Datums- und Zeitformate](#) beschrieben ein.
5. Speichern und schließen Sie die XML-Datei.
6. Starten Sie den Front-End-Server neu.

Hostnamensanzeige

Wenn Sie mit Webanwendungen auf mehreren Front-End-Servern arbeiten, kann es nützlich sein, zu wissen, auf welchem Host Sie gerade arbeiten. Silk Central stellt eine Einstellung zur Verfügung, mit der der Hostname des Front-End-Servers in der Titelleiste des Webbrowsers angezeigt werden kann.

Anzeigen und Verbergen des Hostnamen in der Registerkarte des Webbrowsers

So zeigen Sie den Hostnamen in der Registerkarte des Webbrowsers an oder blenden ihn aus:

1. Stoppen Sie den Front-End-Server der zu bearbeitenden Instanz auf der Seite **Instanzen-Verwaltung**.
2. Öffnen Sie die Datei `SccFrontendBootConf.xml` in einem Texteditor.

Diese Datei befindet sich standardmäßig in C:\Program Files (x86)\Silk\Silk Central 18.5\instance_<Instanznummer>_<Instanzname>\Conf\FontendServer auf dem Front-End-Server.

3. Suchen Sie den XML-Tag `DisplayHostNameInTitleBar` im Abschnitt `Options` der Datei.
4. Wenn Sie den Wert `true` festlegen, dann wird der Hostname des Front-End-Servers in der Registerkarte des Webbrowsers angezeigt, wenn Sie Silk Central aufrufen. Wenn Sie den Wert `false` festlegen – das ist der Standardwert –, wird kein Hostname angezeigt, und wenn Sie eine andere Zeichenfolge als Wert angeben, wird diese Zeichenfolge angezeigt. Der aktuell in Silk Central ausgewählte Arbeitsbereich wird immer angezeigt.

Wenn der XML-Tag auf `true` gesetzt ist, zeigt der Browser z.B.: `<Arbeitsbereich> | HOSTNAME`.

Wenn der XML-Tag auf `false` gesetzt ist, zeigt der Browser: `<Arbeitsbereich> | Silk Central`.

Wenn benutzerdefinierter Text eingegeben wird, z.B. `MeinEigenerText`, zeigt der Browser folgendes an: `<Arbeitsbereich> | MeinEigenerText`.

Wenn der XML-Tag leer gelassen wird, zeigt der Browser: `<Arbeitsbereich>`.

5. Speichern und schließen Sie die XML-Datei.
6. Starten Sie den Front-End-Server neu.

Speichern von Anhängen und Ergebnisdateien auf dem Dateisystem

Standardmäßig speichert Silk Central alle Anhänge und Ergebnisdateien in der Datenbank, aber Sie können Silk Central so konfigurieren, dass es diese Dateien auf dem Dateisystem des Anwendungsservers speichert.

Obwohl es nicht empfehlenswert ist, Anhänge und Ergebnisdateien getrennt von den anderen Daten zu speichern, haben Sie evtl. gute Gründe diesen Ansatz zu bevorzugen (z.B. Kosten für Datenbank-

Speicherplatz). Ein Nachteil dieses Ansatzes ist, dass Sie Ihre Daten doppelt warten müssen, d.h. Sie müssen ein Backup Ihrer Datenbank als auch Ihres Dateisystems machen. Wenn ein Datenbank-Backup eingespielt wird, muss auch das Dateisystem wiederhergestellt werden.

 **Vorsicht:** Wenn Sie die Option aktivieren, dass Dateien auf dem Dateisystem gespeichert werden, stellen Sie sicher, dass niemals Änderungen an der Struktur dieses Speicherortes durchgeführt werden, und niemals Dateien verschoben, geändert oder gelöscht werden. Nur die Silk Central-Dienste und das System, das Sie für Backups und Wiederherstellungen verwenden, sollten Schreibrechte auf das angegebene **Dateiablage-Verzeichnis** haben.

1. Aktivieren Sie den Wartungsmodus auf der zu bearbeitenden Instanz auf der Seite **Instanzen-Verwaltung**. Weitere Information finden Sie unter [Wartungs-Modus](#).
2. Melden Sie sich auf Ihrer Instanz als System-Administrator an und trennen Sie die Datenbankverbindung. Weitere Informationen finden Sie unter [Trennen der Verbindung zu einer Datenbank](#).
3. Stoppen Sie die zu bearbeitende Instanz auf der Seite **Instanzen-Verwaltung**.
4. Öffnen Sie die Datei `ScAppServerBootConf.xml` mit einem Texteditor.
Diese Datei befindet sich standardmäßig in `C:\Program Files (x86)\Silk\Silk Central 18.5\instance_<Instanznummer>_<Instanzname>\Conf\AppServer` auf dem Anwendungsserver.
5. Suchen Sie den XML-Tag `<StoreFilesOnFileSystem>` im Abschnitt `<Config>/<RdbmsSpecifics>` der Datei. Setzen Sie den Wert dieses Tags auf `true`.
6. Speichern und schließen Sie die XML-Datei.
7. Starten Sie die Instanz auf der Seite **Instanzen-Verwaltung** wieder.
8. Melden Sie sich auf Ihrer Instanz wieder als System-Administrator an. Auf der **Datenbank**-Seite sehen Sie ein neues Feld namens **Dateiablage-Verzeichnis**, in das Sie einen lokalen Pfad eingeben müssen (z.B. `c:/sc_files/testdb`). Dieser wird zum Speichern von Anhängen und Ergebnisdateien verwendet. Dieser Pfad muss bereits vorhanden sein und die Dienste des Front-End- und des Anwendungsservers müssen vollen Zugriff auf diesen Ordner haben.
9. Klicken Sie auf **Datenbank verbinden**.

Nun werden sämtliche Anhänge und Ergebnisdateien auf dem angegebenen Speicherort gespeichert. Anhänge und Ergebnisdateien die bereits in der verbundenen Datenbank gespeichert sind werden schrittweise auf das Dateisystem verschoben. Sollte das Dateisystem nicht verfügbar sein, speichert Silk Central die Dateien in Datenbank-Blob-Tabellen und verschiebt sie zu einem späteren Zeitpunkt auf das Dateisystem, wenn dieses wieder verfügbar ist.

Achtung: Es gibt zur Zeit keine Möglichkeit, Dateien automatisch zurück in die Datenbank zu verschieben. Aktivieren Sie diese Option somit nur, wenn Sie permanent Dateien auf dem Dateisystem speichern möchten.

Konfigurieren von LQM Reporting Updater

Hier wird beschrieben, wie die Einstellungen (z. B. das Intervall) des Threads zur Aktualisierung der LQM Reporting-Tabellen (LQM Reporting Updater) konfiguriert werden.

So konfigurieren Sie die Einstellungen des LQM Reporting Updaters:

1. Stoppen Sie den Anwendungsserver der zu bearbeitenden Instanz auf der Seite **Instanzen-Verwaltung**.
2. Öffnen Sie die Datei `TmAppServerHomeConf.xml` mit einem Texteditor.
Diese Datei befindet sich standardmäßig in `C:\Program Files (x86)\Silk\Silk Central 18.5\instance_<Instanznummer>_<Instanzname>\Conf\AppServer` auf dem Anwendungsserver.

3. Suchen Sie das XML-Tag `LQMReporting`.

Folgende Einstellungen können geändert werden:

UpdateInterval	Legt das Intervall (in Sekunden) fest, in dem die LQM Reporting-Tabellen mit den neuesten Daten aktualisiert werden.
MSSqlUpdateBatchSize	Die Anzahl der Testtabellen, die gleichzeitig verarbeitet werden können. Die Batchgröße bestimmt, in welchem Umfang Speicher- und Prozessorressourcen auf dem Anwendungsserver für die Aktualisierung verwendet werden. Diese Einstellung gilt nur für MS SQL Server-Datenbanken.
OracleUpdateBatchsize	Diese Einstellung hat die gleiche Wirkung wie <i>MSSqlUpdateBatchSize</i> , sie wird aber für Oracle-Datenbanken verwendet.
QueryTimeout	Legt das Zeitlimit in Sekunden fest, nach dem Abfragen im LQM Reporting-Aktualisierungsprozess abgebrochen werden. 0 oder ein negativer Wert bedeutet, dass für die Abfragen kein Zeitlimit gilt.
OracleCheckForUpdateStrategy	Bestimmt die Art und Weise, wie beim Aktualisierungsprozess aus den Quelltabellen gelesen wird. Sie können zwischen <code>NOWAIT</code> und <code>WAIT</code> wählen. <ul style="list-style-type: none">• <code>NOWAIT</code>: Wenn der Aktualisierungsprozess versucht, aus den Quelltabellen zu lesen, ein anderer Prozess aber gerade in diese Tabellen schreibt, wird der Aktualisierungsprozess beendet und der Vorgang beim nächsten Aufruf wiederholt.• <code>WAIT</code>: Der Aktualisierungsprozess fordert eine Tabellensperre an, wartet, bis andere Prozesse nicht mehr auf die Tabellen zugreifen, und liest dann die Daten aus den Quelldateien. Diese Einstellung hat den Vorteil, dass der Prozess immer ausgeführt wird, da er nicht auf das Entsperren einer Tabelle warten muss. Jedoch müssen alle anderen Prozesse, die nach Abschluss der LQM-Aktualisierung auf die Tabelle zugreifen möchten, auf die Freigabe der Tabellensperre durch den Aktualisierungsprozess warten.

4. Speichern und schließen Sie die XML-Datei.

5. Starten Sie den Anwendungsserver neu.

Ausführungstermine für die automatische LDAP-Synchronisierung planen

Wenn Sie Benutzergruppen aus LDAP-Servern in Ihr Silk Central-System importiert haben, können Sie einen Ausführungstermin festlegen, zu dem Ihre Silk Central-Gruppen automatisch mit den Änderungen auf dem LDAP-Server synchronisiert werden.

So legen Sie einen Ausführungstermin fest, zu dem Ihre Silk Central-Gruppen automatisch mit den Änderungen auf dem LDAP-Server synchronisiert werden:

1. Stoppen Sie den Anwendungsserver der zu bearbeitenden Instanz auf der Seite **Instanzen-Verwaltung**.

2. Öffnen Sie die Datei `TmAppServerHomeConf.xml` mit einem Texteditor.

Diese Datei befindet sich standardmäßig in `C:\Program Files (x86)\Silk\Silk Central 18.5\instance_<Instanznummer>_\<Instanzname>\Conf\AppServer` auf dem Anwendungsserver.

3. Suchen Sie den XML-Tag `LdapUpdate`.

Folgende Einstellungen können geändert werden:

- ScheduledTime** Zeitpunkt (hh:mm, 24h-Uhr) zu dem die Daten von LDAP das erste Mal aktualisiert werden. `ScheduledTime` wird in der Zeitzone des Anwendungsserver-Systems interpretiert. Lassen Sie diese Einstellung leer, um die automatische Synchronisierung zu deaktivieren.
- UpdateIntervallInMinutes** Dieses Intervall (in Minuten) definiert, wie oft die LDAP-Gruppen und Benutzer synchronisiert werden, und startet relativ zur angegebenen `ScheduledTime`. Minimalwert ist 1.

4. Speichern und schließen Sie die XML-Datei.

5. Starten Sie den Anwendungsserver neu.

Zwischenspeicherung von Daten in Tests

In Silk Central werden Daten in **Tests** zwischengespeichert, um die Skalierbarkeit des Front-End-Servers zu verbessern und die Datenbanklast zu verringern, wenn mehrere Benutzer gleichzeitig an einem Projekt arbeiten. Die **Testhierarchie** und Testfilter haben einen wesentlichen Einfluss auf Front-End- und Datenbankserver. Da die **Testhierarchie** und die Filter für bestimmte Projekte von verschiedenen Benutzern gemeinsam genutzt werden können, bietet sich die Zwischenspeicherung in diesen Bereichen an.

Zwischenspeicherung in Testhierarchien

Der **Testhierarchie**-Cache enthält sämtliche Hierarchieinformationen für Projekte, die sich im Arbeitsspeicher befinden, und überprüft die Datenbank in regelmäßigen Abständen auf Änderungen in der Hierarchie. Administratoren können das Verhalten des Caches mithilfe der Einstellung `Cache/TestPlanTree/CheckForChangesInterval` in der Konfigurationsdatei `TMFrontendBootConf.xml` anpassen. Diese Einstellung definiert den Zeitraum (in Sekunden), nach dem Hierarchieinformationen spätestens aktualisiert werden. Unabhängig von dieser Einstellung wird der Cache sofort aktualisiert, wenn ein Test, ein Ordner oder ein Container auf demselben Front-End-Server geändert wird. Die Einstellung `Cache/TestPlanTree/CheckForChangesInterval` wird nur wirksam, wenn Änderungen auf einem anderen Front-End-Server durchgeführt werden. Wenn ein Projekt länger als eine Stunde von keinem Benutzer verwendet wird, wird der gesamte Projekthierarchie-Cache gelöscht. Das Projekt wird dann beim nächsten Zugriff eines Benutzers neu geladen.

Zwischenspeicherung in Testfiltern

Im Filter-Cache werden die IDs von Tests, die die Kriterien bestimmter Filter erfüllen, für einen bestimmten Zeitraum zwischengespeichert, der sich nach der Einstellung für die minimale Cache-Dauer und nach der Ausführungszeit der einzelnen Filter richtet. Administratoren können dieses Verhalten mit zwei Eigenschaften beeinflussen, die sich unter `Cache/FilterCache/` in der Konfigurationsdatei `TMFrontendBootConf.xml` befinden.

Die Eigenschaft `MinimalLifeTime` legt den Zeitraum (in Sekunden) fest, nach dem ein Filterergebnis frühestens aus dem Cache entfernt werden kann. Mit der Eigenschaft `LifeTimeMultiplier` kann diese Mindestspeicherdauer mit der Zeit in Beziehung gesetzt werden, die für die Ausführung der Filterabfrage benötigt wird. Wenn Sie beispielsweise den Multiplikator > 0 festlegen, ergibt sich die maximale Dauer für die Zwischenspeicherung eines Ergebnisses aus der `MinimalLifeTime`, oder der Ausführungsdauer der Abfrage, multipliziert mit `LifeTimeMultiplier`. Wenn Sie für eine Filterabfrage, deren Ausführung 1 Sekunde dauert, den Standardwert 30 für beides, für `MinimalLifeTime` und `LifeTimeMultiplier` übernehmen, bleibt das Filterergebnis 30 Sekunden lang im Cache. Dauert die Ausführung der Filterabfrage ein halbe Sekunde, bleibt das Ergebnis ebenfalls 30 Sekunden im Cache. Bei einer Ausführungsdauer von 2 Sekunden wird es jedoch 60 Sekunden zwischengespeichert.

Cache für Schlüsselwort-Empfehlungen

Wenn Sie im **Keyword-Driven Test Editor** Schlüsselwörter zu einem schlüsselwortgetriebenen Test oder einer Schlüsselwort-Sequenz hinzufügen, empfiehlt Silk Central welches Schlüsselwort Sie evtl. als nächstes verwenden möchten. Empfohlene Schlüsselwörter erscheinen oben in der Schlüsselwort-Liste und zeigen in einem Balkendiagramm an, wie hoch die Empfehlung von Silk Central ist.

Über die Eigenschaft `RecommendationCache/ExpireAfterWrite` in der Konfigurationsdatei `TMFrontendBootConf.xml` können Administratoren das Intervall einstellen, in welchem der Cache für Schlüsselwort-Empfehlungen aktualisiert wird.

JMX-Messdaten für die Zwischenspeicherung

Silk Central enthält JMX-Werte zur Überwachung von zugrunde liegenden Java-Prozessen und anderen prozessspezifischen Messdaten. Die JMX-Daten für den **Testhierarchie**- und Testfilter-Cache befinden sich in der JMX-Messdatenhierarchie unter `borland.com/Frontend/TM`.

 **Hinweis:** Diese und weitere Messdaten können mit Silk Performance Explorer und anderen Tools nachverfolgt werden.

JMX-Messdaten für die Zwischenspeicherung in Tests

Die JMX-Daten für den **Testhierarchie**- und den Filter-Cache befinden sich auf Ihrem Front-End-Server in der JMX-Messdatenhierarchie unter `borland.com/Frontend/TM`.

Messdaten für den Testhierarchie-Cache

Für den **Testhierarchie**-Cache sind zwei grundlegende Messdaten verfügbar. `TestPlanTreeCache` liefert Informationen darüber (*NumberOfCachedProjects*), wie viele Projekte sich gegenwärtig im Cache befinden. Alle Details des Projekt-Caches werden über den zweiten Messwert bereitgestellt: `TestPlanTreeCache_<Nummer>`. Dieser umfasst folgende Messwerte:

Messwert	Beschreibung
Hits	Die Anzahl der Zugriffe auf den Cache ohne implizite Datenbankanforderungen.
LastUpdateCheckDurationInMillis	Die Dauer der letzten Prüfung auf Aktualisierungen in der Datenbank in Millisekunden, siehe <i>LastUpdateCheckTime</i> .
LastUpdateCheckTime	Der Zeitpunkt der letzten Überprüfung auf Aktualisierungen.
LastUpdateDurationInMillis	Die Dauer der letzten Aktualisierung des Caches in Millisekunden, siehe <i>LastUpdateTime</i> , die aufgrund einer Änderung durchgeführt wurde.
LastUpdateTime	Der Zeitpunkt der letzten Cache-Aktualisierung, die aufgrund einer Änderung in der Testhierarchie durchgeführt wurde.
TreeInitializationTimeInMillis	Die Zeit in Millisekunden, die für das Laden der gesamten Projekthierarchie in den Cache erforderlich war. Dieser Wert ändert sich nicht, solange der Projekt-Cache geladen ist.
TreeSize	Die Anzahl der Testknoten im Projekt, d. h. Container, Ordner und Tests.

Messwert	Beschreibung
UpdateChecks	Die Anzahl der Überprüfungen auf Änderungen der Testhierarchie des Projekts, die seit der Initialisierung des Projekthierarchie-Caches durchgeführt wurden.
Updates	Die Anzahl der Aktualisierungen der zwischengespeicherten Hierarchie, die nach Änderungen an der Testhierarchie durchgeführt wurden.

Messdaten für den Filter-Cache

Der Messwert *TestPlanFilterCache* umfasst die folgenden drei Informationen:

Messwert	Beschreibung
Hits	Die Anzahl der Zugriffe auf den Cache, bei denen keine separate Ausführung des Filters für die Datenbank erforderlich war.
Misses	Gibt an, wie oft der Filter ohne Zugriff auf den Filter-Cache für die Datenbank ausgeführt wurde.
Größe	Die aktuelle Anzahl der zwischengespeicherten Filterergebnisse.

Konfigurieren der JMX-Einstellungen

Silk Central bietet eine Reihe von Standardports für die Konfiguration von JMX-Einstellungen.

Verfügbare Servergruppen für die Konfiguration von JMX-Einstellungen

Die Kommunikation über diese Standardports verläuft standardmäßig unverschlüsselt. SSL wird also nicht ausgeführt.



Wichtig: Micro Focus übernimmt keinerlei Verantwortung für Ihre JMX-Sicherheitseinstellungen. Bitte stellen sie sicher, dass Ihre IT-Abteilung die JMX-Sicherheit entsprechend konfiguriert.

festlegen	Beschreibung
com.sun.management.jmxremote.ssl	SSL ist standardmäßig auf <i>false</i> festgelegt.
com.sun.management.jmxremote.authenticate	Authentifizierung ist standardmäßig auf <i>false</i> festgelegt.

Sie können diese Einstellungen in den *processconfig*-Dateien in `C:\Program Files (x86)\Silk\Silk Central 18.5\instance_<Instanznummer>_<Instanzname>\Conf` ändern. Beachten Sie, dass die JMX-Verbindung unsicher ist, solange eine der zwei Einstellungen noch auf *false* festgelegt ist.

Wenn Sie über JMX auf Informationen zugreifen oder Aktionen ausführen möchten, benötigen Sie die JMX-Verbindung. Klicken Sie auf  um den **Einstellungen**-Dialog zu öffnen. Wählen Sie auf der Registerkarte **Server** den gewünschten Server aus und kopieren Sie die **JMX-Verbindung**. Weitere Information finden Sie unter [Verwalten von Instanzen](#).

JMX-Messdaten für die Zwischenspeicherung in Tests

Die JMX-Daten für den **Testhierarchie**- und den Filter-Cache befinden sich auf Ihrem Front-End-Server in der JMX-Messdatenhierarchie unter `borland.com/Frontend/TM`.

Messdaten für den Testhierarchie-Cache

Für den **Testhierarchie**-Cache sind zwei grundlegende Messdaten verfügbar. `TestPlanTreeCache` liefert Informationen darüber (*NumberOfCachedProjects*), wie viele Projekte sich gegenwärtig im Cache befinden. Alle Details des Projekt-Caches werden über den zweiten Messwert bereitgestellt: `TestPlanTreeCache_<Nummer>`. Dieser umfasst folgende Messwerte:

Messwert	Beschreibung
Hits	Die Anzahl der Zugriffe auf den Cache ohne implizite Datenbankanforderungen.
LastUpdateCheckDurationInMillis	Die Dauer der letzten Prüfung auf Aktualisierungen in der Datenbank in Millisekunden, siehe <i>LastUpdateCheckTime</i> .
LastUpdateCheckTime	Der Zeitpunkt der letzten Überprüfung auf Aktualisierungen.
LastUpdateDurationInMillis	Die Dauer der letzten Aktualisierung des Caches in Millisekunden, siehe <i>LastUpdateTime</i> , die aufgrund einer Änderung durchgeführt wurde.
LastUpdateTime	Der Zeitpunkt der letzten Cache-Aktualisierung, die aufgrund einer Änderung in der Testhierarchie durchgeführt wurde.
TreeInitializationTimeInMillis	Die Zeit in Millisekunden, die für das Laden der gesamten Projekthierarchie in den Cache erforderlich war. Dieser Wert ändert sich nicht, solange der Projekt-Cache geladen ist.
TreeSize	Die Anzahl der Testknoten im Projekt, d. h. Container, Ordner und Tests.
UpdateChecks	Die Anzahl der Überprüfungen auf Änderungen der Testhierarchie des Projekts, die seit der Initialisierung des Projekthierarchie-Caches durchgeführt wurden.
Updates	Die Anzahl der Aktualisierungen der zwischengespeicherten Hierarchie, die nach Änderungen an der Testhierarchie durchgeführt wurden.

Messdaten für den Filter-Cache

Der Messwert `TestPlanFilterCache` umfasst die folgenden drei Informationen:

Messwert	Beschreibung
Hits	Die Anzahl der Zugriffe auf den Cache, bei denen keine separate Ausführung des Filters für die Datenbank erforderlich war.
Misses	Gibt an, wie oft der Filter ohne Zugriff auf den Filter-Cache für die Datenbank ausgeführt wurde.
Größe	Die aktuelle Anzahl der zwischengespeicherten Filterergebnisse.

JMX-Messdaten für die Überwachung von LQM Reporting Updater

Messdaten für LQM Reporting Updater

Die folgenden Messdaten sind verfügbar:

Messwert	Beschreibung
LastDataLoadResetTime	Der Zeitpunkt, zu dem die LQM Reporting-Tabellen das letzte Mal zurückgesetzt wurden. Wenn dieses Attribut den Wert Null hat, wurde während der Lebensdauer des Prozesses kein Reset durchgeführt.
LastDeleteDurationInMillis	Die Zeit, die zum Entfernen gelöschter Knoten aus den LQM Reporting-Tabellen benötigt wurde.
LastDeleteTestsCnt	Die Anzahl der Tests, die bei der letzten Ausführung gelöscht wurden.
LastInsertLQMTestsDuration	Die Zeit, die zum Einfügen neuer Tests in die Tabelle <code>LQM_Tests</code> erforderlich war.
LastInsertLQMTestPDAsDuration	Die Zeit, die zum Einfügen neuer Tests in die Tabelle <code>LQM_TestPDAs</code> erforderlich war.
LastInsertLQMTestUDAsDuration	Die Zeit, die zum Einfügen neuer Tests in die Tabelle <code>LQM_TestUDAs</code> erforderlich war.
LastRunFromDate	Der Beginn des Zeitraums, der im aktuellen Aktualisierungszyklus verarbeitet wird.
LastRunToDate	Das Ende des Zeitraums, der im aktuellen Aktualisierungszyklus verarbeitet wird.
LastSelectChangedDataIterateDurationInMillis	Die Zeit, die für das Iterieren geänderter Daten aufgewendet wurde.
LastSelectChangedDataQueryDurationInMillis	Die Zeit, die für das Abfragen geänderter Daten aufgewendet wurde.
LastTotalUpdateDurationInMillis	Die Gesamtdauer der zuletzt durchgeführten Aktualisierung.
LastUpdateFixedAttributesDurationInMillis	Die Dauer der letzten Aktualisierung fester Attribute.
LastUpdatePDAAttributesDurationInMillis	Die Dauer der letzten Aktualisierung der Tabelle <code>LQM_TestPDAs</code> .
LastUpdatesNeededCheckDurationInMillis	Die Dauer (in Millisekunden) der letzten Überprüfung auf neue oder geänderte Daten.
LastUpdatesNeededCheckOracleWaitForTableLocksDuration	Oracle-Datenbanken erfordern bei der Überprüfung auf aktualisierte Tests ein besonderes Vorgehen. In bestimmten Fällen muss gewartet werden, bis Transaktionen, die andere Prozesse mit Testtabellen durchführen, abgeschlossen sind. Diese Wartezeit ist in diesem Attribut angegeben.
LastUpdateTestsDurationInMillis	Die Dauer der letzten Aktualisierung von Eigenschaften in der Tabelle <code>LQM_Tests</code> .
LastUpdateUDAttributesDurationInMillis	Die Dauer der letzten Aktualisierung der Tabelle <code>LQM_TestUDAs</code> .

JMX-Messdaten für DataMart

DataMart Updater Messwerte

Die JMX-Daten für DataMart Updater befinden sich auf dem Anwendungsserver in der JMX-Wertehierarchie unter `borland.com/DataMart/TM`:

Messwert	Beschreibung
AverageCheckDurationInMilliseconds	Durchschnittszeit in Millisekunden für die Überprüfung von aktualisierten Zeilen
AverageUpdateDurationInMilliseconds	Durchschnittszeit in Millisekunden für die Aktualisierung von Zeilen
FailedCheckCount	Anzahl fehlgeschlagener Überprüfungen von Aktualisierungen
FailedUpdateCount	Anzahl fehlgeschlagener Aktualisierungen
FastestCheckInMilliseconds	Kürzeste Zeit in Millisekunden für die Überprüfung von aktualisierten Zeilen
FastestUpdateInMilliseconds	Kürzeste Zeit in Millisekunden für die Aktualisierung von Zeilen
ID	ID des DataMart Updater
IntervallInMilliseconds	Intervall in Millisekunden, in welchem der DataMart Updater ausgeführt wird
LastBlockedRunDate	Die Zeit um welche die Ausführung das letzte Mal blockiert wurde (wait for exclusive access failed)
LastFailedRunDate	Die Zeit um welche die Ausführung das letzte Mal fehlgeschlagen ist
LastSuccessfulRunDate	Die Zeit um welche die Ausführung das letzte Mal erfolgreich durchgelaufen ist
LatestDataLoadInfo	Information über die aktuellste Datenlast
SlowestCheckInMilliseconds	Längste Zeit in Millisekunden für die Überprüfung von aktualisierten Zeilen
SlowestUpdateInMilliseconds	Längste Zeit in Millisekunden für die Aktualisierung von Zeilen
SlowestWaitForExclusiveAccessInMilliseconds	Längste Zeit in Millisekunden für das Warten auf exklusiven Zugriff
StartupDate	Die Zeit um welche der DataMart Updater initialisiert wurde
SuccessfulCheckCount	Anzahl erfolgreicher Überprüfungen von Aktualisierungen
SuccessfulUpdateCount	Anzahl erfolgreicher Aktualisierungen

DataMart-Dienst Messwerte

Die JMX-Daten für den DataMart-Dienst befinden sich auf dem Anwendungsserver in der JMX-Wertehierarchie unter `borland.com/DataMart/Service`:

Messwert/Operation	Beschreibung
Aktiviert	Zeigt an, ob der DataMart-Dienst aktiviert oder deaktiviert ist.
disable()	Deaktiviert den DataMart-Dienst.
enable()	Aktiviert den DataMart-Dienst.

Messwert/Operation	Beschreibung
isEnabled()	Fragt ab, ob der DataMart-Dienst aktiviert oder deaktiviert ist.

JMX-Messdaten für die LDAP-Synchronisierung

Die JMX-Daten für die LDAP-Synchronisierung befinden sich auf dem Anwendungsserver in der JMX-Wertehierarchie unter `borland.com/LdapUpdater`.

Messwert/Operation	Beschreibung
Enabled	Zeigt an, ob die automatische LDAP-Synchronisierung aktiviert oder deaktiviert ist.
LastDurationInMillis	Die Dauer der letzten LDAP-Synchronisierung in Millisekunden.
enable()	Aktiviert die automatische LDAP-Synchronisierung.
disable()	Deaktiviert die automatische LDAP-Synchronisierung.

Hostnamenauflösung des Ausführungsservers

Ein Ausführungsserver wird unter Umständen nicht mehr vom Anwendungsserver erkannt, wenn sich seine IP-Adresse geändert hat. Wenn der Anwendungsserver neu gestartet wird, sollte er vom Ausführungsserver wieder erkannt werden.

Java speichert die Hostnamenauflösung in einem Cache, um sie vor DNS-Spionageangriffen zu schützen. In Silk Central können die Ergebnisse positiver Hostnamenauflösungen unendlich lange im Cache gespeichert werden. Dies lässt sich jedoch ändern, indem die Datei `java.security` auf dem Anwendungsserver bearbeitet wird. Dadurch wird der Anwendungsserver in die Lage versetzt, die Ausführungsserver selbst dann zu erkennen, wenn sich ihre IP-Adresse geändert hat.

Weitere Informationen über diese Java-Einstellung finden Sie auf der Seite [Networking Properties](#).

Deaktivieren der Zwischenspeicherung von Hostnamenauflösungen

So legen Sie fest, dass Hostnamenauflösungen niemals zwischengespeichert werden:

1. Stoppen Sie den Anwendungsserver der zu bearbeitenden Instanz auf der Seite **Instanzen-Verwaltung**.

2. Öffnen Sie die Datei `java.security` in einem Texteditor.

Diese Datei befindet sich standardmäßig in `C:\Program Files (x86)\Silk\Silk Central 18.5\instance_<Instanznummer>_<Instanzname>\lib\jre\lib\security` auf dem Anwendungsserver. Falls Ihr Anwendungsserver im 64-Bit-Modus läuft, verwenden Sie stattdessen den Ordner `jre64\lib\security`.

3. Suchen Sie die Zeile `#networkaddress.cache.ttl=-1` und ändern Sie sie auf `networkaddress.cache.ttl=0`.



Hinweis: Das Kommentarzeichen "#" muss entfernt werden, damit diese Anweisung wirksam wird.



Vorsicht: Diese Änderung sollte mit Ihrem Netzwerkadministrator abgestimmt werden, da dadurch Sicherheitseinstellungen berührt werden.

4. Speichern und schließen Sie die Datei.
5. Starten Sie den Anwendungsserver neu.

Konfigurieren des Silk Central-Standorts in Issue Manager

Hier wird beschrieben, wie der Standort der Silk Central-Installation in Issue Manager konfiguriert wird. Aufgrund dieser Konfiguration ist eine Nachverfolgung von Problemen in Issue Manager zu den entsprechenden Tests in Silk Central möglich. Weitere Informationen zur Verwendung der Nachverfolgungsfunktion finden Sie in der Issue Manager-Dokumentation.

So konfigurieren Sie den Silk Central-Standort in Issue Manager:

1. Stoppen Sie den Front-End-Server der zu bearbeitenden Instanz auf der Seite **Instanzen-Verwaltung**.
2. Öffnen Sie die Datei `SRFrontendBootConf.xml` in einem Texteditor.
Diese Datei befindet sich standardmäßig in `C:\Program Files (x86)\Silk\Silk Central 18.5\instance_<Instanznummer>_<Instanzname>\Conf\FrontendServer` auf dem Front-End-Server.
3. Suchen Sie die XML-Tags `Alm\ElementServiceEndpoint` und `Alm\LinkServiceEndpoint`.
4. Ersetzen Sie in beiden Tags den Standardwert `localhost:19120` durch die Host- und Portinformationen Ihrer Silk Central-Installation.
Wenn für die Silk Central-Installation derselbe Front-End-Server wie für die Issue Manager-Installation verwendet wird, und Sie für den Tomcat-Webserver den Standardport nutzen, können Sie die Standardwerte beibehalten.
5. Speichern und schließen Sie die XML-Datei.
6. Wenn Sie nicht den Standardport verwenden, passen Sie die Datei `configuration.xml` in `\instance_<Instanznummer>_<Instanzname>\wwwroot\AlmServices1.0` an. Suchen Sie den XML-Tag `connectString` und geben sie die korrekten Ports ein.

Beispiel:

```
<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. Starten Sie den Front-End-Server neu.

Deaktivieren nicht verwendeter Ports auf Ausführungsservern

Je nachdem, ob Sie eine SSL-Verbindung oder eine unsichere Verbindung zwischen dem Anwendungsserver und den Ausführungsservern verwenden, können Sie den jeweils nicht benötigten Port deaktivieren. Außerdem können Sie den Tomcat-Standardport deaktivieren, da dieser von Silk Central nicht genutzt wird.

Die folgenden Schritte müssen auf jedem Ausführungsserver durchgeführt werden, auf dem der nicht verwendete Port deaktiviert werden soll.

So deaktivieren Sie nicht verwendete Ports auf dem Ausführungsserver:

1. Halten Sie den Ausführungsserver an.

2. Öffnen Sie die Datei `SccExecServerBootConf.xml` in einem Texteditor.
Diese Datei befindet sich standardmäßig in `C:\Program Files (x86)\Silk\Silk Central 18.5 Execution Server\conf\execserver` auf dem Ausführungsserver.
3. Suchen Sie die XML-Tags `InsecurePort` und `SSLPort` im Abschnitt `RmiProxy` der Datei.
4. Das weitere Vorgehen hängt davon ab, ob Sie eine SSL- oder eine unsichere Verbindung zwischen dem Anwendungs- und dem Ausführungsserver eingerichtet haben:

SSL-Verbindung	Setzen Sie den <code>InsecurePort</code> -Wert auf 0.
Unsichere Verbindung	Setzen Sie den <code>SSLPort</code> -Wert auf 0.
5. Speichern und schließen Sie die XML-Datei.
6. Starten Sie den Ausführungsserver neu.

Festlegen der Anzahl zuletzt angezeigter Berichte

So legen Sie die maximale Anzahl von Berichten fest, die im Listenfeld **Zuletzt verwendete Berichte** angezeigt werden:

1. Stoppen Sie den Front-End-Server der zu bearbeitenden Instanz auf der Seite **Instanzen-Verwaltung**.
2. Öffnen Sie die Datei `SccFrontendBootConf.xml` in einem Texteditor.
Diese Datei befindet sich standardmäßig in `C:\Program Files (x86)\Silk\Silk Central 18.5\instance_<Instanznummer>_<Instanzname>\Conf\FontendServer` auf dem Front-End-Server.
3. Suchen Sie den XML-Tag `<MRUListSize>` im Abschnitt `<Report>` der Datei.
Der Standardwert für dieses Tag ist 10.
4. Setzen Sie den Wert auf die Maximalzahl zuletzt angezeigter Berichte in dem Listenfeld **Zuletzt verwendete Berichte** fest.
5. Speichern und schließen Sie die XML-Datei.
6. Starten Sie den Front-End-Server neu.

Speichereinstellungen für Silk Central-Server

In diesem Abschnitt wird beschrieben, wie Sie die Speichereinstellungen der Silk Central-Server ändern können, wenn ein Fehler aufgrund von Speichermangel auftritt.

Die Größe des Java Heaps des Silk Central-Front-End-Servers und des Anwendungsservers wird standardmäßig auf 512 MB eingestellt (2048 MB für 64-Bit Front-End-Server). Falls Fehler aufgrund von Speichermangel angezeigt werden, zum Beispiel wenn Sie ein Projekt in Silk Central kopieren, versuchen Sie die Größe des Heaps am Front-End-Server oder Anwendungsserver zu erhöhen.

Der folgende Fehler ist ein Indikator dafür, dass die Größe des Java Heaps zu klein ist:

```
java.lang.RuntimeException: java.lang.OutOfMemoryError: Java heap space at
com.segue.scc.webgui.module.console.ProjectsUnit
$CopyProjectThread.run(ProjectsUnit.java:1473) Caused by:
```

```
java.lang.OutOfMemoryError: Java heap space. Dieser Fehler wird im Logfile des Front-End-
Servers oder des Anwendungsservers aufgeführt. Ein weiterer Hinweis ist die folgende Fehlermeldung Das
System arbeitet an der Grenze seiner Kapazität. Aus Sicherheitsgründen können
sich keine weiteren Benutzer mehr anmelden, welche angezeigt wird, wenn Sie versuchen,
sich auf Silk Central anzumelden.
```

Erhöhen der Größe des Java Heaps auf einem Silk Central-Server

Erhöhen Sie die Größe des Java Heaps auf einem Silk Central-Server, wenn Sie Fehler aufgrund von Speichermangel angezeigt bekommen.

Um die Größe des Java Heaps am Front-End oder Anwendungsserver zu erhöhen:

1. Stoppen Sie die zu bearbeitende Instanz auf der Seite **Instanzen-Verwaltung**.
2. Öffnen Sie mit einem Texteditor die Datei `sc_<Server>.processconfig` des Servers, für die Sie die Speicher-Einstellungen ändern möchten. Der Standardpfad für diese Dateien lautet `C:\Program Files (x86)\Silk\Silk Central 18.5\instance_<Instanznummer>_<Instanzname>\Conf`.
3. Setzen Sie für 32-Bit-JVMs den Wert des Tags `<JvmOption32bit name="-Xmx" unter <JvmOptions32bit>`. Setzen Sie für 64-Bit-JVMs den Wert des Tags `<JvmOption name="-Xmx" unter <JvmOptions>`.
4. Speichern und schließen Sie die XML-Datei.
5. Starten Sie die Instanz erneut.

Festlegen der maximalen Größe von Testschritt-Ergebnisdateien

Sie können die Größe von Ergebnisdateien begrenzen, die Tester während der Durchführung manueller Tests im Fenster **Manuelles Testen** an Testschritte anhängen können. Weitere Informationen finden Sie unter *Anhängen von Ergebnisdateien*.

So legen Sie die maximale Größe von Testschritt-Ergebnisdateien fest:

1. Stoppen Sie den Front-End-Server der zu bearbeitenden Instanz auf der Seite **Instanzen-Verwaltung**.
2. Öffnen Sie die Datei `ScFrontendBootConf.xml` in einem Texteditor.
Diese Datei befindet sich standardmäßig in `C:\Program Files (x86)\Silk\Silk Central 18.5\instance_<Instanznummer>_<Instanzname>\Conf\FrontendServer` auf dem Front-End-Server.
3. Suchen Sie das XML-Tag `<MaximumResultFileSizeInBytes>`. Der Standardwert für dieses Tag ist 104857600 (100 MB).
4. Legen Sie den Wert auf die gewünschte maximale Dateigröße fest. Geben Sie die Dateigröße in Byte ein.
5. Speichern und schließen Sie die XML-Datei.
6. Starten Sie den Front-End-Server neu.

Speichern von Perzentil-Markierungsdaten für Silk Performer-Testergebnisse

Silk Performer-Testergebnisse enthalten eine große Menge Perzentil-Markierungsdaten, welche viel Platz in der Datenbank brauchen (`TM_PerfReportPercentileMarker`-Tabelle). Deshalb ist das Speichern dieser Informationen standardmäßig ausgeschaltet. So schalten Sie das Speichern von Perzentil-Markierungsdaten frei, wann immer Silk Performer-Testergebnisse gespeichert werden:

1. Stoppen Sie den Anwendungsserver der zu bearbeitenden Instanz auf der Seite **Instanzen-Verwaltung**.
2. Öffnen Sie die Datei `TmAppServerHomeConf.xml` mit einem Texteditor.
Diese Datei befindet sich standardmäßig in `C:\Program Files (x86)\Silk\Silk Central 18.5\instance_<Instanznummer>_<Instanzname>\Conf\AppServer` auf dem Anwendungsserver.
3. Suchen Sie den XML-Tag `Config/SilkPerformerResultStorage/StorePercentileMarkerData`. Die Standardeinstellung dieses Tags lautet `false`.

4. Setzen Sie den Wert auf `true`.
5. Speichern und schließen Sie die XML-Datei.
6. Starten Sie den Anwendungsserver neu.

Index

A

- Agenten-Cluster für Lasttests
 - Entfernen 50
 - Hochladen 50
 - Seite 51
 - Silk Performer 50
- Agenten-Cluster-Datei für Lasttests
 - Ändern 50
 - Hinzufügen 50
 - Löschen 50
- Agenten-Cluster-Dateien für Lasttests
 - bearbeiten 51
- Aktualisieren 16
- Anmeldeoptionen
 - Anpassen der Cookie-Dauer 53
 - Erweitert 52
 - Konfigurieren der Option "Benutzerdaten merken" 53
- Anmeldung
 - Benutzerdaten merken 52
 - Cookie-Dauer 52
 - Erweiterte Optionen 52
 - Konfigurieren der Option "Benutzerdaten merken" 53
- anpassen
 - Datums- und Zeitformate 56
- Anpassen
 - Cookie-Dauer 53
- Anwendungsserver
 - Festlegen einer Servergruppe 45
 - Installieren 12
 - Speicherort 45
- Anwendungsserver-Logs
 - Seite für Systemadministratoren 52
- Anzahl festlegen
 - Zuletzt angezeigte Berichte 68
- Anzeigen
 - Hostnamen in Webbrowsern 57
- Architektur
 - Übersicht 5
- attachments
 - Auf dem Dateisystem speichern 57
- Auf dem Dateisystem speichern
 - attachments 57
 - Ergebnisdateien 57
- Ausführungsdauer
 - Verdächtig 54
- Ausführungsserver
 - Deaktivieren nicht verwendeter Ports 25, 67
 - Hostnamenauflösung 66
 - Konfigurieren von benutzerdefinierten SSL-Ports 25
- Ausführungsserverdienst starten
 - Service Manager 29
- Ausführungsserverdienst stoppen
 - Service Manager 29
- automatische Benutzerkonto-Erstellung
 - LDAP 46

B

- bearbeiten
 - LDAP-Server 47

- Bearbeiten
 - Diagrammserver 42
- BIRT
 - SSL-Verbindungen aktivieren 24

C

- Cookie-Dauer
 - Anpassen 53

D

- Dateien
 - Speicherort 5
- Datenbanken
 - ALM URIs 34
 - Berechtigungen 32
 - Datenbank (Seite) 35
 - erstellen 33
 - IDs 34
 - Rollen 32
 - Übersicht 31
 - Verbindung trennen 34
 - Zugreifen 33
- Datum und Zeit
 - Benutzerdefinierte Einstellungen 55
- Datumsformate
 - anpassen 56
- DBMS 31
- deaktivieren
 - Nicht verwendete Ports auf Ausführungsservern 25, 67
 - Zwischenspeichern von Hostnamenauflösungen 66
- Diagrammserver
 - Bearbeiten 42
 - Hinzufügen 41
 - Installieren 12
 - Seite 42
 - Servergruppen 41
 - Verbindungen entfernen 42
- Dienste
 - wird gestartet 26
 - wird gestoppt 26

E

- E-Mail-Server
 - Info 43
 - Konfigurieren 43
 - Seite 43
- Entfernen
 - Instanzen 26
- Ergebnisdateien
 - Auf dem Dateisystem speichern 57
- erhöhen
 - Java Heaps erhöhen 68
- erstellen
 - Datenbanken 33

- Erweiterte Einstellungen
 - Konfigurieren 52
- Erzeugen eines Lizenzierungsschemas 18
- Evaluation
 - Installation 11
- externe Systeme
 - die über SSL kommunizieren 26

F

- Festlegen
 - Verdächtige Ausführungsdauer 54
- Formate
 - Datum und Zeit 55
- Freier Festplattenspeicher 32
- Front-End-Server
 - Installieren 12
 - Lastausgleichsmechanismus konfigurieren 29
 - Logs 52

G

- Größe der Java Heaps
 - erhöhen 68

H

- hinzufügen
 - Instanzen 26
 - LDAP-Server 46
- Hinzufügen
 - Diagrammserver 41
- Hostkennungen 18
- Hostname
 - Anzeigen in Webbrowsern 57
 - Verbergen in Webbrowsern 57
- Hostnamen anzeigen
 - Webbrowser 57
- Hostnamenauflösung
 - Deaktivieren der Zwischenspeicherung 66
- Hotfix
 - Installieren 16, 28

I

- Infrastruktur
 - Verwalten 23
- installieren
 - Ausführungsserver 14
 - Überblick 10
 - Windows-Ausführungsserver 14
- Installieren
 - Einzelplatzinstallation 11
 - Evaluationsversion 11
 - Hotfix 16, 28
 - Linux-Ausführungsserver 15
 - Produktiv-Umgebung 12
- Instanzen
 - Entfernen 26
 - hinzufügen 26
 - löschen 26

- Übersicht 23
- Verwalten 26
- Wartung 26

J

- JMX
 - Verbindung 26
- JMX-Einstellungen
 - konfigurieren 62
- JMX-Messdaten
 - LDAP-Synchronisierung 66
 - überwachen von DataMart 64
 - Überwachen von LQM Reporting Updater 63

K

- konfigurieren
 - JMX-Einstellungen 62
 - LQM Reporting Updater 58
 - Option "Benutzerdaten merken" 53
 - Silk Central-Standort 67
- Konfigurieren
 - Benutzerdefinierte SSL-Ports für Ausführungsserver 25
 - Erweiterte Einstellungen 52
- Konten
 - Systemadministrator 37

L

- Lastausgleichsmechanismus
 - konfigurieren für Front-End-Server 29
 - Übersicht 29
- LDAP
 - Authentifizierung 45
 - Gruppen synchronisieren 59
 - Integration 46
- LDAP-Authentifizierung
 - Gemischter Modus 46
 - Logik 46
 - Standardmodus 46
- LDAP-Server
 - automatische Benutzerkonto-Erstellung 46
 - bearbeiten 47
 - hinzufügen 46
 - löschen 49
 - Seite 49
 - Testen der Verbindung 49
- LDAP-Server bearbeiten
 - Dialog 46
- Linux-Ausführungsserver 15
- Lizenzen
 - Ein- und Auschecken 17, 39
- Lizenzierung
 - Testen einer Verbindung 20
 - Übersicht 17
- Lizenzierungsschema 18
- Lizenzserver
 - Anforderungen 19
 - Konfiguration ändern 19
- Lizenztypen 17, 39

- Logdateien
 - Speicherort 5
- löschen
 - Instanzen 26
 - LDAP-Server 49
- LQM Reporting Updater
 - konfigurieren 58

M

- Mandanten
 - bearbeiten 38
 - Berechtigungen 40
 - Entfernen 38
 - erstellen 37
 - Info 37
 - Seite 40
 - Standard 39
- MS SQL Server 31

N

- Neue Version 16
- Neuer LDAP-Server
 - Dialog 46

O

- Oracle
 - Freier Festplattenspeicher 32
 - Temporärer Tablespace, Größe 32

P

- Perzentil-Markierungsdaten
 - Silk Performer-Ergebnisse 69
 - Speichern 69
- Ports
 - Deaktivieren nicht verwendeter auf Ausführungsservern 25, 67
- Produktiv-Umgebung
 - Installationen 12

R

- RDBMS 31
- Richtlinien
 - Sichere Umgebung 23

S

- Server
 - Größe der Java Heaps erhöhen 68
 - Speichereinstellungen 68
- Service Manager
 - Ausführungsserverdienst starten 29
 - Ausführungsserverdienst stoppen 29
- Sichere Umgebung
 - Richtlinien 23
- Silk Central-Standort

- Konfigurieren in Issue Manager 67
- Silk Meter
 - Ändern von Lizenzservern 19
 - Deinstallieren 19
 - Installieren 19
 - Installieren auf Lizenzservern 19
 - Konfiguration ändern 19
 - Testen einer Verbindung 20
- Silk Performer
 - Agenten-Cluster für Lasttests 50
- Silk Performer-Ergebnisse
 - Perzentil-Markierungsdaten 69
- Speichereinstellungen
 - Server 68
- Speichern
 - Perzentil-Markierungsdaten 69
- SQL 31
- SSL
 - Sichere Webserver-Verbindungen 23
 - Umgang mit selbstsignierten Zertifikaten 26
- SSL-Verbindungen
 - aktivieren für BIRT 24
- Synchronisieren
 - Gruppen aus LDAP 59
- System-Proxy
 - Client-Aktivierung 44
 - Konfigurieren 44
 - Seite 44
- Systemadministrator
 - Konten 37
- Systemdiagnose
 - anzeigen 51
 - Systemdiagnose (Seite) 51
- Systemverwaltung
 - Systemadministrator 30
 - Übersicht 30

T

- Temporärer Tablespace, Größe 32
- Testen
 - Verbindung zu LDAP-Servern 49
- Tests
 - JMX-Messdaten für die Zwischenspeicherung 61, 62
 - Zwischenspeicherung von Daten 60
- Testschritt-Ergebnisdateien
 - Festlegen der maximalen Größe 69

U

- Übersicht
 - Architektur 5
 - Instanzen 23

V

- Verbergen
 - Hostnamen in Webbrowsern 57
- Verbindung
 - JMX 26
- Verbindung trennen

- Datenbanken 34
- Verdächtige Ausführungsdauer
 - Festlegen 54
- Verwalten
 - Infrastruktur 23
 - Instanzen 26

W

- Wartung
 - Instanzen 26
- Webbrowser
 - Anzeigen des Hostnamens 57
 - Hostnamen anzeigen 57
 - Verbergen des Hostnamens 57
- Webserver-Verbindungen
 - SSL 23
- Windows-Ausführungsserver 14

- wird gestartet
 - Dienste 26
- wird gestoppt
 - Dienste 26

Z

- Zeitformate
 - anpassen 56
- Zugreifen
 - Datenbanken 33
- Zuletzt angezeigte Berichte
 - Anzahl festlegen 68
- Zwischenspeicherung
 - JMX-Messdaten in Tests 61, 62
- Zwischenspeicherung von Daten
 - Tests 60