

Service Desk 7.4 Installation Guide

May 2017

Legal Notices

For information about legal notices, trademarks, disclaimers, warranties, export and other use restrictions, U.S. Government rights, patent policy, and FIPS compliance, see <https://www.microfocus.com/about/legal/>.

Copyright © 2017 Micro Focus Software Inc. All Rights Reserved.

Contents

About This Guide	5
1 Overview	7
2 System Requirements	9
2.1 Micro Focus Service Desk Requirements	9
2.1.1 Server Requirements	9
2.1.2 Database Requirements	11
2.1.3 System Integration	12
2.2 Micro Focus Service Desk Appliance Requirements	12
2.2.1 Server Requirements	12
3 Installing and Uninstalling the Micro Focus Service Desk	15
3.1 Downloading the Micro Focus Service Desk Software	15
3.2 Installing Micro Focus Service Desk	15
3.2.1 Operating System Supports a GUI Installer	15
3.2.2 Operating System Does Not Support Direct Execution of the JAR files	16
3.2.3 Operating System Does Not Support a GUI Installer	16
3.3 Creating the Schema	16
3.4 Uninstalling Micro Focus Service Desk	17
4 Upgrading the Micro Focus Service Desk	19
4.1 Pre-Upgrade	19
4.2 Upgrading the Service Desk	19
4.3 Post Upgrade	27
5 Micro Focus Service Desk Appliance Deployment	29
5.1 Deploying the Appliance	29
5.2 Configuring the Appliance Settings	30
5.2.1 Starting and Stopping Service Desk using the Terminal	30
5.2.2 File location Details	30
6 Upgrading Micro Focus Service Desk Appliance	33
6.1 Pre-Upgrade	33
6.2 Upgrading the Service Desk Appliance	34
6.3 Post Upgrade	36
7 Enabling HTTPS for Micro Focus Service Desk	39
7.1 Enabling HTTPS on Windows devices	39
7.2 Enabling HTTPS on Linux devices	41
7.3 Enabling HTTPS on Appliance	42
7.4 Enabling HTTPS on Appliance Prior to 7.3 Version	44

8	Micro Focus Service Desk Web Server SSL Certificate Installation	49
8.1	Generating the Certificate Signing Request	49
8.2	Installing the SSL Certificates to the Keystore	49
8.3	Configuring the SSL Connector	50
8.4	Migrating the External Certificates	51
8.4.1	Migrating the External Certificates from Service Desk 7.2 or earlier Appliance Versions	51

About This Guide

This *Micro Focus Service Desk Installation Guide* includes information to help you successfully install Micro Focus Service Desk on a device.

The information in this guide is organized as follows:

- ♦ Chapter 1, “Overview,” on page 7
- ♦ Chapter 2, “System Requirements,” on page 9
- ♦ Chapter 3, “Installing and Uninstalling the Micro Focus Service Desk,” on page 15
- ♦ Chapter 5, “Micro Focus Service Desk Appliance Deployment,” on page 29
- ♦ Chapter 4, “Upgrading the Micro Focus Service Desk,” on page 19
- ♦ Chapter 6, “Upgrading Micro Focus Service Desk Appliance,” on page 33

Audience

This guide is intended for administrators.

Feedback

We want to hear your comments and suggestions about this manual and the other documentation included with this product. Please use the User Comments feature at the bottom of each page of the online documentation.

Additional Documentation

Micro Focus Service Desk is supported by other documentation that you can use to learn about and implement the product. For additional documentation, see the [Novell Service Desk documentation Web site \(http://www.novell.com/documentation/servicedesk71/\)](http://www.novell.com/documentation/servicedesk71/).

1 Overview

Micro Focus Service Desk is a complete service management solution that allows you to easily monitor and solve service issues so that there is minimal disruption to your organization, which allows users to focus on the core business. Micro Focus Service Desk provides an online support system to meet the service requirements of all your customers, administrators, supervisors, and technicians.

Micro Focus Service Desk gives you the ability to reduce your mean time to repair (MTTR) and continually improve your service management environment by streamlining and automating your service desk function. By applying industry-acknowledged best practices, Micro Focus Service Desk's fully integrated service management tool allows you to solve, submit, track and manage requests through e-mail, PDA or a convenient customer portal.

The key capabilities include:

- ◆ User-friendly interface that offers an easy-to-use Knowledge Base and Request tracking system for your customers.
- ◆ Easy-to-use tools that enable technicians to offer the most effective and efficient support service.
- ◆ Comprehensive management and reporting for the service desk, its technicians, and all support issues.
- ◆ Ability to use Micro Focus ZENworks Configuration Management bundle management features from the Micro Focus Service Desk user interface.

The Micro Focus Service Desk software solution is completely Web-based and is highly scalable. The application can be deployed on Windows or Linux and supports a variety of RDBMS.

Micro Focus Service Desk has the following editions available:

- ◆ **Micro Focus Service Desk for Incident Management:** Includes Incident, Configuration, and Service Level Management (Basic) functionality with an emphasis on internal or external customer support.
- ◆ **Micro Focus Service Desk for ITIL Management:** A comprehensive service management solution that is fully compliant with Information Technology Infrastructure Library (ITIL) standards. Micro Focus Service Desk for ITIL Management supports eleven core ITIL processes including Request, Incident, Problem, Change, Configuration, and Service Level Management. This enterprise-wide solution delivers complete customer service and support for any size of organization.

2 System Requirements

The following sections provide the system requirements for Micro Focus Service Desk:

- ◆ [Section 2.1, “Micro Focus Service Desk Requirements,” on page 9](#)
- ◆ [Section 2.2, “Micro Focus Service Desk Appliance Requirements,” on page 12](#)

2.1 Micro Focus Service Desk Requirements

The following sections list the Micro Focus Service Desk requirements:

- ◆ [Section 2.1.1, “Server Requirements,” on page 9](#)
- ◆ [Section 2.1.2, “Database Requirements,” on page 11](#)
- ◆ [Section 2.1.3, “System Integration,” on page 12](#)

2.1.1 Server Requirements

The server where you install Micro Focus Service Desk must meet the following requirements:

Item	Requirements
Server Usage	<p>Your server might be capable of handling tasks in addition to the tasks expected for Micro Focus Service Desk. However, we recommend that any server where you install the Micro Focus Service Desk software be used only for service desk purposes.</p> <p>For example, you would not want the server to do the following:</p> <ul style="list-style-type: none">◆ Host Micro Focus eDirectory / Active Directory◆ Be a terminal server◆ Be a GroupWise / Exchange server◆ Be an SQL Server

Item	Requirements
Operating System	<p>Windows:</p> <ul style="list-style-type: none"> ◆ Windows Server 2008 SP1 64-bit (Enterprise and Standard editions) ◆ Windows Server 2008 SP2 64-bit (Enterprise and Standard editions) ◆ Windows Server 2008 R2 64-bit (Enterprise and Standard editions) ◆ Windows Server 2008 R2 SP1 64-bit (Enterprise and Standard editions) ◆ Windows Server 2012 64-bit (Enterprise and Standard editions) ◆ Windows Server 2012 R2 64-bit (Enterprise and Standard editions) <p>Linux:</p> <ul style="list-style-type: none"> ◆ RHEL 6.x (64-bit) ◆ SUSE Linux Enterprise Server 12 (SLES 12) 64-bit ◆ SUSE Linux Enterprise Server 12 SP1 (SLES 12 SP1) 64-bit
Processor	Minimum: Pentium IV 2.8 GHz (x86 and x86_64), or equivalent AMD or Intel processor
RAM	2 GB minimum; 4 GB recommended
Disk Space	5 GB minimum for installing; 10 GB recommended for running. Depending on the amount of content you store as attachments, this number can vary greatly.
Display resolution	1024 × 768 with 256 colors minimum
Hostname Resolution	<p>Server names must support DNS requirements, such as not having underscores in their names. Acceptable characters are the letters a-z (uppercase and lowercase), numbers, and the hyphen (-).</p> <p>The server must be able to resolve its own hostname to its IP address by using a method such as DNS or an entry in the hosts file.</p>
IP Address	<p>The server must have a static IP address or a permanently leased DHCP address.</p> <p>An IP address must be bound to all NICs on your target server.</p> <p>The installation hangs if it is trying to use a NIC that does not have an IP address bound to it.</p>
Web Browser	<p>The following browsers are supported:</p> <ul style="list-style-type: none"> ◆ Internet Explorer 11 ◆ Firefox 52 and prior versions (32-bit) ◆ Firefox 52 ESR and prior versions (32-bit)
JDK/JRE	Sun 64 bit JDK 8
Firewall Settings: TCP Ports	<p>Port 80 is the non-secure port.</p> <p>Port 443 is the secure port.</p>
Virtual Machine Environments	The Micro Focus Service Desk software can also be installed on virtual machines running any of the above mentioned operating systems.

2.1.2 Database Requirements

Micro Focus Service Desk requires an external database to function. The database must meet the following requirements:

Item	Requirements
Database Version	<ul style="list-style-type: none">◆ Microsoft SQL Server 2008 SP1, SP2 and SP3◆ Microsoft SQL Server 2008 R2 SP1◆ Microsoft SQL Server 2012◆ Microsoft SQL Server 2012 R2◆ Microsoft SQL Server 2014◆ MySQL v5.0 to v5.7◆ Oracle Database 12c◆ PostgreSQL v8.3 to v9.7
TCP Ports	<p>The database server must allow communication on the database port. For MS SQL, make sure to configure static ports for the database server.</p> <p>The default ports are:</p> <ul style="list-style-type: none">◆ 1433 for MS SQL◆ 3306 for MySQL◆ 5432 for PostgreSQL◆ 1521 for Oracle <p>IMPORTANT: You can change the default port number if you have a conflict. However, you must make sure that the port is opened for the Micro Focus Service Desk to talk to the database.</p>
WAN	<p>The Micro Focus Service Desk server and the database must reside on the same network segment. If they are separated by a WAN, this configuration is not supported.</p>
Default Character Set	UTF-8 character set.
Collation	Make sure that the database is case insensitive before setting it up.
Database User	<p>When you create a user account to be used by Micro Focus Service Desk to communicate to its database, ensure the following:</p> <ul style="list-style-type: none">◆ For MS SQL, the user account requires the DBO privilege◆ For Oracle, the user account requires ACCESS_ANY_WORKSPACE, CREATE_ANY_WORKSPACE, UNLIMITED TABLESPACE, CONNECT, and RESOURCE <p>NOTE: Create a separate user account for Micro Focus Service Desk. It is recommended not to create Micro Focus Service Desk objects under SYSDBA or System account.</p> <p>All databases must use password-based authentication. Integrated authentication with Active Directory or eDirectory is not supported.</p>

Item	Requirements
Database Settings	Regardless of the SQL environment, the database sizing must have a minimum of 10 MB for data and 5 MB for the associated transaction log. It is advisable to let these grow as needed unless you want to spend time directly managing them. If you think you will log large numbers of cases with Micro Focus Service Desk, start with larger sizes.
Database Schema	When you use a browser to connect to Micro Focus Service Desk for the first time after installation, you can choose the desired database type. You are also provided with a script to create the schema. For more information on the schema creation, see Section 3.3, “Creating the Schema,” on page 16.

2.1.3 System Integration

Service Desk 7.4 supports integration with the following:

- ♦ ZENworks 2017

2.2 Micro Focus Service Desk Appliance Requirements

Micro Focus Service Desk Appliance is a 64-bit (x86_64) virtual machine. The following sections provide the requirements for deploying Micro Focus Service Desk Appliance to a virtual infrastructure:

- ♦ [Section 2.2.1, “Server Requirements,” on page 12](#)

2.2.1 Server Requirements

The server where you install Micro Focus Service Desk Appliance must meet the following requirements:

Table 2-1 Server Requirements

Item	Requirements
Hypervisor	VMware ESX / ESXi 4 / ESXi v5.1
Virtual Machine Configuration	Micro Focus Service Desk Appliance requires the following minimum configuration that have been preconfigured by default: <ul style="list-style-type: none"> ♦ RAM: 2 GB minimum ♦ Disk Space: 20 GB minimum ♦ Display resolution: 1024 × 768 with 256 colors minimum.
Hostname Resolution	The server must resolve device hostnames.
IP Address	Appliance initially starts with the IP address allocated from DHCP. You can change the IP address to static IP by using the Appliance Management menu during the configuration of Appliance. For more information on configuring appliance, see Section 5.2, “Configuring the Appliance Settings,” on page 30.

Item	Requirements
Database	Micro Focus Service Desk Appliance is available with the embedded PostgreSQL database. However, you can change the database after the appliance is up and running. For information on the supported databases see, Section 2.1.2, “Database Requirements,” on page 11.

3 Installing and Uninstalling the Micro Focus Service Desk

The Micro Focus Service Desk software solution is completely Web-based and is highly scalable. The application can be deployed on Windows or Linux and supports a variety of RDBMS. Ensure that the device on which you want to install Micro Focus Service Desk has Java installed and is up and running.

Perform the following steps to download and install the Micro Focus Service Desk software on the device:

- ♦ [Section 3.1, “Downloading the Micro Focus Service Desk Software,” on page 15](#)
- ♦ [Section 3.2, “Installing Micro Focus Service Desk,” on page 15](#)
- ♦ [Section 3.3, “Creating the Schema,” on page 16](#)
- ♦ [Section 3.4, “Uninstalling Micro Focus Service Desk,” on page 17](#)

3.1 Downloading the Micro Focus Service Desk Software

- 1 On the [Micro Focus Downloads page \(http://download.novell.com\)](http://download.novell.com), search for Micro Focus Service Desk.
- 2 Continue with installing Micro Focus Service Desk. For more information on installing Micro Focus Service Desk, see [Section 3.2, “Installing Micro Focus Service Desk,” on page 15](#).

3.2 Installing Micro Focus Service Desk

Ensure that the device on which you want to install Micro Focus Service Desk has Java installed and running.

Depending on the operating system installed on the device, you can use one of the following methods to install Micro Focus Service Desk.

- ♦ [Section 3.2.1, “Operating System Supports a GUI Installer,” on page 15](#)
- ♦ [Section 3.2.2, “Operating System Does Not Support Direct Execution of the JAR files,” on page 16](#)
- ♦ [Section 3.2.3, “Operating System Does Not Support a GUI Installer,” on page 16](#)

3.2.1 Operating System Supports a GUI Installer

- 1 Double-click the downloaded `installer.jar` file.
- 2 Follow the on-screen prompts.

3.2.2 Operating System Does Not Support Direct Execution of the JAR files

- 1 Execute the following command to run the installer from the command line:

```
java -jar Installer.jar
```
- 2 Follow the on-screen prompts.

3.2.3 Operating System Does Not Support a GUI Installer

- 1 Execute the following command to run the installer in console mode:

```
java -jar Installer.jar -console
```
- 2 Follow the on-screen prompts.

3.3 Creating the Schema

When you use a browser to connect to Micro Focus Service Desk for the first time after it is installed, you are prompted to choose the desired database type and are also provided with a script to create the database schema.

- 1 Use a Web browser to open the following page on the device:

```
http://<DNS_name_or_IP_address_of_device>:<port>
```

Replace *DNS_name_or_IP_address_of_device* with the DNS name or the IP address of the server on which the Micro Focus Service Desk has been installed and replace *port* with the port number used during the installation.

- 2 On the Application Setup page, fill in the following fields:

Database Type: Select a supported database platform from the list. For a list of the supported database platforms, see [Section 2.1.2, “Database Requirements,” on page 11](#).

Server Host: Specify the DNS name or the IP address of the database server. We recommend that you specify the DNS name to avoid any reconfiguration when the database server connection details change.

Server Port: Depending on the selected database type, the default port is automatically displayed. However, if you changed the default port during the installation of the database server, specify the changed port.

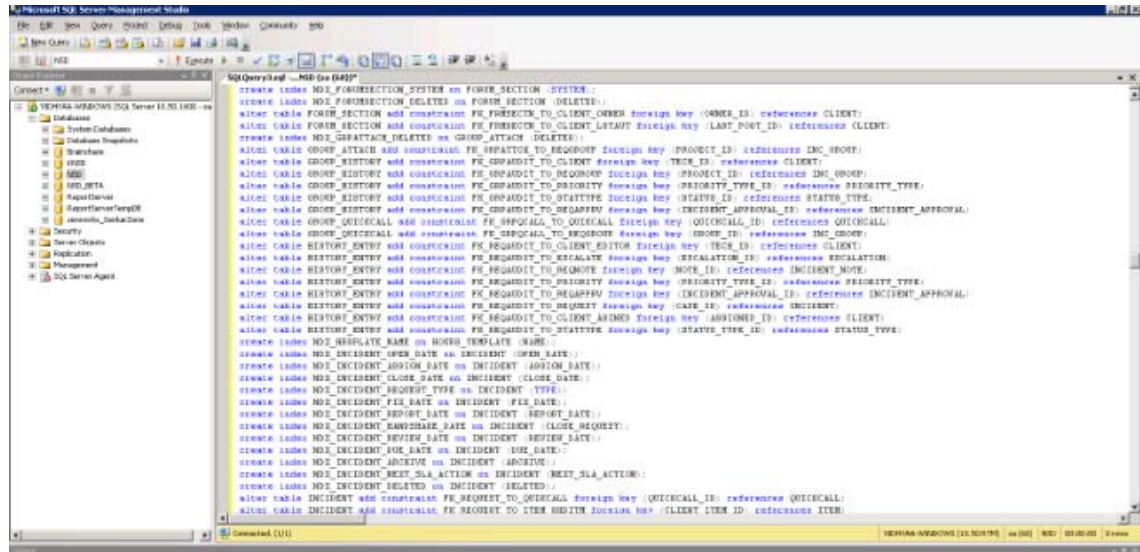
Database Name: Specify the name of a blank database on the database server for exclusive use by Micro Focus Service Desk.

Username: Specify the user to be created for use by Micro Focus Service Desk.

Password: Specify the password for the Micro Focus Service Desk user.

- 3 Click **Test** to test if the Micro Focus Service Desk can access the database server and the blank database. If a successful message is displayed, continue with [Step 4](#). If not, ensure that the details are correctly specified on the Application Setup page in [Step 2](#).
- 4 Click **Advanced**, then click **Create**. The Application Setup page displays a database script that must be executed to populate the database with tables.
- 5 Select the text on the Application Setup page by pressing CTRL+A. Copy the selected content, paste it into a file, and save the file.
- 6 Click **Done**.
- 7 Load the saved file into the database query tool of the database server that you are using.

The following figure displays the MS SQL Server Query Tool.



- 8 After the successful execution of the script, the browser displays the following Application Setup page:
- 9 Click **Save** to store the connection details and initialize the connection with Micro Focus Service Desk.
- 10 The Micro Focus Service Desk login page is displayed.
- 11 Use one of the following credentials to log into Micro Focus Service Desk:
 - ◆ **Administrator Credentials:** Username: admin; Password: admin
 - ◆ **Supervisor Credentials:** Username: super; Password: super

For details on using and configuring Micro Focus Service Desk in your environment, see [Administrator Guide](#) and [User Guide](#).

3.4 Uninstalling Micro Focus Service Desk

To uninstall Micro Focus Service Desk from a device:

- 1 Locate the **uninstaller.jar** file on the device.

For the default installation of Micro Focus Service Desk, the file is available in the `/usr/local/ServiceDesk/Uninstaller` directory on the device.

- 2 Open a command prompt and change to the directory that contains the **uninstaller.jar** file.
- 3 Execute the following command to run the uninstaller.

```
shell> java -jar uninstaller.jar
```


4 Upgrading the Micro Focus Service Desk

The following sections contains information about upgrading the Micro Focus Service Desk:

- ♦ [Section 4.1, “Pre-Upgrade,” on page 19](#)
- ♦ [Section 4.2, “Upgrading the Service Desk,” on page 19](#)
- ♦ [Section 4.3, “Post Upgrade,” on page 27](#)

4.1 Pre-Upgrade

Prior to upgrading to Service Desk 7.4, ensure that you perform the following:

- ♦ If you are using Customized Banners in Micro Focus Service Desk, then back up the contents from `<installation-location>/ServiceDesk/Server/webapps/LiveTime/images/banners/custom`.
- ♦ If you are using the Customized CSS and upgrading from Service Desk 7.2, then back up the CSS file located at `<installation-location>/ServiceDesk/LiveTime/Style/novell-7.0.css`
- ♦ If any configuration is changed in the Tomcat server such as the `web.xml`, `server.xml`, then ensure that you note the changes.
- ♦ If any configuration is changed in Java such as the `catalina.sh`, then ensure that you note the changes.
- ♦ If SSL is configured and you want to use the same certificates, then back up the certificates and keys.
- ♦ Ensure that you have a verified backup of your existing database.

IMPORTANT: Service Desk supports no more than two major versions behind the latest release (N-2). Since the latest version is Service Desk 7.4 (N) the 7.3 (N-1) and 7.2 (N-2) versions are also supported.

4.2 Upgrading the Service Desk

To upgrade to Micro Focus Service Desk 7.4 from previous releases the device must meet the requirements described in [Chapter 2, “System Requirements,” on page 9](#).

Perform the following steps on the device:

- 1 Back up the existing database.
- 2 Uninstall the previous version of Micro Focus Service Desk that is installed on the device. For information on uninstalling Micro Focus Service Desk.

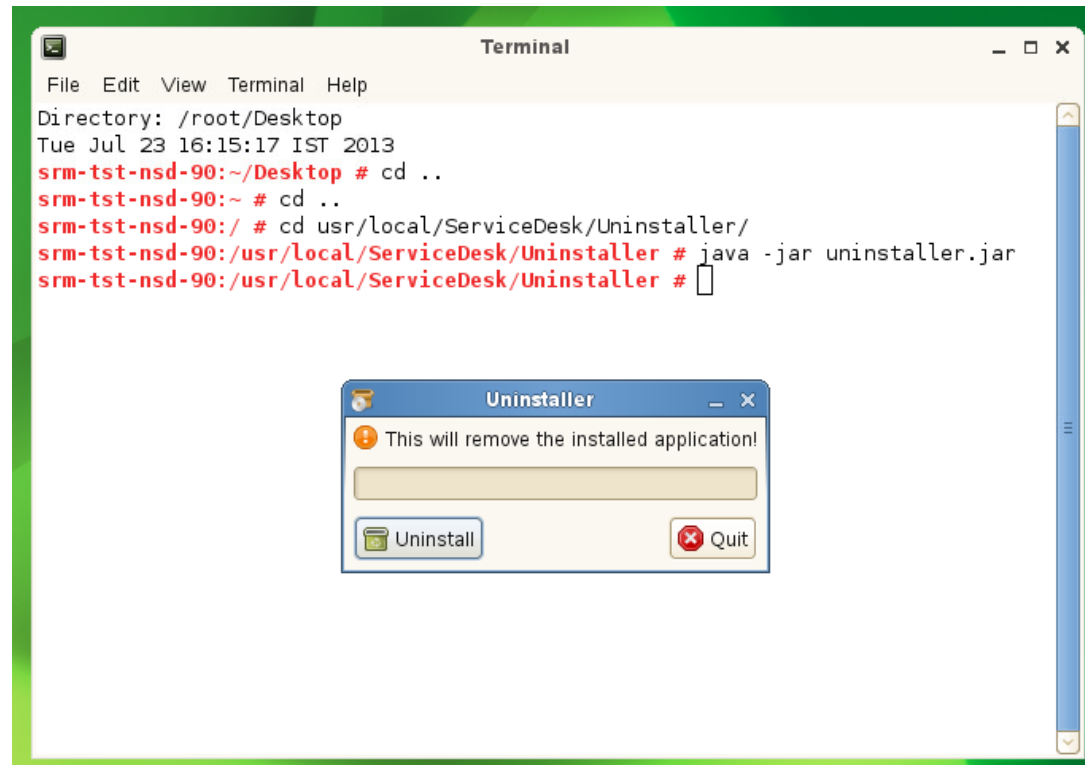
To unistall Micro Focus Service Desk from a device:

1. Locate the `unistaller.jar` file on the device.

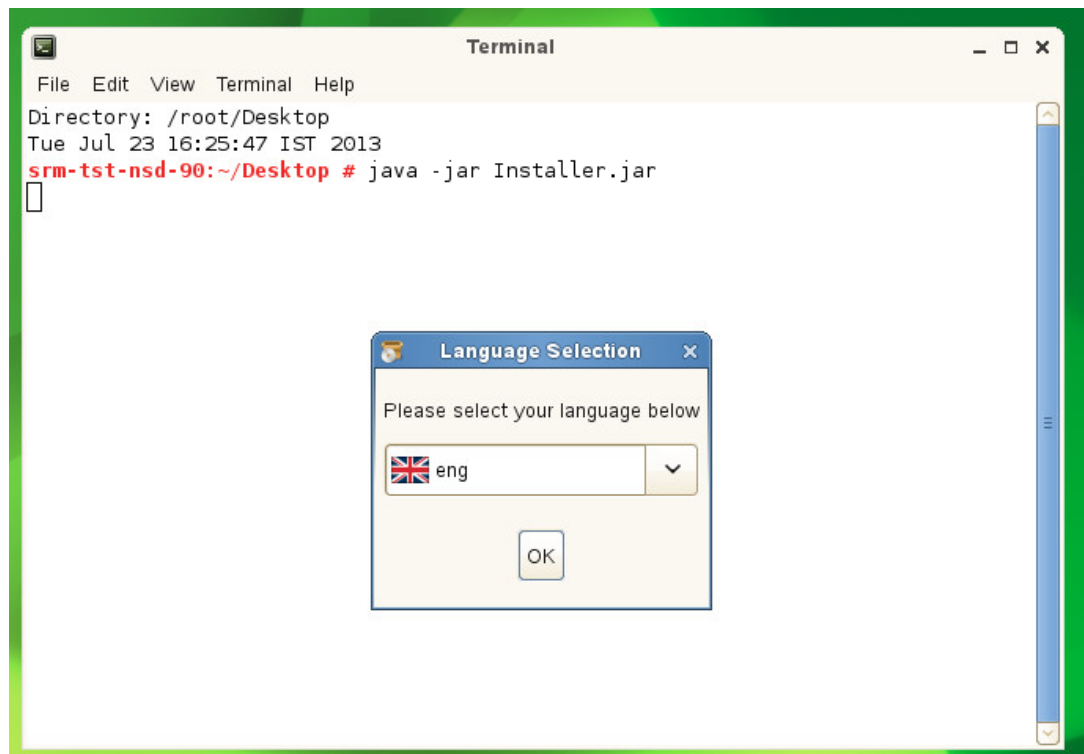
For the default installation of Micro Focus Service Desk, file is available at the following locations on the device:

- ♦ **Linux:** /usr/local/ServiceDesk/Uninstaller
- ♦ **Windows:** C:\Program Files\Service Desk\Uninstaller\Uninstaller.jar

2. In the command prompt, change to the directory that contains the `uninstaller.jar` file.
3. Execute the shell `> java -jar uninstaller.jar` command to run the uninstaller.
4. Click **Uninstall**.



3. Download the new Micro Focus Service Desk installer. For more information on downloading the Service Desk installer, see *Micro Focus Service Desk* in [Micro Focus Download website](#).
4. Run the new installer to install Micro Focus Service Desk in the same path you had previously installed. To run the new installer:
 1. Locate the `installer.jar` file.
 2. Run the `java -jar Installer.jar` command and complete the installation.



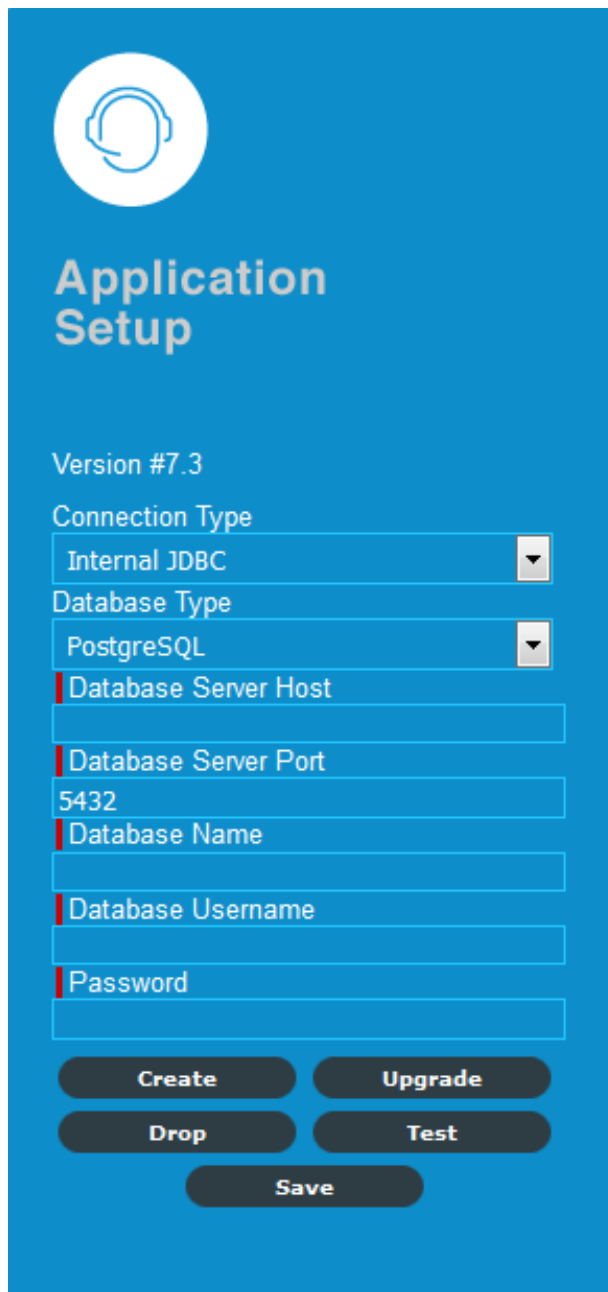
NOTE: During installation, overwrite the existing files in the folder.



- 5 Use a Web browser to open the following page on the device:

`http://<DNS_name_or_IP_address_of_device>:<port>`

Replace *DNS_name_or_IP_address_of_device* with the DNS name or the IP address of the server on which the Micro Focus Service Desk has been installed and replace *port* with the port number used during the installation.

The image shows a mobile application interface for 'Application Setup'. At the top left is a white circular icon containing a headset. Below it, the title 'Application Setup' is displayed in white text. Underneath the title, the text 'Version #7.3' is shown. The main section contains several form fields: 'Connection Type' with a dropdown menu set to 'Internal JDBC'; 'Database Type' with a dropdown menu set to 'PostgreSQL'; 'Database Server Host' (empty text input); 'Database Server Port' (text input containing '5432'); 'Database Name' (empty text input); 'Database Username' (empty text input); and 'Password' (empty text input). At the bottom of the form are five buttons: 'Create', 'Upgrade', 'Drop', 'Test', and 'Save', arranged in two rows. The first row contains 'Create' and 'Upgrade', the second row contains 'Drop' and 'Test', and the 'Save' button is centered below the second row. All buttons are dark blue with white text.

- 6 On the Application Setup page, specify the database details.
- 7 Click **Test** to ensure the database connection is correct.



Application Setup

Version #7.3

Connection Type

Internal JDBC

Database Type

PostgreSQL

Database Server Host

localhost

Database Server Port

5432

Database Name

mfsd

Database Username

postgres

Password

●●●●●●●●

Successfully connected to the database.

Create

Upgrade

Drop

Test

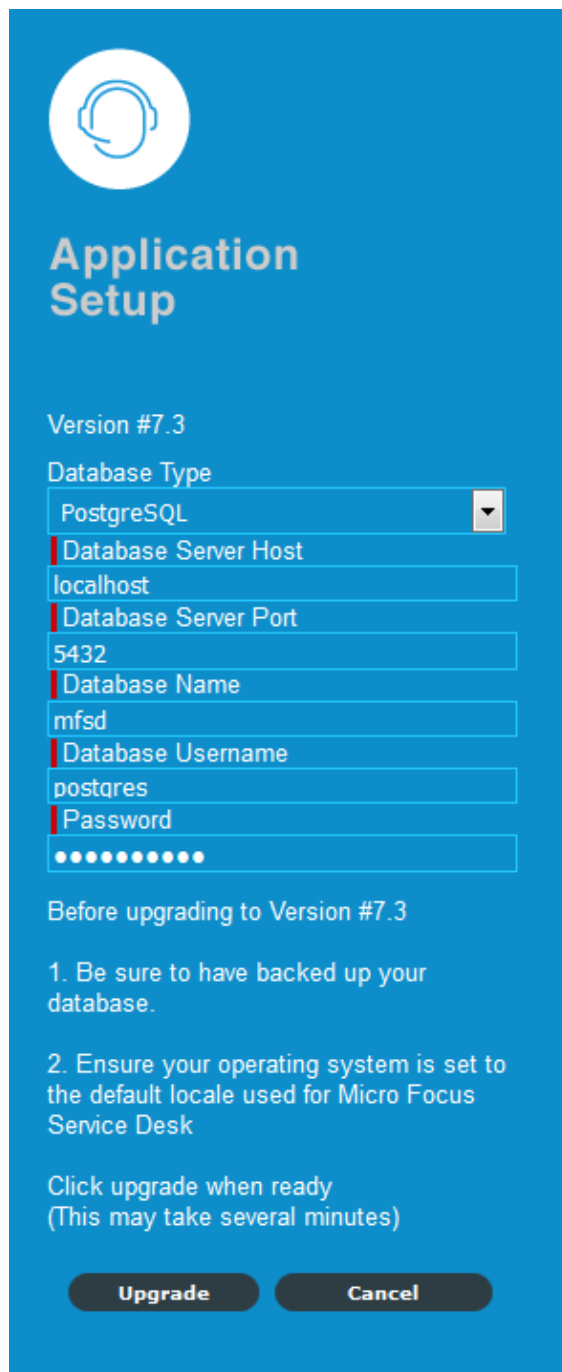
Save

8 Click Advanced.

9 Click Upgrade.

- 10 Click **Upgrade** again for the upgrade to proceed.

NOTE: Ensure that the database and the server devices are running and do not restart the device.



The image shows a blue dialog box titled "Application Setup" with a headset icon. It contains configuration fields for a PostgreSQL database: Database Type (PostgreSQL), Database Server Host (localhost), Database Server Port (5432), Database Name (mfsd), Database Username (postgres), and Password (masked with dots). Below the fields, it lists instructions for upgrading to version 7.3, such as backing up the database and setting the locale. At the bottom, there are "Upgrade" and "Cancel" buttons.

Application Setup

Version #7.3

Database Type
PostgreSQL

Database Server Host
localhost

Database Server Port
5432

Database Name
mfsd

Database Username
postgres

Password
●●●●●●●●

Before upgrading to Version #7.3

1. Be sure to have backed up your database.
2. Ensure your operating system is set to the default locale used for Micro Focus Service Desk

Click upgrade when ready
(This may take several minutes)

Upgrade **Cancel**



Application Setup

Version #7.3

Migration code is running to update to the latest version. This may take several minutes or several hours depending on the database size.

Upgrade is in progress. Do not restart the application.

■

Status:Upgrading Schema - Executing Pre Upgrade.

- 11 When the upgrade is complete, click **Close**. This will automatically save the upgrade task.

IMPORTANT: On SLES 12 or SLES 12 SP1, after uninstalling Service Desk, reboot the device and then install Service Desk.



Application Setup

Version #7.3

Migration code is running to update to the latest version. This may take several minutes or several hours depending on the database size.

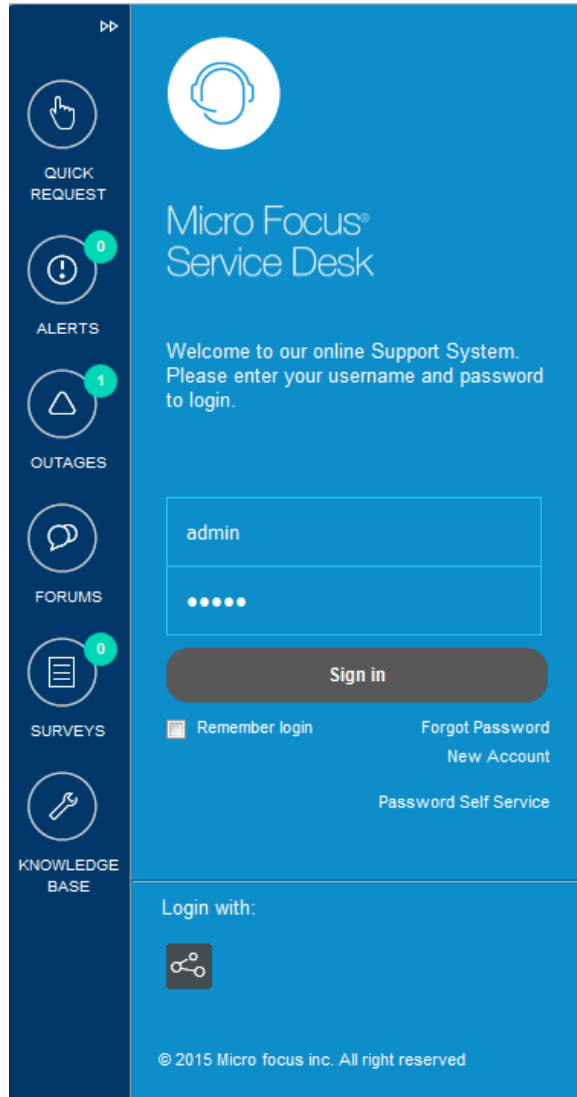
Upgrade is in progress. Do not restart the application.

Status: Upgrade task completed successfully.

Database has been successfully upgraded to Version #7.3

Close

12 Login to Micro Focus Service Desk by using the role credentials.



4.3 Post Upgrade

After you upgrade to Service Desk 7.4, ensure that you perform the following:

- ◆ Restore the Custom Banners at `<installation-location>/ServiceDesk/Server/webapps/LiveTime/images/banners/custom` in the Service Desk 7.4.
- ◆ Restore the Customized CSS file in the Service Desk 7.4 at `<installation-location>/ServiceDesk/LiveTime/Style/novell-7.0.css`

If you are upgrading from Service Desk 7.1, then customize the CSS in the Service Desk 7.4 again.

- ◆ If you have made any changes in the Tomcat server such as the `web.xml`, `server.xml` files, then update those changes.
- ◆ If you have made any changes in the Java such as the `catalina.sh` file, then update those changes.
- ◆ If you have configured SSL, then reconfigure the SSL settings.

5 Micro Focus Service Desk Appliance Deployment

Micro Focus Service Desk 7.4 is available as a virtual appliance that can be deployed to a supported virtual infrastructure. Micro Focus Service Desk Virtual Appliance (Micro Focus Service Desk Appliance) is built on the customized 64-bit Linux Just Enough Operating System (JeOS).

To deploy Micro Focus Service Desk Appliance, perform the tasks in the following sections:

- ◆ [Section 5.1, “Deploying the Appliance,” on page 29](#)
- ◆ [Section 5.2, “Configuring the Appliance Settings,” on page 30](#)

5.1 Deploying the Appliance

Before you begin to deploy Micro Focus Service Desk Appliance, perform the following tasks:

- 1 Ensure that the virtual machine to which you want to deploy Micro Focus Service Desk Appliance meet the requirements listed in [Section 2.2, “Micro Focus Service Desk Appliance Requirements,” on page 12](#).

- 2 Create a new virtual machine with the preinstalled Micro Focus Service Desk Appliance by importing the Micro Focus Service Desk Appliance image.

You can download the Micro Focus Service Desk Appliance image from the [Micro Focus Service Desk Download Site](#).

To import the Micro Focus Service Desk Appliance image to a virtual infrastructure:

- 2a Start the VMware VSphere Client application.
 - 2b Click **File > Deploy OVA Template** to launch the Deploy OVA Template Wizard.
 - 2c On the Source page, select one of the following options, then click **Next**.
 - ◆ **Select from file** to browse for and select the `.ova` file that contains the Micro Focus Service Desk Appliance image.
 - ◆ **Deploy from URL** to download the `.ova` file from the Web server.
 - 2d Follow the prompts to complete the deployment of the `.ova` file.
 - 2e After the deployment is complete, click **Done**.
- 3 (Optional) Take a snapshot of the virtual machine that you created in [Step 2](#).
 - 4 Power on the virtual machine on which you imported the Micro Focus Service Desk Appliance image.

The Configuration Wizard is launched automatically.

- 5 Continue with [Section 5.2, “Configuring the Appliance Settings,” on page 30](#).

5.2 Configuring the Appliance Settings

After importing the Micro Focus Service Desk Appliance image to your virtual machine, perform the following to configure Micro Focus Service Desk Appliance:

- 1 On the License Agreement page, accept the **End User License Agreement** and then click **Next**.
- 2 On the License Agreement page, accept the **SUSE License Agreement** and then click **Next**.
- 3 On the Language page, choose the required **Language** to install the Service Desk, then click **Next**.
- 4 On the Keyboard Language page, select the required **Language** to configure the Service Desk, then click **Next**.
- 5 On the System Keyboard Configuration page, configure the keyboard layout, then click **Next**.
- 6 On the Host and Domain page, specify the following information to access the Service Desk:
 - ♦ **Hostname:** The Fully Qualified Domain Name (FQDN) associated with the appliance IP address. For example, `server.domain.com`.
The hostname must be resolvable, or some features in Service Desk do not work properly. Server names must support the DNS requirements, or the Service Desk login fails. Acceptable characters are the letters a-z (uppercase and lowercase), numbers, and the hyphen (-).
 - ♦ **Domain Name:** .
- 7 On the Network Setup page, select the network setup, and then click **Next**.
- 8 On the Network Configuration page, select **Edit** to update network settings, and then click **Next**.
- 9 On the Clock and Timezone page, configure the time zone and clock settings to be used in your system, then click **Next**.
The configuration might take some time and the Appliance Main Menu screen is displayed.
- 10 On the Main Menu, select **Enter new root password (1)** to change the root password, specify **Root Password** and **Confirmation**.
You cannot configure Service Desk Appliance until you change the password.
- 11 Use the displayed Browser URL (`https://<FQDN>`) for administering the appliance and configuring Service Desk.

5.2.1 Starting and Stopping Service Desk using the Terminal

You can use the following commands to start, stop, and restart Service Desk services:

- ♦ `/etc/init.d/livetime start`
- ♦ `/etc/init.d/livetime stop`
- ♦ `/etc/init.d/livetime restart`

5.2.2 File location Details

The Appliance related files are available in the following location:

- ♦ Micro Focus Service Desk Installation: `/opt/novell/nsd/servicedesk/Server/webapps`
- ♦ Micro Focus Service Desk Resources Directory: `/LiveTime`

The log files are available in the following location:

- ♦ The location of `logging.properties` file which is used for changing the level of logging is:

/opt/novell/nsd/servicedesk/Server/webapps/LiveTime/WEB-INF/LiveTime.woa/
Contents/Resources/logging.properties

- ◆ **Micro Focus Service Desk Application related logs:** /LiveTime/Logs
- ◆ **Tomcat server related logs:** /opt/novell/nsd/servicedesk/Server/logs

6 Upgrading Micro Focus Service Desk Appliance

This chapter contains information about upgrading your existing implementation of Micro Focus Service Desk that runs on the appliance.

For upgrade information, see the following:

- ◆ [Section 6.1, “Pre-Upgrade,” on page 33](#)
- ◆ [Section 6.2, “Upgrading the Service Desk Appliance,” on page 34](#)
- ◆ [Section 6.3, “Post Upgrade,” on page 36](#)

IMPORTANT

- ◆ From Service Desk 7.3, the directory structure has been changed as follows:
 - ◆ Resource directory: `/LiveTime`
 - ◆ Application related logs: `/LiveTime/Logs`
 - ◆ Service Desk installation location: `/opt/novell/nsd/servicedesk`
 - ◆ Tomcat server related logs: `/opt/novell/nsd/servicedesk/Server/logs`
 - ◆ Terminal commands to Start and Stop the Service Desk 7.4 application:
 - ◆ `/etc/init.d/livetime start`
 - ◆ `/etc/init.d/livetime stop`
 - ◆ `/etc/init.d/livetime restart`
 - ◆ The “in-place upgrade” option is no longer supported.
 - ◆ Service Desk supports no more than two major versions behind the latest release (N-2). Since the latest version is Service Desk 7.4 (N) the 7.3 (N-1) and 7.2 (N-2) versions are also supported.
-

6.1 Pre-Upgrade

Prior to upgrading to Service Desk 7.4, ensure that you perform the following:

- ◆ If you are using Custom Banners in Micro Focus Service Desk, then back up the contents from `/usr/share/tomcat6/webapps/LiveTime/images/banners/custom` folder to an external storage.
- ◆ If you are using the Customized CSS and upgrading from Service Desk 7.2, then copy the CSS file located at `/LiveTime/Style/novell-7.0.css` to an external storage.
- ◆ If any configuration is changed in the Tomcat server such as the `web.xml`, `server.xml`, then ensure that you note the changes.
- ◆ If any configuration is changed in Java such as the `catalina.sh`, then ensure that you note the changes.
- ◆ If SSL is configured and you want to use the same certificates, then back up the certificates and keys.

- ♦ The network or DNS related configuration will not be migrated. Hence, you need to note the details.
- ♦ Ensure that you have a verified the backup of your existing appliance and the external database, if applicable.
- ♦ The `/Livetime` folder contains a few important files that need to be backed up.

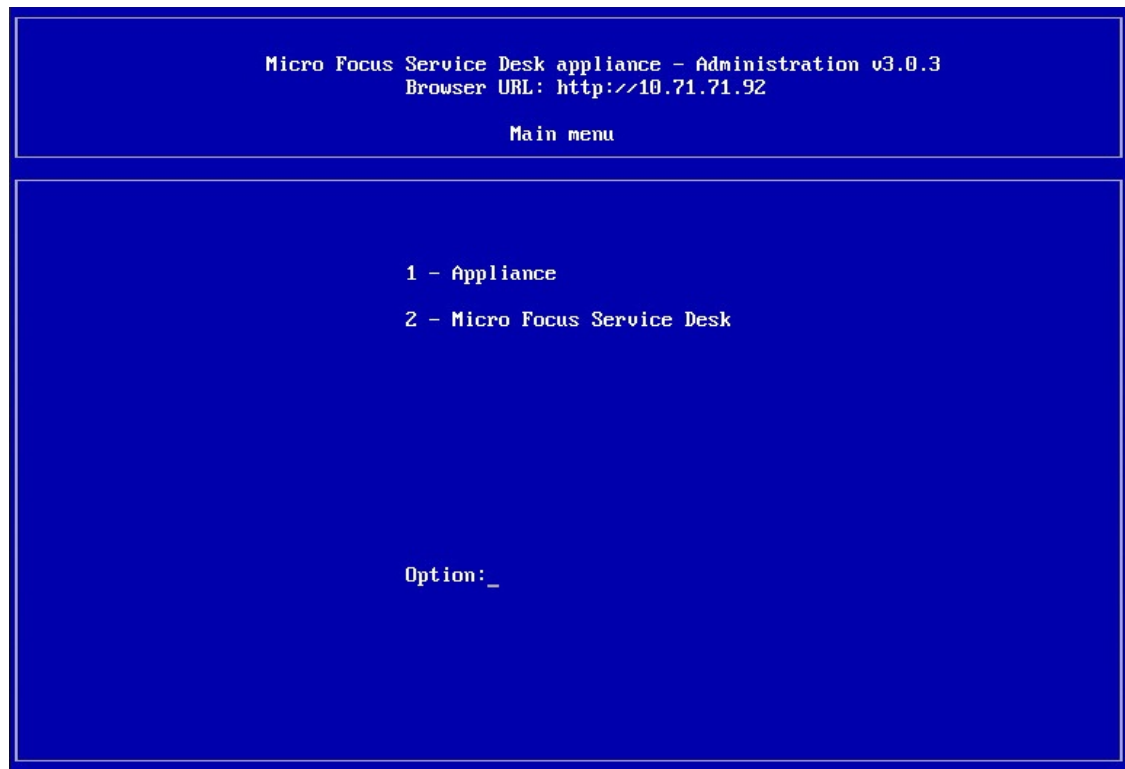
IMPORTANT: Service Desk supports no more than two major versions behind the latest release (N-2). Since the latest version is Service Desk 7.4 (N) the 7.3 (N-1) and 7.2 (N-2) versions are also supported.

6.2 Upgrading the Service Desk Appliance

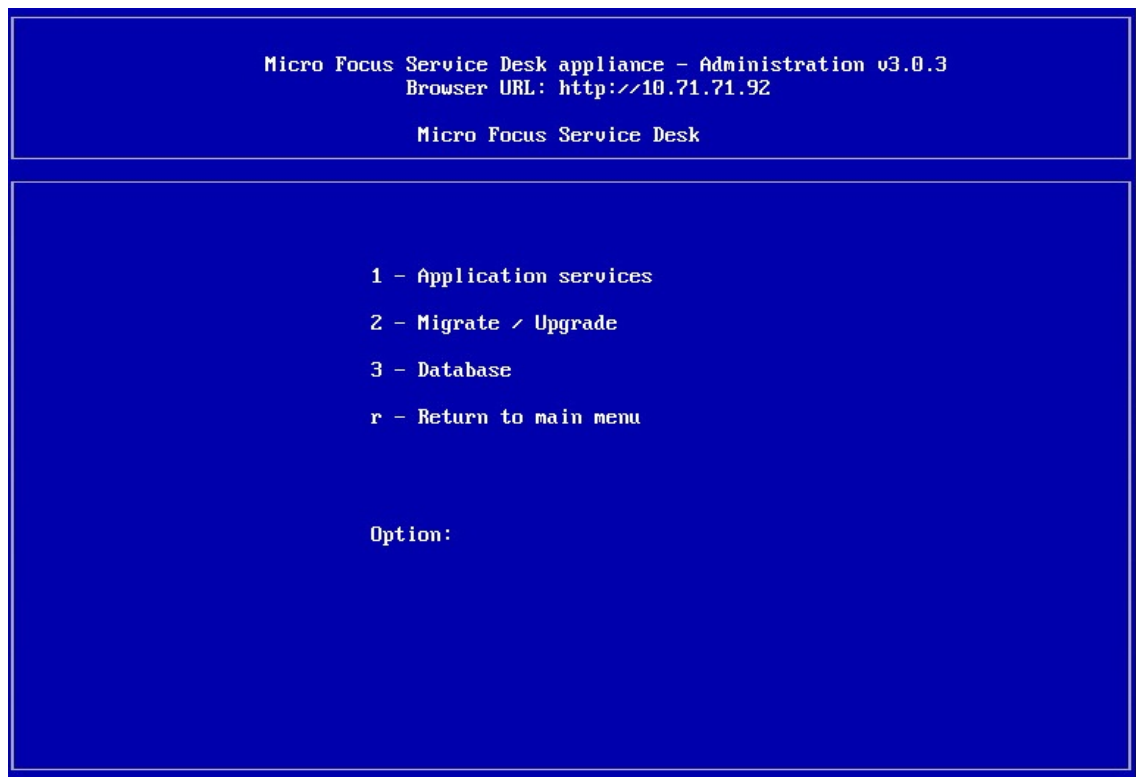
Service Desk Appliance will be upgraded by bringing the new appliance side-by-side. The Service Desk configuration and data is transferred to the new appliance which then becomes your production environment. Your old appliance is shutdown and no longer used.

To upgrade the Service Desk 7.4 Appliance:

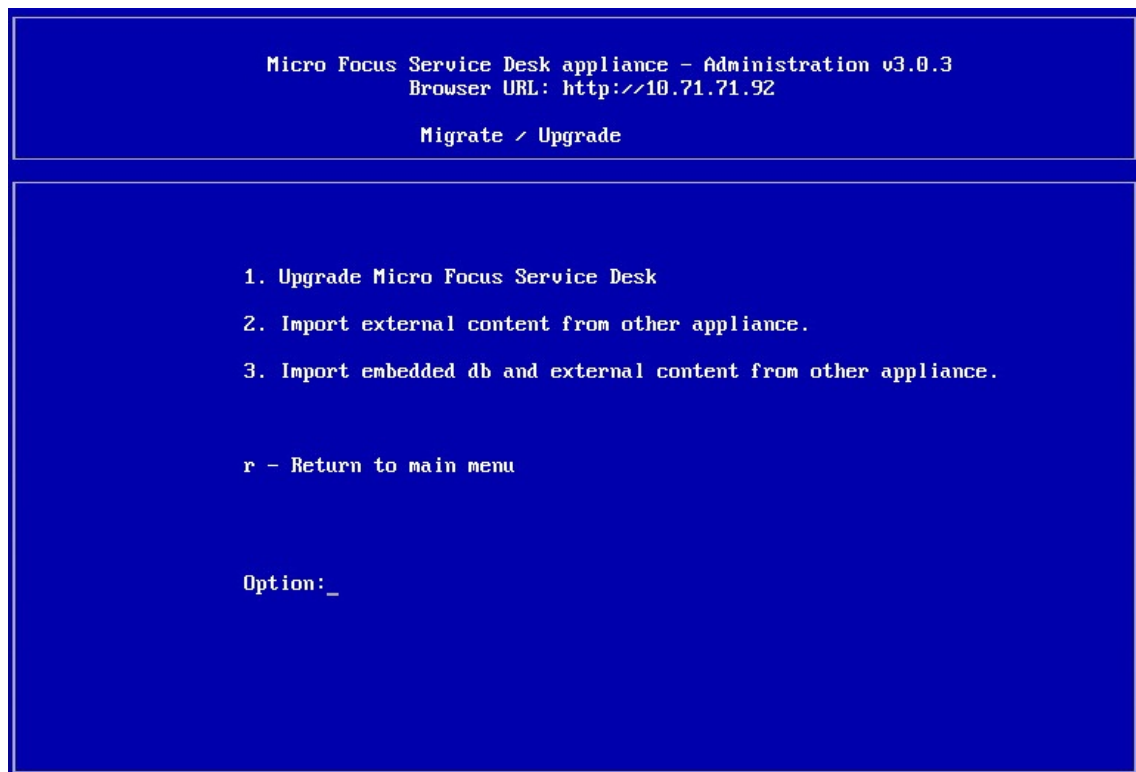
- 1 Deploy the Micro Focus Service Desk Appliance on a VMware ESX Server and configure the network.
- 2 Connect to the Micro Focus Service Desk Appliance by using the VMware ESX console.



- 3 In the Micro Focus Service Desk Appliance main menu, select **Micro Focus Service Desk**.



4 Select **Migrate/Upgrade**.



5 If you are using an external database, select **Import external content from other appliances**.

Take complete backup of the existing database. This helps you in reverting the appliance upgrade.

Or

If you are using the internal embedded database, select **Import embedded db and external content from other appliances**.

- 6 Enter the IP address of your existing Appliance Server.
- 7 Follow the instructions on the wizard by answering Yes to all questions.
- 8 Power off the existing Appliance Server.
- 9 After the upgrade is complete, connect to Micro Focus Service Desk Appliance 7.4 through a browser and enter your database connection details.

If you are using embedded database, the connection details are as follows:

Parameter	Value
Database Type	PostgreSQL
Server Host	127.0.0.1
Server Port	5432
Database	nsd
User name	nsd
Password	linux

- 10 Click **Test** to ensure that the database connection is correct.
- 11 Click **Advanced**.
- 12 Click **Upgrade** twice.
- 13 Click **Save** when the migration is complete.
A message informing you to enter a new license appears. You can find these details in NCC.
- 14 Configure the network settings and DNS in the Service Desk appliance again. These settings should match the previous server version.
- 15 Enable the Firewall settings (in the **Appliance Main Menu**, select **Alter Firewall Configuration**).
Ensure to select **Enable Firewall Automatic Starting**.

6.3 Post Upgrade

After you upgrade to Service Desk 7.4 Appliance, ensure that you perform the following:

- ♦ Restore the Custom Banners located at `/opt/novell/nsd/servicedesk/Server/webapps/LiveTime/images/banners/custom` in the Service Desk 7.4 Appliance.
- ♦ Restore the Customized CSS file in the Service Desk 7.4 Appliance located at `/LiveTime/Style/novell-7.0.css`

If you are upgrading from Service Desk 7.1, then you need to customize the CSS in Service Desk 7.4 again.

- ♦ If you have made any changes in the Tomcat server such as the `web.xml`, `server.xml` files, then update the changes.
- ♦ If you have made any changes in Java such as the `catalina.sh` file, then update the changes.

- ♦ If you have configured SSL, then reconfigure the SSL settings.
- ♦ Reconfigure the network or DNS settings.

To configure network settings, go to the **Appliance Main Menu** and select **Alter Network Configuration**.

7 Enabling HTTPS for Micro Focus Service Desk

This chapter contains information about enabling Hyper Text Transfer Protocol Secure (HTTPS) on Micro Focus Service Desk.

SSL is a protocol that provides security for communication between client and server by implementing encrypted data and certificate-based authentication. SSL is one of the most common ways of integrating secure communication on the Internet as it is a well-supported protocol.

HTTPS is a secure version of the Hyper Text Transfer Protocol (http). It is the result of layering HTTP on top of the SSL/TLS protocol, thus adding the security capabilities of SSL/TLS to standard HTTP communications. It uses public and private key pair to encrypt the data flow between client and server.

Enabling HTTPS on Micro Focus Service Desk:

In order to enable HTTPS protocol on Micro Focus Service Desk, you first need create a public and private key pair to be used for encryption.

Micro Focus Service Desk application can be installed on Windows or Linux platforms. It is also available as a virtual appliance.

You can enable HTTPS on the following platforms:

- ◆ [Section 7.1, “Enabling HTTPS on Windows devices,” on page 39](#)
- ◆ [Section 7.2, “Enabling HTTPS on Linux devices,” on page 41](#)
- ◆ [Section 7.3, “Enabling HTTPS on Appliance,” on page 42](#)
- ◆ [Section 7.4, “Enabling HTTPS on Appliance Prior to 7.3 Version,” on page 44](#)

7.1 Enabling HTTPS on Windows devices

To enable HTTPS on Windows devices, perform the following:

- 1 Generate a self-signed certificate:
 - 1a Launch the command prompt.
 - 1b Go to the Java installation path. For example, `C:\Program Files\Java\jdk1.7.0_55\bin>`
 - 1c Execute the `keytool -genkey -alias xxxx -keyalg RSA` command.
 - 1d Specify the password for keystore.
 - 1e Specify the hostname in the Fully Qualified Domain Name (FQDN) and organization details.
After executing the `keytool` command, the `keytool` generates a public key and private key pair and stores it in the `users` folder.
 - 1f Copy the keystore file from the `users` folder to the root of your hard drive.
Delete the `tcnative-1.dll` file from the `$ServiceDesk/Server/bin` folder to process the SSL requests.

2 Enable SSL for Service Desk:

- 2a To enable the SSL connection, enable HTTPS in the `server.xml` file located at `$ServiceDesk/Server/conf#`
- 2b Add the Keystore password in the `server.xml` file.

For the below example we have mentioned 'novell' as password. Remove the comment around node to enable SSL.

```
<!--
<Connector port="8443"
protocol="org.apache.coyote.http11.Http11NioProtocol"
    maxThreads="150" SSLEnabled="true" scheme="https" secure="true"
    clientAuth="false" sslProtocol="SSL" sslEnabledProtocols="TLSv1.2"
    KeystorePass="novell"
ciphers="TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,TLS_RSA_WITH_AES_128_GCM_SHA256,TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256,TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256,TLS_DHE_RSA_WITH_AES_128_GCM_SHA256,TLS_DHE_DSS_WITH_AES_128_GCM_SHA256,SSL_RSA_WITH_RC4_128_MD5,SSL_RSA_WITH_RC4_128_SHA,TLS_DHE_RSA_WITH_AES_256_CBC_SHA,TLS_DHE_RSA_WITH_AES_256_CBC_SHA256,TLS_DHE_DSS_WITH_AES_128_CBC_SHA,TLS_DHE_DSS_WITH_AES_128_CBC_SHA256,TLS_DHE_DSS_WITH_AES_256_CBC_SHA,TLS_DHE_DSS_WITH_AES_256_CBC_SHA256,TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA,TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA,TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384,TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA,TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256,TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA,TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384,TLS_ECDH_RSA_WITH_AES_128_CBC_SHA,TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256,TLS_ECDH_RSA_WITH_AES_256_CBC_SHA,TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384,TLS_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_AES_256_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA256" />
-->
```

3 Test the HTTPS URL.

The application should be able to run on HTTPS using the `https://localhost:8443` or `https://<IP address>:8443` URL.

4 Enable only HTTPS:

- 4a Stop the LiveTime services.
- 4b Open the `Web.xml` file located at `C:\Program Files\ServiceDesk\Server\conf` and add the following content before the `</web-app>` markup:

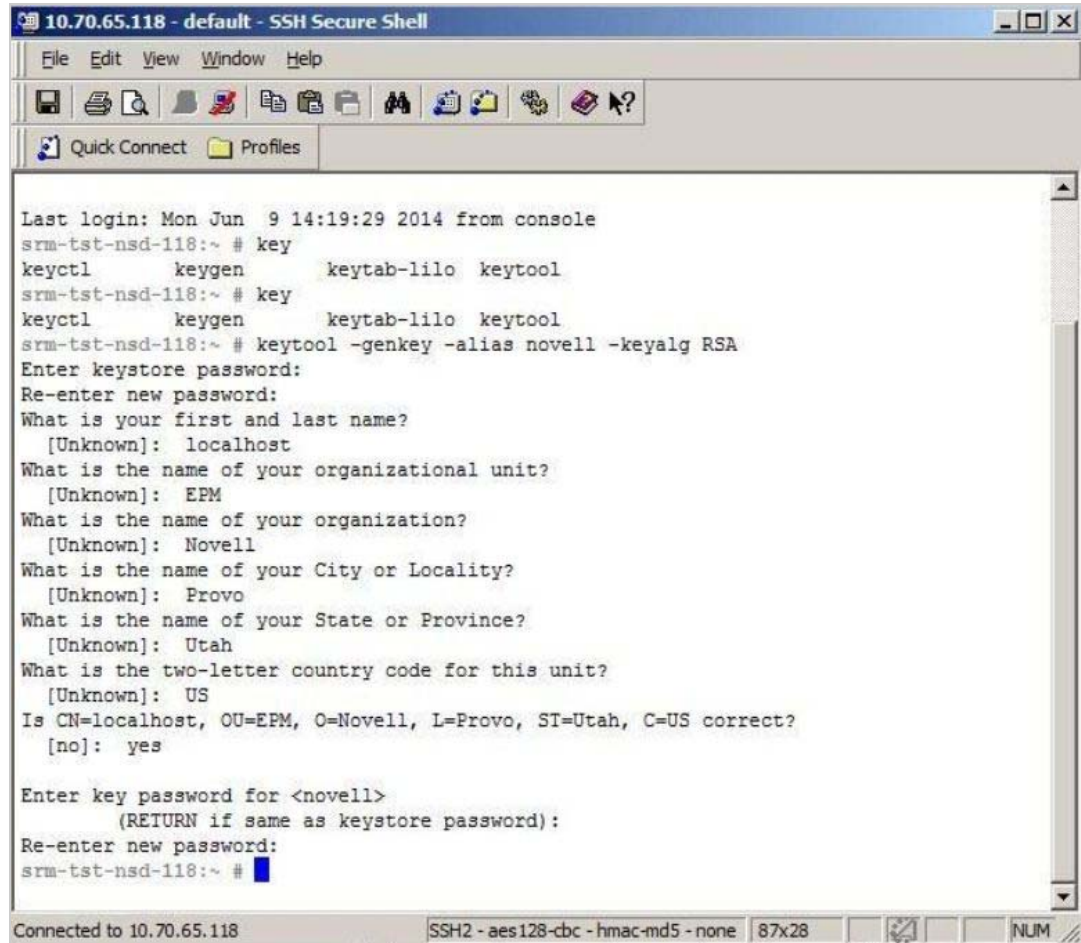
```
<security-constraint>
<web-resource-collection>
<web-resource-name>Protected Context</web-resource-name>
<url-pattern>/*</url-pattern>
</web-resource-collection>
<!--auth-constraint goes here if you require authentication-->
<user-data-constraint>
<transport-guarantee>CONFIDENTIAL</transport-guarantee>
</user-data-constraint>
</security-constraint>
```

5 Restart the services.

7.2 Enabling HTTPS on Linux devices

To enable HTTPS on Linux devices, perform the following:

- 1 Generate a self-signed certificate:
 - 1a Open the SSH Secure Shell and execute the `keytool` command.



```
10.70.65.118 - default - SSH Secure Shell
File Edit View Window Help
Quick Connect Profiles

Last login: Mon Jun  9 14:19:29 2014 from console
srm-tst-nsd-118:~ # key
keyctl      keygen      keytab-lilo keytool
srm-tst-nsd-118:~ # key
keyctl      keygen      keytab-lilo keytool
srm-tst-nsd-118:~ # keytool -genkey -alias novell -keyalg RSA
Enter keystore password:
Re-enter new password:
What is your first and last name?
[Unknown]: localhost
What is the name of your organizational unit?
[Unknown]: EPM
What is the name of your organization?
[Unknown]: Novell
What is the name of your City or Locality?
[Unknown]: Provo
What is the name of your State or Province?
[Unknown]: Utah
What is the two-letter country code for this unit?
[Unknown]: US
Is CN=localhost, OU=EPM, O=Novell, L=Provo, ST=Utah, C=US correct?
[no]: yes

Enter key password for <novell>
(RETURN if same as keystore password):
Re-enter new password:
srm-tst-nsd-118:~ #
```

- 1b Specify the password for keystore.
- 1c Specify the hostname name in the Fully Qualified Domain Name (FQDN) and organization details.

After executing the `keytool` command, the `keytool` generates a public key and private key pair and stores it in the `keystore` file located at `jre/lib/security/cacerts`.

The certificates need to be signed by a Certificate Authority to add into the trusted store.

- 2 Enable SSL for Service Desk:
 - 2a To enable SSL connection, enable HTTPS in the `server.xml` file located at `/usr/local/ServiceDesk/Server/conf#`.
 - 2b Add the Keystore password in the `server.xml` file.

For the below example we have mentioned 'novell' as password. Remove the comment around node to enable SSL.

```
<!--
```

```

<Connector port="8443"
protocol="org.apache.coyote.http11.Http11NioProtocol"

  maxThreads="150" SSLEnabled="true" scheme="https" secure="true"

  clientAuth="false" sslProtocol="SSL" sslEnabledProtocols="TLSv1.2"

  KeystorePass="novell"
ciphers="TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,TLS_RSA_WITH_AES_128_GCM_SHA256,TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256,TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256,TLS_DHE_RSA_WITH_AES_128_GCM_SHA256,TLS_DHE_DSS_WITH_AES_128_GCM_SHA256,SSL_RSA_WITH_RC4_128_MD5,SSL_RSA_WITH_RC4_128_SHA,TLS_DHE_RSA_WITH_AES_256_CBC_SHA,TLS_DHE_RSA_WITH_AES_256_CBC_SHA256,TLS_DHE_DSS_WITH_AES_128_CBC_SHA,TLS_DHE_DSS_WITH_AES_128_CBC_SHA256,TLS_DHE_DSS_WITH_AES_256_CBC_SHA,TLS_DHE_DSS_WITH_AES_256_CBC_SHA256,TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA,TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA,TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384,TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA,TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256,TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA,TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384,TLS_ECDH_RSA_WITH_AES_128_CBC_SHA,TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256,TLS_ECDH_RSA_WITH_AES_256_CBC_SHA,TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384,TLS_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_AES_256_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA256" />
-->

```

2c Save and restart the server.

3 Test the HTTPS URL.

The application should be able to run on HTTPS using the `https://localhost:8443` or `https://<IP address>:8443` URL.

4 Enable only HTTPS:

4a Stop the LiveTime services.

4b Open the `web.xml` file located at `usr/local/ServiceDesk/Server/conf` and add the following content before the `</web-app>` markup:

```

<security-constraint>
<web-resource-collection>
<web-resource-name>Protected Context</web-resource-name>
<url-pattern>/*</url-pattern>
</web-resource-collection>
<!--auth-constraint goes here if you require authentication-->
<user-data-constraint>
<transport-guarantee>CONFIDENTIAL</transport-guarantee>
</user-data-constraint>
</security-constraint>

```

5 Restart the services.

7.3 Enabling HTTPS on Appliance

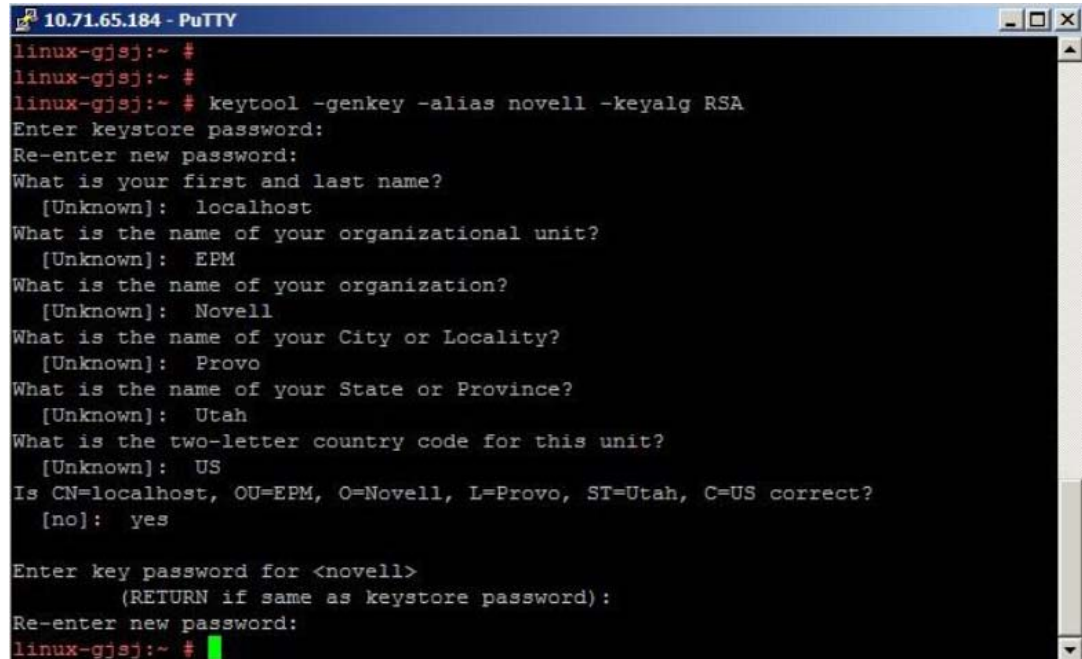
To enable HTTPS on Appliance, perform the following:

1 Generate a self-signed certificate:

1a Open the SSH Secure Shell and execute the `keytool` command.

1b Go to the Java installed path.

- 1c Execute the `keytool -genkey -alias xxxx -keyalg RSA` command.



```
10.71.65.184 - PuTTY
linux-gjsj:~ #
linux-gjsj:~ #
linux-gjsj:~ # keytool -genkey -alias novell -keyalg RSA
Enter keystore password:
Re-enter new password:
What is your first and last name?
  [Unknown]: localhost
What is the name of your organizational unit?
  [Unknown]: EPM
What is the name of your organization?
  [Unknown]: Novell
What is the name of your City or Locality?
  [Unknown]: Provo
What is the name of your State or Province?
  [Unknown]: Utah
What is the two-letter country code for this unit?
  [Unknown]: US
Is CN=localhost, OU=EPM, O=Novell, L=Provo, ST=Utah, C=US correct?
  [no]: yes

Enter key password for <novell>
  (RETURN if same as keystore password):
Re-enter new password:
linux-gjsj:~ #
```

- 1d Specify the password for keystore.

- 1e Specify the hostname name in the Fully Qualified Domain Name (FQDN) and organization details.

After executing the `keytool` command, the `keytool` generates a public key and private key pair and stores it in the keystore file located at `/usr/java/jdk1.8.0_91/jre/lib/security`.

The certificates need to be signed by a Certificate Authority to add into the trusted store.

- 2 Enable the SSL for Service Desk:

- 2a To enable SSL connection, enable HTTPS in the `server.xml` file located at `/opt/novell/nsd/ServiceDesk/Server/conf`.

- 2b Add the Keystore password in the `server.xml` file.

For the below example we have mentioned 'novell' as password. Remove the comment around node to enable SSL.

```
<!--
<Connector port="8443"
protocol="org.apache.coyote.http11.Http11NioProtocol"
  maxThreads="150" SSLEnabled="true" scheme="https" secure="true"
  clientAuth="false" sslProtocol="SSL" sslEnabledProtocols="TLSv1.2"
  KeystorePass="novell"
ciphers="TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,TLS_RSA_WITH_AES_128_GCM_SHA256,TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256,TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256,TLS_DHE_RSA_WITH_AES_128_GCM_SHA256,SSL_RSA_WITH_RC4_128_MD5,SSL_RSA_WITH_RC4_128_SHA,TLS_DHE_RSA_WITH_AES_256_CBC_SHA,TLS_DHE_RSA_WITH_AES_256_CBC_SHA256,TLS_DHE_DSS_WITH_AES_128_CBC_SHA,TLS_DHE_DSS_WITH_AES_128_CBC_SHA256,TLS_DHE_DSS_WITH_AES_256_CBC_SHA,TLS_DHE_DSS_WITH_AES_256_CBC_SHA256,TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA,TLS_ECDHE_ECDSA_WITH_AES_128_CB
```

```
C_SHA256,TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA,TLS_ECDHE_ECDSA_WITH_AES_256
_CBC_SHA384,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_128
_CBC_SHA256,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_256_C
BC_SHA384,TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA,TLS_ECDH_ECDSA_WITH_AES_128
_CBC_SHA256,TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA,TLS_ECDH_ECDSA_WITH_AES_256
_CBC_SHA384,TLS_ECDH_RSA_WITH_AES_128_CBC_SHA,TLS_ECDH_RSA_WITH_AES_128_CB
C_SHA256,TLS_ECDH_RSA_WITH_AES_256_CBC_SHA,TLS_ECDH_RSA_WITH_AES_256_CBC_S
HA384,TLS_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA
_WITH_AES_256_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA256" />
-->
```

2c Save and restart the server.

3 Test the HTTPS URL.

The application should be able to run on HTTPS using the `https://localhost:8443` or `https://<IP address>:8443` URL.

4 Enable only HTTPS:

4a Stop the LiveTime services.

4b Open the `web.xml` file located at `/opt/novell/nsd/servicedesk/server/conf` and add the following content before the closing of `</web-app>` markup:

```
<security-constraint>
<web-resource-collection>
<web-resource-name>Protected Context</web-resource-name>
<url-pattern>/*</url-pattern>
</web-resource-collection>
<!--auth-constraint goes here if you require authentication-->
<user-data-constraint>
<transport-guarantee>CONFIDENTIAL</transport-guarantee>
</user-data-constraint>
</security-constraint>
```

5 Restart the services.

7.4 Enabling HTTPS on Appliance Prior to 7.3 Version

To enable HTTPS for Service Desk Appliance prior to 7.3 version:

In this scenario, `openssl` command is used to generate a key pair. See the following to generate key using the `openssl` command. SSH into appliance and login as root.

1 Copy all the certificates and keys into a single directory.

```
srn-tst-nsd-130:~ # mkdir /root/CA
srn-tst-nsd-130:~ # chmod 770 /root/CA/
srn-tst-nsd-130:~ # cd /root/CA/
```

2 Create a private key and then generate a certificate request

```
srn-tst-nsd-130:~/CA # openssl genrsa -des3 -out nsd-ca.key 2048
Generating RSA private key, 2048 bit long modulus
.....+++
.....+++ e is 65537
(0x10001)
```

```
Enter pass phrase for nsd-ca.key:
Verifying - Enter pass phrase for nsd-ca.key:
srm-tst-nsd-130:~/CA #
```

3 Generate a self-signed root certificate from the generated private key

```
srm-tst-nsd-130:~/CA # openssl req -new -x509 -days 3650 -key nsd-ca.key -out
nsd-ca.crt
```

Specify pass phrase for nsd-ca.key:

Specify information that will be incorporated into your certificate request. Information includes Distinguished Name or a DN and a few mandatory fields.

For a few fields there will be a default value, If you enter '.', the field will be left blank.

Country Name (2 letter code) [AU]:

State or Province Name (full name) [Some-State]: Locality Name (eg, city) []:

Organization Name (eg, company) [Internet Widgits Pvt Ltd]: Organizational Unit Name (eg, section) []:

Common Name (eg, YOUR name) []:

Email Address []:

4 Creation of key and certificate for the web server:

```
srm-tst-nsd-130:~/CA # openssl genrsa -des3 -out nsd-server.key 1024
```

Generating RSA private key, 1024 bit long modulus

.....+++++

.....+
++++ e is 65537

(0x10001)

Enter pass phrase for nsd-server.key:

Verifying - Enter pass phrase for nsd-server.key:

5 Creation of Certificate for web server:

```
srm-tst-nsd-130:~/CA # openssl req -new -key nsd-server.key -out nsd-server.csr
```

Specify pass phrase for nsd-server.key:

Specify information that will be incorporated into your certificate request. Information includes Distinguished Name or a DN and a few mandatory fields.

For a few fields there will be a default value, If you enter '.', the field will be left blank.

Country Name (2 letter code) [AU]:

State or Province Name (full name) [Some-State]: Locality Name (eg, city) []:

Organization Name (eg, company) [Internet Widgits Pty Ltd]: Organizational Unit Name (eg, section) []:

Common Name (eg, YOUR name) []: Email Address []:

Specify additional attributes to be sent with your certificate request.

A change password []:

An optional company name []:

6 Use of our CA to sign our key:

```

srm-tst-nsd-130:~/CA # openssl x509 -req -in nsd-server.csr -out nsd-server.crt
-shal -CA
nsd-ca.crt -CAkey nsd-ca.key -CAcreateserial -days 3650
Signature ok
subject=/C=US/ST=Utah/L=provo/O=novell/OU=epm/CN=srm-tst-nsd-
130.epm.blr.novell.com/emailAddress=ybellur@novell.com
Getting CA Private Key
Specify pass phrase for nsd-ca.key:
srm-tst-nsd-130:~/CA #

```

- 7 Take out the pass phrase from key or specify pass phrase every time whenever Apache is started. To specify pass phrase, Apache only gives you a few seconds to perform before terminating in a bulk.

```

srm-tst-nsd-130:~/CA # openssl rsa -in nsd-server.key -out nsd-server-npp.key
Specify pass phrase for nsd-server.key: writing RSA key
srm-tst-nsd-130:~/CA #

```

Configuring Apache for SSL Connection

- 1 Move the new keys generated to the proper directories in the apache folder /etc/apache2.

```

srm-tst-nsd-130:~/CA # cp nsd-server.crt /etc/apache2/ssl.crt/nsd-ssl.crt
srm-tst-nsd-130:~/CA # cp nsd-server-npp.key /etc/apache2/ssl.key/nsd-ssl.key
srm-tst-nsd-130:~/CA # cp nsd-ca.crt /etc/apache2/ssl.crt/nsd-ca.crt

```

- 2 Launch the text editor to create a virtual host configuration file or you can use the SSH file transfer to edit the file and copy the edited file back to the same location.

```

srm-tst-nsd-130:~/CA # cd /etc/apache2/vhosts.d/
srm-tst-nsd-130:/etc/apache2/vhosts.d # vi nsd-ssl-vhost.conf

```

- 3 Paste the following into the file

```

<IfDefine SSL>
<IfDefine !NOSSL>

<VirtualHost *:443>
#Setup SSL for this virtual host SSL engine on
SSLCipherSuite
ALL:!ADH:!EXPORT56:RC4+RSA:+HIGH:+MEDIUM:+LOW:+SSLv2:+EXP:+eNULL
SSLCertificateFile /etc/apache2/ssl.crt/nsd-ssl.crt
SSLCertificateKeyFile /etc/apache2/ssl.key/nsd-ssl.key
SSLCertificateChainFile /etc/apache2/ssl.crt/nsd-ca.crt
SSLCACertificateFile /etc/apache2/ssl.crt/nsd-ca.crt
SSLProtocol all -SSLv2 -SSLv3
#Fix for IE browsers when using SSL with Apache
SetEnvIf User-Agent ".*MSIE.*" \
nokeepalive ssl-unclean-shutdown \
downgrade-1.0 force-response-1.0
#Custom log file

```

```

CustomLog /var/log/apache2/ssl_request_log ssl_combined
#Apache sends incoming request to Tomcat
JkLogFile "/var/log/tomcat6/mod_jk.log"
    JkLogLevel error
Alias /WebObjects/LiveTime.woa/Contents/WebServerResources/
"/srv/tomcat6/webapps/LiveTime/WEB-INF/LiveTime.woa/Contents/
WebServerResources/"
JkMount /LiveTime/* ajp13
# do not loose time with IP address lookups
    HostnameLookups Off
# needed for named virtual hosts
    UseCanonicalName Off
<IfModule mod_rewrite.c>
    RewriteEngine On
RewriteRule ^/$ /LiveTime/WebObjects/LiveTime.woa [R]
</IfModule>
<Directory />
Options Indexes FollowSymLinks
    AllowOverride None
</Directory>
<FilesMatch \.(?:gif|jpe?g|png|js)$>
Order allow,deny
Allow from all
</FilesMatch>
</VirtualHost>
</IfDefine>
</IfDefine>

```

4 Save the file by pressing ESC and then tpying :wq

5 Apache web server requires a start up flag passing to it to enable SSL. This is available in the apache configuration file located at /etc/sysconfig

```
srm-tst-nsd-130:/ # vi /etc/sysconfig/apache2
```

6 Scroll down the file to find the following line:

```
APACHE_SERVER_FLAGS=""
```

7 Change the APACHE_SERVER_FLAGS="" to APACHE_SERVER_FLAGS="SSL"

8 Save the file by pressing ESC and then tpying :wq

9 Restart the apache server:

```
rcapache2 restart
```

10 Launch your browser at Service Desk Appliance.



Micro Focus Service Desk Web Server SSL Certificate Installation

This chapter contains information about installing Secure Sockets Layer (SSL) certificates to the Keystore, configuring the SSL Connector, and migrating the external certificates.

For information, see the following:

- ◆ [Section 8.1, “Generating the Certificate Signing Request,” on page 49](#)
- ◆ [Section 8.2, “Installing the SSL Certificates to the Keystore,” on page 49](#)
- ◆ [Section 8.3, “Configuring the SSL Connector,” on page 50](#)
- ◆ [Section 8.4, “Migrating the External Certificates,” on page 51](#)

8.1 Generating the Certificate Signing Request

To generate the Certificate Signing Request (CSR):

- 1 Create a keystore, using the following command:

```
keytool -genkey -alias nsdserver -keyalg RSA -keysize 2048 -keystore  
nsdserver.jks -dname "CN=srm-tst-nsd.zenworkslabs.com,OU=EPM, O=MicroFocus  
Inc., L=provo, ST=Utah, C=US"
```

- 2 Generate the CSR, using the following command:

```
keytool -certreq -alias nsdserver -file srm-tst-nsd_zenworkslabs_com.csr -  
keystore nsdserver.jks
```

The certificates need to be signed by a Certificate Authority (CA) to add into the trusted store.

- 3 Save the signed certificate into a local drive or you can also save the certificates by creating a folder under `\LiveTime\SS` it will be easy to back up while upgrading to major versions of Service Desk.

8.2 Installing the SSL Certificates to the Keystore

Navigate to the folder where all the certificates have been placed and ensure that `%JAVA_HOME%` is added as path under environment variable.

We have used the root certificate, intermediate certificate, and the server certificate. If your certificate is signed from the Root Authority, then do not run the intermediate certificate command. In this installation, we have used intermediate certificate.

To install the SSL certificate to keystore:

- 1 Install the SSL Certificate (root) file to your keystore using the following command:

```
C:\>keytool -importcert -keystore nsdserver.jks -alias root -file root.cer
```

- 2 Choose **Y** or **Yes** to trust the certificate.

- 1 Install the SSL Certificate (intermediate) file to your keystore using the following command:

```
C:\>keytool -importcert -keystore nsdserver.jks -alias nsdroot -file
1_root_bundle.crt
```

2 Choose **Y** or **Yes** to trust the certificate.

1 Install the SSL Certificate (server) file to your keystore using the following command:

```
C:\>keytool -importcert -keystore nsdserver.jks -alias nsdserver -trustcacerts
-file 2_srm-tst- nsd.zenworkslabs.com.crt
```

The **Certificate reply was installed in keystore** message is displayed.

2 Choose **Y** or **Yes** to trust the certificate.

3 Use the keystore file (*your_site_name.jks*) to configure your server.

8.3 Configuring the SSL Connector

Before Service Desk can accept secure connections, configure the SSL Connector.

To configure the SSL Connector:

1 In a text editor, open the `server.xml` file.

- ◆ **Windows:** `C:\Program Files\ServiceDesk\Server\conf`
- ◆ **Linux:** `/usr/local/ServiceDesk/Server/Conf`
- ◆ **Appliance:** `/opt/novell/nsd/servicedesk/Server/conf`

2 In the `server.xml` file, locate the connector that you want to use the new keystore to secure.

3 Specify the keystore file name and password in your connector configuration.

Below is an illustration of how the connector should look.

```
<!--
<Connector port="8443" protocol="org.apache.coyote.http11.Http11NioProtocol"
keystoreFile="C:\...\<filename>.jks"
maxThreads="150" SSLEnabled="true" scheme="https" secure="true"
clientAuth="false" sslProtocol="SSL" sslEnabledProtocols="TLSv1.2"
KeystorePass="novell"
ciphers="TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_RSA_WITH_AES_128_GC
M_SHA256,TLS_RSA_WITH_AES_128_GCM_SHA256,TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA25
6,TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256,TLS_DHE_RSA_WITH_AES_128_GCM_SHA256,TLS
_DHE_DSS_WITH_AES_128_GCM_SHA256,SSL_RSA_WITH_RC4_128_MD5,SSL_RSA_WITH_RC4_128
_SHA,TLS_DHE_RSA_WITH_AES_256_CBC_SHA,TLS_DHE_RSA_WITH_AES_256_CBC_SHA256,TLS_
DHE_DSS_WITH_AES_128_CBC_SHA,TLS_DHE_DSS_WITH_AES_128_CBC_SHA256,TLS_DHE_DSS_W
ITH_AES_256_CBC_SHA,TLS_DHE_DSS_WITH_AES_256_CBC_SHA256,TLS_ECDHE_ECDSA_WITH_A
ES_128_CBC_SHA,TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_ECDSA_WITH_AE
S_256_CBC_SHA,TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384,TLS_ECDHE_RSA_WITH_AES_1
28_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_RSA_WITH_AES_256_CB
C_SHA,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384,TLS_ECDH_ECDSA_WITH_AES_128_CBC_SH
A,TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256,TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA,T
LS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384,TLS_ECDH_RSA_WITH_AES_128_CBC_SHA,TLS_EC
DH_RSA_WITH_AES_128_CBC_SHA256,TLS_ECDH_RSA_WITH_AES_256_CBC_SHA,TLS_ECDH_RSA_
WITH_AES_256_CBC_SHA384,TLS_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_128_CBC_
SHA256,TLS_RSA_WITH_AES_256_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA256"/>
-->
```

4 Save and restart the Service Desk services.

8.4 Migrating the External Certificates

To migrate the external certificates on Service Desk from an earlier version to the latest version:

- 1 Back up the `Keystore`, CSR, and the certificates signed by the CA which includes the root certificate, intermediate certificate, and your server certificate.
- 2 Back up the `server.xml` file and paste the changes which was done in the previous release to the latest version of Service Desk `server.xml` file.
- 3 Upgrade to latest version of Service Desk.
For information, see [Chapter 4, "Upgrading the Micro Focus Service Desk," on page 19](#).
- 4 Place the `keystore` file, CSR, and certificates in the same location after upgrade.
- 5 Update the `server.xml` file for SSL which was done pre-upgrade.
- 6 Restart the Service Desk services and check the HTTPS connection.

8.4.1 Migrating the External Certificates from Service Desk 7.2 or earlier Appliance Versions

To migrate the external certificates from Service Desk 7.2 or earlier appliance versions:

- 1 Back up the following files from the old appliance and the CA provider:
 - ♦ `server.key`
 - ♦ `server.cer` (or other base-64 format)
 - ♦ `intermediate.cer / subca.cer`
 - ♦ `rootca.cer`
- 2 Copy the `server.key`, `server.cer`, `intermediate.cer` `subca.cer`, and `rootca.cer` files to the new appliance.
- 3 Run the following command to combine the intermediate and rootca certificate files:

```
cat intermediate.cer rootca.cer > ca-certs.cer
```
- 4 Run the following command to create a PKCS12 keystore based on the existing key and certificates:

```
openssl pkcs12 -export -in server.cer -inkey server.key -chain -CAfile ca-certs.cer -name "my-domain.com" -out servicedesk.p12
```

IMPORTANT: Ensure to use a password to protect the keystore.

- 5 Run the following command to convert the PKCS12 keystore to a Java keystore:

```
keytool -importkeystore -destkeystore servicedesk.jks -srckeystore servicedesk.p12 -srcstoretype PKCS12
```
- 6 Configure the `server.xml` to point to `servicedesk.jks` as specified in the [Section 8.3, "Configuring the SSL Connector," on page 50](#).

