

Service Desk 23.4

Service Desk Appliance Deployment and Administration Reference

October 2023

Legal Notice

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/en-us/legal>.

© Copyright 2008 - 2023 Open Text

The only warranties for products and services of Micro Focus and its affiliates and licensors (“Open Text”) are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Micro Focus shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

About This Guide

This *Service Desk Appliance Deployment and Administration Reference* helps you to deploy and configure Service Desk Appliance to the Service Desk supported virtual infrastructure.

The information in this guide is organized as follows:

- ♦ [Chapter 1, “Overview,” on page 7](#)
- ♦ [Chapter 2, “System Requirements,” on page 9](#)
- ♦ [Chapter 3, “Appliance Deployment,” on page 11](#)
- ♦ [Chapter 4, “Migrating the Appliance,” on page 13](#)
- ♦ [Chapter 5, “Appliance Management,” on page 15](#)
- ♦ [Chapter 6, “System Management,” on page 27](#)
- ♦ [Chapter 7, “Disaster Preparedness and Recovery,” on page 33](#)

Audience

This guide is intended for Service Desk 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

Service Desk is supported by other documentation (in both PDF and HTML formats) that you can use to learn about and implement the product. For additional documentation, see the [Service Desk Documentation site](#).

Contents

About This Guide	3
1 Overview	7
2 System Requirements	9
2.1 System Integration.....	10
3 Appliance Deployment	11
4 Migrating the Appliance	13
4.1 Migrating from ZENworks Service Desk 8.3.x	13
4.2 Migrating from ZENworks Service Desk 23.3.....	13
4.2.1 Pre Migrate	13
4.2.2 Migration.....	14
4.2.3 Post Migrate	14
5 Appliance Management	15
5.1 Ganglia Configuration	15
5.1.1 Enabling Ganglia Monitoring.....	16
5.2 Ganglia Monitoring	17
5.3 Network	17
5.4 Time	17
5.5 Digital Certificates	18
5.5.1 Using the Digital Certificate Tool	18
5.5.2 Using an Existing Certificate and Key Pair.....	19
5.5.3 Activating the Certificate	19
5.5.4 Managing Certificates	20
5.5.5 Renewing Certificates.....	20
5.5.6 Service Desk Ciphers	21
5.6 Storage	22
5.7 System Services	22
5.7.1 Starting, Stopping, or Restarting System Services	23
5.7.2 Setting System Services to Automatic or Manual	23
5.8 Firewall.....	23
5.9 Administrative Passwords.....	23
5.10 Online Update	24
5.11 Shutting Down and Restarting Service Desk Appliance	25
6 System Management	27
6.1 Configuration	27
6.2 Terminal and File Explorer.....	28
6.2.1 Terminal.....	28

6.2.2	File Explorer	29
6.3	Logs	30
6.4	Configuring Service Desk	31
7	Disaster Preparedness and Recovery	33
7.1	Disaster Preparedness	33
7.1.1	External Database	33
7.1.2	Embedded Database	34
7.2	Disaster Recovery	34

1 Overview

Service Desk is available as a virtual Appliance that can be deployed to a supported virtual infrastructure. Service Desk Appliance is built on a customized SUSE Linux Enterprise Server (SLES), and comes pre-installed with Service Desk and thus helps save on operating system license costs.

After deployment, Service Desk can be configured by using an easy to use web based Console. Also, the same console can be used to maintain Service Desk Appliance and perform basic tasks such as executing commands, starting and stopping services, viewing logs, uploading, and downloading files.

You can also tweak basic server settings and monitor the server performance. With the new Service Desk Appliance, it is significantly easier to move to a new major version of Service Desk.

Appliance supports `root` and `sdadmin` users who have access to the following privileges:

- ◆ **Appliance Configuration**
 - ◆ Ganglia Configuration
 - ◆ Ganglia Monitoring
 - ◆ Network (root only)
 - ◆ Time (root only)
 - ◆ Digital Certificates (root only)
 - ◆ Storage (root only)
 - ◆ System Services
 - ◆ Firewall (root only)
 - ◆ Administrative Passwords
 - ◆ Online Update
 - ◆ Shutting Down and Restarting Service Desk Appliance
- ◆ **Service Desk Appliance**
 - ◆ Terminal and File Explorer
 - ◆ Logs
 - ◆ Service Desk Configuration
 - ◆ Technician Portal
 - ◆ Customer Portal
 - ◆ Online Update
 - ◆ Shutting Down and Restarting Service Desk Appliance

2 System Requirements

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

Table 2-1 Service Desk Appliance Requirements

Item	Requirements
Hypervisor	<p>Service Desk Virtual Appliance can be deployed in the following virtual machine environments:</p> <ul style="list-style-type: none">◆ VMware ESXi 6.x◆ SUSE XEN on SLES 12 SP4, SLES 12 SP5, SLES 15, SLES 15 SP1◆ Microsoft Hyper-V Windows 10.0◆ Citrix XenCenter 8.0
Virtual Machine Configuration	<p>Service Desk Appliance requires the following minimum configuration that have been preconfigured by default:</p> <ul style="list-style-type: none">◆ RAM: 4 GB minimum◆ Disk Space: 40 GB minimum◆ CPU Cores: 2 <p>Service Desk requires two hard disks. One hard disk of size 40 GB is pre-configured with the Appliance that uses the SLES 12 SP5 operating system and the other hard disk of minimum size 15 GB should be added for the Service Desk data.</p> <p>Depending on your requirement, you can increase the pre-configured disk space after deploying Service Desk Appliance.</p>
IP Address	<p>The server must have a static IP address or a permanently leased DHCP address.</p>
Database	<p>Service Desk Appliance comes with pre-installed PostgreSQL database. However, you can choose the other supported database and that must meet the database requirements.</p> <p>For more information, see Database Support in the ZENworks Service Desk Platform Support Matrix</p>
Administration Browser	<p>The following are supported web browsers for the Appliance console:</p> <ul style="list-style-type: none">◆ Latest versions of Google Chrome◆ Latest versions of Mozilla Firefox◆ Latest versions of Microsoft EDGE

Item	Requirements
Supported Languages	These are the supported languages for the Appliance console: <ul style="list-style-type: none">◆ English - en◆ French - fr◆ German - de◆ Italian - it◆ Polish - pl◆ Spanish - es

2.1 System Integration

ZENworks Service Desk supports integration with the supported releases of ZENworks Configuration Management.

3 Appliance Deployment

Fresh deployment of ZENworks Service Desk 23.4 is not supported. However, you can deploy ZENworks Service Desk 8.3.x, and then update to ZENworks Service Desk 23.4. ZENworks Service Desk 23.4 is available only through Online channel. If you are already using ZENworks Service Desk 23.3, then you can upgrade using the Online Update channel.

- ♦ To deploy ZENworks Service Desk 8.3.x, see the [Appliance Deployment](#) section in the [Service Desk Appliance Deployment and Administration Reference](#).
- ♦ To update to ZENworks Service Desk 23.4, see [Migrating the Appliance](#).

4 Migrating the Appliance

This chapter contains information about migrating your ZENworks Service Desk Appliance to version 23.4.

ZENworks Service Desk can be migrated to version 23.4 from version 23.3. If you want to migrate from versions older than ZSD 8.3.x, then you need to upgrade to ZSD 8.3.x and then to ZSD 23.4.

Refer to the following section to migrate to ZENworks Service Desk 23.4:

- ◆ [Section 4.1, “Migrating from ZENworks Service Desk 8.3.x,” on page 13](#)
- ◆ [Section 4.2, “Migrating from ZENworks Service Desk 23.3,” on page 13](#)

4.1 Migrating from ZENworks Service Desk 8.3.x

ZENworks Service Desk 23.4 is an incremental update from ZENworks Service Desk 23.3. Upgrading ZENworks Service Desk from ZENworks Service Desk 8.3.x using Online Product Upgrade will automatically upgrade to ZENworks Service Desk 23.4. For more information on the detailed upgrade steps, see [Migrating the Appliance](#).

4.2 Migrating from ZENworks Service Desk 23.3

If you are using ZENworks Service Desk and want to migrate to ZENworks Service Desk 23.4, then refer to the following sections:

- ◆ [Section 4.2.1, “Pre Migrate,” on page 13](#)
- ◆ [Section 4.2.2, “Migration,” on page 14](#)
- ◆ [Section 4.2.3, “Post Migrate,” on page 14](#)

NOTE: ZENworks Service Desk 23.4 will be available only through the Online channel.

4.2.1 Pre Migrate

- ◆ Take a snapshot of ZENworks Service Desk Appliance.
- ◆ If you are using an external database, then take a backup of the database.
- ◆ If any configuration is changed in `/etc/init.d/servicedesk.server` file, then ensure that you note the changes.
- ◆ If any configuration is changed in the Tomcat server such as the `web.xml` and `server.xml` files, then ensure that you note the changes.

4.2.2 Migration

- 1 On the ZENworks Service Desk Appliance home page, in the Appliance Configuration section, click **Online Update**.
- 2 In the Online Update page, select **Needed Patches** from the drop-down, select ZENworks Service Desk 23.4, and then click **Update Now**.
- 3 In the **Update Now** dialog, read the displayed instructions, and then click OK.
- 4 After completing the migration process, reboot the Appliance.

NOTE: While updating the ZENworks Service Desk, the following error message might be displayed when the appliance takes a longer time to update. Ignore the displayed error message as the update will be completed successfully:

An error occurred while communicating with the server.

4.2.3 Post Migrate

After you migrate to ZENworks Service Desk 23.4, ensure that you perform the following:

- ♦ The backup of important configuration file will be available in `/vastorage/backupforzsdv234` location.
- ♦ If you have made any changes in the Tomcat server such as the `web.xml` and `server.xml` files, then update the changes, if the changes are not available in the file.
- ♦ If any memory configuration is modified in the `/etc/init.d/servicedesk.server` file update the same changes, if the changes are not available in the file.
- ♦ In the browser, open the **Technician** portal. The schema upgrade will be initiated automatically, and the upgrade process might be in progress or completed.

A confirmation message is displayed after the upgrade is completed.

If the upgrade fails, then follow the on-screen instructions.

- ♦ If you have customized the CSS, then you should customize it again, if the existing customization does not work. The backup of CSS is available in the `/vastorage/LiveTime/Style` location.

Review and replicate the same customization changes in the following UI locations:

Setup > Customize > User Portal > CSS

Setup > Customize > Customer Portal > CSS

NOTE: 1. In case of any UI related issues, press Ctrl+F5 to refresh the browser cache.

2. If any error is displayed, then you can clear the browser cache and try again. If the error persists, contact Customer Support.
-

5 Appliance Management

In Service Desk Appliance, a web based interface is provided to manage the Appliance. The user interface helps you to configure and perform operations on a Service Desk Server. Based on the logged-in user the tiles are displayed.

To manage Service Desk, see [Chapter 6, “System Management,” on page 27](#).

Service Desk Appliance enables you to reconfigure settings of the Appliance, such as administrative passwords, network settings, and certificate settings.

Service Desk Appliance supports `root` and `sdadmin`. You can use these users to perform any operations on ZENworks Service Desk Appliance. However, some operations can be performed only using the `root` user.

To manage Appliance:

- 1 On a supported web browser, launch the URL to access the Management Console.

The URL (`https://<FQDN>:9443` or `https://<ipaddress>:9443`) that is displayed on the Appliance console.

- 2 Specify the login with root credentials, then click **Log in**.

The following options are displayed in the Appliance Configuration:

- ♦ [Section 5.1, “Ganglia Configuration,” on page 15](#)
- ♦ [Section 5.2, “Ganglia Monitoring,” on page 17](#)
- ♦ [Section 5.3, “Network,” on page 17](#)
- ♦ [Section 5.4, “Time,” on page 17](#)
- ♦ [Section 5.5, “Digital Certificates,” on page 18](#)
- ♦ [Section 5.6, “Storage,” on page 22](#)
- ♦ [Section 5.7, “System Services,” on page 22](#)
- ♦ [Section 5.8, “Firewall,” on page 23](#)
- ♦ [Section 5.9, “Administrative Passwords,” on page 23](#)
- ♦ [Section 5.10, “Online Update,” on page 24](#)
- ♦ [Section 5.11, “Shutting Down and Restarting Service Desk Appliance,” on page 25](#)

5.1 Ganglia Configuration

Ganglia is a scalable, distributed monitoring system that enables you to gather information about the Service Desk Appliance system. The default metrics that you can monitor are CPU, disk, load, memory, network, and process.

NOTE: By default, Ganglia Configuration and Ganglia monitor services will be stopped. If required, you can manually start the Ganglia Configuration and Ganglia monitor services. For more information on enabling Ganglia Monitoring, see [“Enabling Gangila Monitoring”](#).

1 On the Service Desk Appliance home page, in the Appliance Configuration section, click **Ganglia Configuration**.

2 You can change the following configuration options:

- ◆ **Enable Full Monitoring Services:** Select this option to receive and store metrics from other Appliances, and to allow the Ganglia Web Interface to run on the same device as the Service Desk Appliance.

You can disable Ganglia monitoring by clearing this option. You can perform this only if you have a monitoring system that you want to use for Service Desk Appliance, or if you want to configure a dedicated Appliance for viewing monitoring information. (You can do this by selecting **Unicast** below; then specify the DNS name or IP address of the Appliance where monitoring information is stored.)

- ◆ **Enable monitoring on this Appliance:** Select this option to enable Ganglia monitoring on this Appliance.
 - ◆ **Multicast:** Select this option to send monitoring information to other Appliances on the network.
 - ◆ **Unicast:** Select this option to send monitoring information to a single destination.
 - ◆ **Publish to:** Specify the server where Ganglia sends monitoring information while it is running in Unicast mode.
 - ◆ **Monitoring Tool Options:** Select this option to enable the monitoring tool to access this server through http port 9080 using a similar to `http://:9080/gweb/`.

3 (Optional) Click **Reset Database** to remove all existing Ganglia metrics from this Appliance.

This option is not applicable to the Service Desk database.

4 Click **OK**.

For more information about how to use Ganglia monitoring with Service Desk Appliance, see [Section 5.2, “Ganglia Monitoring,” on page 17](#).

5.1.1 Enabling Ganglia Monitoring

Enable Ganglia monitoring by starting the following services:

- ◆ `novell-gmond.service`
- ◆ `novell-gmetad.service`
- ◆ `apache2.service`

To start the service momentarily, run the `systemctl start <service_name>` command.

NOTE: Whenever you restart the Appliance, you should run the command to start the monitoring service.

To enable the services permanently run the `systemctl enable <service_name>` command.

5.2 Ganglia Monitoring

Ganglia is a scalable, distributed monitoring system that enables you to gather information about the Service Desk Appliance system. The default metrics that you can monitor are CPU, disk, load, memory, network, and process. For more information, see [Ganglia](#).

5.3 Network

- 1 On the Service Desk Appliance home page, in the Appliance Configuration section, click **Network**.
- 2 Below **DNS Configuration**, you can modify the name servers, search domains, and gateway settings for the Service Desk Appliance network.
- 3 Below **NIC Configuration**, click the **ID** to modify the IP address, hostname, and network mask of any Network Interface Controller (NIC) associated with the Appliance. (If multiple NICs are configured for Service Desk Appliance, you can configure the additional NICs.)
- 4 Click **OK**, then restart the Appliance to reflect the changes.
- 5 (Optional) In the **Appliance Administration UI (port 9443) Access Restrictions**, specify the IP address of any networks for which you want to allow access to the Service Desk Appliance. Leave this blank to allow any network to access the Service Desk Appliance.
- 6 Click **OK**.

5.4 Time

- 1 On the Service Desk Appliance home page, in the Appliance Configuration section, click **Time**.
- 2 Change the required time configuration options:
 - ♦ **NTP Server:** Specify the NTP server that you want to use for time synchronization. Multiple servers can be specified by providing spaces.
 - ♦ **Region:** Select the region where Service Desk Appliance is located.
 - ♦ **Time Zone:** Select the time zone on which Service Desk Appliance is located.
 - ♦ **Hardware Clock Set to UTC**
- 3 Click **OK**.

5.5 Digital Certificates

The Service Desk Appliance ships with a self-signed digital certificate. Instead of using this self-signed certificate, you must use a trusted server certificate that is signed by a trusted Certificate Authority (CA) such as VeriSign or Equifax, which is a paid service, or, if your organization permits, you can use free CA such as AD, eDir, openldap. Also, update your certificate when you update the Service Desk Appliance software.

Perform the following sections to change the digital certificate for your Service Desk Appliance. You can use the digital certificate tool to create your own certificate and then have it signed by a CA, or you can use an existing certificate and key pair.

- ◆ [Section 5.5.1, “Using the Digital Certificate Tool,” on page 18](#)
- ◆ [Section 5.5.2, “Using an Existing Certificate and Key Pair,” on page 19](#)
- ◆ [Section 5.5.3, “Activating the Certificate,” on page 19](#)
- ◆ [Section 5.5.4, “Managing Certificates,” on page 20](#)
- ◆ [Section 5.5.5, “Renewing Certificates,” on page 20](#)
- ◆ [Section 5.5.6, “Service Desk Ciphers,” on page 21](#)

5.5.1 Using the Digital Certificate Tool

You can perform the following using this page:

- ◆ [“Creating a Self-Signed Certificate” on page 18](#)
- ◆ [“Officially Signing Your Certificate” on page 19](#)

Creating a Self-Signed Certificate

- 1 On the Service Desk Appliance home page, under Appliance Management, click **Digital Certificates**.
- 2 In the **Key Store** drop-down list, ensure that **Web Application Certificates** is selected.
- 3 Click **File > New Certificate (Key Pair)**.
- 4 In the Key Certificate (Key Pair) page, specify the following information:
 - ◆ **Alias:** A name that you want to use to identify and manage certificate.
 - ◆ **Validity (days):** How long you want the certificate to be valid.
 - ◆ **Key Algorithm:** Select RSA or DSA.
 - ◆ **Key Size:** The required key size.
 - ◆ **Signature Algorithm:** The required signature algorithm.
 - ◆ **Common Name (CN):** This must match with the server name in the URL in order for browsers to accept the certificate for SSL communication.
 - ◆ **Organizational Unit (OU):** (Optional) Organizational unit name, such as a department or division.
 - ◆ **Organization (O):** (Optional) Organization name.
 - ◆ **City or Locality (L):** (Optional) City name.

- ♦ **State or Province (ST):** (Optional) State or province name.
 - ♦ **Two-letter Country Code (C):** (Optional) Two-letter country code. For example, US
- 5 Click **OK** to create the certificate.

After creating the self-signed certificate, you can use the certificate in Service Desk.

However, you can get the certificate signed by a trusted CA. The signing of the certificate is an optional step but recommended. For information, see [“Officially Signing Your Certificate” on page 19](#).

Officially Signing Your Certificate

- 1 On the Digital Certificates page, select the certificate that is created, then click **File > Certificate Requests > Generate CSR**.
- 2 Share your digital certificate with a certificate authority (CA), such as VeriSign.
The CA accepts your Certificate Signing Request (CSR) and generates an official certificate based on the CSR information. The CA then shares the new certificate and certificate chain.
- 3 After receiving the official certificate and certificate chain:
 - 3a Go to the Appliance Configuration page and click **Digital Certificates**.
 - 3b Click **File > Import > Trusted Certificate**. Browse for the trusted certificate chain (trusted certificate chain, including intermediate certificate that is received from CA or subordinate CA) that you received from the CA, then click **OK**.
 - 3c Select the self-signed certificate, then click **File > Certification Request > Import CA Reply**.
 - 3d Browse for and upload the official certificate (Server Certificate) to be used to update the certificate information.
 - 3e On the Digital Certificates page, the name in the **Issuer** column for your certificate changes to the name of the CA that stamped your certificate.
- 4 Activate the certificate, for information, see [“Activating the Certificate” on page 19](#).

5.5.2 Using an Existing Certificate and Key Pair

When you are using an existing certificate and key pair, use a `.P12` or `.pfx` key pair format.

- 1 On the Digital Certificates page, in the **Key Store** drop-down, select **Web Application Certificate**.
- 2 Click **File > Import > Trusted Certificate**. Browse for and select your existing certificate, then click **OK**.
- 3 Click **File > Import > Trusted Certificate**. Browse for and select your existing certificate chain for the certificate that you selected in [Step 2](#), then click **OK**.
- 4 Click **File > Import > Key Pair**, then browse for and select `.P12` or `.pfx` key pair file, specify password if required, then click **OK**.
- 5 Activate the certificate, for information see [“Activating the Certificate” on page 19](#).

5.5.3 Activating the Certificate

- 1 On the Digital Certificates page, in the **Key Store** drop-down, select **Web Application Certificates**.
- 2 Select the certificate that you want to activate, click **Set as Active**, then click **Yes**.

- 3 Verify that the certificate and the certificate chain were created correctly by selecting the certificate, then clicking **View Info**.
- 4 Restart the service.

5.5.4 Managing Certificates

All certificates that are included with the Oracle Java package that is bundled with the version of SLES that Service Desk Appliance ships with, are installed when you install Service Desk Appliance.

You can use the Digital Certificates tool on the Service Desk Appliance to remove certificates that are not used by your organization.

Also, you can use the Digital Certificates tool on the Service Desk Appliance to maintain the certificate store by removing certificates that are expired and then installing new certificates as required, according to your organization's security policies.

To access the Digital tool:

- 1 On the Service Desk Appliance home page, under Appliance Management, click **Digital Certificates**.

In the **Key Store** drop-down, under **Web Application Certificates**, all certificates are displayed. Based on requirement, you can delete the unused certificates.

IMPORTANT: The active certificate must not be deleted.

5.5.5 Renewing Certificates

Depending on your current certificate status, ZENworks Service Desk certificate can be renewed by following any of the following scenarios:

Scenario 1: If the certificate is still valid and want to use the same certificate.

1. Share the CSR to the Certificate Authority.
2. Get the official server certificate and certificate chain based on CSR from CA
3. Import the certificate to ZENworks Service Desk by performing the following steps:
 - a. Go to the Appliance Configuration page and click Digital Certificates.
 - b. In the Key Store field, select Web Application Certificates.
 - c. Click File > Import > Trusted Certificate. Browse for the trusted certificate chain that you received from the CA, then click OK.
 - d. Select the self-signed certificate, then click File > Certification Request > Import CA Reply.
 - e. Browse for and upload the official certificate to be used to update the certificate information.

- f. On the Digital Certificates page, the name in the Issuer column for your certificate changes to the name of the CA that stamped your certificate.
 - g. Click View Info to view the validity information.
4. Activate the certificate, for information, see [Activating the Certificate](#).

Scenario 2: If the certificate has expired, or you want to use a new certificate

1. On the Digital Certificates page, select the certificate that is created, then click File > Certificate Requests > Generate CSR.
2. Share the CSR to the Certificate Authority.
3. Get the official server certificate and certificate chain based on CSR from CA
4. Import the certificate to ZENworks Service Desk by performing the following steps:
 - a. Go to the Appliance Configuration page and click Digital Certificates.
 - b. In the Key Store field, select Web Application Certificates.
 - c. Click File > Import > Trusted Certificate. Browse for the trusted certificate chain that you received from the CA, then click OK.
 - d. Select the self-signed certificate, then click File > Certification Request > Import CA Reply.
 - e. Browse for and upload the official certificate to be used to update the certificate information.
 - f. On the Digital Certificates page, the name in the Issuer column for your certificate changes to the name of the CA that stamped your certificate.
 - g. Click View Info to view the validity information.
5. Activate the certificate, for information, see [Activating the Certificate](#).

NOTE: As recommended by top CAs, even though we are renewing the certificate, but in-turn we are creating the certificate every time.

5.5.6 Service Desk Ciphers

Following are the ZENworks Service Desk ciphers that available in the `server.xml` file:

```
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
```

5.6 Storage

If you have created hard disk partitions (`/vastorage` and `/var`), Service Desk Appliance provides tools that allow you to expand the storage space for the `/vastorage` and `/var` partitions.

- 1 On the Service Desk Appliance home page, in the Appliance Configuration section, click **Storage**.
- 2 Use the tools provided by your virtualization platform vendor to expand the virtual disks that contain the partitions you are expanding.
- 3 In the **Appliance Disks Containing Unallocated Free Space**, select the partitions to be expanded.
- 4 Click **Expand partitions**.
Appliance services are stopped, the selected partitions are expanded to the size of their respective disks, and Appliance services are restarted.
- 5 Restart the Appliance so that the operating system detect the disks that are expanded.

5.7 System Services

List of services that is running on the Service Desk Appliance. The following system services are available:

- ♦ SSH
- ♦ Memcached

In the System Services page, you can perform the following actions:

- ♦ [Section 5.7.1, “Starting, Stopping, or Restarting System Services,” on page 23](#)
- ♦ [Section 5.7.2, “Setting System Services to Automatic or Manual,” on page 23](#)

5.7.1 Starting, Stopping, or Restarting System Services

- 1 In the System Services page, select the service that you want to start, stop, or restart.
- 2 Click **Action**, then click **Start**, **Stop**, or **Restart**.

5.7.2 Setting System Services to Automatic or Manual

- 1 On the System Services page, select the service that you want to make automatic or manual.
- 2 Click **Options**, then click **Set as Automatic**, or **Set as Manual**.

If you choose **Set as Automatic**, the SSH services will start automatically when you start the Appliance.

If you choose **Set as Manual**, you need to start or stop the SSH services manually after you start the Appliance.

5.8 Firewall

During the configuration a few ports on Appliance are open. You can view the current firewall configuration from the Service Desk Appliance.

- 1 On the Service Desk Appliance home page, in the Appliance Configuration section, click **Firewall**.
Port numbers are displayed with the current status.

If you have a firewall, you must allow the listed port numbers to ensure that you have a seamless experience with Service Desk Appliance. As a best practice, do not change any port numbers from the default ports.

5.9 Administrative Passwords

- 1 On the Service Desk Appliance home page, in the Appliance Configuration section, click **Administrative Passwords**.
- 2 Specify the new passwords for the `root` and `sdadmin` administrators.
If you are changing the root password, you must first specify the current root password.
- 3 (Optional) Select or clear **Allow root access to SSH**. When this option is selected, the root user is able to SSH to the Appliance. If this option is not selected, only the `zsd` user can SSH to the Appliance.
- 4 Click **OK**.

5.10 Online Update

Online Update enables you to update the Appliance.

- 1 On the Service Desk Appliance home page, in the Appliance Configuration section, click **Online Update**.

You can perform the following actions:

- ♦ **Register:** Enables you to register with Micro Focus Customer Center (MFCC) server or a Local Subscription Management Tool (SMT) server from where you can download software updates and install automatically to update the product.

To register online update service:

1. Click the Register tab.
2. Choose the type of service **Local SMT** (Subscription Management Tool) or **Novell Customer Center** (NCC).

Based on the service type, specify the following:

Local SMT

- ♦ **Hostname:** The hostname of the server from where you want to download.
- ♦ **SSL Cert URL (optional):** The SSL certificate to communicate with the server.
- ♦ **Namespace path (optional):** The name space of the file or directory.

Novell Customer

- ♦ **Email:** The email address to receive the updates on Service Desk suite.
- ♦ **Activation key:** The activation key for the server base license.
- ♦ **Allow data send:** choose how you want to receive the data **Hardware Profile** or **Optional information**.

3. Click **Register**.
- ♦ **Update Now:** After registration, click **Update Now** to trigger downloaded updates.
 - ♦ **Schedule:** After registration, you can configure type of updates to download and whether to automatically agree with the licenses.

To schedule online update:

1. Click the **Schedule** tab.
2. Select a schedule for download updates (Manual, Daily, Weekly, Monthly).

IMPORTANT: We recommend that you schedule online updates only for updating non-interactive security patches on ZENworks Service Desk Appliance 7.5 or later. Rest of the patches including upgrade to newer version of Service Desk can be done manually as it impacts the system and might cause down-time of server.

- ♦ **View Info:** Displays the list of installed and downloaded software updates.
- ♦ **Refresh:** Refreshes the status of updates on the Appliance.

5.11 Shutting Down and Restarting Service Desk Appliance

- 1 On the Service Desk Appliance home page, in the Appliance Configuration section, click **Reboot** or **Shutdown**.

To stop/start/restart the servicedesk service from the console, run the `systemctl start | stop | restart servicedesk` command.

Example: To start the servicedesk service, run the `systemctl start servicedesk`

6 System Management

The user interface helps you to configure and perform operations on a Service Desk Server. Based on the logged-in user the tiles are displayed.

On Service Desk, the `root` or `sdadmin` user has all privileges. The `sdadmin` user is used as a Service Desk administrator to perform day-to-day activities in Service Desk.

The following operations can be performed by `root` and `sdadmin`:

- ◆ Explore all the files and folders of the Appliance system
- ◆ View logs
- ◆ View and edit the Service Desk configuration settings
- ◆ Restart both Appliance and Service Desk
- ◆ Launch a terminal and execute commands

To manage Service Desk Appliance:

- 1 Launch the URL on a supported web browser to access the Management Console.

For example: `https://<FQDN>:9443` or `https://<ipaddress>:9443`

- 2 Specify the login credentials, then click **Log in**.

If you log in as a `root` or `sdadmin` user, the following options are displayed in the Service Desk section:

NOTE: In case of any UI related issues, press Ctrl+F5 to refresh the browser cache.

- ◆ [Section 6.1, “Configuration,” on page 27](#)
- ◆ [Section 6.2, “Terminal and File Explorer,” on page 28](#)
- ◆ [Section 6.3, “Logs,” on page 30](#)
- ◆ [Section 6.4, “Configuring Service Desk,” on page 31](#)

6.1 Configuration

The Service Desk Configuration page is enabled only after Service Desk is successfully configured.

- 1 On the Service Desk Appliance home page, in the **Service Desk Appliance** section, click **Service Desk Configuration**.

The Service Desk Configuration page has the Summary of database configuration.

The Summary enables you to view the Service Desk Server details. This includes information about the Certificate, Service Desk Database, and Appliance details, such as type of hypervisor used, operating system, RAM and file system and HDD details.

The Appliance comes with built-in 40 GB of `rootfs` file system that is mounted on `root` directory. The Additional hard disk that is added will be attached to the `/dev/sdb1` and mounted on `/vastorage`. All Service Desk related configurations, log files, certificates, and binaries are stored on the additional hard disk.

- 2 Click **Database Configuration** to change the password of embedded database or to connect to an external database. This page also displays the current database configurations.

To change the **Embedded Database** password:

2a Choose the **Embedded Database**.

2b Select **Change Password**, specify the new password and confirm, and then click **OK**.

or

To use an **External Database**:

2c Choose **External Database** and click **OK**.

2d Go to the **Appliance Home** page, click **Technician Portal**, and configure the external database.

6.2 Terminal and File Explorer

This tile launches an integrated view for File System Explorer and Terminal.

- ♦ [Section 6.2.1, “Terminal,” on page 28](#)
- ♦ [Section 6.2.2, “File Explorer,” on page 29](#)

6.2.1 Terminal

SSH service needs to be running for terminal to work. SSH service is started by default. If the SSH service is not running, perform the following steps:

- 1 On the Service Desk Appliance home page, in the **Appliance Configuration**, click the **System Services** icon.
- 2 Select the **SSH service** on the System Services page.
- 3 Click **Action**, then click **Start**.

Set the SSH service to **Automatic**, if you want to restart the SSH service automatically after you reboot the device.

- 4 On the Service Desk Appliance home page, in the **Service Desk** section, click **Terminal & File Explorer**.

A new browser window launches two frames that display a **File Explorer** (for performing file operations) and a **Terminal**. Whenever you close the Terminal browser or tab, then a confirmation message is displayed.

If you log in as `sdadmin` or `root` user, you can open a terminal session.

You can perform file operations by using an embedded File Explorer that enables you to transfer content between the local and the remote file systems. You can also open new terminals rooted at any folder in the remote file system.

You can launch more than one terminal by clicking **New Terminal**. By default, a maximum of five terminals can be launched.

To configure with any other value than the default value of the terminal:

- 1 Go to `/etc/opt/novell/base`
- 2 Open the `terminal_config.properties` file.
- 3 Change the `maxTerminalsPerBrowser` value with the required value, then save the file.

To select a theme (foreground and background color) for the terminals:

- 1 Click the **Settings**  icon, then select the required terminal theme.

To create a theme:

- 1 Go to `/etc/opt/novell/base`
- 2 Open the `terminal-themes.xml` file.
- 3 Add your own theme, then save the file. For example:

```
<theme>
  <name>example</name>
  <background-color>#000000</background-color>
  <foreground-color>yellow</foreground-color>
</theme>
```

6.2.2 File Explorer


- 1 On the Service Desk Appliance home page, in the **Service Desk** section, click **Terminal & File Explorer**.










A new browser window launches two frames that display a **File Explorer** (for performing file operations) and a **Terminal** (SSH).

This enables you to perform operations on files and folders.

- ♦ The file operations are based on user privileges (POSIX file permissions).
- ♦ If you log in as `sdadmin`, all file operations are executed as `sdadmin` user.
- ♦ If you log in as `root`, all file operations are executed as `root` user.
- ♦ In the tabular view, a context menu is available with these options: **Open Terminal**, **Refresh**, **Upload**, **Delete**, and **Rename**.
- ♦ The Tree View for Appliance file system displays the Appliance file system as a tree. Only folders are displayed in the tree view. The following options are available **Open Terminal**, **Refresh**, **Cut**, **Copy**, **Paste**, **Delete**, **Rename**, **New Folder**, **Download**, and **Upload**.
- ♦ File explorer enables you to explore the Appliance's (SLES -Unix) file system, breadcrumb navigation, upload, download, refresh, rename, create, delete, or, CCP operations (cut, copy, and paste).

Below the file path, a toolbar is displayed and you can perform the following:

Icon	Name	Description
	Terminal Settings	To change the terminal theme display settings.

Icon	Name	Description
	Select Path	To select file path that is displayed on the breadcrumb.
	Settings	To configure show or hide files.
/	Breadcrumb	Displays the path for selected file or folder.
	Parent Directory	Display the contents of the parent folder in the tabular view.
	Download	To download files and folders under a specified folder.
	Upload	Supports multiple file upload; folder upload is not supported.
	New folder	Creates a folder in the current folder.
	New file	Creates a new file in the current folder.
	Refresh	Updates the tabular view with the latest contents from the Appliance.
	Delete	Enables you to delete multiple files and folders under a specified folder.

6.3 Logs

All log files that are monitored on Service Desk Appliance are organized in a virtual tree structure and path of the particular file or folder is displayed. Log files can be viewed in the Tail mode or View From Start mode.

In the **Tail** mode, a log file is displayed from the end of log file.

All logs for the Appliance, OS and Service Desk are available in the `/var/opt/novell/log/` location.

In the **View From Start** mode, a log file is displayed from the start of the log file. Whenever log files span across multiple version of files, then starting from the first version of that file the content is displayed.

- 1 On the Service Desk Appliance home page, in the **Service Desk** section, click **Logs**.

This enables you to view logs of the Service Desk Server. Logs are categorized based on Appliance logs, operating system logs, and Service Desk logs. With-in Service Desk, logs are categorized based on different components.

Logs has the following options:

- ♦ **View**, **View From Start**, and **Refresh**
- ♦ **Download** enables you to download a log file or a folder.

- ◆ **Resume** and **Pause** enable you to tail log files to see the latest information. You can configure the refresh interval of a tail by specifying the **Refresh** time in **Seconds**. Refresh specifies the interval of time between two requests. By default **Refresh** is set to one second.

Specify **Lines to load** to control the number of lines to be retrieved for the tail interval. By default **Lines to load** is set to 100.

Control the speed in which log file is displayed. Log files are loaded by making multiple HTTP requests in periodic intervals of time. Each request loads a configurable number of lines.

- ◆ **Clear** enables you to clear the current displayed logs. However, logs will not be cleared in Service Desk Appliance. To see the cleared logs, start the log file.
- ◆ **Search** enables you to filter logs based on the search criteria. You can use tail and grep to monitor log files from the terminal. The log viewer provides a GUI for tailing and filtering the content in log files. You can search based on log level such as INFO, ERROR, and DEBUG and also with regular expressions (AND and OR).

6.4 Configuring Service Desk

To configure Service Desk:

- 1 In the **Service Desk Appliance** home page, in the **Service Desk Appliance** section, click **Classic ZENworks Service Desk**.
- 2 In the **ZENworks Service Desk** login page, specify the login credentials that you specified during configuration.

To open the new customer portal, click **New ZENworks Service Desk**.

By default super/super and admin/admin will be your login credentials.

NOTE: If an LDAP User source is configured for a Supervisor super/super is disabled.

7 Disaster Preparedness and Recovery

This section explains how you can protect ZENworks Service Desk data and be prepared if an organizational risk assessment identifies a need for a recovery mechanism. Backing up a database provides a snapshot of the database, where the data is in a consistent state. If you are facing any issues with the product or the database, then the database can be recovered.

- ◆ [Section 7.1, “Disaster Preparedness,” on page 33](#)
- ◆ [Section 7.2, “Disaster Recovery,” on page 34](#)

For best results, ensure that backup copies are made on a consistent, regular basis to minimize the amount of data loss between backups.

7.1 Disaster Preparedness

ZENworks Service Desk can either be used with an embedded or an external database. Based on your database, see the following sections:

- ◆ [Section 7.1.1, “External Database,” on page 33](#)
- ◆ [Section 7.1.2, “Embedded Database,” on page 34](#)

7.1.1 External Database

If you are using an external database, then you have to take a backup of the database and snapshot of the Appliance.

- 1. Database Backup:** If you have taken a backup of the database, then following configurations or data are included in the backup:
 - ◆ e-Mail (Server, Setup)
 - ◆ Licensing (License, Host, Users)
 - ◆ LDAP (Server, Advanced - connection info: Type, Domains, Security, Host or Port number, Username, UserNode or BaseDN, Groups and GUID)
 - ◆ AD or eDir Group Information
 - ◆ AMIE (Setup - connection info: Server Type, DB Type, Hosts or Port number, Name, Username, Schema, Catalog, etc.)
 - ◆ ZENworks (General, OpenID - lists connection info: ZCM Server Address)
 - ◆ Customized privileges
- 2. Appliance Snapshot:** If you take a snapshot of the Appliance, then All CSS and Banners customizations are saved. Database (connection info: Type, Host or Port number, Db, Username, password), Java Heap Memory configurations and the system.properties file.

7.1.2 Embedded Database

If you are using an embedded database that is provided with ZENworks Service Desk Appliance, then just by taking a snapshot of the Appliance (or a take backup of the second disk), you can be prepared for the disaster. Following data are saved by taking snapshot of the appliance:

1. All CSS and Banners customizations that are stored in the second disk.
2. e-Mail (Server, Setup)
3. Licensing (License, Host, Users)
4. Database - connection info: Type, Host or Port number, Db, Username, password)
5. LDAP (Server, Advanced - connection info: Type, Domains, Security, Host or Port number, Username, UserNode or BaseDN, Groups and GUID)
6. AD, AzureAD or eDir Group Information
7. AMIE (Setup - connection info: Server Type, DB Type, Hosts or Port number, Name, Username, Schema, Catalog, etc.)
8. ZENworks (General, OpenID - lists connection info: ZCM Server Address)
9. Customized privileges

7.2 Disaster Recovery

If you are facing any issues with the product or the database, then the backup data enables you to restore your ZENworks Service Desk to a stable state.

IMPORTANT: The data that was captured in the system after taking the backup will be lost. Hence, it is recommended that backup copies are made on a consistent, regular basis to minimize the amount of data loss between backups.

- ♦ If you are using an external database, then ensure that you restore the database backup and roll back the Appliance (or restore second hard disk) to a stable snapshot.
- ♦ If you are using an embedded database, then ensure that you roll back the Appliance (or restore second hard disk) to a stable snapshot.