ZENworks Service Desk - Security Administration Guide

This Security Administration guide provides the best practices and procedures to manage and maintain security of ZENworks Service Desk.

1 Configuring server with 3rd Party Certificate

ZENworks Service Desk, by default, is configured with an internal SSL certificate to facilitate secure communication. However, it is strongly recommended to replace this internal certificate with a certificate signed by a trusted third-party Certificate Authority (CA) for production environments.

The internal certificate provides basic encryption, but it lacks the trust verification that a third-party CA provides. CA-signed certificates undergo a validation process that helps to establish trust between your server and external clients or users.

Incorporating a third-party CA-signed certificate enhances the security and reliability of your deployment, helping to protect sensitive data and ensuring compliance with industry security standards.

For more information, see Digital Certificates in the ZENworks Service Desk Appliance Deployment and Administration References.

2 Password Management

After deploying the ZENworks Service Desk for the first time, two default user accounts will be created. These user accounts are essential for initial setup and access. To ensure security, it is strongly recommended that you change the passwords for both users immediately after deployment.

2.1 Changing Default User Password

After completing the deployment and initial setup, ensure that you assign unique, strong passwords to each of these accounts.

To change the password, log into the portal with each of the default user account and change the password from the My Account page.

For more information, see My Account in the ZENworks Service Desk Administration Guide.

2.2 Change the Internal Database Password

To secure the database against unauthorized access, it is recommended that you change the database passwords immediately after deploying and configuring the ZENworks Service Desk. Using a strong, unique password for the database is crucial to preventing unauthorized access and safeguarding sensitive data.

For more information, see Configuration in the ZENworks Service Desk Administration Guide.

2.3 Use Strong Passwords

To enhance security and protect sensitive information, ensure that you enforce and maintain strong passwords. Enforcing strong password practices mitigates the risk of unauthorized access enhancing the overall security of the application.

- **Internal Users:** While creating a new account for users, ensure that you choose a strong password.
- **User accounts imported from LDAP:** Passwords for these accounts are managed via LDAP.

3 Managing Ports

To enhance the security of your deployment, it is recommended to carefully manage the open ports on your server. Unnecessary ports should not be enabled, and certain ports if enabled, should only be kept open for the shortest duration.

For example, if the database port is opened for a specific task, it should be closed immediately after use to reduce the risk of unauthorized access.

While port 22 (SSH) is open by default for administrative purposes, you can choose to close it if remote access is not needed.

To close a port, perform the following steps:

1. In the ZENworks Service Desk Appliance portal, stop the SSH service.
2. Go to Home, and then System Services.

Additionally, it is a good security practice to periodically review the list of open ports on your server and close any that are no longer in use.

4 Keeping the appliance up to date

To ensure optimal performance and security, it is essential to regularly update the ZENworks Service Desk. Updates often include important security patches, bug fixes, and new features that can protect from vulnerabilities. It is recommended to regularly upgrade to the latest version of the application and apply quarterly security patches.

For more information, see Appliance Migration in the ZENworks Service Desk Appliance Deployment and Administration References.

5 Enable Multi-Factor Authentication (MFA)

Advanced Authentication provides multi-factor authentication to protect sensitive data by using a series of authentication methods.

NetIQ Advanced Authentication can be integrated with the ZENworks Service Desk to provide a more secure way to access the Service Desk portals. The multi-factor authentication can be enabled for all the users imported from an LDAP (non-Azure AD) server and can be configured for all the user roles.

To strengthen the security of user accounts, it is highly recommended to enable Multi-Factor Authentication (MFA) for your application. ZENworks Service Desk supports MFA integration with the Open Text AA server for user accounts imported from an LDAP server.

Enabling MFA adds a layer of security by requiring users to provide a second form of authentication, such as an OTP or push notification, along with their user name and password.

For more information, see ZENworks Service Desk - Advanced Authentication Getting Started.

6 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/en-us/legal.