Self Service Password Reset 4.2

Installation Guide

January 2018

NetIQ

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.netiq.com/company/legal/.

Copyright © 2017 and 2018 NetIQ Corporation. All Rights Reserved.

Contents

About this Book **5**

1 Self Service Password Reset Overview **7**

Self Service Password Reset Key Features . . . 7
Self Service Password Reset Architecture . . . 8
Understanding Challenge-Response Storage Methods . . . 10

2 Planning to Install Self Service Password Reset **11**

Selecting an Appropriate Configuration . . . 11
Securing Self Service Password Reset . . . 13
- Appliance Certificate . . . 13
- HTTPS Certificate (Apache Tomcat and Browsers) . . . 13
- LDAP Server Certificate . . . 14
- Audit Server Certificates . . . 14

Best Practices for Self Service Password Reset . . . 14
- Best Practices for Password Policy . . . 14
- Best Practices for Self Service Password Reset Security . . . 15

High Availability and Load Balancing . . . 15

3 Installing Self Service Password Reset **17**

Obtaining Self Service Password Reset . . . 17
- Downloading the Full Version . . . 17
- Downloading the Trial Version . . . 17

Default Ports for Self Service Password Reset . . . 18
Deployment Requirements of Self Service Password Reset . . . 19
- Deployment Requirements for the Appliance . . . 20
- Deployment Requirements for Self Service Password Reset on Windows . . . 21
- Deployment Requirements for Self Service Password Reset WAR File on Linux . . . 22

Installing Self Service Password Reset . . . 24
- Deploying Self Service Password Reset in the Cloud . . . 24
- Deploying the Self Service Password Reset Appliance . . . 28
- Deploying Self Service Password Reset on Windows . . . 29
- Deploying the WAR File on Linux . . . 30

4 Configuring Your Environment for Self Service Password Reset **33**

Self Service Password Reset Configuration Worksheet . . . 33
Using the Configuration Guide . . . 36
Manually Configuring Self Service Password Reset . . . 37
- Configuring the LDAP Directories . . . 37
- Creating an LDAP Profile for Your Environment . . . 41
- Configuring Databases . . . 41
- Configuring Self Service Password Reset to Work with the External Database . . . 42

Integrating with Other NetIQ Products . . . 43

5 Upgrading or Migrating Self Service Password Reset **45**

Upgrading the Self Service Password Reset Appliance 45
Upgrading the Self Service Password Reset Appliance from 4.0. 45
Upgrading Self Service Password Reset 4.1.0.5 to 4.2 46
Upgrading Self Service Password Reset on Linux 46
Upgrading Self Service Password Reset on Windows 47
Upgrading the Identity Manager Deployment of Self Service Password Reset 48
Migrating Self Service Password Reset 49
Additional Information If Upgrading or Migrating from Self Service Password Reset 3.2 or a Prior Version 50

6 Uninstalling Self Service Password Reset **53**

Removing the Self Service Password Reset Appliance 53
Uninstalling on Linux. 53
Uninstalling on Windows. 53

A Documentation Updates **55**

January 2018 55
December 2017 55
October 2017 55

About this Book

The *NetIQ Self Service Password Reset Installation Guide* provides conceptual information and step-by-step guidance for installation tasks.

Intended Audience

This book provides information for individuals responsible for understanding administration concepts and implementing a secure, distributed administration model.

Systems Administrator

Deploy Self Service Password Reset across a distributed network. Configure language, connectivity, and authentication settings to ensure that users can access and reset passwords without generating a help desk call. Correlate business administrator and data administrator needs. Plus, integrate Advanced Authentication, Identity Manager, Client Login Extension, and Access Manager.

Other Information in the Library

The library provides the following information resources in addition to this guide:

Release Notes

Provides information specific to this release of the Self Service Password Reset product, such as known issues.

Administration Guide

Provides details configuration tasks specific to this release of Self Service Password Reset.

Videos

Provide supplemental information about using Self Service Password Reset. For more information, see the Micro Focus Self Service Password Reset Playlist.

1 Self Service Password Reset Overview

Self Service Password Reset is a web-based password management solution. You can deploy Self Service Password Reset to any web server or application server that supports a web archive. It eliminates users' dependency on administrators' assistance for changing passwords. It brings higher returns by reducing the cost and workload of the help desk. It allows you to ensure that all passwords in the organization comply with established best practice policies.

Self Service Password Reset also provides enhanced security. The user gets authenticated through a series of questions and answers known only to the user. During password reset, Self Service Password Reset uses a challenge-response authentication method to authenticate the user. You can store the challenge-response information in the back-end directory, external database, or local database. Users can change or reset their password and reset any forgotten password by using the configured challenge-response information.

Self Service Password Reset increases a user's productivity by synchronizing changed passwords, eliminating the need for users to wait for password resets and account unlocks. At the same time, the help desk can perform tasks more critical than password resets.

To learn more about Self Service Password Reset, see the following:

- "Self Service Password Reset Key Features" on page 7
- "Self Service Password Reset Architecture" on page 8
- "Understanding Challenge-Response Storage Methods" on page 10

Self Service Password Reset Key Features

Self Service Password Reset provides the following key features and benefits:

- **Easily Change Passwords:** Users can change their password without the help of an administrator.
- **Reset Forgotten Passwords:** Users can reset their passwords by answering challenge questions configured by an administrator. Self Service Password Reset stores the challenge questions and the users' responses for when they forget their password.
- **Recover Forgotten User Name:** Users can easily search for forgotten user names by using the search filter that is configurable by administrators.
- **Configure Challenge-Response Authentication:** Administrators can configure a set of challenge questions for the users. The questions can include random and required questions. The first time users log into Self Service Password Reset, it prompts users to provide answers to these questions. Users can reset their password by answering the same questions they saved earlier.
- **Self-Registration for New Users:** New users can self-register, saving time and money.
- **Activate User Accounts:** Users can reactivate a deactivated on their own account and set a password for it.
- **Edit Profile:** Users can view and update their profiles.
- **Search for People:** Users can search for their information as well as search for information about colleagues. Users can perform an interactive wildcard searches.

- **Simplify Help Desk Support:** The Help Desk Module simplifies administrative tasks, such as resetting passwords, clearing intruder lockout, unlocking user accounts, and debugging user information.
- **Create Password Policies:** Administrators can use password policies to enforce restrictions on the types of passwords that users can create.
- **Generate Usage and Lockout Reports:** Administrators can generate reports for intruder lockout, daily usage statistics, and online log information for debugging purposes.
- **Supports Localization:** Self Service Password Reset provides an easy way to add new languages. Self Service Password Reset provides default localization support for English, Canadian English, Canadian French, Catalan, Chinese Simplified, Chinese Traditional, Danish, Dutch, Hebrew, French, German, Italian, Japanese, Polish, Portuguese (Brazilian), Russian, Spanish, and Swedish.
- **Easily Customized:** Administrators can easily customize Self Service Password Reset to integrate with external web authentication methods as well as integrate with Identity Manager to add automated workflows and account claiming support.
- **Easily Integrated:** Self Service Password Reset easily integrates with a number of our products. It integrates with Access Manager, Advanced Authentication, Client Login Extension, and Identity Manager.

Self Service Password Reset Architecture

Self Service Password Reset is a web-based application that can be deployed to any web server or application server that supports a web archive. This means you can deploy Self Service Password Reset on-premise or in the Cloud.

The depicts the achitecture for Self Service Password Reset.

Self Service Password Reset consists of the following components depicted in Figure 1-1:

- **User Accounts (LDAP):** The LDAP directories contain the user accounts Self Service Password Reset manages. The types of LDAP directories that Self Service Password Reset supports are Active Directory and eDirectory.
- **Tomcat Server:** As you can see in Figure 1-1 on page 9, the Self Service Password Reset application must run on a web server, such as a Tomcat server. If you use the appliance or Windows deployment, Tomcat is included. If you use the WAR file to deploy Self Service Password Reset, you must have a Tomcat web server running.
- **Self Service Password Reset:** Self Service Password Reset is a Java-based web application that contains the following items:
  - **Administration Console:** Self Service Password Reset contains a web-based administration console. Administrators use the administration console to configure Self Service Password Reset, to view recent log events, download the current XML configuration file, manage certificates, and export or import the contents of the local database.

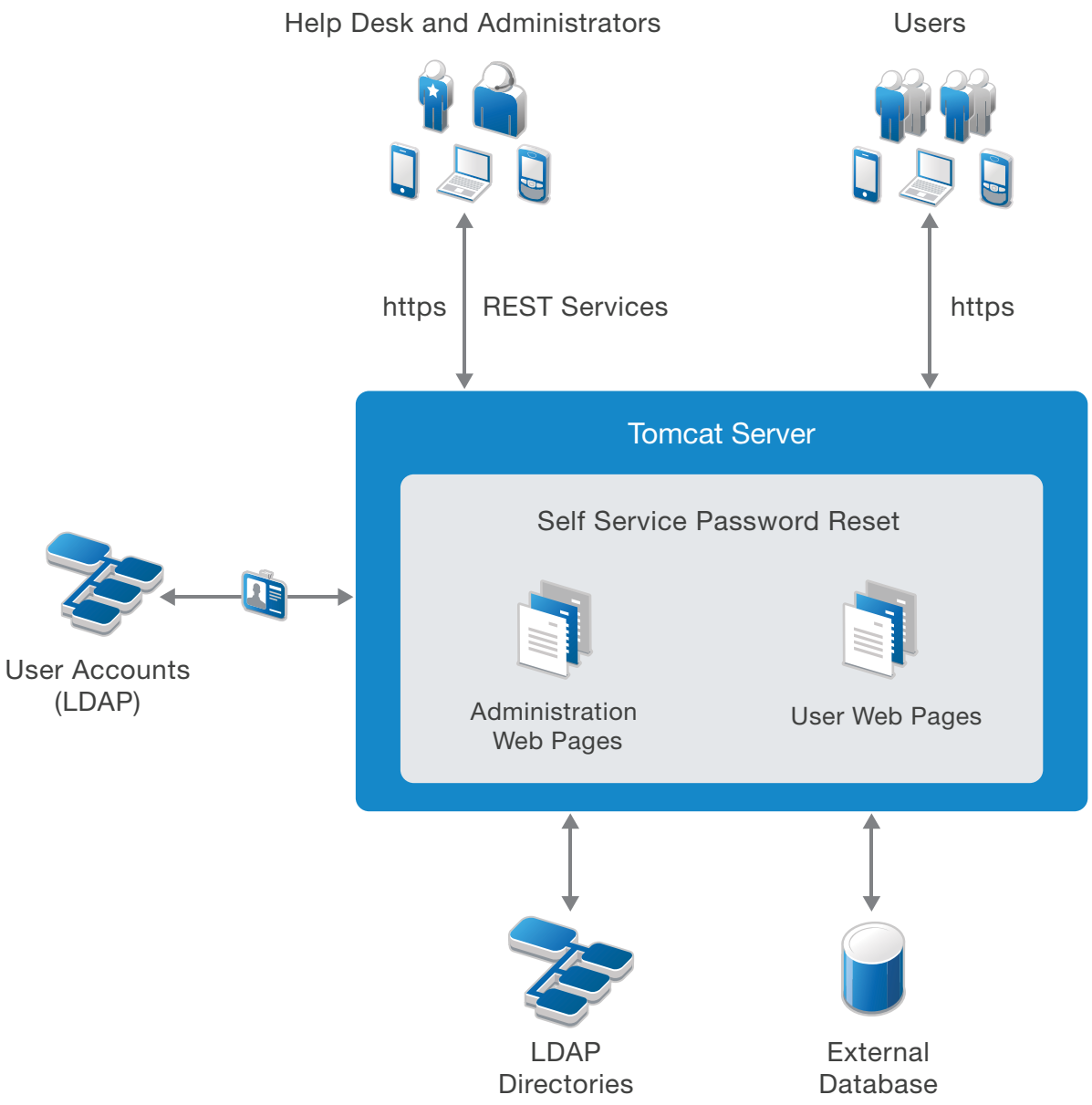
    If you are a help desk administrator, it allows you to manage user accounts, passwords, and reset intruder lockouts.

    You can also programmatically connect to Self Service Password Reset through REST Services. For more information, see the *Self Service Password Reset REST Services Reference*.
  - **Users Web Pages:** Self Service Password Reset provides a web interface for users to manage their passwords. Users access the interface through a browser that is supported on a desktop or a mobile device.

- **LDAP Directories and External Database:** Self Service Password Reset stores the user challenge-responses in LDAP directories or external databases. Self Service Password Reset provides the local database for testing purposes only. Use an external database or an LDAP directory in production environments to store the users' challenge-responses.

  Self Service Password Reset supports Microsoft SQL Server and Oracle.
- **Secure Communications:** By default, the appliance and Windows deployments communicate over HTTPS. The communications for the WAR file deployment depends on how you have your Tomcat web server configured.

Figure 1-1 *Architecture of Self Service Password Reset*



Understanding Challenge-Response Storage Methods

Self Service Password Reset supports the following locations to store users' challenge-responses:

- LDAP directory
- External database
- Local database (test only)

WARNING: Do not use the local database in a production environment as there are no methods to make the local database storage redundant, nor are there optimal backup methods available for the local database.

You can configure Self Service Password Reset to use any of the locations mentioned earlier to save users' challenge-responses. When a user attempts to recover a forgotten password, Self Service Password Reset reads the location that you have configured. Self Service Password Reset reads each configured location until it finds the relevant policy in the order that you specify during configuration.

A valid policy must meet the requirements of the user's current challenge-response policy.

Challenge-responses are stored in the locale that the user's browser selects during configuring responses. During the forgotten password recovery process, Self Service Password Reset uses answers in the same locale regardless of browser locale settings. Self Service Password Reset uses a standardized XML format to store answers. Depending on the configuration that you set for the **Responses Storage Hashing Method** setting, Self Service Password Reset stores answers as plain text or one-way hashed (encrypted) by using PBKDF2WithHmacSHA512 by default and the following as configurable options:

- None (Plain text)
- MD5
- SHA1
- SHA-1 with Salt
- SHA-256 with Salt
- SHA-512 with Salt
- PBKDF2WithHmacSHA1
- PBKDF2WithHmacSHA256
- PBKDF2WithHmacSHA512
- BCrypt
- SCrypt

Self Service Password Reset can read password and challenge policies from eDirectory. After saving a user's challenge-response answers, Self Service Password Reset can optionally write the challenge-response answers to the NMAS challenge-response format in addition to the configured methods. This enables interoperability of Self Service Password Reset with other products such as Novell Client for Windows.

NOTE: Self Service Password Reset does not save help desk challenge-response answers to the NMAS. Self Service Password Reset always considers the NMAS-stored responses as additional responses. Self Service Password Reset prefers to read and is required to store the responses in one of the non-NMAS formats to utilize the additional features of Self Service Password Reset responses.

2 Planning to Install Self Service Password Reset

Self Service Password Reset helps simplify the management of users' credentials. You must plan how best to secure the users' credentials and how to create the correct configuration for your environment and your users' needs.

- "Selecting an Appropriate Configuration" on page 11
- "Securing Self Service Password Reset" on page 13
- "Best Practices for Self Service Password Reset" on page 14
- "High Availability and Load Balancing" on page 15

Selecting an Appropriate Configuration

Self Service Password Reset has a flexible configuration. You must choose what works best for you in your environment to properly configure it. Self Service Password Reset requires a location to install the application, a back-end user store, and a location to store the users' information such as the challenge-response information. Self Service Password Reset provides many different options for these main components. You must decide which components you want to use before installing Self Service Password Reset.

Answer the following questions to select the appropriate configuration for your environment.

What version of Self Service Password Reset are you installing? (Version)

There are two different versions of Self Service Password Reset: a full version and a trial version. For more information, see "Obtaining Self Service Password Reset" on page 17.

Where do you want to install Self Service Password Reset? (Platform)

Select where and what platform you want to use to install Self Service Password Reset. The supported locations and platforms are:

- **On-Premise:** You can install and deploy Self Service Password Reset on premise in your own IT environment. The support platforms for on premise are:
  - **Virtual:** You can deploy the Self Service Password Reset appliance in Hyper-V or VMware.
  - **Linux:** You can deploy the Self Service Password Reset WAR file on SUSE Linux Enterprise Server or Red Hat Enterprise Linux.
  - **Microsoft Windows Server:** You can install Self Service Password Reset with the `.msi` file on a Microsoft Windows Server.
- **In the Cloud:** You can deploy Self Service Password Reset in the following Cloud environments:
  - **Amazon Web Service:** You can deploy the Self Service Password Reset WAR file on SUSE Linux Enterprise Server.
  - **Microsoft Azure Market Place Platform:** You can deploy the Self Service Password Reset .msi file on a Windows Sever 2016 running in Azure.

Where are your users? (User Store)

Self Service Password Reset can manage users' credentials as long the information is in an LDAP directory. Select the LDAP directory that contains the users account that Self Service Password Reset will manage. The supported LDAP directories are:

- Active Directory
- eDirectory

For more information, see "Installing Self Service Password Reset" on page 24.

Where do you want to store the users' information? (Databases or LDAP Directories)

Self Service Password Reset must have access to either a database or an LDAP directory to stores the user's information such as the challenge-response information. Select the location where you want to save the users' information:

- **Local Database:** Self Service Password Reset contains a local database you can use to store the users challenge-responses information.

  WARNING: Do not use the local database in a production environment as there are no methods to make the local database storage redundant, nor are there optimal backup methods available for the local database.

- **External Database:** Best practice is to use an external database to store the users challenge-response information. The external database provides the ability to cluster to the database and easily backup the database. The supported databases are Microsoft SQL Server, PostgreSQL, and Oracle database. For more information, see "Installing Self Service Password Reset" on page 24.

  IMPORTANT: You must have an empty database created to install Self Service Password Reset with the external database. The installers create the appropriate tables and schema for the database that you choose to use.

- **LDAP:** You can securely store the users challenge-responses in the following LDAP directories:
  - **Active Directory:** If you choose to use Active Directory, it must be the same Active Directory domain where you users' accounts reside.
  - **eDirectory:** If you choose to eDirectory, it must be the same eDirectory tree that contains your users' accounts.

    NOTE: eDirectory is currently not support on the Amazon Web Server or in Microsoft Azure Market Place.platforms.

  - **eDirectory with NMAS** You can securely store the users challenge-responses in eDirectory using NMAS. Self Service Password Reset can read password and challenge policies from eDirectory. After saving a user's challenge-response answers, Self Service Password Reset can optionally write the challenge-response answers to the NMAS challenge-response format in addition to the configured methods. This enables interoperability of Self Service Password Reset with other products.

  For more information, see "Installing Self Service Password Reset" on page 24.

Securing Self Service Password Reset

You can deploy Self Service Password Reset along with applications that are available on the internet in the public domain. As an administrator, you must protect Self Service Password Reset so that unauthorized users cannot gain access to it and access users' credentials or make any configuration changes. You must check and control the installation, maintenance, and monitoring processes of Self Service Password Reset to ensure that you are following security best practices.

Depending on how you configure Self Service Password Reset, there are four different certificates you must create, manage, and maintain. Use the following information to help understand or create the certificates required to secure Self Service Password Reset.

- "Appliance Certificate" on page 13
- "HTTPS Certificate (Apache Tomcat and Browsers)" on page 13
- "LDAP Server Certificate" on page 14
- "Audit Server Certificates" on page 14

Appliance Certificate

If you choose to deploy the Self Service Password Reset appliance, you perform all administration and configuration tasks for the appliance over port 9443. The appliance certificate provides SSL encryption over port 9443 so that you perform the configuration and administration task securely.

The configuration process of the appliance generates a certificate using the specified DNS name of the appliance. When you access the administration console for the appliance the first time, you received an error in the browser stating this site is not trusted. You are given the option to trust the site or add an exception for the site. It depends on your browser as to what message you see.

The appliance administration console allows you to generate a new certificate key pair or import an officially signed certificate. For more information, see "Managing Digital Certificates" in the *Self Service Password Reset 4.2 Administration Guide*.

HTTPS Certificate (Apache Tomcat and Browsers)

The HTTPs certificate creates the secure SSL channel between the Self Service Password Reset application, which runs on Apache Tomcat, and the users' browsers. By installing the certificate in the users' browsers, the users do not see any warning messages that the site they are accessing is an untrusted site. It also removes any warning icons in the toolbars of the browsers.

By default, the Self Service Password Reset appliance and Windows deployment contain a certificate that the installation generates. The WAR file deployment does not and you must ensure that the Apache Tomcat web server on the Linux server is configured to use a certificate and communicate over SSL.

Self Service Password Reset uses the following ports for secure SSL traffic. The ports are different depending on the deployment of Self Service Password Reset you use.

- **Appliance:** port 443
- **Windows:** port 8443
- **Linux:** port 8443. This is the default secure port for Apache Tomcat. Depending on how you configured the Linux server, this port might be different.

To stop the untrusted site warning messages, you must create a vendor-signed SSL Certificate and then import that certificate into your users' browsers.

For detailed instructions on how to create a vendor-signed certificate to a to your users' browsers, see the following videos:

- How To Create a Vendor-Signed SSL Certificate Using OpenSSL Part 1
- How To Create a Vendor-Signed SSL Certificate Using OpenSSL Part 2
- How To Create a Vendor-Signed SSL Certificate Using OpenSSL Part 3

LDAP Server Certificate

The LDAP certificate is a certificate used to secure communication between Self Service Password Reset and the LDAP directories.The LDAP directories that contain your users and store the challenge-response information. Self Service Password Reset must trust the LDAP directory's server certificate to create a secure channel between the two products.

Self Service Password Reset manages the LDAP server certificates for you. If you use the Configuration Guide to walk you through configuring Self Service Password Reset, it automatically imports the LDAP server certificate for you. If you manually configure Self Service Password Reset, the Configuration Editor imports the LDAP server certificate for you when you create an LDAP profile. For more information, see "Configuring LDAP Directory Profile" in the *Self Service Password Reset 4.2 Administration Guide*.

Audit Server Certificates

To meet compliance standards, many companies require auditing for password changes, whether the changes came from the users or the help desk. Self Service Password Reset provides an auditing solution that tracks specific events that occur in the system. It also allows you to forward events to a Syslog server for further analysis of the information.

Self Service Password Reset manages the audit server certificates for you. If you use the Configuration Guide to walk you through configuring Self Service Password Reset, it automatically imports the audit server certificate for you. If you manually configure Self Service Password Reset, the Configuration Editor imports the LDAP server certificate for you when you configure an audit server. For more information, see "Auditing for Self Service Password Reset" in the *Self Service Password Reset 4.2 Administration Guide*.

Best Practices for Self Service Password Reset

Use the following information to help you decide how to configure Self Service Password Reset to get the best results.

- "Best Practices for Password Policy" on page 14
- "Best Practices for Self Service Password Reset Security" on page 15

Best Practices for Password Policy

To enhance the security of password policies:

- Use a word list to prevent easily guessable passwords
- Use a shared word list to prevent organizational password value use from becoming common among many users
- Do not allow users to configure challenge questions

- Do not impose complex syntax rules on users; instead, use a specific overall complexity level
- Use a long list of potential random question challenges that are unlikely to have similar answers among different users

For more information, see "Configuring a Profile for a Password Policy" in the *Self Service Password Reset 4.2 Administration Guide*.

Best Practices for Self Service Password Reset Security

To enhance the security of Self Service Password Reset, Micro Focus recommends that you do the following:

- Enable the CAPTCHA support.
- Configure HTTPS for end-to-end security.
- Configure LDAPS for end-to-end security.
- Use a strong encryption protocol for formatted hashed stored responses.
- Configure Self Service Password Reset to see source network addresses for complete audit records to be maintained.

For more information, see "Configuring Security Settings" in the *Self Service Password Reset 4.2 Administration Guide*.

High Availability and Load Balancing

Self Service Password Reset supports high availability and load balancing for user authentications through an L4 switch. You must install and deploy the L4 switch in your environment ensuring that you use session persistence. Self Service Password Reset uses your browser's session storage to facilitate seamless high availability and load balancing. As users are working and their existing sessions change, Self Service Password Reset requires the users to reauthenticate before they can continue their work.

To enable the load balancing and high availability for users authentications:

1. Install an L4 switch and ensure you use session persistence.
2. Deploy two or more separate, yet identical, instances of Self Service Password Reset.
   - **2a** Install and configure a Self Service Password Reset system.
   - **2b** Back up the configuration information. For more information, see "Backing Up Configuration Information" in the *Self Service Password Reset 4.2 Administration Guide*.
   - **2c** Install the second Self Service Password Reset system, then import the configuration information from the first system to the second system. For more information, see "Importing Configuration Information" in the *Self Service Password Reset 4.2 Administration Guide*.
   - **2d** Repeat these steps for each additional system you want to add.
3. Ensure that the L4 switch is configured to use sticky sessions. For a given browser session, the session must remain on the same Self Service Password Reset server over time unless the Self Service Password Reset server becomes unavailable.
4. Follow the L4 switch documentation to configure the L4 switch to provide load balancing for the Self Service Password Reset computers.

As long as you use a remote database, you can view the status of the nodes in the L4 switch through the Configuration Manager. Click the **Nodes** tab in the Configuration Manager and you can see the status of the nodes. The node that is the master is the node that has been running the longest.

3 Installing Self Service Password Reset

This chapter guides you through the process of installing the components and framework required for Self Service Password Reset.

- "Obtaining Self Service Password Reset" on page 17
- "Default Ports for Self Service Password Reset" on page 18
- "Deployment Requirements of Self Service Password Reset" on page 19
- "Installing Self Service Password Reset" on page 24

Obtaining Self Service Password Reset

Self Service Password Reset is available in two types: a trial version and a full version. You access the different version in different locations.

- "Downloading the Full Version" on page 17
- "Downloading the Trial Version" on page 17

Downloading the Full Version

You must have purchased Self Service Password Reset to access the full version of the product. To buy a full version of Self Service Password Reset, see How to Buy. The activation code is in the Customer Center where you download the software. For more information, see Customer Center Frequently Asked Questions.

To access a full version of Self Service Password Reset:

1. Log in to the Customer Center.
2. Click **Software**.
3. In the **Entitled Software** tab, click the appropriate version of Self Service Password Reset for your environment to download.

The Self Service Password Reset files are compressed packages of files that must be decompressed before you can use them. To decompress the Self Service Password Reset distribution packages:

Linux: Use `tar`. For example:

```
tar -zxvf ssprappliance.xxx.x86-x.x.xxx-ovf.tar.gz
```

Windows: Unzip the `.zip` files.

Downloading the Trial Version

We provide a trial version of Self Service Password Reset to allow you to see how the product works. The trial version does have the following limitations:

- After 100 authentications, the system requires a restart to continue functioning.
- After 10,000 authentications, you must reinstall the system.

NOTE: It is possible to upgrade from the trial version to the full version of Self Service Password by exporting the configuration from the trial version and importing the configuration to an installed full version.

To download the trial version:

1. Access the Download page at https://dl.netiq.com.
2. Click the **Find Trial Download** link.
3. Scroll down to find Self Service Password Reset, then click **Download**.
4. Enter your information to receive an email with the download link.

   IMPORTANT: You must enter a valid email address or you do not receive the email that contains the link to download the trial version.

5. After you receive the email, click the link then download the appropriate version for your environment.
6. (Conditional) Extract the compressed file for the appliance.

   NOTE: The OVF file includes a pointer to the `.vmdk` files; extract and store the contents of the `.tar.gz` file within the same folder. Do not rename the files.

   6a (Conditional) If you are using Windows, unzip the file to extract the appliance so that you can access the OVF file or the Hyper-V file.

   6b (Conditional) If you are using Linux, use the following command to extract the image:

The Self Service Password Reset files are compressed packages of files that must be decompressed before you can use them. To decompress the Self Service Password Reset distribution packages:

Linux: Use `tar`. For example:

```
tar -zxvf ssprappliance.xxx.x86-x.x.xxx-ovf.tar.gz
```

Windows: Unzip the `.zip` files.

Default Ports for Self Service Password Reset

Self Service Password Reset uses various ports to communicate with the LDAP directories, the databases, and the browsers. The following table lists the default ports Self Service Password Reset uses to help you plan your installation. You must open these ports in your firewall for Self Service Password Reset to work.

Table 3-1 *Self Service Password Reset Appliance Default Ports*

Component	Port	Protocol	Description
Inbound Traffic			
Appliance Management	9443	HTTPS	Appliance management for Self Service Password Reset. For more information, see "Managing the Appliance" in the *Self Service Password Reset 4.2 Administration Guide*.
Apache Tomcat	8080	HTTP	

Component	Port	Protocol	Description
Apache Tomcat	8443	HTTPS	
Outbound Traffic			
SMTP	25	SMTP	SMTP messages to an email server.
Audit	514	UDP/IP	For more information, see the documentation for the Syslog server that you are using.
SMS		HTTP or HTTPS	For more information, see the documentation for the SMS gateway that you are using.
CAPTCHA			For more information, see http://www.captcha.net/.
Remote Database	Configurable		For more information, see the: ◆ Oracle documentation ◆ PostgreSQL documentation ◆ SQL Server documentation
LDAP	Configurable default 389		For more information, see the LDAP directory documentation that you are using.
LDAPS	Configurable default 636		For more information, see the LDAP directory documentation that you are using.

Deployment Requirements of Self Service Password Reset

Ensure that you meet the following deployment requirements for you selected platform. For example, if you are deploying the Self Service Password Reset appliance, ensure that you have met the deployment requirements for the appliance.

- "Deployment Requirements for the Appliance" on page 20
- "Deployment Requirements for Self Service Password Reset on Windows" on page 21
- "Deployment Requirements for Self Service Password Reset WAR File on Linux" on page 22

Deployment Requirements for the Appliance

The following table contains the minimum requirements required to deploy the Self Service Password Reset appliance. Ensure that you meet these minimum requirements before deploying the appliance.

Table 3-2 *Self Service Password Reset Appliance Requirements*

Component	Requirements
Virtual Systems	◆ Hyper-V versions 4.0 ◆ VMware ESX 5.5 or later **NOTE:** Your VMware license must be Enterprise or Enterprise Plus if you want to use remote serial connections. For more information, please refer to VMware support. For more information, see the VMware documentation (https://www.vmware.com/support/pubs/).
Memory	2 GB of RAM
Hard disk space	40 GB
Browsers	◆ Mozilla Firefox 54.0.1 or later ◆ Google Chrome 59.0.3071 or later ◆ Microsoft Internet Explorer 11.0.43 or later ◆ Edge 40.15063 or later
IP Ports	Ensure that the default ports for the Self Service Password Reset appliance are open in your firewall. For more information, see "Default Ports for Self Service Password Reset" on page 18.
LDAP Directories	◆ NetIQ eDirectory ◆◆ 9.0 SP3 ◆◆ 8.8 SP8 Patch 10 or later ◆ Microsoft Active Directory ◆◆ 2016 (Only supported with Self Service Password Reset Patch Update 2 or later) ◆◆ 2012 **IMPORTANT:** Self Service Password Reset does not support the Active Directory Global catalog services. Instead, you can configure multiple profiles for different domains to represent the data repository for each domain. For more information about creating multiple profiles, see "Configuring Policies" in the *Self Service Password Reset 4.2 Administration Guide*.
Remote Databases	◆ Microsoft SQL Server ◆◆ 2016 (Only supported with Self Service Password Reset Patch Update 2 or later) ◆◆ 2012 ◆ Oracle Database 12c ◆ PostgreSQL 9.6.3

Component	Requirements
License	The appliance is the only platform that requires a license. The license is required to receive online updates. Obtain the license from the Customer Care Center. You add the license to the appliance administration console after you complete the installation. For more information, see "Performing an Online Update" in the *Self Service Password Reset 4.2 Administration Guide*.

After you have met the deployment requirements, you must deploy the appliance. For more information, see "Deploying the Self Service Password Reset Appliance" on page 28.

Deployment Requirements for Self Service Password Reset on Windows

The following table contains the minimum requirements required to deploy the Self Service Password Reset on a Windows server. Ensure that you meet these minimum requirements before starting the installation.

Table 3-3 *Self Service Password Reset on Windows Requirements*

Component	Requirements
Windows Platforms	◆ Microsoft Windows Server ◆◆ 2016 (Only supported with Self Service Password Reset Patch Update 2 or later) ◆◆ 2012 R2 (64-bit)
Cloud Platforms	◆ Microsoft Azure Market Place Platform ◆◆ Windows Server 2016 VM
Memory	1 GB of RAM **NOTE:** Azure DS1_V2 Standard size
Hard disk space	5 GB
Browsers	◆ Mozilla Firefox 54.0.1 or later ◆ Google Chrome 59.0.3071 or later ◆ Microsoft Internet Explorer 11.0.43 or later ◆ Edge 40.15063 or later
IP Ports	Ensure that the default ports for the Self Service Password Reset appliance are open in your firewall. For more information, see "Default Ports for Self Service Password Reset" on page 18.

Component	Requirements
LDAP Directories	◆ NetIQ eDirectory ◆◆ 9.0 SP3 ◆◆ 8.8 SP8 Patch 10 or later **NOTE:** eDirectory is not currently supported in Amazon Web Service or Azure environments. ◆ Microsoft Active Directory ◆◆ 2016 (Only supported with Patch Update 2 or later) **IMPORTANT:** Self Service Password Reset does not support the Active Directory Global catalog services. Instead, you can configure multiple profiles for different domains to represent the data repository for each domain. For more information about creating multiple profiles, see "Configuring Policies" in the *Self Service Password Reset 4.2 Administration Guide*. ◆◆ Active Directory Domain Service (AD DS) **NOTE:** This version of the Active Directory Domain Service is only supported when you deploy the `.msi` file on Azure. ◆◆ 2012
Remote Databases	◆ Microsoft SQL Server ◆◆ 2016 (Only supported with Self Service Password Reset Patch Update 2 or later) ◆◆ 2012 ◆ Oracle Database 12c ◆ PostgreSQL 9.6.3
Java	Java JDK 1.8.0_141 (Java 8u141) **NOTE:** The `.msi` file supplies this version of Java and installs it for you. Any other version of Java is not supported.
Apache Tomcat	Apache Tomcat 8.5.16 **NOTE:** The `.msi` file supplies this version of Apache Tomcat and installs it for you. Any other version of Apache Tomcat is not supported.

After you have met deployment requirements, you must install Self Service Password Reset on a Windows server. For more information, see "Deploying Self Service Password Reset on Windows" on page 29.

Deployment Requirements for Self Service Password Reset WAR File on Linux

The following table contains the minimum requirements required to deploy the Self Service Password Reset on a Linux server. Ensure that you meet these minimum requirements before starting the installation.

Table 3-4 Self Service Password Reset WAR File Requirements on Linux

Component	Requirements
Linux Platforms	◆ SUSE Linux Enterprise Server 12 SP2 or later (64-bit) ◆ SUSE Linux Enterprise Server 11 SP4 (64-bit) ◆ Red Hat Enterprise Linux 7.3 or later (64-bit)
Cloud Platforms	◆ Amazon Web Service EC2 Linux Platform ◆ SUSE Linux Enterprise Server 12 SP3 (HVM), SSD Volume
Memory	1 GB of RAM **NOTE:** AWS EC2 instance type: t2.micro
Hard disk space	5 GB
Browsers	◆ Mozilla Firefox 54.0.1 or later ◆ Google Chrome 59.0.3071 or later ◆ Microsoft Internet Explorer 11.0.43 or later ◆ Edge 40.15063 or later
IP Ports	Ensure that the default ports for the Self Service Password Reset appliance are open in your firewall. For more information, see "Default Ports for Self Service Password Reset" on page 18.

LDAP Directories	◆ NetIQ eDirectory
	  ◆ 9.0 SP3
	  ◆ 8.8 SP8 Patch 10
	  NOTE: eDirectory is not currently supported in Amazon Web Service or Azure environments.
	◆ Microsoft Active Directory
	  ◆ 2016 (Only supported with Patch Update 2 or later)
	  IMPORTANT: Self Service Password Reset does not support the Active Directory Global catalog services. Instead, you can configure multiple profiles for different domains to represent the data repository for each domain. For more information about creating multiple profiles, see "Configuring Policies" in the *Self Service Password Reset 4.2 Administration Guide*.
	  ◆ Active Directory Domain Service (AD DS)
	  NOTE: This version of the Active Directory Domain Service is only supported when you deploy the WAR file on AWS.
	  ◆ 2012

Remote Databases	◆ Microsoft SQL Server
	  ◆ 2016 (Only supported with Patch Update 2 or later)
	  ◆ 2012
	◆ Oracle Database 12c
	◆ PostgreSQL 9.6.3

Component	Requirements
Java	Java JDK 1.8.0_141 (Java 8u141) or later of Java 1.8.0_*xxx* **IMPORTANT:** You must install this version of Java on the Linux server prior to deploying the WAR file. You must be familiar with the installation, configuration, and maintenance of Java.
Apache Tomcat	◆ Apache Tomcat 8.5.16 or later of Apache Tomcat 8.5.*x* ◆ Apache Tomcat 8.0.45 or later of Apache Tomcat 8.0.*x* **IMPORTANT:** You must install this version of Apache Tomcat on the Linux server prior to deploying the WAR file. You must be familiar with the installation, configuration, and maintenance of Apache Tomcat.

After you have met the deployment requirements, you must deploy the WAR file. For more information, see "Deploying the WAR File on Linux" on page 30

Installing Self Service Password Reset

Before you install Self Service Password Reset, you must decide where you want to install it. Do you want to install it on-premise or in the Cloud? If you choose to install Self Service Password Reset in the Cloud, there are some prerequisites you must meet and have a good understanding of the Cloud environment.

Next, you must select a platform specific installer for your environment. Use the following information to install the platform specific version that is appropriate for your environment.

- "Deploying Self Service Password Reset in the Cloud" on page 24
- "Deploying the Self Service Password Reset Appliance" on page 28
- "Deploying Self Service Password Reset on Windows" on page 29
- "Deploying the WAR File on Linux" on page 30

Deploying Self Service Password Reset in the Cloud

You can deploy Self Service Password Reset in Amazon Web Service (AWS) or Microsoft Azure Marketplace. The following documentation is for only when you deploy Self Service Password Reset in one of the Cloud environments. Use the following information to deploy Self Service Password Reset in the Cloud.

- "Deploying Self Service Password Reset in Amazon Web Services" on page 24
- "Deploying Self Service Password Reset on Azure" on page 27

Deploying Self Service Password Reset in Amazon Web Services

Self Service Password Reset supports deploying the WAR file in the Amazon Web Service (AWS} on a SUSE Linux Enterprise 12 SP3 Server that connects to Active Directory Domain Services which contains your users accounts you want to manage. Currently, this is the only scenario that has been tested and is supported for Self Service Password Reset. Use the following information to deploy Self Service Password Reset on AWS.

- "Prerequisites for Deploying Self Service Password Reset on AWS" on page 25
- "Supported Deployment Scenario for Self Service Password Reset on AWS" on page 25

- "Accessing the AWS EC2 SLES12 SP3 Instance Using SSH on Linux" on page 26
- "Deploying the WAR File on the AWS EC2 SLES 12 SP3 Instance" on page 26

Prerequisites for Deploying Self Service Password Reset on AWS

You must meet the following prerequisite to deploy Self Service Password Reset on AWS:

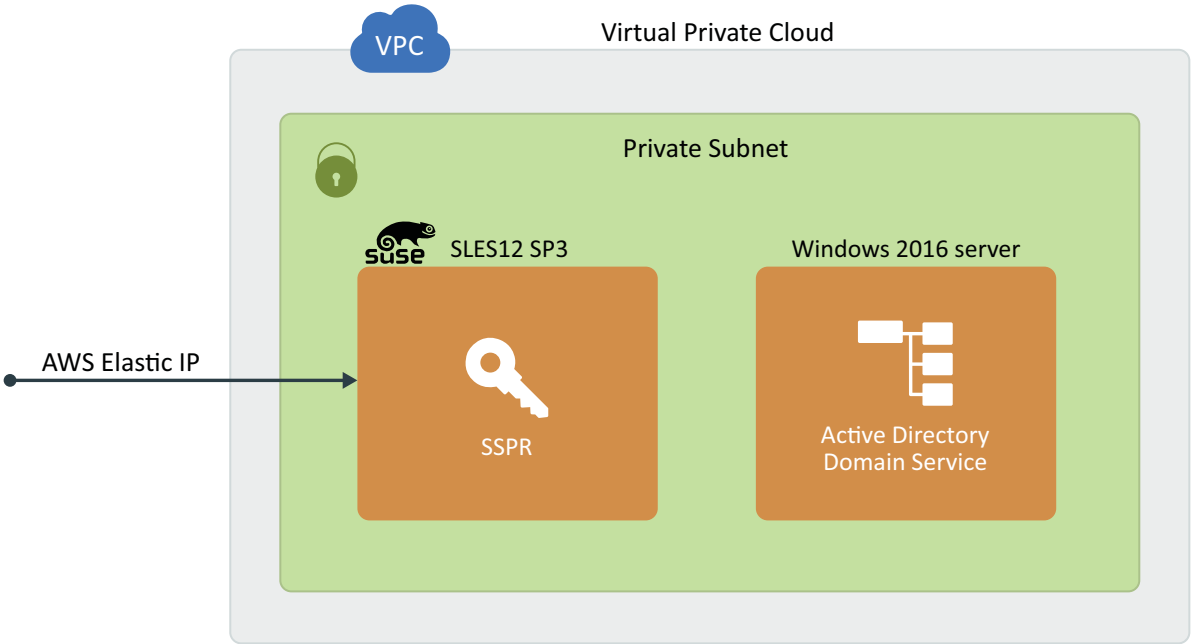
- You must have an AWS account. For more information, see "Getting Started with Amazon Elastic Container Service".
- You must have a basic understanding of Amazon Elastic Compute Cloud (EC2). For more information, see Amazon Elastic Compute Cloud Documentation.
- You must have a basic understanding of the networking on AWS. For example, you must understand:
  - Virtual Private Cloud (VPC)
  - Subnets
  - Network address translation (NAT)
  - Security group

  For more information, see Networking Products with AWS.
- You must have a basic understanding deploying Microsoft Windows 2016 server on AWS. For more information, see Getting Started with a Service.
- You must have a basic understanding of Microsoft Active Directory running on AWS. For more information, see Microsoft Active Directory.

Supported Deployment Scenario for Self Service Password Reset on AWS

You can configure the Self Service Password Reset Amazon Web Services (AWS) environment in several ways. The following example NetIQ tested and supports.

Figure 3-1 *Overview of AWS Deployment*



Specifically, you deploy an AWS Elastic Compute Cloud (EC2) SLES12 instances and a Windows 2016 EC2 instance in an AWS Virtual Private Cloud (VPC) connected with a common subnet. The SLES12 instance hosts Self Service Password Reset with an elastic IP assigned. The Windows 2016 instance hosts Active Directory that stores all of the user accounts that you want to manage.

Deploying the EC2 instance of SUSE Linux Enterprise Server and the Windows 2016 server running Active Directory into an EC2 instance is beyond the scope of this documentation. For more information, see: and in the AWS documentation.

- **SUSE Linux Enterprise Server:** "SUSE Linux Enterprise Server on Amazon EC2" in the AWS documentation.
- **Microsoft Windows 2016 Server:** "Running a Recipe on a Windows Instance" and "Microsoft Active Directory" in the AWS documentation.

In this scenario, this is the first deployment of Self Service Password Reset into AWS. This means you must create a new security group for Self Service Password Reset. A security group is a a virtual firewall that controls the traffic for one or more instances. AWS associates each security group with a list of firewall rules to secure associated EC2 instances. You must create a security group that contains the firewall rules for Self Service Password Reset.

Accessing the AWS EC2 SLES12 SP3 Instance Using SSH on Linux

You must access the RSA key pair file you downloaded when creating the SLES 12 SP3 instance. The key pair file name is similar to *SSPR*`_keypair.pem.txt`. Protect this file using a Linux command such as:

```
chmod 500 SSPR_keypair.pem.txt
```

To access the new instance using SSH, issue a Linux command such as:

```
ssh -i "SSPR_keypair.pem.txt" ec2-user@ec2-34-216-102-176.us-west-
2.compute.amazonaws.com
or
ssh -i "SSPR_keypair.pem.txt" ec2-user@34.216.102.176
```

The `-i "SSPR_keypair.pem.txt"` parameter instructs SSH to apply the downloaded *identity file* from which the identity (private key) for public key authentication is read. The `ec2-user@` parameter indicates the default user name used by SSH to connect to the instance.

Deploying the WAR File on the AWS EC2 SLES 12 SP3 Instance

After you have created the AWS EC2 SLES 12 SP3 instance, you must deploy the Self Service Password Reset WAR file. Deploying the WAR file on a SLES 12 SP3 server on AWS the same as if you installed SLES 12 SP3 on a physical server.

Self Service Password Reset is a web application you must install Apache Tomcat and Java on the SLES 12 SP3 instance before deploying the WAR file.

1. Download the Self Service Password Reset War file. For more information, see "Obtaining Self Service Password Reset" on page 17.
2. You must complete the prerequisites of installing Apache Tomcat, Java, and set the correct environment variables before deploying the WAR file. For more information, see "Prerequisites for Deploying the WAR File" on page 30.
3. Deploy the WAR file into the Apache Tomcat instance running on the AWS EC2 SLES 12 SP 3 instance. For more information, see "Deploying the WAR File on Linux" on page 30.

After you have deployed the WAR file you must configure this instance of Self Service Password Reset to connect to the AWS EC2 Windows 2016 server instance running Active Directory. For more information, see Chapter 4, “Configuring Your Environment for Self Service Password Reset,” on page 33.

Deploying Self Service Password Reset on Azure

Self Service Password Reset supports deploying the `.msi` file on Azure on a Windows 2016 Server that connects to Active Directory Domain Services which contains your users’ accounts you want to manage. Currently, this is the only scenario that has been tested and is supported for Self Service Password Reset. Use the following information to deploy Self Service Password Reset on Azure.

- “Prerequisites” on page 27
- “Supported Deployment Scenario of Self Service Password Reset on Azure” on page 27
- “Installing the .msi File on the Windows 2016 Deployed In Azure” on page 28

Prerequisites

You must meet the following prerequisites to deploy Self Service Password Reset on Azure:

- You must have a basic understanding of Azure and the following concepts:
  - Source environments
  - Virtual networks (VNets)
  - Storage Accounts
  - Subnets
  - Networking security groups (NSG)

  For more information, see Microsoft Azure Documentation.
- You must have a basic understanding of AD DS on Azure. For more information, see “Creating an Active Directory Domain Services (AD DS) on Azure”.
- You must have an Azure account. For more information, see Microsoft Azure Account.
- You must deploy the Windows 2016 server in Azure that will run Self Service Password Reset. For more information, see “Windows Virutal Server Documentation”.

Supported Deployment Scenario of Self Service Password Reset on Azure

There are many different ways you can configure the Self Service Password Reset on Azure. The following is a tested and supported example.

The tested and supported scenario consists of two Azure Windows 2016 Server VM instances deployed in an Azure Virtual Network (VNet) connected with a common subnet. You dedicate one Windows 2016 Server VM instance to hosting Active Directory Domain Services (AD DS). You dedicate the other Windows 2016 Server VM instance to hosting Self Service Password Reset where you assign a Public IP address.

The installation of Active Directory Domain Services (AD DS) into a second Windows 2016 Server instance is beyond the scope of this section. For more information, see “Creating an Active Directory Domain Services (AD DS) on Azure”.

Installing the .msi File on the Windows 2016 Deployed In Azure

After you have deployed the Windows 2016 Server, you must now install the `.msi` file to install Self Service Password Reset.

1. Download a copy of the Self Service Password Reset `.msi` file from the download site. For more information, see "Obtaining Self Service Password Reset" on page 17.
2. Copy the `.msi` file to the Windows 2016 VM using Remote Desktop. For more information, see "Remote Desktop Service".
3. Access the `.msi` file on the Windows 2016 VM, then launch the Self Service Password Reset installer.
4. Follow the prompts to complete the installation. For more information, see "Deploying Self Service Password Reset on Windows" on page 29.

After the installation completes, you must configure Self Service Password Reset to communicate to the second Windows 2016 VM server that has Active Directory Domain Services installed and where your user accounts reside.

After installing Self Service Password Reset, you must configure it using a compatible web browser. Since the Windows 2016 Server VM has a public address, this configuration can occur from any internet-connected machine by browsing to the Self Service Password Reset port. For this example it is:

`https://netiq-sspr.westus.cloudapp.azure.com:8443/sspr`

The steps for configuring Self Service Password Reset are the same whether it is deployed on-premise or in the Cloud. For more information, see Chapter 4, "Configuring Your Environment for Self Service Password Reset," on page 33.

Deploying the Self Service Password Reset Appliance

You can deploy a virtual appliance that contains Self Service Password Reset as one of the installation options. The currently supported platforms for the appliance are VMware and Hyper-V. We recommend that you have a good understanding of the virtual platform before deploying the appliance.

Before you deploy the appliance, ensure that you meet all of the appliance requirements and that you have downloaded and extracted the appropriate version of the appliance. For more information, see "Deployment Requirements for the Appliance" on page 20.

To deploy the Self Service Password Reset appliance:

1. Deploy the appliance to your virtual environment. For more information, see:

   Hyper-V: Importing a Virtual Machine.

   VMware: Deploy an OVF Template.
2. Power on the appliance.
3. Select the appropriate language, then read the license and click **Accept**.
4. Use the following information to configure the appliance:

   root Password

   Specify a password for the `root` user on the appliance.

   NTP Server

   Specify a primary and secondary NTP server used to keep time on the appliance.

Region and Time Zone

Select your region and time zone.

Hostname and Networking options

Specify a hostname for the appliance, then select whether to use a static IP address or DHCP. If you use a static IP address, you must specify the IP address, subnet mask, the gateway, and the DNS servers.

5 Click **Finish** and wait for the appliance initialization to complete.

After you complete the deployment of the appliance, you must configure your environment to work with Self Service Password Reset. For more information, see Chapter 4, "Configuring Your Environment for Self Service Password Reset," on page 33.

NOTE: The appliance is the only platform that requires a license for online updates. You must obtain the license from the Customer Care Center. After you have the license, you install the license through the appliance administration console. For more information, see "Performing an Online Update" in the *Self Service Password Reset 4.2 Administration Guide*.

Deploying Self Service Password Reset on Windows

Installing Self Service Password Reset on Windows server is another configuration option. There is a `.msi` executable file that installs Self Service Password Reset on a Windows server. Use the following information to install Self Service Password Reset on Windows.

Ensure that you have met all of the installation requirements for installing Self Service Password Reset on Windows and that you have downloaded an extracted the `.msi` file before beginning the installation. For more information, see "Deployment Requirements for Self Service Password Reset on Windows" on page 21.

To install Self Service Password Reset on Windows:

1 Launch the `sspr.x.x.msi` file.

2 Read the notice for Self Service Password Reset, then click **Next**.

3 Read and accept the end user license, then click **Next**.

4 Specify the path for the installation of Self Service Password Reset, then click **Next**.

5 In **Configure SSPR-Service URLs**, specify the following:

Shutdown Port

Specify the port number for Apache Tomcat shutdown port.

HTTPS Secure Port

Specify the secure port for Self Service Password Reset service.

Open Secure HTTPS Port

Select the firewall setting for Self Service Password to use on the Windows server. The installer selects the open HTTPS Windows firewall port by default. The options for the firewall are:

All

This enables users to use Self Service Password Reset on a domain, private or public networks.

Domain

This enables users to use Self Service Password Reset on a domain network only.

Private

This enables users to use Self Service Password Reset on a private network.

Public

This enables users to use Self Service Password Reset on a public network.

6 Click **Next**, then click **Install**.

7 Click **Install**.

8 Record the **HTTPS Secure URL**, then click **Finish**.

After completing the installation, you must configure your environment to work with Self Service Password Reset. For more information, see Chapter 4, "Configuring Your Environment for Self Service Password Reset," on page 33.

Deploying the WAR File on Linux

Self Service Password Reset is a web application. When you install Self Service Password Reset, you are deploying a WAR (Web application ARchive) file as Java servlet application running on the Apache Tomcat web server. The WAR file contains an Apache Tomcat implementation of the Self Service Password Reset application. The following procedures work for the supported distributions of Linux.

- "Prerequisites for Deploying the WAR File" on page 30
- "Setting Operating System Environment Variables" on page 31
- "Deploying the Self Service Password Reset WAR File" on page 31

Prerequisites for Deploying the WAR File

You must have Java and Apache Tomcat installed and running on Linux before you deploy the WAR file. If you already have Java and Tomcat installed, proceed to "Setting Operating System Environment Variables" on page 31. Follow these steps to install and validate the installation of Java and Tomcat.

To install Java and Tomcat:

1 Install Java 8. For more information, see "JDK 8 and JRE 8 Installation".

Verify `JAVA_HOME` (or `JRE_HOME`) path is set appropriately by entering:

```
echo $JAVA_HOME
```

or

```
echo $JRE_HOME
```

2 Install Tomcat 8. For more information, see "Tomcat Setup".

3 Start Tomcat by executing the `catalina.sh` script in the *`Tomcat_Home`*`/bin` directory.

```
./catalina.sh start
```

4 Validate you can access `http://localhost:`*`port`*. The default port is 8080.

Check the `Tomcat_Home/logs/catalina.out` file for any errors if you are unable to access the default Tomcat page.

Setting Operating System Environment Variables

Self Service Password Reset, as a Java servlet application running on Apache Tomcat, requires several operating system environmental variables to be set. There are various methods for setting environmental variables depending on the operating system. The recommended place to specify these variables is a `setenv` script. For more information, see Section 3.4 in the Apache Tomcat documentation.

The following are the Self Service Password Reset specific environment variables:

- `SSPR_APPLICATIONPATH` (Required): Specifies where Self Service Password Reset stores its configuration data file (`SSPRConfiguration.xml`). This file contains all of the Self Service Password Reset configuration data. The specified path must exist prior to starting Self Services Password Reset.

  For example: `export SSPR_APPLICATIONPATH="/etc/opt/microfocus/sspr"`
- `CATALINA_OPTS`: Allows specification of additional options for the Java command that starts Apache Tomcat. The recommended Java options for the Self Service Password Reset Java servlet application running on Apache Tomcat include:
  - `-Xms`

    Specifies the initial heap memory allocation pool.
  - `-Xmx`

    Specifies the maximum heap memory allocation pool for a Java Virtual Machine (JVM).

  Setting the initial and maximum heap memory size to the same size is a best practice because the JVM does not increase heap memory size at runtime. The recommended SSPR heap memory size is 1 GB (1024 MB). For more information about how to set Java heap size, see the Apache Tomcat documentation.

  For example: `export CATALINA_OPTS="-Xms1024M -Xmx1024M"`

The following is an example of a `setenv` script located here `Tomcat_Home/bin/setenv.sh`:

```
export SSPR_APPLICATIONPATH="/etc/opt/microfocus/sspr"
export CATALINA_OPTS="-Xms1024M -Xmx1024M"
```

Deploying the Self Service Password Reset WAR File

After you have installed Java and Apache Tomcat and they are running with the appropriate OS environmental variables set, you must deploy the Self Service Password Reset WAR file. Ensure that you have downloaded and extracted the file. For more information, see “Obtaining Self Service Password Reset” on page 17.

To deploy the WAR file on Linux:

1. Copy the sspr.war file to the *`Tomcat_Home`*`/webapps/` directory.

   When Apache Tomcat discovers the `sspr.war` file in the `Tomcat_Home/webapps/` directory, Apache Tomcat auto-deploys Self Service Password Reset in an automatically created directory; *`Tomcat_Home`*`/webapps/sspr/`.
2. Stop Apache Tomcat by running the `catalina.sh` script in the *`Tomcat_Home`*`/bin` directory.

   ```
   ./catalina.sh stop
   ```
3. Start Apache Tomcat by running the `catalina.sh` script in the *`Tomcat_Home`*`/bin` directory.

   ```
   ./catalina.sh start
   ```

After deploying the WAR file, you must configure your environment to work with Self Service Password Reset. For more information, see Chapter 4, “Configuring Your Environment for Self Service Password Reset,” on page 33.

4 Configuring Your Environment for Self Service Password Reset

After you have installed Self Service Password Reset, you must configure your environment to allow Self Service Password Reset to work. You can manually configure your environment, or you can use the Configuration Guide that comes with Self Service Password Reset.

The Self Service Password Reset Configuration Guide walks you through configuring your environment. It creates certificates for you, it provides LDIF files to extend the schema for the LDAP directories, and it shows you what rights you must have in the LDAP directories for Self Service Password Reset to work. It also helps you configure a secure connection to an external database if that is your configuration choice.

If you manually configure your environment, you must create and manage certificates, configure the LDAP directories by extending schema and assigning rights, and you must configure the external databases to communicate with Self Service Password Reset.

You must complete these configuration tasks before you can use Self Service Password Reset.

- "Self Service Password Reset Configuration Worksheet" on page 33
- "Using the Configuration Guide" on page 36
- "Manually Configuring Self Service Password Reset" on page 37
- "Integrating with Other NetIQ Products" on page 43

Self Service Password Reset Configuration Worksheet

Use the following worksheet to gather the required information to use the Configuration Guide or to manually configure your environment.

Table 4-1 *Self Service Password Reset Configuration Worksheet*

Component	❑	Gather the following information:
Feature Usage Statics		
	❑	Decide whether to allow NetIQ to gather statistical data about how you use Self Service Password Reset. We use this information to focus development on the most used features. You must select whether to enable or disable this feature. You can turn this feature on through the Configuration Editor. For more information, see "Configuring the Telemetry Options "in the *Self Service Password Reset 4.2 Administration Guide*.
LDAP Directory Information		
	❑	Full DNS name or IP address and the port of the LDAP server **NOTE:** Do not use a virtual address or a proxy server address.

Component	❑	Gather the following information:
	❑	LDAP server certificates Self Service Password Reset manages the LDAP server certificates for you. When you define the default LDAP profile or create a new profile, the Configuration Editors imports the LDAP service certificate for you.
	❑	Fully qualified LDAP distinguished name (DN) of the proxy administrator credentials For security reasons, create a proxy LDAP administrator that has sufficient rights to administer the users that log in to this system.
	❑	Fully qualified DN of the root container of your LDAP users You can add additional containers after the Configuration Guide completes.
	❑	Fully qualified DN of an LDAP administrators group A group in your LDAP directory to use to control administrative access to Self Service Password Reset.
	❑	Fully qualified DN of an LDAP test user Self Service Password Reset uses this test user to periodically test the connection between the LDAP server and the system.
	❑	LDAP attribute permissions You must change the LDAP attribute permissions to allow Self Service Password Reset to manage your users' credentials. The Configuration Guide displays the specific permissions you must change for your environment. If you perform a manual install, you must change these same attribute permissions for your environment. For more information, see "Configuring the LDAP Directories" on page 37.
Self Service Password Reset URL		
	❑	URL to this deployment of Self Service Password Reset that the users access The fully qualified hostname of the server running Self Service Password Reset.
Challenge-Response Storage Local Database		**NOTE:** Select one of the locations to store the challenge-response information: local database, LDAP, or remote database.
	❑	Local database - Testing Only Use for testing only and nothing else must be done to your environment.
Challenge-Response Storage LDAP		

Component	❑	Gather the following information:
	❑	LDAP You must extend the schema in your LDAP directory and assign rights to allow Self Service Password Reset to manage the users. If you are using eDirectory, you can allow the Configuration Guide to extend the schema for you or you can manually extend the schema with the provided files. For Active Directory, you must manually extend the schema using the provided files. For more information, see "Configuring the LDAP Directories" on page 37.
Challenge-Response Storage Remote Database		
	❑	Empty database You must install an empty database that Self Service Password Reset supports. The configuration process adds the appropriate tables and schema to the database.
	❑	Database driver You must download the JDBC driver from the website of the database you are using. You upload the JAR or ZIP file during the configuration of Self Service Password Reset.

	❑	Database class
		
		You must specify the Java class name of the JDBC driver. For example:
		
		◆ **Microsoft SQL:**
		`com.microsoft.sqlserver.jdbc.SQLServerDriver`
		◆ **Microsoft SQL using jTDS:**
		`net.sourceforge.jtds.jdbc.Driver`
		◆ **Oracle:** `oracle.jdbc.OracleDriver`
		◆ **PostgreSQL:** `org.postgresql.Driver`

	❑	Database connection string This setting configures the Java JDBC database driver with the information required to reach your database server such as IP address, port number, and database name. For example: ◆ **Microsoft SQL:** `jdbc:sqlserver://`*`host.example.net`*`:`*`port`*`;`*`databaseName`*`=SSPR` ◆ **Microsoft SQL using jTDS:** `jdbc:jtds:sqlserver://host.example.net:`*`port`*`/SSPR` ◆ **Oracle:** `jdbc:oracle:thin:@//`*`host.example.net`*`:1521/SSPR` ◆ **PostgreSQL:** `jdbc:postgresql://`*`host:port/database`*

Component	❑	Gather the following information:
	❑	Library Path - Microsoft SQL only Set the appropriate values for JAVA_OPTS in catalina.bat in the `tomcat/bin` folder. For more information, see the Tomcat documentation.
	❑	Database user name A user name that Self Service Password Reset uses to authenticate to the database.
	❑	Database password The password of the database user Self Service Password Reset uses to authenticate to the database.

Using the Configuration Guide

After you have completed the Self Service Password Reset installation, you must configure your environment to use Self Service Password Reset. Self Service Password Reset contains a Configuration Guide that walks you through configuring your environment. The Configuration Guide simplifies the configuration process for you.

To use the Configuration Guide:

1. Ensure that you have gathered all of the information in the worksheet before proceeding. For more information, see "Self Service Password Reset Configuration Worksheet" on page 33.
2. Access the appropriate URL for your deployment.

   Appliance

   ```
   https://dns-name/sspr
   ```

   Windows

   ```
   https://localhost:8443/sspr
   ```

   WAR File

   ```
   https://localhost:port/sspr
   ```
3. Accept the license agreement.
4. Click **Start Configuration Guide**.
5. Follow the instructions for your environment.

   NOTE: The Configuration Guide displays information unique to your environment and your configuration choices.

6. (Conditional) If you are using Active Directory, you must manually extend the schema in the LDAP directories to work with Self Service Password Reset. For more information, see "Configuring the LDAP Directories" on page 37.

After you completed the Configuration Guide, you can now configure Self Service Password Reset for you environment. Proceed to "Getting Started" in the *Self Service Password Reset 4.2 Administration Guide*.

If you are using eDirectory to store the challenge-response information, there is one post-configuration step you must perform. You must install the iManager Password Management plugin and enable the Universal Password policy. For more information, see "Managing Password" in the *eDirectory Administration Guide*.

Manually Configuring Self Service Password Reset

If you choose to manually configure Self Service Password Reset, there are a number of different tasks you must perform. Complete the following tasks in the order listed, to manually configure Self Service Password Reset and your environment.

1. Gather the information listed in the worksheet.

   For more information, see "Self Service Password Reset Configuration Worksheet" on page 33.
2. Manually configure your LDAP directory by extending the schema and assigning permissions.

   For more information, see "Configuring the LDAP Directories" on page 37.
3. Manually create an LDAP profile in the Self Service Password Reset Configuration Editor.

   For more information, see "Creating an LDAP Profile for Your Environment" on page 41.
4. Manually configure your external database to store the challenge-response information.

   For more information, see "Configuring Databases" on page 41.
5. Manually define the database settings in the Self Service Password Reset Configuration Editor.

   For more information, see "Configuring Self Service Password Reset to Work with the External Database" on page 42.

After you have completed the manual configuration of your environment, you can now configure Self Service Password Reset. Proceed to "Getting Started" in the *Self Service Password Reset 4.2 Administration Guide*.

Configuring the LDAP Directories

To allow Self Service Password Reset to store the challenge-response information in an LDAP directory, you must extend the LDAP directory schema and assign specific permissions to attributes in the LDAP directory. This allows Self Service Password Reset to manage the passwords for your users.

Self Service Password Reset provide `.ldif` files that manually extend the schema for the LDAP directories and change the permissions that allow Self Service Password Reset to work. You can access the `.ldif` files here: `https://sspr.server.com/sspr/public/reference/` on your Self Service Password Reset application. The `.ldif` files are also included in the Configuration Guide for the appliance and for the Windows installer.

WARNING: Extending the schema and changing rights in your LDAP directory permanently changes the LDAP directory. Ensure that your LDAP directory administrator performs these steps. If the directory is not healthy or there are communication problems in your network, changing the schema can cause problems.

Self Service Password Reset contains an LDAP Permissions tool that reads your Self Service Password Reset configuration file. The LDAP Permissions tool lists all of the required rights for your environment depending on the components of Self Service Password Reset you have enabled. The rights listed in the tool change depending on the Self Service Password Reset modules you enable. The following steps are guidelines for what rights you need in your environment for Self Service

Password Reset to work. It is best to use the LDAP Permissions tool to see all of the rights specific to your deployment of Self Service Password Reset. For more information, see "Viewing LDAP Permissions Recommendations" in the *Self Service Password Reset 4.2 Administration Guide*.

Use the following information to extend the LDAP directory schema and assign rights:

- "Configuring eDirectory" on page 38
- "Configuring Active Directory" on page 40

Configuring eDirectory

Before you extend the schema or change any rights to make Self Service Password Reset work with eDirectory, you must install the iManager Password Management plugin and enable the Universal Password policy. For more information, see "Managing Password" in the *eDirectory Administration Guide*.

Self Service Password Reset uses eDirectory attributes to store the following user data:

- The last time a user changed the password
- The last time Self Service Password Reset sent an email notification to the user about password expiry
- Secret questions and answers

Use the following information to modify eDirectory:

- "Extending the eDirectory Schema" on page 38
- "Modifying eDirectory Rights to Grant Permissions" on page 39

Extending the eDirectory Schema

You must use eDirectory tools to extend the eDirectory schema with the `edirectory-schema.lidf` file. You can access this file here: `https://sspr.server.com/sspr/public/reference/ldap-schema.jsp`.

Depending on your platform, you must use a different eDirectory tool to extend the schema. The steps for extending the schema are in the eDirectory documentation. For more information, see "Manually Extending the Schema" in the *NetIQ eDirectory Administration Guide.*

The `edirectory-schema.ldif` file adds the following Self Service Password Reset attributes to the eDirectory schema:

- `pwmEventLog`
- `pwmResponseSet`
- `pwmLastPwdUpdate`
- `pwmGUID`
- `pwmOTPsecret`

Modifying eDirectory Rights to Grant Permissions

Self Service Password Reset requires permission to perform all operations in eDirectory. For instructions on how to change eDirectory rights, see "eDirectory Rights" in the *eDirectory Administration Guide*.

Use the LDAP Permissions tool to determine the proper rights for your environment and your configuration of Self Service Password Reset. For more information about the LDAP Permissions tool, see "Viewing LDAP Permissions Recommendations" in the *Self Service Password Reset 4.2 Administration Guide*.

Set up the following user rights:

- Proxy User Rights
- Authenticated User Rights
- Other Rights

Proxy User Rights

Users with generic proxy user rights perform operations such as pre-authentication. Proxy users need the following rights to user containers:

- Browse rights to `[Entry Rights]`
- Read and Compare rights to the `pwmResponseSet` and `Configured Naming (CN)` attribute
- Read, Compare, and Write rights to `objectClass`, `passwordManagement`, `pwmEventLog`, and `pwmLastPwdUpdate`

IMPORTANT: If you enable the New User Registration module for Self Service Password Reset, you must enable the Create right to the `[Entry Rights]`. The `edirectory-rights.ldif` file does not add this right. To add the Create right to the `[Entry Rights]`, use the **Modify Trustees** task of the `Rights` role in iManager.

Authenticated User Rights

Users with authenticated user rights perform operations based on the permissions associated with the user's connection. Authenticated users need the following rights for their own user entries:

- Browse rights to `[Entry Rights]`
- Read, Compare, and Write rights, Inherited to [This] for `pwmResponseSet`
- Write rights, Inherited rights to `[This]` for `pwmLastPwdUpdate`

Other Rights

Depending on the Self Service Password Reset configuration, users might need other rights assigned as well. In most cases, Self Service Password Reset interacts with the directory by using the user's LDAP connection. The user must have LDAP rights to execute operations. For example:

- **Update Profile Module:** Users must have all rights to read attributes that are part of the Update Profile module and Write rights to any attributes they must write to.
- **Help Desk Module:** Users must have Read rights to search and display attributes of users whom they administer. Users must also have Write rights to any attributes modified by the Help Desk module through configured actions or password setting and unlocking accounts.

Configuring Active Directory

If you intend to install Self Service Password Reset with Active Directory and you want the challenge-response information to be stored in Active Directory, you must extend the schema and assign user rights to store data in Active Directory.

Self Service Password Reset provides `.ldif` files that extend the schema and assign the correct rights to your Active Directory. You can access these files here: `https://sspr.server.com/sspr/public/reference/ldap-schema.jsp`.

After you extend the directory schema, you must give permissions to access objects, including the group policy, organizational units, and containers. Assigning users' rights include authorizing read or write rights to Self Service Password Reset directory schema attributes.

The `AD-schema.ldif` file extends the schema on the server and enables you to assign user rights. You must determine containers and organizational units that need Self Service Password Reset access. You must know their distinguished names (DN) so that you can assign rights to each container and organizational unit separately.

You can use the LDAP Permissions tool to determine what rights you must change in Active Directory for each Self Service Password Reset module you enable. For more information, see "Viewing LDAP Permissions Recommendations" in the *Self Service Password Reset 4.2 Administration Guide*.

You can also extend the Active Directory schema to the root of the domain and assign rights to each container and the organizational unit below the root.

- "Extending the Active Directory Schema" on page 40
- "Assigning User Rights" on page 41

Extending the Active Directory Schema

You must use Active Directory tools to extend the schema. You use the `AD-schema.ldif` file provided here `https://sspr.server.com/sspr/public/reference/ldap-schema.jsp` to extend the schema.

Log in as the domain administrator and run the schema extension file on an Active Directory domain controller or computer that is connected to the Active Directory domain. Following the instructions provided in the Microsoft documentation. For more information, see Methods for Extending Schema.

The `.ldif` file adds the following Self Service Password Reset attributes to the directory schema:

- `pwmEventLog`
- `pwmResponseSet`
- `pwmLastPwdUpdate`
- `pwmToken`
- `pwmOTPSecret`

In a multi-server environment, schema updates occur after server replication. To ensure that the schema synchronized through your environment you can perform a schema cache update. For more information, see Schema Cache.

Assigning User Rights

To store the data against the new Self Service Password Reset schema attributes, assign user permissions to objects in the directory. Assign rights to the attributes added through the schema extension to all of the objects that access the Self Service Password Reset data, including the following:

- User objects
- User containers
- Group policies
- Organizational units

If you assign rights to containers and organizational users, the rights filter down to the associated user objects.

IMPORTANT: Do not assign rights at the user level or object level.

To assign rights, use the Microsoft documentation. For more information, see Configuring User Rights.

You can also assign rights to a Password Settings object (PSO) to add a fine-grained password and account lockout policy for Active Directory. For more information, see Create a PSO.

Creating an LDAP Profile for Your Environment

After you have manually configured your LDAP directory, you must now create an LDAP profile for your environment in the Self Service Password Reset Configuration Editor. You will use the information from the worksheet to configure the LDAP Profile.

However, you must know the additional information to manually create an LDAP profile. You must know:

- A user name attribute you want to use when viewing users in Self Service Password Reset
- A GUID attribute that is unique to all users that are managed by Self Service Password Reset
- Attributes to use for logging into Self Service Password Reset
- Attribute used for user groups

For instructions and more information, see "Configuring Policies" in the *Self Service Password Reset 4.2 Administration Guide*.

Configuring Databases

Self Service Password Reset uses two types of databases:

- **Local Database:** Self Service Password Reset uses a local database for storing local data. The local database requires no administration or maintenance and the default values are sufficient.
- **External Database:** Self Service Password Reset uses an external database to store data for certain functions. Any standard JDBC database that supports a standard Java JDBC driver works. Self Service Password Reset connects to the database and creates the necessary tables. You can configure multiple Self Service Password Reset instances to the same database instance. Self Service Password Reset officially supports MS SQL database and Oracle database.

You must manually configure the database to save the challenge-response information from Self Service Password Reset. You must work with a database administrator to completed the tasks.

To configure the database:

1. Create a database.

   For more information about how to create a database, see the related product documentation.
2. Create a database administrator for that database. You must specify this administrator during Self Service Password Reset configuration.
3. Create a user and associate it with the database you created in Step 1.
4. (Conditional) If you are using the Microsoft SQL database, ensure that the user has enabled the SQL server authentication mode and has suitable rights to open the database, which is the SQL Server Authentication mode. For more information, see "Choosing an Authentication Mode."

Configuring Self Service Password Reset to Work with the External Database

After you have created the external database, you must configure Self Service Password Reset to communicate with the database. Self Service Password Reset uses the JDBC driver for the specific database. Download the JDBC driver from the vendor's website to connect to the JDBC database.

To configure an external database to store the challenge-response information:

1. Ensure that you have downloaded the JDBC driver from the vendor's website.
2. Log in to Self Service Password Reset at `https://dns-name/sspr` as an administrator.
3. In the toolbar, click your name.
4. Click **Configuration Editor**.
5. Click **Default Settings**.
   - **5a** Select the LDAP directory type you are using.
   - **5b** Select where to store information as **Remote Database**
   - **5c** In the toolbar, click **Save changes**.
6. (Conditional) If you are using anything other than Active Directory to store challenge-response information in an external database, click **Modules > Authenticated > Forgotten Password > Settings**.
   - **6a** Set **Response Read Location** to **Database**.
   - **6b** Set **Response Write Location** to **Database**.
   - **6c** Click **Save**.
7. Click **Settings** > **Database (Remote)** > **Connection**.
8. Use the following information to configure the database connection:

   Database Driver

   Upload the JDBC database driver you downloaded from the vendor's website.

   Database Class

   Specify the Java class name of the JDBC driver. For example:

   - **Microsoft SQL:** `com.microsoft.sqlserver.jdbc.SQLServerDriver`
   - **Microsoft SQL using jTDS:** `net.sourceforge.jtds.jdbc.Driver`
   - **Oracle:** `oracle.jdbc.OracleDriver`

- **PostgreSQL:** `org.postgresql.Driver`

Database Connection String

Specify the database connections string that configures the Java JDBC database driver with the information required to reach your database server such as IP address, port number, and database name. For example:

- **Microsoft SQL:** `jdbc:sqlserver://host.example.net:port;databaseName=SSPR`
- **Microsoft SQL using jTDS:** `jdbc:jtds:sqlserver://host.example.net:port/SSPR`
- **Oracle:** `jdbc:oracle:thin:@//host.example.net:1521/SSPR`
- **PostgreSQL:** `jdbc:postgresql://host:port/database`

Database User Name

Specify the name of the user who can connect to the database.

Database Password

Specify a password for the database user.

Database Vendor

Select the vendor for your database. The options are **Other** or **Oracle**.

9 Click **Test Database Connection** to validate in the information you entered.

10 In the toolbar, click **Save changes**.

Integrating with Other NetIQ Products

Self Service Password Reset integrates with other NetIQ products to simplify password management for your environment. Integrating the different products enhances the users' experience of managing their own passwords and helps reduce costs for your company. Self Service Password Reset integrates with the following products:

- **NetIQ Access Manager:** For more information, see "Integrating Self Service Password Reset with NetIQ Access Manager" in the *Self Service Password Reset 4.2 Administration Guide*.
- **NetIQ Advanced Authentication:** For more information, see "Integrating Self Service Password Reset with Advanced Authentication" in the *Self Service Password Reset 4.2 Administration Guide*.
- **NetIQ Identity Manager:** For more information, see "Integrating Self Service Password Reset with NetIQ Identity Manager" in the *Self Service Password Reset 4.2 Administration Guide*.

5 Upgrading or Migrating Self Service Password Reset

If you have Self Service Password Reset installed and configured, you can upgrade Self Service Password Reset to the latest version or migrate it to a new platform or new hardware. The upgrade steps are different for each platform. Follow the instructions that are specific to your platform: the appliance, Linux, or Windows.

Since Self Service Password Reset is a web application, the steps to add a patch update are the same as when you upgrade Self Service Password Reset. For more information, see "Adding a Patch Update" in the *Self Service Password Reset 4.2 Administration Guide*.

- "Upgrading the Self Service Password Reset Appliance" on page 45
- "Upgrading Self Service Password Reset on Linux" on page 46
- "Upgrading Self Service Password Reset on Windows" on page 47
- "Upgrading the Identity Manager Deployment of Self Service Password Reset" on page 48
- "Migrating Self Service Password Reset" on page 49
- "Additional Information If Upgrading or Migrating from Self Service Password Reset 3.2 or a Prior Version" on page 50

Upgrading the Self Service Password Reset Appliance

Depending on your current version of Self Service Password Reset, there are two different ways you can upgrade Self Service Password Reset.

- "Upgrading the Self Service Password Reset Appliance from 4.0" on page 45
- "Upgrading Self Service Password Reset 4.1.0.5 to 4.2" on page 46

Upgrading the Self Service Password Reset Appliance from 4.0

Upgrading the Self Service Password Reset appliance is a manual process and it is different that updating the appliance. Upgrading the appliance is when you move to another release rather than applying a update. For more information about updates, see "Performing an Online Update" in the *Self Service Password Reset 4.2 Administration Guide*.

To upgrade Self Service Password Reset from 4.0 to 4.1 or 4.2 is a manual process. Ensure that you follow all of the steps to complete the upgrade process.

To upgrade the appliance:

1. Create a backup of your current configuration information.
   - **1a** Log in to Self Service Password Reset at `https://dns-name/sspr` as an administrator.
   - **1b** In the toolbar, click your name.

1c Click **Configuration Manager**.

1d Back up the configuration XML file.

1d1 Under **Configuration Activities**, click **Download Configuration**.

1d2 Save the `SSPRConfiguration.xml` file to a safe location.

2 Download the new version of the Self Service Password Reset appliance.

3 Deploy the new version of the Self Service Password Reset appliance. For more information, see "Deploying the Self Service Password Reset Appliance" on page 28.

4 Restore the Self Service Password Reset configuration file. For more information, see "Importing Configuration Information" in the *Self Service Password Reset 4.2 Administration Guide*.

5 Log in to Self Service Password Reset at `https://dns-name/sspr` as an administrator and verify that all of the configuration information is correct.

Upgrading Self Service Password Reset 4.1.0.5 to 4.2

You can upgrade Self Service Password Reset 4.1.0.5 appliance to 4.2 using the method listed above, or you can use a new feature that simplifies the upgrade process.

IMPORTANT: You must apply the latest updates to perform the upgrade. If you do not have the latest updates applied, the upgrade fails.

To Upgrade the 4.1.0.5 appliance to 4.2:

1 Create a backup of your current configuration information.

1a Log in to Self Service Password Reset at `https://dns-name/sspr` as an administrator.

1b In the toolbar, click your name.

1c Click **Configuration Manager**.

1d Back up the configuration XML file.

1d1 Under **Configuration Activities**, click **Download Configuration**.

1d2 Save the `SSPRConfiguration.xml` file to a safe location.

2 Log in to the appliance administration console as an administrator.

```
https://mycompany.example.com:9443
```

3 Click **Product Upgrade**, then follow the prompts to upgrade the appliance.

4 After the upgrade completes, log in to Self Service Password Reset to ensure that the upgrade completed successfully.

Upgrading Self Service Password Reset on Linux

If you installed Self Service Password Reset by deploying the WAR file on a Linux server, you must use the following steps to upgrade your deployment.

Since Self Service Password Reset is a Java servlet application running Apache Tomcat, the steps to add a patch update are the same as upgrading Self Service Password Reset. For more information, see "Adding a Patch Update" in the *Self Service Password Reset 4.2 Administration Guide*.

To upgrade Self Service Password Reset on Linux:

1. Download the most recent version of Self Service Password Reset WAR file from the NetIQ Patch Finder download website.
2. Create a backup of your current configuration information.
   - **2a** Log in to Self Service Password Reset at `https://dns-name/sspr` as an administrator.
   - **2b** In the toolbar, click your name.
   - **2c** Click **Configuration Manager**.
   - **2d** Back up the configuration XML file:
     - **2d1** Under **Configuration Activities**, click **Download Configuration**.
     - **2d2** Save the `SSPRConfiguration.xml` file to a safe location.
3. (Optional) If you have made any customization in Self Service Password Reset such as changes in the user interface copy these for later reference.

   For more information, see "Customizing the Theme of Self Service Password Reset" in the *Self Service Password Reset 4.2 Administration Guide*.
4. Stop Apache Tomcat by running the `catalina.sh` script in the *`Tomcat_Home`*`/bin` directory.

   ```
   ./catalina.sh stop
   ```
5. Copy the updated `sspr.war` to the *`Tomcat_Home/`*`webapps` directory.

   NOTE: Ensure that you have set the `SSPR_APPLICATION` operating system environment variable in the `setenv` file. For more information, see ""Setting Operating System Environment Variables" on page 31".
6. Restart the Apache Tomcat service by running the `catalina.sh` script in the *`Tomcat_Home`*`/bin` directory.

   ```
   ./catalina.sh start
   ```
7. Log in to Self Service Password Reset at `https://dns-name/sspr` as an administrator and verify that all of the configuration information is correct.

Upgrading Self Service Password Reset on Windows

If you deployed Self Service Password Reset using the `.msi` file, you must use the following procedure to upgrade your deployment.

1. Download the most recent version of Self Service Password Reset `.msi` file from the NetIQ Patch Finder download website.
2. Create a backup of the current configuration information.
   - **2a** Log in to Self Service Password Reset at `https://dns-name/sspr` as an administrator.
   - **2b** In the toolbar, click your name.
   - **2c** Click **Configuration Manager**.
   - **2d** Back up the configuration XML file.
     - **2d1** Under **Configuration Activities**, click **Download Configuration**.
     - **2d2** Save the `SSPRConfiguration.xml` file to a safe location.

       NOTE: This is for backup purposes only.

3 (Optional) If you have made any customization in Self Service Password Reset such as changes in the user interface copy these for later reference.

   For more information, see "Customizing the Theme of Self Service Password Reset" in the *Self Service Password Reset 4.2 Administration Guide*.

4 Run the `.msi` file.

5 Follow the prompts to install the new version.

6 (Optional) Restore any customization.

7 Log in to Self Service Password Reset at `https://dns-name/sspr` as an administrator and verify that all of the configuration information is correct.

Upgrading the Identity Manager Deployment of Self Service Password Reset

If you deployed Self Service Password Reset the integrated installer from the Identity Manager installation, there are separate steps you must perform to upgrade Self Service Password Reset.

To upgrade Self Service Password Reset from an Identity Manager deployment:

1 Ensure that you are running a supported version of Identity Manager and Self Service Password Reset. For more information, see "Supported Versions" in the *Self Service Password Reset 4.2 Administration Guide*.

2 Download the most recent version of Self Service Password Reset WAR file from the NetIQ Patch Finder download website.

3 Ensure that you have configured an administrator user for Self Service Password Reset.

   3a Log in to Self Service Password Reset at `https://dns-name/sspr` as an administrator.

   3b In the toolbar, click your name.

   3c Click **Configuration Editor**.

   3d Click **Modules > Administrator > Administrator Permission**.

   3e Ensure that the LDAP filter you defined includes an administrator user.

4 Create a backup of your current configuration information.

   4a Log in to Self Service Password Reset at `https://dns-name/sspr` as an administrator.

   4b In the toolbar, click your name.

   4c Click **Configuration Manager**.

   4d Under **Configuration Activities**, click **Download Configuration**.

   4e Save the `SSPRConfiguration.xml` file to a safe location.

5 (Optional) If you have made any customization in Self Service Password Reset such as changes in the user interface copy these for later reference.

   For more information, see "Customizing the Theme of Self Service Password Reset" in the *Self Service Password Reset 4.2 Administration Guide*.

6 Lock the Self Service Password Reset configuration file by accessing the Configuration Manager, then clicking **Restrict Configuration**.

7 Stop Apache Tomcat by running the stop script located in the `/etc/init.d/idmapps_tomcat_init` directory.

```
/etc/init.d/idmapps_tomcat_init stop
```

8 Delete the following directories:

- `Tomcat_home/webapps/sspr`
- `Tomcat_home/work/Catalina/localhost`

9 Copy the updated `sspr.war` to the *`Tomcat_Home/`*`webapps` directory.

NOTE: Ensure that you have set the `SSPR_APPLICATION` operating system environment variable in the `setenv` file. For more information, see "“Setting Operating System Environment Variables” on page 31".

---

10 Restart the Apache Tomcat service by running the start script in the `/etc/init.d/idmapps_tomcat_init` directory.

```
/etc/init.d/idmapps_tomcat_init start
```

11 Import the configuration information you backed up prior to the upgrade.

11a Log in to Self Service Password Reset at `https://`*`dns-name`*`/sspr` as an administrator.

11b In the toolbar, click your name.

11c Click **Configuration Manager**.

11d Click **Import Configuration**, then browse to and select the `SSPRConfiguration.xml` file you created earlier.

12 (Optional) Copy any customization as required.

NOTE: If you uploaded a ZIP file to the configuration editor in you previous Self Service Password Reset version, the file is embedded in the `SSPRConfiguration.xml` file you imported previously so you do not need to complete the following steps.

12a Log in to Self Service Password Reset at `https://`*`dns-name`*`/sspr` as an administrator.

12b In the toolbar, click your name.

12c Select **Configuration Editor**.

12d Click **Settings > User Interface > Look & Feel > Custom Resource Bundle**.

12e Browse to and select the Custom Resource Bundle file, then click **Upload File**.

13 Configure the setting that integrates Self Service Password Reset with Identity Manager.

13a Log in to Self Service Password Reset at `https://`*`dns-name`*`/sspr` as an administrator.

13b In the toolbar, click your name.

13c Click **Configuration Editor > Default Settings > LDAP Vendor Default Settings**.

13d Select **NetIQ IDM / OAuth Integration**.

13e Select **Save changes**.

14 Verify that all of the configuration information is correct and if you imported the customization, that Self Service Password Reset restored all of the customizations.

Migrating Self Service Password Reset

Migrating is different from upgrading by moving to new hardware (physical or virtual) or moving to a new platform. The steps for migrating Self Service Password Reset are the same no matter what platform you are using.

To migrate Self Service Password Reset

1. (Conditional) If you are currently running Self Service Password Reset 3.2 or a prior version, ensure that you review the Forgotten Password verification methods or you will have errors. For more information, see "Additional Information If Upgrading or Migrating from Self Service Password Reset 3.2 or a Prior Version" on page 50.
2. Create a backup of the current configuration information.
   - **2a** Log in to Self Service Password Reset at `https://dns-name/sspr` as an administrator.
   - **2b** In the toolbar, click your name.
   - **2c** Click **Configuration Manager**.
   - **2d** Back up the configuration XML file.
     - **2d1** Under **Configuration Activities**, click **Download Configuration**.
     - **2d2** Save the `SSPRConfiguration.xml` file to a safe location.
3. (Optional) If you have made any customization in Self Service Password Reset such as changes in the user interface copy these for later reference.

   For more information, see "Customizing the Theme of Self Service Password Reset" in the *Self Service Password Reset 4.2 Administration Guide*.
4. Deploy the new version of Self Service Password Reset on the new hardware or new platform. For more information, see Chapter 3, "Installing Self Service Password Reset," on page 17.
5. Restore the Self Service Password Reset configuration file to the new installation. For more information, see "Importing Configuration Information" in the *Self Service Password Reset 4.2 Administration Guide*.
6. (Optional) If you have made any customization in Self Service Password Reset such as changes in the user interface restore these changes.

   For more information, see "Customizing the Theme of Self Service Password Reset" in the *Self Service Password Reset 4.2 Administration Guide*.
7. Log into the system as a user and ensure that all of the feature function.

Additional Information If Upgrading or Migrating from Self Service Password Reset 3.2 or a Prior Version

If you are running Self Service Password Reset 3.2 or a prior versions and have the Forgotten Password module configured, you must perform additional steps to stop errors occurring during the upgrade or migration process.

Self Service Password Reset 3.3 and above contains a new configuration option for forgotten password verification methods. If you upgrade without reviewing these new options, when you access the Forgotten Password Module it returns an error of `SSPR Error 5006 - The username is not valid or is not eligible to use this feature`. (Bug 979153)

To fix the error, you must review the forgotten password verification methods and change these options for your environment.

To review the forgotten password verification methods:

1. Log in as an administrator to Self Service Password Reset at `https://dns-name/sspr`.
2. In the toolbar, click your name.
3. Click **Configuration Editor** > **Modules** > **>** **Forgotten Password** > **Forgotten Password Profiles** > **default** > **Verification Methods**.

If you have created a different profile, select that name instead of **default**.

4 Review the verification methods and change these options for your environment.

5 Click **Save changes**.

6 Uninstalling Self Service Password Reset

Self Service Password Reset provides a way for you to uninstall it. Select the appropriate information for your deployment of Self Service Password Reset.

- "Removing the Self Service Password Reset Appliance" on page 53
- "Uninstalling on Linux" on page 53
- "Uninstalling on Windows" on page 53

Removing the Self Service Password Reset Appliance

To uninstall the appliance, power off the appliance and then delete the image from your virtual environment. If you are using an L4 switch, ensure to remove the IP address of this appliance from the L4 switch.

Uninstalling on Linux

1. Stop Apache Tomcat by running the `catalina.sh` script in the *`Tomcat_Home`*`/bin` directory.

   ```
   ./catalina.sh stop
   ```

2. (Optional) Save the XML Configuration file to another location for future use.
3. (Optional) Back up the local database if you stored the challenge-response information in it.
   - **3a** In the Configuration Manager, click **LocalDB**.
   - **3b** Click **Download LocalDB**, then save the local database to a safe location.
4. Delete both the *`Tomcat_Home`*`/webaps/sspr` directory and the *`Tomcat_Home`*`/webaps/sspr.war` file.
5. Reboot the Linux server to complete the uninstall process.

Uninstalling on Windows

1. Stop Apache Tomcat by one of the following methods:
   - Right-click the Tomcat icon in the System tray, then select **Stop**.
   - Run the **catalina.bat** script in the *`Tomcat_Home`*`\bin` directory.

     ```
     catalina stop
     ```

2. (Optional) Save the XML Configuration file to another location for future use.

   For more information, see "Backing Up Configuration Information" in the *Self Service Password Reset 4.2 Administration Guide*.

3. (Optional) Back up the local database if you stored the challenge-response information in it.
   - **3a** In the Configuration Manager, click **LocalDB**.
   - **3b** Click **Download LocalDB**, then save the local database to a safe location.
4. From the Windows Control Panel, uninstall Self Service Password Reset.
5. Reboot the Windows Server to complete the uninstall process.

A Documentation Updates

The following sections contain a list of changes to the documentation.

- "January 2018" on page 55
- "December 2017" on page 55
- "October 2017" on page 55

January 2018

Location	Change
"Self Service Password Reset Architecture" on page 8	Added information about supporting Self Service Password Reset in the Cloud.
"Selecting an Appropriate Configuration" on page 11	Added information about supporting Self Service Password Reset in the Cloud.
"Deployment Requirements of Self Service Password Reset" on page 19	Added information about supporting Self Service Password Reset in the Cloud.
"Deploying Self Service Password Reset in the Cloud" on page 24	Added this new section.

December 2017

Location	Change
"Deployment Requirements of Self Service Password Reset" on page 19	Added support for Microsoft Windows Server 2016, SQL Server 2016, and Active Directory 2016. These versions are only supported with Patch Update 2 or later.

October 2017

Location	Change
"Migrating Self Service Password Reset" on page 49	Added this section.
"Additional Information If Upgrading or Migrating from Self Service Password Reset 3.2 or a Prior Version" on page 50	Added this section.