Self Service Password Reset 4.8

Administration Guide

July 2024

Legal notice

© Copyright 2023 Micro Focus or one of its affiliates.

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

For additional information, such as certification-related notices and trademarks, see http://www.microocus.com/about/legal/.

Contents

About this book 9

1 Self Service Password Reset overview 11

Self Service Password Reset key features . . . 11
Self Service Password Reset architecture . . . 12
Understanding challenge-response storage methods . . . 14

2 Getting started 17

Logging in to the Administration Console . . . 17
Working with configuration editor . . . 18
Working with the configuration manager . . . 19
Using the dashboard . . . 20
Configuring macros for messages and actions . . . 22

3 Configuring Self Service Password Reset 23

Configuring basic settings . . . 23
- Configuring application settings . . . 23
- Configuring IP address of the Appliance . . . 24
- Configuring localization settings . . . 25
- Configuring session management settings . . . 25
- Configuring the telemetry options . . . 25

Configuring profiles . . . 26
- Creating a profile . . . 26
- Managing profiles . . . 27

Configuring security settings . . . 28
- Configuring security for Self Service Password Reset . . . 28
- Configuring web security . . . 29

Importing certificates to create an HTTPS connection to browsers . . . 34
Configuring intruder detection . . . 35
Configuring external web services with REST . . . 35

Part I Configuring Self Service Password Reset settings 37

4 Configuring LDAP profiles and settings 39

Configuring LDAP directory profile . . . 39
Configuring LDAP settings . . . 41
- Configuring the global LDAP settings . . . 42
- Configuring Microsoft Active Directory settings . . . 42
- Configuring NetIQ edirectory settings . . . 43
- Configuring the Oracle directory server settings . . . 47

Updating the LDAP certificates . . . 47
- Updating the LDAP directory certificate when it is not expired . . . 47

Updating the LDAP directory certificate after it expires . . . 48

5 Configuring authenticated modules for Self Service Password Reset 49

Configuring the account information module . . . 49
Configuring the administrators module . . . 50
Configuring the change password module . . . 51
Configuring the delete account module . . . 53
Enabling the delete account module . . . 53
Configuring the delete account module to delete accounts from integrated products . . . 53
Configuring the Help Desk module . . . 55
Enabling and configuring the Help Desk module . . . 55
Configuring the advanced search for the Help Desk module . . . 56
Configuring the people search module . . . 57
Enabling and configuring the people search module . . . 57
Configuring the advanced search option in the people search module . . . 58
Configuring one-time password . . . 58
Configuring the setup security questions module . . . 59
Configuring the shortcut menu module . . . 59
Configuring the update profile module . . . 60

6 Configuring public modules for Self Service Password Reset 61

Configuring forgotten password module . . . 61
Configuring the forgotten password profile . . . 62
Configuring the forgotten password settings . . . 68
Configuring the OAuth2 verification method for the forgotten password module . . . 74
Configuring the forgotten user name module . . . 75
Configuring the new user registration module . . . 75
Enabling the user activation module . . . 77

7 Configuring policies 79

Configuring challenge policy . . . 79
Configuring password policies . . . 82
Configuring a profile for a password policy . . . 83
Configuring the word list settings . . . 90

8 Configuring settings 93

Customizing the theme of Self Service Password Reset . . . 93
Creating the Self Service Password Reset resource bundle . . . 94
Implementing the custom resource bundle . . . 94
Example of customizing a home page . . . 95
Reference for Self Service Password Reset CSS syntax . . . 96
Customizing user interface features . . . 97
Customizing the text of Self Service Password Reset . . . 98
Customizing email masking regular expression . . . 98
Configuring CAPTCHA . . . 99
Configuring email notification settings . . . 99
Configuring email settings . . . 100
Configuring email templates . . . 100

HTTPS server . . . 101
Configuring password settings . . . 102
Configuring SMS notification settings . . . 102
Configuring the SMS gateway . . . 102
Configuring the SMS messages . . . 105
Configuring Self Service Password Reset for Single Sign-On client . . . 106
Configuring basic authentication for Single Sign-On . . . 106
Configure HTTP for Single Sign-On . . . 107
Configuring OAuth Single Sign-On . . . 107
Configuring token settings . . . 110
Verifying the email token in a different browser session . . . 111
Sending notifications for expiring passwords . . . 112
Configuring Self Service Password Reset for password expiration notifications . . . 112
Enabling the emails for password expiration notifications . . . 114
Verifying the password expiration notification configuration . . . 114
Word lists . . . 114
Enabling Self Service Password Reset proxy user for accessing the RESTful web services . . . 116

Part II Configuring integrations 119

9 Integrating Self Service Password Reset with NetIQ access manager 121

Configuring access manager to integrate with Self Service Password Reset . . . 121
Configuring proxy service for Self Service Password Reset . . . 122
Configuring protected resources for Self Service Password Reset . . . 122
Configuring Single Sign-On to Self Service Password Reset . . . 123
Configuring Single Sign-On to Self Service Password Reset when password is not available . . . 124
Configuring single sign-on with OAuth2 tokens . . . 125
Configuring Self Service Password Reset to integrate with access manager . . . 127
Configuring redirection URLs . . . 127
Configuring Self Service Password Reset parameters for access manager . . . 127
Using request parameters . . . 128
Using a command servlet . . . 129
Configuring Self Service Password Reset to access the OAuth2 application . . . 130
Additional integration options with access manager . . . 132
Integrating the forgotten password module with access manager . . . 132
Deleting user accounts in access manager from the delete account module . . . 133
Creating accounts for social users in Self Service Password Reset using the new user registration module . . . 134
Adding the device management link to the update profile page . . . 134

10 Integrating Self Service Password Reset with advanced authentication 137

Prerequisites . . . 137
Configuring advanced authentication to integrate with Self Service Password Reset . . . 138
Configuring Self Service Password Reset for advanced authentication . . . 139

11 Integrating Self Service Password Reset with NetIQ identity manager 143

Supported versions . . . 143
Installing Self Service Password Reset with the identity manager integrated installer . . . 144
Integrating a standalone Self Service Password Reset with identity manager . . . 144

Configure OAuth settings for Self Service Password Reset 144
Set the Self Service Password Reset theme to match the identity manager theme 146
Configure syslog audit server 146
Enabling Self Service Password Reset proxy users to read passwords from edirectory 147

12 Integrating Self Service Password Reset with client login extension 149

Prerequisites 149
Configuring Self Service Password Reset for client login extension 150
Configuring client login extension 150

Part III Maintaining Self Service Password Reset 153

13 Managing Self Service Password Reset 155

Backing up configuration information 155
Importing configuration information 155
Viewing LDAP permissions recommendations 156
Uploading the seed list 157
Updating seed list 157
Uploading the seed list 158
Configuring data analysis 158
Configuring reporting 159
Viewing the reports 159
Configuring logging 159
Configuring logging settings 160
Viewing logs 160
Auditing for Self Service Password Reset 161
Configuring auditing 161
Forwarding auditing information 161
Configuring auditing for user history 162
CEF audits and customization 162
Adding a patch update 163
Adding a patch update to the Appliance 163
Adding a patch update to Linux 163
Adding a patch update to Windows 164

14 Managing the Appliance 165

Setting administrative passwords 166
Configuring network setting 167
Adding additional hosts to the hosts file 167
Configuring time settings 168
Accessing system services 168
Managing Appliance certificates 169
Creating or signing the digital certificates 169
Using an existing certificate and key pair 170
Activating the certificate 171
Configuring the firewall 171
Sending information to support 171
Adding a field patch to the Appliance 172
Performing an online update 172

Performing a product upgrade 174
Using the administrative commands 174
Rebooting or shutting down the Appliance 175
Logging out 175

15 Troubleshooting Self Service Password Reset 177

Configuring locked and unlocked modes 177
When to run Self Service Password Reset in the unlocked configuration mode 178
How to lock and unlock the Self Service Password Reset configuration 179
Troubleshooting connections 181
Troubleshooting Self Service Password Reset with the provided tools 182
Troubleshooting with the dashboard 182
An unexpected LDAP error for the test user in the configuration manager 183
One or more responses is not correct error for users on mobile devices 183
No automated emails from the SMTP server 184
Accessing the configuration editor and configuration manager directly 184
Troubleshooting user issues with Self Service Password Reset 184
Obtaining the user debug information 185
Users in Active Directory see delays in accessing the user website 185
Users did not complete the forgotten password process 186
Helping users change the default language of Self Service Password Reset 186
How to enable Windows desktop to support forgotten password reset 186
How to make Self Service Password Reset honor the Active Directory password history policy 187
Troubleshooting the challenge set policy 187
Troubleshooting error codes 187
Troubleshooting Single Sign-On issue with OAuth 187
Self Service Password Reset throws 404 error when upgrading WAR file to 4.7 version 188
An error while upgrading the Self Service Password Reset Appliance to 4.7 version 189
Issue with Self Service Password Reset site URL after online upgrade 190
Server utilization reaches 100% 190

About this book

The *NetIQ Self Service Password Reset Administration Guide* provides conceptual and step-by-step guidance for administrative tasks.

Intended audience

This book provides information for individuals responsible for understanding administration concepts and implementing a secure, distributed administration model. Administrators must have a good understanding of networks, LDAP directories, databases, and Cloud systems. This guide does not provide detailed information about these connected systems.

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, 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 Self Service Password Reset, such as known issues.

Installation Guide

Provides installation steps specific to this release of Self Service Password Reset.

Videos

Provide supplemental information about using Self Service Password Reset. For more information, see the Self Service Password Reset Youtube playlist (https://www.youtube.com/playlist?list=PL8yfmcqTN8GGyKZ7_akvzAAjmIneyJXW1).

1 Self Service Password Reset overview

Self Service Password Reset is a web-based password management solution. You can deploy 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 11
- "Self Service Password Reset architecture" on page 12
- "Understanding challenge-response storage methods" on page 14

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:** Administrators create or provision LDAP accounts for the users, then the users claim these accounts for the first authentication and set a password through the Activation module.
- **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 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), Spanish, Swedish, and Norwegian.
- **Easily customized:** Administrators can easily customize Self Service Password Reset to integrate with external web authentication methods as well as integrate with NetIQ Identity Manager to add automated workflows and account claiming support.

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. The Figure 1-1 depicts the architecture for Self Service Password Reset.

Self Service Password Reset consists of the following components:

- **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, eDirectory, and Oracle Directory Server.
- **Tomcat server:** As you can see in Figure 1-1 on page 13, the Self Service Password Reset application must run on a web server, such as a Tomcat server.
- **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.

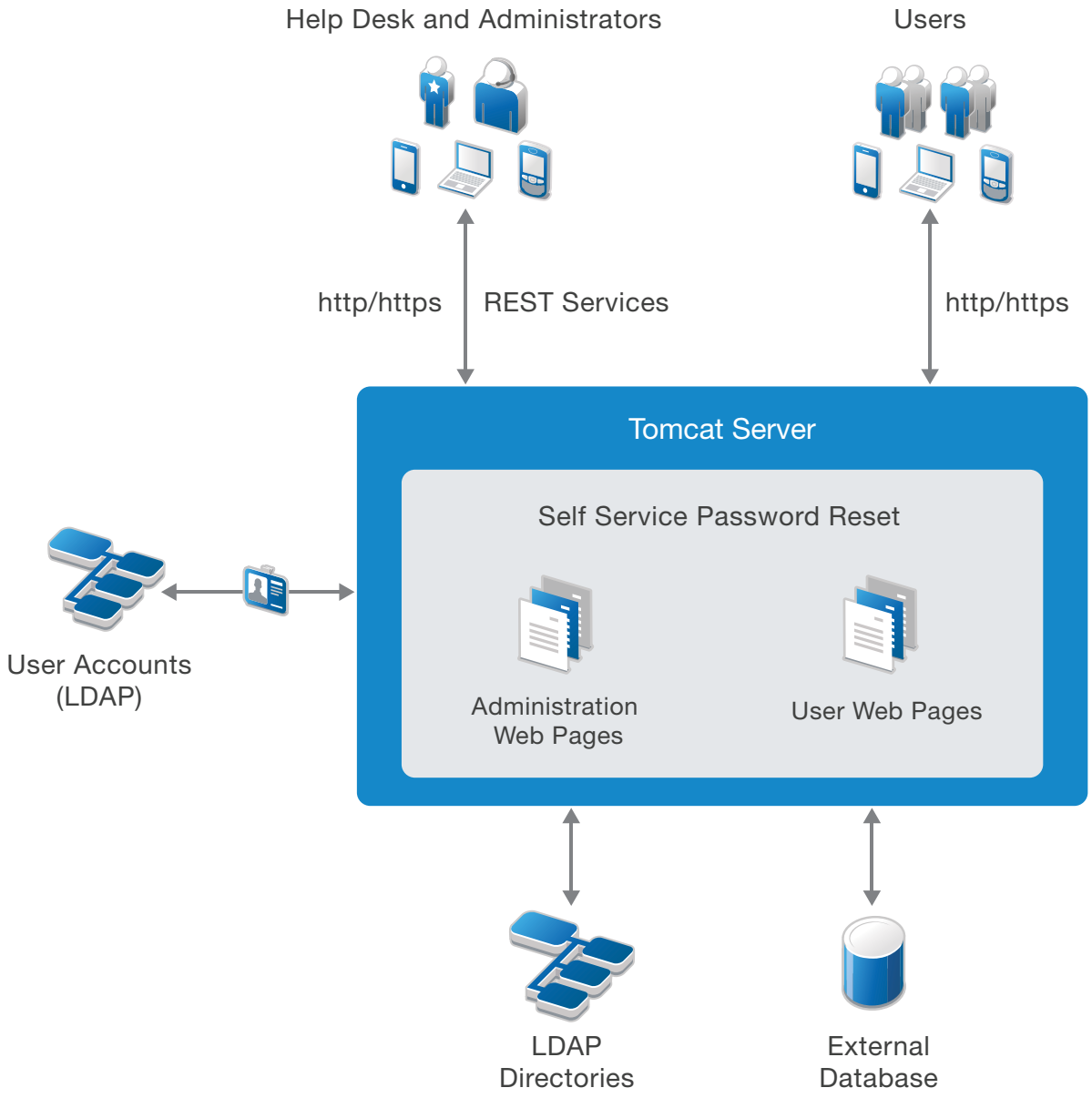
    You can also programmatically connect to Self Service Password Reset through REST Services. For more information, see the *Self Service Password Reset REST Services Reference*.
  - **Users web pages:** Self Service Password Reset provides a web interface for users to manage their passwords. The users 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.

  IMPORTANT: Use the external database in production environments. This allows you to cluster the external database and backup the database.

  Self Service Password Reset supports Microsoft SQL Server, PostgreSQL, and Oracle.

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.

The local database storage limit is 102,400 bytes (1024 * 100 bytes).

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 Getting started

After you have configured your environment to work with Self Service Password Reset, you must configure the options you want to use in Self Service Password Reset. Most options do not work until you either enable the option or configure the option.

After the Configuration Guide completes, it points to you to log into the Self Service Password Reset administration console. The administration console allows you manage and configure all aspects of Self Service Password Reset.

If you deployed the appliance for Self Service Password Reset, there is a separate administration console for the management of the appliance. For more information, see Chapter 14, "Managing the Appliance," on page 165.

The administration console consists of many different tools to help you configure and manage your Self Service Password Reset deployment. Use the following information to help you use the administration console.

- "Logging in to the Administration Console" on page 17
- "Working with configuration editor" on page 18
- "Working with the configuration manager" on page 19
- "Using the dashboard" on page 20
- "Configuring macros for messages and actions" on page 22

Logging in to the Administration Console

The administration is part of the Self Service Password Reset web application, so you access it through a URL.

1. Access the Self Service Password Reset administration console.

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

   The *dns-name* is the fully qualified hostname of the server running Self Service Password Reset.
2. Specify the administration user name you specified during the Configuration Guide process. For more information about Configuration Guide, refer Using the configuration guide.
3. Specify the password of the administration user.
4. Click **Sign In**.

The administration console takes you to the Home page that contains the default modules for Self Service Password Reset The majority of these modules need additional configuration to have them work for your users.

Working with configuration editor

Configuration Editor is part of the administration console. It is a powerful tool that enables system administrators to configure modules, settings, and profiles for Self Service Password Reset.

To access the configuration editor:

1. Log in to the Self Service Password Reset administration console as an administrator.

   `https://localhost:port/sspr`

2. In the toolbar, click your name, then click **Configuration Editor**.
3. Specify the password for the Configuration Editor.

   This password is different from the administrator user's password. You created this password during the Configuration Guide process.

4. (Conditional) Select **Remember the configuration password for 1 hour** if you want Self Service Password Reset to remember the Configuration Editor password for one hour.

The Configuration Editor allows you to do the following:

- **Configure settings for Self Service Password Reset:** You can configure the default settings that define how a user can use Self Service Password Reset. You can also define directory profiles, modules, and templates for the users. The following chapters provide detailed information on to configure the different features.
- **Search for configuration settings:** To quickly access a particular setting you can search for it by using the **Search** field in the Configuration Editor. The **Search** field displays the result while you type. To get the exact result, type the complete name of the setting or type the complete description.
- **Change the configuration editor password:** To change the password for the **Configuration Editor**, select the **Set configuration password** in the top-right corner of the Configuration Editor.
- **Save configuration settings:** To save the configuration updates for all the settings, select the **Save** icon on the top-right corner of the Configuration Editor.
- **View modification details:** For each modified setting you can view the modification details such as, when a setting was modified and who modified the setting. When you save the configuration settings, the **Configuration Editor** prompts you to confirm the changes. The confirmation dialog box includes a list of modified settings. After administrators save the configuration setting, administrators that have access to the **Configuration Manager** can view the last modified details of all the settings.
- **Change the precedence order of the setting fields:** To change the precedence of each field, use the arrow keys that are adjacent to the respective fields. You can change the precedence order for any setting that includes multiple fields.
- **Collapse and expand all the configuration options:** To expand all the configuration options together, select the plus (+) icon at the bottom of the left pane. To collapse all the options together, select the minus (-) icon at the bottom of the left pane.

- **Apply filter to view only the required settings:** Apply filters for settings so that Self Service Password Reset displays only those settings that you need by selecting the filter icon at the bottom of the left pane:
  - **Setting level:** You can choose to view limited settings or advanced settings by setting the scroll bar appropriately. If the scroll bar is in the middle, all the required and some additional settings are displayed.
  - **Modified:** You can choose to view all the settings or only the modified settings by selecting **All**, or **Modified**.

You can access the Configuration Editor directly without authenticating to troubleshoot issues. For more information, see "Accessing the configuration editor and configuration manager directly" on page 184.

Working with the configuration manager

The **Configuration Manager** is part of the administration console. It is for maintenance tasks of Self Service Password Reset and daily management tasks such as monitoring the health of the system.

To access the configuration manager:

1. Log in to the Self Service Password Reset administration console as an administrator.

   `https://localhost:port/sspr`

2. In the toolbar, click your name, then click **Configuration Manager**.

The **Configuration Manager** allows you to do the following:

- **View the configuration status:** In order to configure features in Self Service Password Reset you must run the Configuration Guide or manually configure your environment to work with Self Service Password Reset. If you have not completed these tasks, the Configuration Manager shows that under **Configuration Status**. For more information, see "Configuring your environment for Self Service Password Reset" in the *Self Service Password Reset 4.8 Installation Guide*.
- **View the health:** The Configuration Manager allows you to view the health of the different components of Self Service Password Reset under **Health**. It displays the health of the connected LDAP directories, if the platform is functioning, and if you have configured updates for the appliance.
- **Import or export the configuration file:** Self Service Password Reset stores all of the configuration settings you make in the Configuration Editor in a configuration file. You can download the configuration file and save it for backup purposes or if you are upgrading the system. The Configuration Manager allows you to export and import this configuration file.
- **Download reports:** The Configuration Manager allows you to generate and download reports for troubleshooting purposes. There is configuration summary report, a permissions report for the LDAP directory permissions, and a bundle of logs for troubleshooting.
- **View certificates:** The Configuration Manager allows you to view the certificates Self Service Password Reset requires to maintain secure connections between it and the users. Self Service Password Reset manages secure information such as the users' credentials. For more information, see "Importing certificates to create an HTTPS connection to browsers" on page 34.

- **Manage the local database:** Self Service Password Reset contains a local database that stores configuration information. The Configuration Manager allows you to export and import that local database for backup purposes.

  NOTE: Self Service Password Reset provides the local database for testing purposes only. For production environments, you must use an external database or an LDAP directory.

  The local database storage limit is 102,400 bytes (1024 * 100 bytes).

You can access the Configuration Manager directly without authenticating to troubleshoot issues. For more information, see "Accessing the configuration editor and configuration manager directly" on page 184.

Using the dashboard

Self Service Password Reset provides a Dashboard that allows you easily manage your system. The Dashboard displays detailed information about user activity, helps you maintain a healthy system, and many more things. Use the following information to help you use the Dashboard effectively.

To view the dashboard:

1. Log in to Self Service Password Reset at `https://dns-name/sspr` as an administrator.
2. Click **Administration**.
3. Use the following the information to help you manage your system:

   User Activity

   Displays all of the user activity on the Self Service Password Reset system. This information is part of the auditing service provided by Self Service Password Reset. For more information, see "Auditing for Self Service Password Reset" on page 161.

   Data Analysis

   Displays the reporting information for Self Service Password Reset. You must enable the **Directory Reporting** setting for this to work. For more information, see "Configuring data analysis" on page 158.

   More Options > Event Log

   Displays a details view of all events logged for the Self Service Password Reset system. You can search for the event by text about the event and the event name.

   More Options > Token Lookup

   Search for any tokens that are open and stuck. You use a token in emails and for one-time password (OTP). You use this if you have an open OTP token that is stuck. Use this for troubleshooting purposes.

   More Options > URL References

   Displays a list of all of the URLs Self Service Password Reset uses. The full URL is the site URL with these paths appended. For example, `https://mycompany.com/password/sspr` is the URL to access the application.

   More Options > Application Reference

   Displays developer-level documentation about Self Service Password Reset.

Status

Displays information about web sessions, LDAP connections, password changes, authentications, intruder attempts, reads to the local or external database, and writes to the local or external database. It displays all of this information for the last minute, the last hour, or the last day.

Health

Displays the health of the connections to the different components of Self Service Password Reset. You use this information for troubleshooting purposes. For more information, see "Troubleshooting connections" on page 181.

About

Displays the version information about Self Service Password Reset. It also displays how long the system has been running, the site URL that users access, license information and a number of other items.

Services

Displays all of the services that compose Self Service Password Reset. It also displays the status, location, and health of the services.

LocalDB

Displays information about the local database such as the word list size, the shared password history size, the number of audit records, and many other items. Use this information for troubleshooting purposes.

NOTE: Self Service Password Reset provides the local database for testing purposes only. For production environments, you must use an external database or an LDAP directory.

The local database storage limit is 102,400 bytes (1024 * 100 bytes).

LocalDB Sizes

Displays the size of all of the records in the local database. Use this information for troubleshooting purposes and to ensure that you are not running out of disk space on the local database.

Java

Displays a lot of information about Java for troubleshooting purposes. For example, it displays the version number, the Java vendor, the Java Home path, how much memory it uses, and much more information.

Threads

Displays all of the Self Service Password Reset threads and the states of the threads. Use this information for troubleshooting purposes.

4 When you are on the Dashboard, click **Home** to return to the main page.

Configuring macros for messages and actions

Self Service Password Reset macros provide administrators with a powerful and flexible method to tailor some Self Service Password Reset configuration settings and messages for the users and their environments.

Self Service Password Reset macros make use of two reserved symbols: at sign **@** and the colon **:**.

- Each macro begins and ends with the **@**symbol.
- The **:** is used to separate fields in macros with multiple fields.
- Any macro that includes a literal @ or : symbol must escape these characters with a slash /, such as /@ or /:.

To test macros:

1. Log in to Self Service Password Reset at `https://dns-name/sspr` as an administrator.
2. In the toolbar, click your name.
3. Click **Configuration Editor**.
4. Click **Open macro help and reference** in the top right corner of the **Configuration Editor**.
5. Enter the macro in the **Input** field, then click **Test**.

   If the macro is correct, the **Configuration Editor** displays the output.

This page in the **Configuration Editor** contains the schema for the macros and some common examples of macros.

3 Configuring Self Service Password Reset

This chapter helps you configure and customize Self Service Password Reset. For example, you can configure password policy settings, reporting, and authentication settings.

- "Configuring basic settings" on page 23
- "Configuring profiles" on page 26
- "Configuring security settings" on page 28
- "Importing certificates to create an HTTPS connection to browsers" on page 34
- "Configuring intruder detection" on page 35
- "Configuring external web services with REST" on page 35

Configuring basic settings

Self Service Password Reset allows you to configure basic settings to control functionality and behavior of the applications through the following settings.

- "Configuring application settings" on page 23
- "Configuring IP address of the Appliance" on page 24
- "Configuring localization settings" on page 25
- "Configuring session management settings" on page 25
- "Configuring the telemetry options" on page 25

Configuring application settings

The Application Settings help you define the following settings for Self Service Password Reset:

- Site URL: The URL used in email macros and other user-facing communications to provide a link for users to easily access the website. For example, if a user tries to reset their password using the **Forgotten Password** option, the email verification token and a reset password link will be sent to their email.
- Forward URL: SSPR will direct users to this URL once they complete any activity that doesn't require logout. By default, SSPR directs users to the SSPR menu page after completing any activity. You can override the default URL by adding a new value.
- Logout URL: When a user clicks the **Logout** button, SSPR directs users to the configured **Logout URL** page. By default, SSPR directs them to the SSPR logout page.
- Home URL: The URL that redirects users after they click on the **Home** button. By default, SSPR directs users to the SSPR menu page after completing any activity.
- Intro URL: The URL that opens when the user tries to launch the SSPR. You can add any module starting with a slash (/), such as /public, /private, /public/forgottenpassword, and so on.

For example, if an administrator sets **/public** in the **Add Value** field, the SSPR user page displays all the public modules that are accessible by any user while launching the SSPR application.

- Idle Timeout Seconds: The number of seconds after which SSPR deactivates an authenticated session. By default, the value is set to 300 seconds.

  NOTE: The minimum value can be set to 60 seconds.

- Hide Configuration Health Warnings: Hides the health warnings about configuration issues from the **Health** status monitoring on the **Configuration Manager** page.
- HTTP Proxy: The URL of the HTTP proxy server that acts as an intermediary between a client and a server. An HTTP (Hypertext Transfer Protocol) proxy server is a type of proxy server that handles HTTP requests and provides an important role in managing and securing SSPR access. If the value is blank, the system uses no proxy server.
- HTTP Proxy Exceptions: The URL's that are excluded from going through the configured HTTP proxy server. It provides a flexible and customizable way to manage SSPR access through an HTTP proxy server, enabling network administrators to balance the need for security, privacy, and accessibility to the resources that are critical for their organization.
- App Property Overrides: An override application property is a setting that allows you to change the value of a property in your application's configuration file. Overriding a property value can be useful in certain situations, such as when a default property value is not suitable for your specific use case, or when you need to temporarily change a property value for testing or troubleshooting purposes.
- Character Set for decoding inbound data: Specify the default character set for decoding inbound parameters. The acceptable values for the default character set can be found in the Java Standard Charset documentation.

Use these settings to customize Self Service Password Reset for your users.

To configure the application settings:

1. Log in to Self Service Password Reset at `https://dns-name/sspr` as an administrator.
2. In the toolbar, click your name.
3. Click **Configuration Editor**.
4. Click **Settings > Application > Application**.
5. Follow the help instructions to configure the different settings.
6. In the toolbar, click **Save changes**.

Configuring IP address of the Appliance

1. Access the command line console of the appliance.
2. Run the following command as root:

   ```
   yast novell-vainit
   ```

3. After making the desired changes, reboot the appliance.

Configuring localization settings

Self Service Password Reset provides localization support by default for the following languages: English, Catalan, Chinese Simplified, Chinese Traditional, Danish, Dutch, French, German, Italian, Japanese, Polish, Portuguese (Brazilian), Russian, Spanish, and Swedish.

The Configuration Editor allows you to simplify changes which language to display to your users.

To change the localization settings:

1. Log in to Self Service Password Reset at `https://dns-name/sspr` as an administrator.
2. In the toolbar, click your name.
3. Click **Configuration Editor**.
4. Click **Settings > Application > Localization**.
5. Follow the help to configure the localization settings.
6. In the toolbar, click **Save changes**.

Configuring session management settings

Self Service Password Reset allows you to control the browser sessions for the users. Use these setting to configure the browser sessions for your users. You also you these setting to send password expiration notifications. For more information, see "Sending notifications for expiring passwords" on page 112.

To configure sessions management settings:

1. Log in to Self Service Password Reset at `https://dns-name/sspr` as an administrator.
2. In the toolbar, click your name.
3. Click **Configuration Editor**.
4. Click **Settings > Application > Session Management**.
5. Follow the help to configure the session management settings.
6. In the toolbar, click **Save changes**.

Configuring the telemetry options

Self Service Password Reset contains a feature to gather statistical usage information about Self Service Password Reset. This information allows NetIQ to see which features are used the most and focus development resources on those features.

When you run the Configuration Guide, you have the option to enable or disable this feature. However, you can enable and disable this feature through the Configuration Editor as well.

To enable or disable the telemetry options:

1. Log in to Self Service Password Reset at `https://dns-name/sspr` as an administrator.
2. In the toolbar, click your name.
3. Click **Configuration Editor**.
4. Click **Settings > Application > Telemetry**.

5 Enable or disable the feature, then follow the help to configure the additional telemetry settings.

6 Click **Save changes**.

Configuring profiles

Self Service Password Reset allows you to define profiles that are user groups on which you can apply policies for different features. You define the profile in the module for the policy for the feature. By default, Self Service Password Reset creates a default profile named **default** for each module or policy that can use a profile. The profile name is **default** and you view and create the profiles in the Configuration Editor for the specific module or policy.

You create profiles for the following modules and policies:

- Delete Account module
- Help Desk module
- Update Profile module
- Forgotten Password module
- New User Registration module
- Challenge policies
- Password policies

It is not a requirement to create additional profiles, but it helps you manage what features the users access and use.

- "Creating a profile" on page 26
- "Managing profiles" on page 27

Creating a profile

When you create a new profile, the name you specify for the user group is the profile name for the module or policy. You must choose the profile name before adding the profile to the list because Self Service Password Reset does not allow you to rename the profile name.

To create a profile:

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

2 In the toolbar, click your name.

3 Click **Configuration Editor**.

4 Expand the appropriate module or policy.

5 Click **Edit List**.

6 Click **Add Profile**.

7 Specify a profile name.

The profile name has the following requirements:

- Starts with a letter (a-Z)

- Contains only letter, numbers, and hyphens
- Length between 2 and 15 characters

IMPORTANT: You cannot rename the profile name.

8 Click **OK** to create the profile.

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

Managing profiles

The Self Service Password Reset allows you to manage the profiles for each module or policy. If you have defined the **default** profile and you want to use most of the configuration options for a new profile, you can copy an existing profile to create a new profile. The Configuration Editor also allows you to view and append the profile list by using the **Edit List** option, plus change the precedence of profiles.

To manage profiles:

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

2 In the toolbar, click your name.

3 Click **Configuration Editor**.

4 Expand the appropriate module or policy.

5 Click **Edit List**.

6 To change the order that Self Service Password Reset presents the profiles to the users, click the up or down arrow to the right of the profile name.

7 To copy a profile:

   7a Click **Copy** to the right of the profile name.

   7b Specify a name for the new profile.

   The profile name has the following requirements:

   - Starts with a letter (a-Z)
   - Contains only letter, numbers, and hyphens
   - Length between 2 and 15 characters

   IMPORTANT: You cannot rename the profile name.

   7c Click **OK** to save the profile.

8 To delete a profile:

   8a Click **Delete** to the right of the profile name.

   8b Click **OK** to confirm the deletion.

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

Configuring security settings

Self Service Password Reset provides different security settings for the security of the users' information and passwords it manages. Ensure that you configure the security for Self Service Password Reset because it manages your users' credentials.

- "Configuring security for Self Service Password Reset" on page 28
- "Configuring web security" on page 29

Configuring security for Self Service Password Reset

Self Service Password Reset allows you to increase the security of the application through using security keys, reverse DNS, and the length of the sessions.

If you have imported the remote TLS connection certificates in to Self Service Password Reset, you can change how Self Service Password Reset reads the certificate. By default, Self Service Password Reset imports the entire remote TLS certificate chain into the configuration. At the time of connection, Self Service Password Reset reads the remote TLS certificate chain and compare all presented certificates with the stored configuration and allow a connection only if all certificates match. Self Service Password Reset allows you to change the configuration to have Self Service Password Reset only compare and match the Root CA Certificate to the Root CA Certificate in the Self Service Password Reset configuration.

To configure the security settings:

1. Log in to Self Service Password Reset at `https://dns-name/sspr` as an administrator.
2. In the toolbar, click your name.
3. Click **Configuration Editor**.
4. Click **Settings > Security > Application**.
5. Configure the following Application Security settings:

Field	Description
Security Key	Specify a Security Key used for cryptographic functions such as token verification. SSPR requires a value if you enabled tokens for any of the modules and configured a token storage method. SSPR uses this value similar to how a cryptographic security certificate uses the private key. If configured, this value must be at least 32 characters in length. The longer and more random this value, the more secure its uses are. If multiple instances of these values are in use, you must configure each instance with the same value. Upon initial setup, SSPR assigns a random security key to this value that you can change at any time. However, any outstanding tokens or other material generated by an old security key becomes invalid.
Enable Reverse DNS	Enable this option for SSPR to use its reverse DNS system to record the hostname of the client. In some cases, this might cause performance issues, so you can disable this option if you are not using it.
Show Detailed Error Messages	Enable this option to display detailed error messages. Although this information is useful for the administrators during configuration, this detailed information might be confusing and pose a security hazard in some cases. SSPR ignores this setting until you close the Configuration Guide.
Maximum Session Duration	Specify the maximum duration of a session (in seconds). Having a maximum session lifetime prevents certain types of long-term session fixation attacks. The default value is set to 28800 seconds.
Certificate Validation Mode	Specify how SSPR validates outbound SSL/TLS certificate. Specify one of the following validation modes: ◆ Entire Certificate Chain ◆ Root Certificate Only

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

Configuring web security

Self Service Password Reset is a web application. It provides a number of settings to help you increase the security of the communication over the web and to protect against web attacks. Use the following setting to help increase the security for the web communications.

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

2 In the toolbar, click your name.

3 Click **Configuration Editor**.

4 Click **Settings > Security > Web Security**.

5 Configure the following Web Security settings:

Field	Description
Enable Form Nonce	Enable this option to request a nonce (or unique key) for each form to prevent certain types of cross-site scripting (XSS) attacks.
Sticky Session Verification	Enable this option to verify browser sessions using an HTTP redirect and verification code. This verification confirms that the browser can correctly establish a session with the server. Verification also confirms that the browser either supports cookies or URL sessions (if enabled). The communication channel between the browser and application server is 'sticky' when there are multiple server instances. Additionally, it helps prevent some types of XSS attacks. The pre-loaded browser cache displays a `please wait` screen to the user during the verification. This has the added benefit that the browser `pre-caches` many of the HTTP resources (JavaScript, CSS, images, and so forth) before it loads any actual pages.
Disallowed HTTP Inputs	Specify the disallowed values. If any input values (on any HTTP parameter) match the disallowed value patterns, SSPR truncates the matching portion from the input.
Use X-Forwarded-For Header	If present, use the X-Forwarded-For HTTP header value as the client IP address instead of the HTTP connection source. Typically, upstream proxies add X-Forwarded-For headers or firewalls and might be the only reliable way to identify the user's source IP address.
Allow Roaming Source Network Address	Enable this option to allow SSPR to access a single HTTP session from different source IP addresses. Some load balancing or proxy network infrastructures might require this, but it is recommended to disable it in most cases. Especially since typical sessions are very short, there is no practical reason for a user to access the same session from multiple client addresses.

Field	Description
Required HTTP Headers	If specified, any HTTP/S request sent to this SSPR application server must include these headers. This feature is helpful if you have an upstream security gateway, proxy, or web server and want only to allow sessions from the gateway and deny direct access to this SSPR application server from clients. The settings must be in the name = value format. If the upstream security gateway, proxy, or web server is not set for these names/value headers, you will no longer be able to access this SSPR application server. **NOTE:** If the client you are using to access this server does not set the headers configured, this SSPR server will become inaccessible.
Permitted IP Network Addresses	Enable this option to enable SSPR only to permit connections originating from the specified IP address ranges. If disabled (default), SSPR allows any source IP address. **NOTE:** Supported range specifications are: ◆ Full IPv4 address, such as 12.34.56.78. ◆ Full IPv6 address, such as 2001:18e8:3:171:218:8bff:fe2a:56a4. ◆ Partial IPv4 address, such as 12.34 (which matches any IP addres starting 12.34. ◆ IPv4 network/netmask, such as 18.25.0.0/255.255.0.0. ◆ IPv4 or IPv6 CIDR slash notation, such as 18.25.0.0/16 or 2001:18e8:3:171::/64.
Page Leave Notice Timeout	Specify a timeout period to determine when a user navigates away from any page. Based on this, the browser sends a notice to the server. The next time the browser requests a page, SSPR checks the timeout to determine if the last page leave time was greater than the timeout, and if so, it invalidates the user's session. This has the effect of logging out the users that navigate away from SSPR without explicitly logging out. You can disable this feature by setting the time limit to 0. If set to zero, you disable this feature.
Prevent HTML Framing	Enable this option to prevent browsers from displaying SSPR inside an IFrame. SSPR does this by setting the X-Frame-Options HTTP Header to DENY on all pages.

Field	Description
Redirect Whitelist	Specify a list of partial URL fragments. Any attempt to set the forward URL or logout URL via request parameter must match a URL fragment listed here: ◆ SSPR attempts to match each item from the beginning of the requested URL string. ◆ SSPR decodes and parses the redirect URL before checking it against the whitelist. ◆ If an error occurs when setting a redirect URL, set the debug logs to TRACE and watch the output as the error occurs. ◆ SSPR does not permit wildcards or case mismatches, and the values must match exactly. ◆ If a fragment has the prefix regex, SSPR treats the remainder of the fragment as a regular expression. Regular expression matches must match the entire URL.

HTTP Content Security Policy Header	Set the HTTP Content-Security-Policy header. This header instructs the browser to limit the locations from which it loads fonts, scripts, and CSS files.
	If you need to change the CSP (Content Security Policy) for more restricted security, edit the default CSP by clicking the **Edit** icon , and change the CSP.
	Following is a suggested CSP with more security:
	`default-src 'self'; style-src 'self' 'unsafe-inline';`
	`script-src https://www.google.com/recaptcha/ https://www.gstatic.com/recaptcha/ 'self' 'unsafe-eval' 'unsafe-inline' 'nonce-%NONCE%' ;`
	`frame-src https://www.google.com/recaptcha/ https://www.gstatic.com/recaptcha/; base-uri 'self' ;`

HTTP Strict Transport Security	Set the HTTP strict transport security header. This header instructs the browser to use only HTTPS to access the website. Following is the default configuration: `max-age=600; includeSubDomains.`

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

Importing certificates to create an HTTPS connection to browsers

The information in this section is only for the Self Service Password Reset appliance and Windows installations. If you have deployed the WAR file on Linux, see the Apache Tomcat documentation. For more information, see the *SSL/TLS Configuration HOW-TO* section in the *Apache Tomcat 8 Documentation*.

Self Service Password Reset manages your users' credentials and you must ensure that it communicates over secure channels to secure the users' credentials. When you run the Configuration Guide, Self Service Password Reset auto-generates certificates and private keys that it uses to create the HTTPS connections. These auto-generated certificates and private keys are not created by a well-known or commercial certificate authority. This means that if you use these certificates, the users see a warning message in their browser stating the connection is not secure.

To have the message stop you must generate and import a commercial X.509 certificate. The X.509 certificate must contain the following information:

- The X.509 public and private key pair.
- The corresponding X.509 certificate.
- All of the root certificates in the key chain. This includes the server certificate and keypair, plus the certificate authority (CA) certificate and any intermediate CA certificates.

Self Service Password Reset supports two files types. The file types are:

- A PKCS12 also known as PFX file. This is a common format for backing up and transferring an X.509 public key certificate and it's matching private key, along with the root certificates.
- A Java or Tomcat key file. This is commonly used by Java applications to store their X.509 public key certificates, private keys, and root certificates.

NOTE: On previous Windows installations, customers would have created the key file via Tomcat and managed it directly.

The following steps for the Windows installation and the appliance version of Self Service Password Reset.

To import a commercial X.509 certificate:

1. You must generate the appropriate certificate for your environment.
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 **Settings > HTTPS Server**.
6. Follow the help to import the X.509 certificate.
7. In the toolbar, click Save **changes**, then restart the server if required.

After you have imported the certificate, you can view the details of the certificate in the Configuration Manager. For more information, see "Working with the configuration manager" on page 19.

Configuring intruder detection

Self Service Password Reset contains a built-in intruder detection independent of what your LDAP directory provides. The intruder detection for the LDAP directories is meant to stop any human attacks on the Self Service Password Reset user store. You want to ensure that the intruder detection limits in the LDAP directory are lower than the Self Service Password Reset intruder detection limits.

Self Service Password Reset can be exposed directly to the internet, NetIQ added this additional layer of detection to help protect against robotic or automatic attacks. Self Service Password Reset always honors the internal intruder detection (if enabled) of the LDAP directory. The intruder detection setting in Self Service Password Reset must be much higher than the LDAP directory intruder detection settings.

Set the triggers to be sufficiently high so that normal user usage does not cause an application-level intruder detection. Self Service Password Reset honors the configured timeout period because the system is under a robotic or automatic attack. The help desk or administrator cannot unlock accounts due to the Self Service Password Reset intruder detection.

To configure the intruder lockout settings:

1. Log in to Self Service Password Reset at `https://dns-name/sspr` as an administrator.
2. In the toolbar, click your name.
3. Click **Configuration Editor**.
4. Click **Settings > Intruder Detection > Intruder Settings**.
5. Follow the help to configure the intruder settings.
6. Click **Settings > Intruder Detection > Intruder Timeouts**.
7. Follow the help to configure the intruder timeout settings.
8. In the toolbar, click **Save changes**.

Configuring external web services with REST

Self Service Password Reset REST integration with any product that supports REST. It also allows you to support external web authentications through REST. REST is a web service architecture that allows for interoperability between different applications on the internet using a defined standard. You must have a good knowledge and understand of REST to use these settings.

These settings are intended for the developers and the component integrators to integrate Self Service Password Reset with other external sources. The REST services help keep the session more secure for the users. For more information, see the REST documentation on the Self Service Password Reset documentation web page under **Reference**.

To configure the REST settings:

1. Log in to Self Service Password Reset at `https://dns-name/sspr` as an administrator.
2. In the toolbar, click your name.
3. Click **Configuration Editor**.
4. Click **Settings > Web Services > REST Clients**.

5. Follow the help to configure the different REST client settings. The help contains detailed examples for each setting.
6. Click **Settings > Web Services > Rest Services**.
7. Follow the help to configure the different REST services settings.
8. In the toolbar, click **Save changes**.

Configuring Self Service Password Reset settings

4 Configuring LDAP profiles and settings

Self Service Password Reset helps manage your users' credentials if you store the users' credentials in an LDAP directory. Self Service Password Reset supports Active Directory, eDirectory, and Oracle Directory Server. The system helps you manage the users' credentials by providing a help desk module where help desk administrators can reset the users' credentials. It also provides a self-service option where users can retrieve their own credentials or new users can create accounts.

When you use the Configuration Guide to configure your environment for Self Service Password Reset, it prompts you to enter information about the LDAP directory that contains your users. You must now create an LDAP profile for the selected directory and define settings for that profile. The profiles that you define are user groups on which you can apply policies for different features of Self Service Password Reset.

Use the following information to configure LDAP directory profiles and settings for your environment.

- "Configuring LDAP directory profile" on page 39
- "Configuring LDAP settings" on page 41
- "Updating the LDAP certificates" on page 47

Configuring LDAP directory profile

Self Service Password Reset allows you to configure multiple LDAP directory profiles depending on your environment. During the Configuration Guide process, you defined the default profile for your environment. You can change the information for the default profile or create new profiles. If you are manually configuring Self Service Password Reset, you must create an LDAP directory profile.

NOTE: You can create as many LDAP directory profiles that you need, however, the profiles must be of the same type. For example, they must be all eDirectory or all Active Directory.

Each LDAP profile defines a unique LDAP data environment that depends on the directory type and configuration. Each profile can have multiple redundant servers defined that must be shared on all the servers. For more information on creating an additional profile, see "Configuring profiles" on page 26. The following steps explain how to edit or create the **default** profile.

Gather the following information before configuring the default LDAP profile or creating a new LDAP profile.

Table 4-1 Required information to create an LDAP profile

	Information	Description
❑	LDAP URLs	Add a list of LDAP servers in URL format that SSPR uses for a fail-over configuration. SSPR uses the servers in the order they appear in this list. If the first server is unavailable, SSPR uses the next available server in the list. **NOTE:** LDAP load balancers and VIP are not supported.
❑	LDAP Certificates	Self Service Password Reset imports the LDAP server certificate from the LDAP server during the Configuration Guide process. The Configuration Editor imports a certificate for you at any time if you do not use the Configuration Guide.
❑	LDAP Proxy User and Password	Create a user in your LDAP directory that Self Service Password Reset uses to access the LDAP directory. The user must have the following rights: ◆ Browse users and manage password attributes of the user object ◆ Create object rights in the new user container (if enabled)
❑	LDAP Contextless Login Roots	Obtain the fully qualified distinguished name (FDN) for the root context where the users reside. You can have one or more contexts for contextless login for your users. However, do not add many contexts because Self Service Password Reset searches each context serially and it will impact the performance of Self Service Password Reset. **NOTE:** It is not recommended to specify the Domain-Controller context.
❑	LDAP Test User	Create an LDAP test user account that Self Service Password Reset uses to validate the health of the LDAP server. The new test user account must have the same privileges and policies as any other users in the system.
❑	LDAP User Attributes	You must define what LDAP user attributes Self Service Password Reset uses for user names, GUID, naming attribute (cn or uid), last password, group, email address, SMS destination address, password history, and an attribute that stores the response information from the challenge-response.

Before configuring the default LDAP profile or creating a new profile, ensure that you gather the information listed above in Table 4-1.

To configure LDAP profiles:

1. Log in to Self Service Password Reset at `https://dns-name/sspr` as an administrator.
2. In the toolbar, click your name.

3 Ensure that you have gathered the information listed in Table 4-1.

4 Click **Configuration Editor**.

5 To define the connection to the LDAP directory:

   5a Click **LDAP > LDAP Directories > default > Connection**.

   5b Use the help instructions and the information in Table 4-1 to define the LDAP connection to Self Service Password Reset.

   5c Click **Test LDAP Profile** to test if Self Service Password Reset is able to read the data of the users in this LDAP profile.

6 To configure the login setup:

   6a Click **LDAP > LDAP Directories > default > Login Setup.**

   6b Use the help instructions to define the user name search filter, the user selectable login contexts, and the LDAP profile display name.

7 To configure the user attributes for the LDAP directory:

   7a Click **LDAP > LDAP Directories > default > User Attributes.**

   7b Use the help instructions to define the user attributes Self Service Password Reset uses in your LDAP directory.

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

Configuring LDAP settings

Self Service Password Reset enables you to configure settings to control interactions of Self Service Password Reset with the LDAP directory that contains your users. You can select a template to configure the settings. Self Service Password Reset provides templates to set default settings for your back-end directories. Changing the template only affects default values. You can change the template at any time. Changing a template does not affect the modified settings.

Self Service Password Reset provides the following templates for supported directories:

- Active Directory
- Oracle Directory Server
- Identity Manager/ OAuth Integration

To configure Identity Manager/ OAuth Integration see, Identity Manager and Chapter 11, “Integrating Self Service Password Reset with NetIQ identity manager,” on page 143 and Chapter 9, “Integrating Self Service Password Reset with NetIQ access manager,” on page 121.

Use the following information to configure the settings for the other LDAP directory templates.

- “Configuring the global LDAP settings” on page 42
- “Configuring Microsoft Active Directory settings” on page 42
- “Configuring NetIQ edirectory settings” on page 43
- “Configuring the Oracle directory server settings” on page 47

Configuring the global LDAP settings

The Global settings control the interaction with an LDAP directory. These settings are not applicable to the user's LDAP profile. For more information about configuring LDAP for a profile see, "Configuring LDAP directory profile" on page 39.

To configure the global LDAP settings:

1. Log in to Self Service Password Reset at `https://dns-name/sspr` as an administrator.
2. In the toolbar, click your name.
3. Click **Configuration Editor**.
4. Select the LDAP directory template for your LDAP directory.
   - **4a** Click **Default Settings > LDAP Vendor Default Settings**, then select the LDAP directory you are using.

     NOTE: If you select **NetIQ eDirectory**, you can configure NMAS settings. See, "Configuring NetIQ edirectory settings" on page 43.
   - **4b** In the toolbar, click **Save changes**.
5. In the toolbar, click your name.
6. Click **Configuration Editor**.
7. Click **LDAP > LDAP Settings > Global**.
8. Use the help information to configure the global settings for the LDAP directories.
9. In the toolbar, click **Save changes**.

Configuring Microsoft Active Directory settings

Self Service Password Reset allows you to change the settings for Microsoft Active Directory.

To change the Microsoft Active Directory settings:

1. Log in to Self Service Password Reset at `https://dns-name/sspr` as an administrator.
2. In the toolbar, click your name.
3. Click **Configuration Editor**.
4. Click **Default Settings > LDAP Vendor Default Settings > Microsoft Active Directory**.
5. Select **LDAP > LDAP Settings > Microsoft Active Directory**.
6. Configure the Active Directory settings use the help.
7. In the toolbar, click **Save changes**.

Configuring NetIQ edirectory settings

You can use either eDirectory or eDirectory with NMAS as the back-end directory. These settings allow you to change the eDirectory setting configuring during the Configuration Guide.

- "Configuring edirectory challenge set options" on page 43
- "Configuring the LDAP edirectory settings" on page 43
- "Calculating password strength using the entropy calculator" on page 44

Configuring edirectory challenge set options

When the back-end directory is eDirectory, you can configure NMAS. All NMAS operations require an SSL connection to the directory. Benefits of this configuration include:

- Validation of passwords against the NMAS password policy.
- Email notifications for failed password operations, such as when a password coming from a connected system does not comply with the password policies.
- Better error messages when using universal password policies
- Better error handling during the change password process

If you must apply the policy settings for the challenge sets that you configured in NMAS, perform the following:

To change the policy settings for the challenge sets:

1. Log in to Self Service Password Reset at `https://dns-name/sspr` as an administrator.
2. In the toolbar, click your name.
3. Click **Configuration Editor**.
4. Click **LDAP > LDAP Settings > NetIQ eDirectory > eDirectory Challenge Sets**.
5. Define the eDirectory challenge sets using the help.
6. In the toolbar, click **Save changes**.

Configuring the LDAP edirectory settings

Apart from configuring the NMAS extension, you can configure some additional parameters for eDirectory.

To configure NetIQ edirectory:

1. Log in to Self Service Password Reset at `https://dns-name/sspr` as an administrator.
2. In the toolbar, click your name.
3. Click **Configuration Editor**.
4. Click **Default Settings** > **LDAP Vendor Default Settings** , then select **NetIQ eDirectory**.
5. Click **LDAP > LDAP Settings > NetIQ eDirectory > eDirectory Settings**.
6. Configure eDirectory settings using the help.
7. In the toolbar, click **Save changes**.

Calculating password strength using the entropy calculator

Self-Service Password Reset evaluates the strength or entropy of a password based on its length and the number of characters it contains. This computes how easy or difficult it is for an attacker to crack the new password through guessing or other possible fraudulent methods.

When a user changes the password, the entropy calculator evaluates the strength of specified password. You can use the evaluated strength to automatically apply specific password policy defined in eDirectory and determine the expiration date of the password mapped to a specific user account.

Configuring entropy-based policy

Before configuring entropy based policy, navigate to **Configuration Editor > Modules > Authenticated > Change Password** and ensure that your setup meets the following prerequisites:

- **Show Strength Meter** is enabled.
- **Strength Meter Algorithm** is set to **Nist - Entropy calculator**.

NOTE: The Password Entropy functionality can be used with any strength meter algorithms. It works with other algorithm but might not We recommend you to configure Entropy with Nist - Entropy calculator.

To configure entropy based policy and display the password expiration interval:

1. Log in to Self Service Password Reset at `https://dns-name/sspr` as an administrator.
2. Navigate to **Configuration Editor > LDAP > LDAP Settings > NetIQ eDirectory > eDirectory Settings**.
3. Enable the **Enable Entropy based Policy** option.
4. In **Entropy based Policy Mapping**, perform the following:
   - **4a** Move the slider and set the minimum value for the following category:
     - Low
     - Medium
     - High
     - Very High

     The value set for each category represents the minimum threshold for each category. The evaluated password strength of a password is used to determine and align to the corresponding category. The password strength is measured in bits.

     NOTE: While you set the minimum value for each category, ensure that the value is equal or higher than the lower category.

     For example, if the minimum value for the category **Low** is 20, then the minimum value must be higher than 20 for the category **Medium**.

   - **4b** Click **Add LDAP Policy** against each category and select the appropriate password policy.
5. (Conditional) If you want to display the password validity period on the **Change Password** screen, select **Display Expiry interval during change password**. This displays the duration until when the password is valid to users while the users set the password on the **Change Password** screen

By default, the **Display Expiry interval during change password** option is disabled.

6 Click **Save changes** in the toolbar.

Understanding password entropy

Consider that Thomas is an administrator of an organization and he is required to achieve the following:

- Implement the following requirements for the password:
  - Minimum number of characters: 8
  - Allow special characters
  - Allow spaces as characters
  - Allow pass phrases
  - Restrict commonly used passwords (for example, p@ssw0rd and other common phrases)
  - Restrict contextual specific passwords (for example, user's first name or personal attributes)
- Assign the password policies of eDirectory for each password strength range. The password strength range is calculated using Entropy algorithm as follows:

Password Strength Range (in bits)	Map to the eDirectory Policy
28 to 50	60 days Password policy
51 to 100	90 days Password policy
101 to 112	180 days Password policy
113 to any value	200 days Password policy

NOTE: If the password strength is less than 28 bits then it is considered as very low category. You can configure password reject policy for very low category as per your requirement using the Minimum Password Strength configuration. The Password Strength configuration restricts the passwords strength falling below the configured Low category threshold.

For more information about Minimum Password Strength configuration, see Configuring password policies.

Thomas must perform the following steps to achieve the preceding requirements:

1 Log in to SSPR as an administrator.

2 Navigate to **Configuration Editor > Modules > Authenticated > Change Password**.

3 Select **Display Phrases in Randoms** to allow users to set multiple words with space as the password. For example, train engines.

4 Select **Nist - entropy Calculator** from **Strength Meter Algorithm**.

5 Navigate to **LDAP > LDAP Settings > NetIQ eDirectory > eDirectory Settings**.

6 Select **Enable Entropy based Policy** to calculate the strength of user-specified password using the entropy calculator and map a policy to each category.

7 Set the minimum value and map the corresponding policy for each category as follows:

Category	Minimum Value	eDirectory Policy
Low	28	60 days Password
Medium	51	90 days Password
High	101	180 days Password
Very High	113	200 days Password

8 Select **Display Expiry interval during change password**. This displays the password validity duration while the users set the password on the **Change Password** screen.

9 Save changes.

After Thomas configures the password entropy policy, the following are possible scenarios for end-users:

Scenario	Calculated entropy	eDirectory Policy	Result
A user specifies `encourage` as the password in the **Change Password** screen	26.5	Reject Password	User is required to set a new password. **NOTE:** The SSPR rejects the password only if the Minimum Password Strength is configured. For more information about Minimum Password Strength configuration, see Configuring password policies.
A user specifies `encourage77` as the password in the **Change Password** screen	34	60 days Password policy	Password is set and a message `password expires in 60 days` is displayed to the user.
A user sets the password as `encouragement@123` in the **Change Password** screen	62.7	90 days Password policy	Password is set and a message `password expires in 90 days` is displayed to the user.
A user sets the password as `Electronic Communication@123` in the **Change Password** screen	105.3	180 days Password policy	Password is set and a message `password expires in 180 days` is displayed to the user.

Scenario	Calculated entropy	eDirectory Policy	Result
A user sets the password as `Electronic&Electrical Communication` in the **Change Password** screen	130.8	200 days Password	Password is set and a message `password expires in 200 days` is displayed to the user.

Configuring the Oracle directory server settings

Self Service Password Reset allows you to change settings for the Oracle Directory Server setting.

To change the Oracle directory server settings:

1. Log in to Self Service Password Reset at `https://dns-name/sspr` as an administrator.
2. In the toolbar, click your name.
3. Click **Configuration Editor**.
4. Click **Default Settings > LDAP Vendor Default Settings > Oracle Directory Server**.
5. Select **LDAP > LDAP Settings > Oracle DS**.
6. Configure the Oracle Directory Server settings using the help.
7. In the toolbar, click **Save change**.

Updating the LDAP certificates

To ensure that you have a secure connection between the LDAP directory and Self Service Password Reset, you must import a certificate in to Self Service Password Reset through the Configuration Editor or with the Configuration Guide. For more information about securing Self Service Password Reset with certificates, see "Securing Self Service Password Reset" in the *Self Service Password Reset 4.8 Installation Guide*.

Certificates always have an expiration date for security reasons. You must import a new certificate from the LDAP directory at some point. There are two different ways to do this depending upon if the certificate is expired or not.

- "Updating the LDAP directory certificate when it is not expired" on page 47
- "Updating the LDAP directory certificate after it expires" on page 48

Updating the LDAP directory certificate when it is not expired

If you know when the LDAP certificate if about to expire, you can import a newly updated certificate from the LDAP directory into Self Service Password Reset using the Configuration Editor.

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

4 Click **LDAP > LDAP Directories > *default* > Connection**.

   Select the appropriate profile for the LDAP directory.

5 Under **LDAP Certificates**, click **Clear** to delete the old certificate.

6 Click **Import From Server**.

   The Configuration Editor contacts the LDAP directory server and obtains a new certificate for you.

7 Click **OK**.

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

Updating the LDAP directory certificate after it expires

If the LDAP certificate has expired, that means you can not log into the Configuration Editor through normal means and you receive an error -5017. You must unlock the configuration before you can import a new LDAP directory certificate which enables logins again and lock the configuration.

To unlock the configuration and change the LDAP directory certificate while the certificate is expired:

1 Unlock the configuration using the specific steps for your platform. For more information, see "How to lock and unlock the Self Service Password Reset configuration" on page 179.

2 After you have unlocked Self Service Password Reset, access the SSPR login page and click **Configuration Editor**.

3 Click **LDAP > LDAP Directories > *default* > Connection**.

   Select the appropriate profile for the LDAP directory.

4 Under **LDAP Certificates**, click **Clear** to delete the old certificate.

5 Click **Import From Server**.

   The Configuration Editor contacts the LDAP directory server and obtains a new certificate for you.

6 Click **OK**.

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

8 Lock the configuration using the steps for your platform. For more information, see "How to lock and unlock the Self Service Password Reset configuration" on page 179.

5 Configuring authenticated modules for Self Service Password Reset

Self Service Password Reset contains many different modules to provide different functionality presented to users. You can configure settings in the module to apply to different user groups by creating different profiles. For more information, see Chapter 7, "Configuring policies," on page 79.

Self Service Password Reset divides the modules into two different categories: authenticated and public. This chapter contains the configuration information for the authenticated modules. For information about the public modules, see Chapter 6, "Configuring public modules for Self Service Password Reset," on page 61.

The authenticated modules require the users to be authenticated to Self Service Password Reset to access and use the modules. Use the following information to enable and configure the authenticated modules for Self Service Password Reset.

- "Configuring the account information module" on page 49
- "Configuring the administrators module" on page 50
- "Configuring the change password module" on page 51
- "Configuring the delete account module" on page 53
- "Configuring the Help Desk module" on page 55
- "Configuring the people search module" on page 57
- "Configuring one-time password" on page 58
- "Configuring the setup security questions module" on page 59
- "Configuring the shortcut menu module" on page 59
- "Configuring the update profile module" on page 60

Configuring the account information module

As an administrator, you can allow users to see their account information through the user web page. When you enable the **Account Information** module, the user web page displays an **My Account** tile after the users log in to Self Service Password Reset. The **My Account** tile allows users to view the history of their changed password, the password policy, and details about their account.

To configure the account information module:

1. Log in to Self Service Password Reset at `https://dns-name/sspr` as an administrator.
2. In the toolbar, click your name.
3. Click **Configuration Editor**.
4. Click **Modules > Authenticated > Account Information**.

5 Use the help to configure the Account Information module settings.

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

After you configure the Account Information module through the **Configuration Editor**, users can access their own information through the user web page, but they must be authenticated. A new Account Information tile appears on the web page. The users see the following information about their own accounts:

- User information
- Password status
- Forgotten password status
- Session information
- Password policy details
- Password history

Configuring the administrators module

Self Service Password Reset allows you define criteria to determine if users can access the Administration module. The Administration module allows users that are members of this group to access the Dashboard, the Configuration Editor, and the Configuration Manager. For more information about these features, see Chapter 2, "Getting started," on page 17.

You must specify an LDAP group or define an LDAP filter or to search for users that you want to have administrative rights. When Self Service Password Reset finds the users that match the search criteria, it automatically assigned users the administration rights.

To define the criteria for administrators:

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

2 In the toolbar, click your name.

3 Click **Configuration Editor**.

4 Click **Modules > Authenticated > Administration**.

5 Specify the query for the users you want to be administrators. You can query by using **Add Filter** to define the LDAP filter that includes the object class, and by using **Add Group** that includes the LDAP group.

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

Configuring the change password module

Users can change their passwords whenever they want by using Self Service Password Reset. Self Service Password Reset allows administrators to customize the password change experience for the users from the beginning to the end. The Change Password module allows you to configure actions the users must perform before changing their password. It also allows you to configure tasks the users must perform after they changed their passwords.

Here is a list of some of the options you can configure for the users:

- Define permissions the users must have to change their password.
- Logout users after they change their passwords.
- Require users to specify their existing passwords to change their passwords.
- Show a password strength meter that is configurable among many other options.

  The Self-Service Password Reset evaluates password strength or entropy based on factors like length and character composition. It classifies passwords into the different strength level such as Very Weak, Weak, Good, Strong, and Very Strong.

  To display the password strength meter on the SSPR UI:

  - Enable **Show Strength Meter**.
  - Navigate to **Strength Meter Algorithm** and select the required algorithm type.

  SSPR offers three Strength Meter Algorithms:

  - Traditional – built in algorithm
  - zxcvbn – open source library
  - Nist – Entropy calculator

NOTE: By default the **Strength Meter Algorithm** is set to **Traditional built-in algorithm**.

Below are some examples of good and bad passwords.

Strength Level	Example	Explanation
Very Strong	C0mpl3xP@$$w0rd!	This password is very strong due to its length, complexity, and the use of a mix of characters, making it highly secure.
Strong	MySecur3P@ssw0rd	This password is strong due to its length, complexity, and the inclusion of various character types.
Good	SecurePwd123!	This password is good as it includes a mix of uppercase and lowercase letters, numbers, and a special character.
Weak	qwerty	This password is weak as it is a common keyboard pattern and lacks complexity.
Very Weak	password123	This password is very weak as it is a common and easily guessable sequence of characters.

- Allow use of phrases as the password (for example, electric wire) using the **Display Phrases in Randoms** option.

When the users click **Change Password**, the web page lists the prerequisites for users to change their password. If you want to change the text of the listed items, Self Service Password Reset allows you to do that. For more information, see the **Password Rule Text** setting in "Configuring a profile for a password policy" on page 83.

To configure the change password settings:

1. Log in to Self Service Password Reset at `https://dns-name/sspr` as an administrator.
2. In the toolbar, click your name.
3. Click **Configuration Editor**.
4. Click **Modules > Authenticated > Change Password**.
5. Use the detailed help to configure the different available settings.
6. In the toolbar, click **Save changes**.

Configuring the delete account module

You can configure Self Service Password Reset to allow users to delete their own accounts. By default, Self Service Password Reset does not enable this module. If you enable the Delete Account module, the user web page displays a new tile of **Delete My Account**. When a user clicks the tile, Self Service Password Reset walks the users through the deleting their accounts.

- "Enabling the delete account module" on page 53
- "Configuring the delete account module to delete accounts from integrated products" on page 53

Enabling the delete account module

Self Service Password Reset allows you to create multiple profiles for the Delete Account module. If you want to create additional profiles for the Delete Account module, see "Configuring profiles" on page 26.

To enable and configure the delete account module:

1. Log in to Self Service Password Reset at `https://dns-name/sspr` as an administrator.
2. In the toolbar, click your name.
3. Click **Configuration Editor**.
4. Click **Modules > Authenticated > Delete Account > Profiles**.
5. Configure the **default** profile and additional profiles you need for the Delete Account module with help.
6. Enable the Delete Account module.
   - **6a** Click **Modules > Authenticated > Delete Account > Settings > Enable Delete Account**.
   - **6b** Select **Enable** to enable the Delete Account module.
7. In the toolbar, click **Save changes**.

If you have configured the New User Registration feature in Self Service Password Reset, when users access the user web page, they can create an account again at any time. For more information, see "Configuring the new user registration module" on page 75.

Configuring the delete account module to delete accounts from integrated products

Self Service Password Reset allows to you do further integration with any integrated products by deleting user account information from the integrated products when a user deletes their own accounts using the Delete Account module.

Self Service Password Reset is able to delete the account information from the integrated products through REST APIs. The integrated products must have defined REST APIs for the delete action that you add as a pre-delete action to the Delete Account module configuration.

By default, the Delete Account module is not enabled and you must enable it to have this functionality in Self Service Password Reset. During the configuration of the Delete Account module, you can configure actions that Self Service Password Reset performs prior to deleting the user account from the user store location.

When you enable the Delete Account module, there is a **Pre-Delete Actions** option. You can define the REST APIs from the integrated products that delete the user account information from the integrated products when users delete their accounts from Self Service Password Reset.

The following is an example of how to configure Access Manager to delete user accounts from the Access Manager user stores when users delete their accounts from the Self Service Password Reset Delete Account module.The steps are the same for any integrated products, except for the REST call details.

Example of enabling deletes to flow to access manager:

1. Ensure that you completed the integration tasks to integrate Self Service Password Reset and Access Manager. For more information, see Chapter 9, "Integrating Self Service Password Reset with NetIQ access manager," on page 121.
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 **Modules > Authenticated > Delete Account > Settings.**
6. Enable the Delete Account module, then click **Save changes** in the toolbar.
7. Click **Modules > Authenticated > Delete Account**, then select the appropriate profile for your users. For more information, see "Configuring LDAP directory profile" on page 39.
8. Configure the Delete Account module to contain a pre-delete action:
   - **8a** In the **Pre-Delete Actions** field, click **Add Action**.
   - **8b** Specify a descriptive name for the action, then click **OK**.

     NOTE: This name must not contain any special characters. For example, no spaces are allowed.
   - **8c** Add a description of what the action does.
   - **8d** Select **webservice**, then click **Options**.
   - **8e** Define the REST API from Access Manager:
     - **8e1** In **HTTP Method**, select **Delete**.
     - **8e2** In **HTTP Headers**, click **Edit**.
       - **8e2a** Click **Add Header**.
       - **8e2b** In the **Name** field specify `Authorization Value` and the **Value** field specify `Base64 Encoded` *`admin username:password`*.

         NOTE: The admin username:password is your Access Manager administrator account that is in the LDAP identity store Self Service Password Reset uses.
       - **8e2c** Click **OK** twice.
     - **8e3** In **URL**, specify the REST call for the Access Manager delete the entire user history.

```
https://idp-url:8443/nidp/risk/rest/basic/v1/admin/
history?userDN=@Encode:urlParameter:[[@LDAP:dn@]]@
```

8e4 Leave the **Body** field empty. It is only used for POST REST calls.

8e5 Click **Import From Server** to have Self Service Password Reset import the certificate from Access Manager to establish a secure connection.

8e6 Click **OK**.

9 Ensure that you configure any other appropriate options for your environment, then click **Save changes** in the toolbar.

Configuring the Help Desk module

Self Service Password Reset provides a Help Desk module that helps you define criteria for help desk administrators. Help desk administrators can view user account data except for passwords, such as password modification, login details, last password change, account status, and so forth.

The major tasks of help desk administrators include resetting passwords, unlocking intruder locked accounts, assigning temporary passwords, managing users' challenge-responses, and deleting a user account. Enable these settings to allow help desk administrators to perform their tasks.

To perform help desk administrator activities, a user must be a member of an LDAP directory group that has required rights. If a user is a member of the correct LDAP directory group, when the user logs into Self Service Password Reset, they now see the Help Desk module as a new tile on the home page.

In the following scenarios, users cannot reset their passwords using the configured challenge-responses and call the help desk to reset passwords for them:

- When users forget the saved answers to the challenge questions.
- When users have not set up challenge-responses.

The Help Desk module is not enabled by default. You must enable the Help Desk module. Also, if you would like to have an Advanced Search option available in the Help Desk module, there are additional configuration steps you must perform.

- "Enabling and configuring the Help Desk module" on page 55
- "Configuring the advanced search for the Help Desk module" on page 56

Enabling and configuring the Help Desk module

By default, the Help Desk module is not enable. You must enable the Help Desk module and create a profile for your help desk users. You can create as many different profiles as you require. For more information, see "Configuring profiles" on page 26.

You must also configure the details, the options, and verification methods for each profile you create. use the following information and help to enable and configure the Help Desk module.

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

4 Click **Modules > Authenticated > Help Desk > Profiles > *default* > Details**, then configure the details of the default profile for the Help Desk module using the help.

5 Click **default > Options** to configure the options for the Help Desk module with the help.

6 Click **default > Verification** to configure the verification options for the Help Desk module with the help.

7 Enable the Help Desk module.

   7a Click **Modules > Authenticated > Help Desk > Settings > Enable Help Desk Module**.

   7b Select **Enable** to enable the Help Desk module.

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

Configuring the advanced search for the Help Desk module

Self Service Password Reset allows help desk administrators to search user details by using wildcard searches. For example, if the help desk user types *a*b* in the search field, the search result displays the list of users with names that include the letter *a* followed by any letter and then include the letter *b* as the last letter of the name. Self Service Password Reset also allows auto-complete (Ajax) searches that search the user details while they type. It also allows the help desk users to search for multiple attributes at the same time.

If the default searching abilities are not sufficient for your environment, you can enable an Advance Search option for the Help Desk module to allow the help desk administrations to limit the search by additional options. To enable the Advance Search option for the Help Desk Module:

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

2 In the toolbar, click your name.

3 Click **Configuration Editor**.

4 To enable the **Advanced Search** option.

   4a Click **Modules > Authenticated > Help Desk > Profiles > *default* > Options**.

   4b In the **Enable Advanced Search** field, select **Enable (True)** to enable the advanced search.

5 To add the ability to select attributes to search:

   5a Click **Modules > Authenticated > Help Desk > Profiles > *default* > Details**.

   5b In the **Help Desk Search Attributes** field, add the attributes the help desk administrators can use for searching.

6 To add the determine what the search results are:

   6a Click **Modules > Authenticated > Help Desk > Profiles > *default* > Details**.

   6b In the **Help Desk Search Results** field, change the attribute from **text** to **select** to have it appear in the Help Desk module.

7 In the toolbar, click **Save Changes**.

Configuring the people search module

The People Search module allows anyone to use the People Search option to search for people and view the details of the people. You can see details such as user name, email address, photo (if specified), and an organizational chart. The organizational chart displays the details of other users who report to the selected user (in a hierarchy) and also with the details of the user's manager. The arrow displays the user's level in the hierarchy.

Self Service Password Reset requires that the users who use People Search have read permission to view all the attributes that the People Search module displays. Self Service Password Reset uses wildcards or Ajax search (searching and displaying results while typing).

- "Enabling and configuring the people search module" on page 57
- "Configuring the advanced search option in the people search module" on page 58

Enabling and configuring the people search module

By default, the People Search module is not enabled. You must enable and configure the People Search module for your users to have access to it. There are also a number of features that are not enabled by default in the People Search module. Some of the features that you must enable are:

- The organization chart view
- Printing the organization chart
- A link to email your team
- The ability to export the organization chart

You must enable the People Search module and then configure the module to do what is appropriate for your environment.

To enable and configure the people search module:

1. Log in to Self Service Password Reset at `https://dns-name/sspr` as an administrator.
2. In the toolbar, click your name.
3. Click **Configuration Editor**.
4. Click **Modules > Authenticated > People Search**.
5. In the **Enable People Search** field, select **Enable (True)** to enable the People Search module.
6. Configure the appropriate settings for your environment using the help.
7. In the toolbar, click **Save changes**.

Configuring the advanced search option in the people search module

You can configure Self Service Password Reset to allow users to search for their colleagues' information and also configure the attributes the People Search module displays in the search result.

If the basic search is not enough for your users, you can enable an **Advanced Search** option in the People Search module.

1. Log in to Self Service Password Reset at `https://dns-name/sspr` as an administrator.
2. In the toolbar, click your name.
3. Click **Configuration Editor**.
4. Click **Modules > Authenticated > People Search**.
5. In the **Enable Advanced Search** field, select **Enable (True)**.
6. To add the ability to select attributes to search:
   - **6a** Click **Modules > Authenticated > People Search**.
   - **6b** In the **Search Attributes** field, add the attributes the help desk administrators can use for searching.
   - **6c** Change the option **text** to **select** to allow users to select the attribute in a search.
7. In the toolbar, click **Save changes**.

Configuring one-time password

The one-time password feature (OTP) enables the users to create a secret when they enroll their mobile devices. Also, you can enable OTP so that users can use it to reset their password during forgotten password process. You can enable OTP through a mobile application for authentication. To use this feature, you need the mobile application that has the rfc6238 generator. For example, Google Authenticator or OTP Authenticator.

To use the OTP feature the configuration for the **Verification Methods** setting must be set to **Required** and when the users log in, they must enroll their mobile devices.

NOTE: You must ensure that the time (in seconds) for LDAP server, Self Service Password Reset server, and the mobile device is synchronized because the 6-digit TOTP is valid only for 30 seconds. The time difference of 5 seconds is acceptable.

You can choose to include challenge-response or OTP for forgotten password process by using the **Verification Methods** settings under **Forgotten Password Profiles**. For more information about Forgotten Password Profiles, see "Configuring forgotten password module" on page 61.

To configure one-time password:

1. Log in to Self Service Password Reset at `https://dns-name/sspr` as an administrator.
2. In the toolbar, click your name.
3. Click **Configuration Editor**.
4. Click **Modules > Authenticated > Setup OTP**.

5 Define a profile for the LDAP users you want to use OTP. For more information, see "Configuring LDAP directory profile" on page 39.

6 Use the help to configure the OTP settings for your users.

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

Configuring the setup security questions module

During the login process, the login page automatically redirects users to the Challenge-Response page. Users set up the responses for challenge questions on this page. When users forget their passwords and try to reset it, Self Service Password Reset prompts for the configured questions and asks the users to specify the correct answers. When the answers match with the responses saved earlier by the users, Self Service Password Reset allows the users to reset their passwords. To configure the challenge-response policy for different profiles, see "Configuring profiles" on page 26.

Apart from configuring random and required questions, you can configure a number of other important settings such as force response setup, the case of the responses, and so forth. All of these components are part of the Setup Security Questions module.

To configure the setup security questions module:

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

2 In the toolbar, click your name.

3 Click **Configuration Editor**.

4 Click **Modules > Authenticated > Setup Security Questions**.

5 Configure the settings for the Security Questions using the help.

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

Configuring the shortcut menu module

The Shortcut Menu module displays a list of links. To make it visible and available for users, you must enable the Shortcut Menu module. After enabling this feature, users can access it on the Main Menu of the user web page for Self Service Password Reset. You can add a number of shortcuts for users.

To configure the shortcut menu module:

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

2 In the toolbar, click your name.

3 Click **Configuration Editor**.

4 Click **Modules > Authenticated > Shortcut Menu.**

5 Configure the settings to enable the Shortcut Menu module using the help.

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

Configuring the update profile module

You can enable users to view and update their profile attributes. This is feature is available on the Main Menu of Self Service Password Reset. Ensure that the attributes you configure in the Update Profile module have the required rights in the LDAP directory. For more information, see "Viewing LDAP permissions recommendations" on page 156.

You can create as many profiles as you require for your environment for the Update Profile module. You can define different settings for each profile to present different information to each group of users defined in each profile. For more information, see "Configuring profiles" on page 26.

Enabling the Update Profile module allows users to see an Update Profile tile on the main Self Service Password Reset page that takes the users to the Update Profile page. Self Service Password Reset displays the different options to the users on the Update Profile page that you configure. Including customized links or the specific attributes, you want the users to be able to edit. For an example of adding customized links, see "Adding the device management link to the update profile page" on page 134. The attributes displayed to the users are their name, email, photo, and so forth.

To configure the update profile module:

1. Log in to Self Service Password Reset at `https://dns-name/sspr` as an administrator.
2. In the toolbar, click your name.
3. Click **Configuration Editor**.
4. Click **Modules > Authenticated > Update Profile > Update Profile Profiles > default**.
5. Configure the settings for the default profile or any additional profiles for the Update Profile module using the help.
6. Enable the Update Profile module:
   - **6a** Click **Modules > Authenticated > Update Profile > Update Profile Settings**.
   - **6b** Enable the **Enable Update Profile** setting to enable the module.
7. In the toolbar, click **Save changes**.

6 Configuring public modules for Self Service Password Reset

Self Service Password Reset contains many different modules to provide different functionality presented to users. You can configure settings in the module to apply to different user groups by creating different profiles. For more information, see Chapter 7, “Configuring policies,” on page 79.

Self Service Password Reset divides the modules into two different categories: authenticated and public. This chapter contains the information about how to configure the public modules. For information about the authenticated modules, see Chapter 5, “Configuring authenticated modules for Self Service Password Reset,” on page 49.

The public modules are available to any users that access the Self Service Password Reset user page. These modules are public because these services are available for users that have forgotten their credentials, new users that do not have an account yet, or to active user accounts. Use the following information to configure the public modules for Self Service Password Reset.

- “Configuring forgotten password module” on page 61
- “Configuring the forgotten user name module” on page 75
- “Configuring the new user registration module” on page 75
- “Enabling the user activation module” on page 77

Configuring forgotten password module

Using the Forgotten Password module, you can enable users to recover a forgotten password without contacting the help desk. After enabling this feature, the **Forgotten Password** option is displayed on the user login web page.

The Forgotten Password module uses different verification methods to let users recover their passwords. To know more about the verification methods, see Understanding verification methods.

For example, the administrator can set a challenge or a one-time password (OTP) for changing the password. It enforces the user to answer challenge questions or specifying an OTP to reset the forgotten password.

To enable this feature, perform the following actions:

- “Configuring the forgotten password profile” on page 62
- “Configuring the forgotten password settings” on page 68
- “Configuring the OAuth2 verification method for the forgotten password module” on page 74

Configuring the forgotten password profile

When you configure a Forgotten Password profile, users of that group can reset their passwords by using the verification method that you define in that profile. You can define a default profile for all users. You can also create different profiles for different user groups.

Understanding verification methods

Self Service Password Reset provides the following verification methods:

- **Previous authentication:** Checks if a user has used the same browser previously for authentication. Self Service Password Reset requires the users to use the same browser for the Forgotten Password module to work.
- **LDAP attributes:** Requires the user to specify the values for any LDAP attributes that you specified in the **Required LDAP Attributes** setting.

  If you have upgraded Self Service Password Reset from an earlier version where LDAP attributes were required for the Forgotten Password process, then ensure that you specify the LDAP attributes under the **Required LDAP Attributes** option and mark this verification method as **Required**.
- **Challenge/Response answers:** Requires the users to answer the challenge-response questions.
- **SMS/Email token verification:** Allows users to use the token verification through SMS or email.

  If you have upgraded Self Service Password Reset from an earlier version where the password send method was set as a token, then ensure that you mark this verification method as **Required**.

  NOTE: The SSPR session is specific to the browser that is being used. If the user copies the email verification link provided in the email manually, it is recommended to paste the email verification link into the same browser session in which the user initiated the SSPR process.

- **OTP (Mobile device) verification:** Requires the user to use the one-time password (OTP) during the forgotten password process.
- **External responses:** Allows the user to use the responses that are stored in the external web services server. This is applicable if you have specified the external web service server URL in **Settings > Web Services > REST Clients > External Remote Responses REST Server URL**.
- **OAuth2:** Allows you to create an OAuth2 connection between Self Service Password Reset and any application that supports OAuth2.
- **Advanced authentication:** Self Service Password Reset deprecated this method of connecting to NetIQ Advanced Authentication. If you have used this method in the past, it still works. However, if you want to configure a new deployment of Advanced Authentication with Self Service Password Reset, you must use the OAuth2 verification method.

You can customize the text and descriptions for these methods that users see through **Display Text** options in the Configuration Editor. Under Display, search for **Field_VerificationMethod*Method*** and **Description_VerificationMethod*Method*** where ***Method*** is the name of the verification method.

In this Section

- "Configuring the default profile" on page 63
- "Creating a new profile" on page 68

Configuring the default profile

You can configure the existing profiles in the default section. To configure a default profile, perform the following actions:

- "Configuring definitions" on page 63
- "Configuring the OAuth connection to an external application" on page 65
- "Configuring options" on page 67

Configuring definitions

1. Log in to Self Service Password Reset as an administrator.
2. In the top-right corner of the Dashboard screen, click the user name.
3. Click **Configuration Editor**.
4. Navigate to **Modules > Public > Forgotten Password > Profiles > default > Definition.**
5. Configure the following settings:
   - Forgotten Password Profile Match
   - Verification Methods
   - Token Send Method
   - Forgotten Password Recovery Mode
   - New Password Send Method
   - Required LDAP Attributes

Forgotten Password Profile Match

Add an LDAP filter to define the set of users that Self Service Password Reset assigns to this profile.

1. Click **Add Filter**.
2. Select the filter for profiles in **LDAP Profile**.
3. Specify a valid LDAP filter in **LDAP Search Filter**.
4. Specify the LDAP base DN in **LDAP Base DN (Optional)**.
5. Click **View Matches**.

You can add a new group of users to the Forgotten Password profile.

1. Click **Add Group**.
2. Select the filter for filtering the profiles in **LDAP Profile**.
3. Specify the LDAP base DN in **LDAP Group DN**.
4. Click **View Matches**.

Verification Methods

The verification method that you require the users to use must be set to Required (placing the vertical bar to the extreme right). You can also include multiple optional methods as required methods by specifying that number in **Minimum Optional Required**.

For example, if you set the verification method `Challenge/Response Answers` to **Required** and set `OTP (Mobile Device) Verification` to **Optional** with no value specified in **Minimum Optional Required**, then the users are required to answer the challenge-response or to skip it using the one-time password for verification during the forgotten password process.

In a scenario where the verification method is challenge-response and OTP is optional, users can choose to skip enrolling for OTP. But during the forgotten password process, if you enabled OTP with the **Force Setup-but allow user to skip** setting, the login page prompts users to enroll for OTP with an option to skip it. Self Service Password Reset prompts the Active Directory users to enroll for OTP before a password is reset and prompts eDirectory users to enroll after the password is reset.

For more information about verification methods, see Understanding verification methods.

Token Send Method

Select one of the following methods for sending the token code or a new password to a user:

- Email-Send to the Email address

  NOTE: The SSPR session is specific to the browser that is being used. If the user copies the email verification link provided in the email manually, it is recommended to paste the email verification link into the same browser session in which the user initiated the SSPR process.
- SMS- Send via SMS
- User choice - If both SMS and email address are available, the user decides

Forgotten Password Recovery Mode

Select one of the following recovery modes:

- Allow user to set password
- Send new password
- Send new password and mark as expired

New Password Send Method

Select one of the following methods for sending the new password to users if the **Forgotten Password Success Action** is set to **Send new password**:

- Email-Send to the Email address
- SMS- Send via SMS

Required LDAP Attributes

Add the required LDAP attributes for forgotten password authentication. Users must provide these attributes as part of the forgotten password authentication process. Perform the following steps to add a new LDAP attribute:

1. Click **Add Item**.
2. Specify a name for the attribute in **Required LDAP Attributes - New Form**.
3. Click **OK**.

6 Click **Save changes**.

Configuring the OAuth connection to an external application

Configure the OAuth2 connection to an external application if you select OAuth 2 as a verification method. For more information, see Configuring the OAuth2 verification method for the forgotten password module.

Perform the following actions to configure OAuth settings:

1 Log in to Self Service Password Reset as an administrator.

2 In the top-right corner of the Dashboard screen, click the user name.

3 Click **Configuration Editor**.

4 Navigate to **Modules > Public > Forgotten Password > Profiles > default > OAuth.**

5 Configure the following OAuth settings:

- OAuth Login URL
- OAuth Code Resolve Service URL
- OAuth Profile Service URL
- OAuth Web Service Server Certificate
- OAuth Client ID
- OAuth Shared Secret
- OAuth User Name/DN Login Attribute
- OAuth Inject User Name Value

OAuth Login URL

Specify the OAuth server login URL. This URL is to redirect users for authentication.

1. Click **Add Value**.
2. Specify the login URL in **Edit Value - OAuth Login URL**.

   For example, `https://oauthserver.example.com/osp/a/idm/auth/oauth2/grant`.
3. Click **OK**.

OAuth Code Resolve Service URL

Specify the OAuth Token / Code Resolve Service URL. This web service URL resolves the artifact sent by the OAuth identity server.

1. Click **Add Value**.
2. Specify the login URL in **Edit Value - OAuth Code Resolve Service URL**.

   For example, `https://oauthserver.example.com/osp/a/idm/auth/oauth2/authcoderesolve`.
3. Click **OK**.

OAuth Profile Service URL

Specify the web service URL provided by the identity server to send the attribute data of a user.

1. Click **Add Value**.
2. Specify the login URL in **Edit Value - OAuth Profile Service URL**.

   For example, `https://oauthserver.example.com/osp/a/idm/auth/oauth2/getattributes`.
3. Click **OK**.

OAuth Web Service Server Certificate

Click **Import from Server** to import the web server certificate.

OAuth Client ID

Specify the OAuth client ID used in the remote system for your service. The OAuth identity service provider provides you this ID.

1. Click **Add Value**.
2. Specify the OAuth client ID in **Edit Value - OAuth Client ID**.
3. Click **OK**.

OAuth Shared Secret

Specify the OAuth shared secret used in the remote system for your service. The OAuth identity service provider provides you this value.

1. Click **Store Value**.
2. Specify the client secret from the OAuth server in **New Password**.
3. Specify the same client secret in **Confirm Password**.
4. Specify the length of the client secret.
5. Click **Store Password**.

OAuth User Name/DN Login Attribute

Specify the attributes to request from the OAuth server which Self Service Password Reset uses as the user name for local authentication.

1. Click **Add Value**.
2. Specify the OAuth username/DN attributes in **Edit Value - OAuth User Name/DN Login Attribute**.
3. Click **OK**.

OAuth Inject User Name Value

Specify the user name value to send as part of the redirect request.

1. Click **Add Value**.
2. Specify the OAuth inject username in **Edit Value - OAuth Inject User Name Value**.

   For example, @LDAP:DN@.
3. Click **OK**.

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

Configuring options

1 Log in to Self Service Password Reset as an administrator.

2 In the top-right corner of the Dashboard screen, click the user name.

3 Click **Configuration Editor**.

4 Navigate to **Modules > Public > Forgotten Password > Profiles > default > Option.**

5 Configure the following settings:

Field	Description
Allow Intruder Unlock	When a user forgets the password and performs many failed login attempts, the account is intruder locked. Enable this option to allow the user to unlock the account instead of resetting the password.
Allow Forgotten Password when Locked	Enable this option to allow users to use the Forgotten Password feature when the account is intruder locked in LDAP. This feature is not available when a user is using NMAS stored responses.
Allow Token Resend	Enable this option to allow users to send a token again, if the user did not receive it in first attempt.

Field	Description
Minimum Password Lifetime Options	These options manage the behavior of the password when a user tries to use the Forgotten Password feature while their password is within the minimum password policy lifetime window of their effective password policy. These options are only relevant if the user has an effective minimum password lifetime as part of their password policy. Select one of the following options: ◆ Allow- Allow normal action (ignore minimum lifetime) ◆ UnlockOnly- Allow only intruder password unlock ◆ None- Prevent usage of forgotten password

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

Creating a new profile

Using **Edit List,** you can create a new Forgotten Password profile and add a list of forgotten password policies.

NOTE: It is recommended not to modify the default list unless it is critical to define different forgotten password behavior for different users.

Profile names must meet the following requirements:

- Start with a letter (a-Z).
- Contain only letters, numbers, and hyphens.
- Length between 2 and 15 characters.

Perform the following steps to add a new profile:

1. Click **Add Profile**.
2. Specify the profile name in **Forgotten Password Profile - Add Value**.
3. Click **OK**.

For more information about profile selection by LDAP filter, see Forgotten Password Profile Match.

Configuring the forgotten password settings

To complete the configuration of the Forgotten Password module, you must also configure the Forgotten Password settings. The settings allow you to set up actions that the Forgotten Password process performs during the password recovery process.

NOTE: If you are using Active Directory when users change their passwords, Self Service Password Reset examines the password history only when the **Minimum Password Age** is set to `0` and the proxy is disabled. If **Minimum Password Age** is not `0`, it is important that users set a new password to complete Forgotten Password sequence.

During the Forgotten Password process, Self Service Password Reset uses the challenge-response information for the users to secure this process. Self Service Password Reset allows you to store the challenge-response information in different security hashing methods.

1. Log in to Self Service Password Reset as an administrator.
2. In the top-right corner of the Dashboard screen, click the user name.
3. Click **Configuration Editor**.
4. Click **Modules > Public > Forgotten Password > Settings**.
5. Configure the following Forgotten Password settings:

Enable Forgotten Password

Enable this option to make forgotten password recovery available to users.

Forgotten Password User Search Form

Specify the form fields for the Activate User module. Self Service Password Reset requires users to enter each attribute.

Forgotten Password User Search Filter

Click **Add Value** and add an LDAP search filter in **Edit Value - Forgotten Password User Search Filter**. Self Service Password Reset uses this value to search for users during the forgotten password recovery. The LDAP search filter must include each attribute in **Forgotten Password User Search Form**. Self Service Password Reset replaces tokens made of a form item name (such as `cn`) enclosed with a percent sign `%cn%` with values provided by the user.

For example, if the Activate User Form included the attributes `cn` and `sn`, then this filter might be appropriate:

```
(&(objectClass=person)(cn=%cn%)(sn=%sn%)
```

If you do not specify this setting, Self Service Password Reset automatically generates a search filter based on the required items in **Forgotten Password User Search Form**.

Response Read Location

Select the location from where Self Service Password Reset reads the responses. If you select an option with multiple values, Self Service Password Reset reads each location until it finds a stored response. By default, the Response Read Location is set to **LDAP**.

Following are the available set of locations:

- LDAP
- LDAP, Database
- LDAP, Database, LocalDB
- LDAP, LocalDB
- LDAP, LocalDB, Database
- Database
- Database, LDAP
- Database, LDAP, LocalDB
- Database, LocalDB
- Database, LocalDB, LDAP
- LocalDB
- LocalDB, Database
- LocalDB, Database, LDAP
- LocalDB, LDAP
- LocalDB, LDAP, Database

Response Write Location

Select the location where Self Service Password Reset writes the responses. Self Service Password Reset writes to all storage methods when users configure their response answers. By default, the Response Read Location is set to **LDAP**.

Following are the available set of locations:

- LDAP
- LDAP, Database
- LDAP, LocalDB
- LDAP, Database, LocalDB
- Database
- Database, LocalDB
- LocalDB

IMPORTANT: It is not recommended to use the Local DB to store responses in a production environment. It is not possible to make the Local DB storage redundant and no optimal backup methods are available for the Local DB.

Response Storage Hashing Method

Select a method of hashing which Self Service Password Reset uses to store responses. Storing the responses as the plain text might facilitate synchronization or migration to other systems but is not secure.

This setting controls how Self Service Password Reset writes the responses. Self Service Password Reset can read stored responses in other formats, and it cannot convert existing responses until a user receives the responses. Use the reporting engine to identify and count the hash types in use. By default, the Response Storage Hashing Method is set to **PBKDF2WithHmacSHA512**.

Forgotten Password Post Actions

These actions are executed after a user completes the forgotten password sequence successfully and the user's password has been modified.

For example, if you set to update the phone number in LDAP action, the phone number of the user will get updated once the user completes the forgotten password sequence successfully.

1. Click **Add Action** and specify the name of the action in **New Action**.
2. Click **Actions** to set the post actions
3. Select any of the following action:
   - LDAP Action
   - Web Service Action

Adding a new LDAP action

a. Specify the LDAP attribute in **Attribute Name** and click **OK**.

b. Click the **Edit** icon to edit the LDAP Action.

c. Specify the LDAP attribute value.

d. Select the required action from the following **Operation Type**.
   - Replace (Remove all existing values)
   - Add (Append new value)
   - Remove (Remove specified value)

e. Click **OK**.

Adding a new web service action

a. Specify the web service URL in **URL** and click **OK**.

b. Click the **Edit** icon to edit the Web Service Action.

c. Select the required **HTTP Method** from the following:
   - Delete
   - Get
   - Post
   - Put
   - Patch

d. Click **Edit** in **HTTP Header** to add a new header rule.

e. Specify the web service URL in **URL**.

f. Specify the username of the user that is configured for Business Central Server in **Basic Auth Username**.

g. Specify the password of the user that is configured for Business Central Server in **Basic Auth Password**.

h. Click **Edit** in **Success Status Codes** to edit the status success code.

i. Click **Import Certificate** to import web service certificate.

j. Click **OK**.

Enable Bogus User Policy

Enable this option to have forgotten password act as if the invalid user searches are valid, and display such users with a fake forgotten password policy. This policy prevents username discovery.

The **Enable Bogus User Policy** option only supports **Email Token Verification** and **Challenge/Response Answers** verification methods, both separately and combined.

If both the **Email Token Verification** and **Challenge/Response Answers** verification methods are set to required, then the **Email Token Verification** method is always considered the first method, regardless of the order of the verification methods.

Configuring the OAuth2 verification method for the forgotten password module

If you select OAuth2 as a verification method for the Forgotten Password module, you must configure additional settings to create the OAuth2 connection. OAuth2 is an authorization framework that enables other applications to gain access to Self Service Password Reset through this secure protocol. For more information, see the *OAuth 2.0 Documentation*.

To configure the OAuth2 verification method properly, you must obtain information from the application you are connecting to through this method. Here is a list of the information you must get from the connecting application:

- ❒ Login URL from the OAuth server
- ❒ OAuth code resolve service URL from the OAuth server
- ❒ Web service URL of the identity server that contains attribute data about the users
- ❒ OAuth web service server certificate
- ❒ OAuth client from the OAuth identity service provider
- ❒ OAuth shared secret from the OAuth identity service provider
- ❒ OAuth user name or DN login attribute from the OAuth server
- ❒ User name value to inject as part of the `/grant` redirect request

---

NOTE: The remote OAuth server must support the non-standard `/sign` endpoint for this to work.

For example, if you are using Advanced Authentication as the application for the OAuth2 verification method, you must obtain information from Advanced Authentication to complete the configuration. Also, you must perform configuration steps in the connected application to finish the OAuth2 configuration.

To configure the OAuth2 verification method for the forgotten password module:

1. Ensure that you have set the **OAuth2** verification method to **Required** or **Optional** in the **Verification Methods** of the Forgotten Password profile.
2. Log in to Self Service Password Reset as an administrator.
3. In the toolbar, click the user name.
4. Click **Configuration Editor**.

5 Click **Modules > Public > Forgotten Password > Profiles > OAuth**.

6 Use the information you obtained to configure the OAuth settings. For information about fields, see "Configuring the OAuth connection to an external application" on page 65.

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

8 Configure the connected application to accept the OAuth2 connection by providing the OAuth URL endpoint from Self Service Password Reset. The URL base must be the value found in the **Settings > Application > Application > Site URL** with `/public/OAuth` at the end of the URL. For example:

```
https://sspr.example.com/sspr/public/OAuth
```

9 Select the HTTP method to invoke the Identity Server's OAuth Profile/UserInfo Service. The HTTP method returns the user-related attribute data for Single Sign-on and Forgotten Password modules. By default, the HTTP method is set to POST. However, the administrator can select the GET method for making a request to the Identity server's OAuth Profile/UserInfo Service.

To select the HTTP method, navigate to **Settings > Single Sign On (SSO) Client > OAuth > OAuth Profile / UserInfo Service Method Type**.

Configuring the forgotten user name module

Self Service Password Reset allows users to recover a forgotten user name without contacting the help desk through the Forgotten User Name module. The Forgotten Password User Name module is a configurable feature. After enabling this feature, users see the **Forgotten User Name** option on the user login web page.

The module is available to the public because the users forgot their user name and cannot authenticate to Self Service Password Reset. You can configure a search filter and attributes that enable users to search for a forgotten user name.

To configure the forgotten user name module:

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

2 In the toolbar, click your name.

3 Click **Configuration Editor**.

4 Click **Modules > Public > Forgotten User Name**.

5 Configure the settings to enable the Forgotten User Name module using the help.

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

Configuring the new user registration module

You can enable users to create a new user account by clicking **New User Registration** on the login page of Self Service Password Reset. You can specify the attributes that the new user must have to register and the actions that the system must perform when it creates a new user. It also allows you to define actions that it will perform after a user completes the registration process. For an example,

the New User Registration module allows you to forward users to a specific URL after the registration process completes. For an example, see "Creating accounts for social users in Self Service Password Reset using the new user registration module" on page 134.

By default, Self Service Password Reset uses LDAP attributes the users must have to register. You can use a remote REST API to provide the information instead of using the LDAP attributes. However, you must configure a REST client through the Configuration Editor. To access the REST client in the Configuration Editor, click **Settings > Web Services > REST Clients**. You must have the REST client information to configure these settings. For more information, see ""Configuring external web services with REST" on page 35".

If you want to create different profiles for different user groups, you can use the **Edit List** option and create different profiles. For more information about creating and configuring the profiles see, "Configuring profiles" on page 26.

When a new user completes the registration, Self Service Password Reset generates a random name that is included as an LDAP name or entry ID in the LDAP directory. You can specify the appropriate value in the directory as the display name or entry ID by using the **LDAP Entry ID Definition** setting. The display name or the entry ID can be name, email address, or any other information that is provided in the **New User Form**.

NOTE: The proxy user requires additional rights to create new users through the New User Registration module. For more information, see "Proxy user rights" in the *Self Service Password Reset 4.8 Installation Guide*.

To configure the new user registration module:

1. Log in to Self Service Password Reset at `https://dns-name/sspr` as an administrator.
2. In the toolbar, click your name.
3. Click **Configuration Editor**.
4. Click **Modules > Public > New User Registration > default**.
5. Configure the settings for the New User Registration module using the help.
6. Enable the New User Registration module:
   - **6a** Click **Modules > Public > New User Registration > New User Settings**.
   - **6b** Enable the **Enable New User Registration** setting to enable the module.
7. In the toolbar, click **Save changes**.

After you have enabled and configured the New User Registration profile, the user web page now contains a new link of **New user registration**. Any new users can create an account for themselves through this new link.

Enabling the user activation module

The User Activation module allows first-time users to activate their LDAP accounts and set passwords. This module adds a password (and other items if specified as an activation or post-activation action) to an existing but not yet claimed LDAP account.This feature helps the users activate their accounts after an administrator or an automated process creates the LDAP accounts for the users.

You must enable the Activation module for users to be able to claim their accounts if they have never authenticated with their LDAP account. Self Service Password Reset provides many different configuration options for the Activation module. For example, you can define pre-activation and post-activation actions a user must perform.

To enable user activation:

1. Log in to Self Service Password Reset at `https://dns-name/sspr` as an administrator.
2. In the toolbar, click your name.
3. Click **Configuration Editor**.
4. Click **Modules > Public > Modules > User Activation**.
5. Configure the User Activation Module settings using the help.
6. In the toolbar, click **Save changes**.

7 Configuring policies

This chapter describes how to configure Self Service Password Reset policies for the challenge-response information and for passwords. You can profiles on which you can apply password policies and challenge policies. For more information, see "Configuring profiles" on page 26.

This chapter includes the following:

- "Configuring challenge policy" on page 79
- "Configuring password policies" on page 82

Configuring challenge policy

You can configure the challenge-response policy for a profile that a specific group of users must use for populating the response answers. You can define challenge questions on the Challenge Profiles page for different profiles. For more information about additional profiles, see "Configuring profiles" on page 26.

A Self Service Password Reset administrator can configure the random and required questions for the users to use for resetting their passwords. You can also configure random and required questions that any help desk person can use for authenticating the users to reset their password. You can configure each random question. The random questions and the required questions for challenge-response can be set in the required locale. You can restrict users to use specific answers to the challenge questions. Such as the following:

- Provide the number of characters from the questions that can be used in the answer.
- Configure the number of random or required challenge questions presented to the users and the number of challenge questions they must answer.
- Enable the word list dictionary so that the users do not use an answer that is present in the word list.
- Enable the word list to include the answers provided for the random questions. You must enable this option per locale you use.

Use the following information to configure one or more profiles for the challenge-response information.

To configure a profile for challenge-response:

1. Log in to Self Service Password Reset at `https://dns-name/sspr` as an administrator.
2. In the toolbar, click your name.
3. Click **Configuration Editor**.
4. Click **Policies > Challenge Policies > default**.
5. Configure the following settings:
6. Click **Policies** > **Challenge Policies > default**.

Challenge Profile Match

Specify an LDAP filter to search for users that have the permissions to set up Challenge/Responses.

1. Click **Add Filter**.
2. Select the filter for profiles in **LDAP Profile.**
3. Specify the valid LDAP filter in **LDAP Search Filter**.
4. Specify the LDAP base DN in **LDAP Base DN (Optional)**.
5. Click View Matches.

You can add a new group of users to the Challenge Profile Match.

1. Click **Add Group**.
2. Select the filter for filtering the profiles in **LDAP Profile**.
3. Specify the LDAP base DN in **LDAP Group DN**.
4. Click **View Matches**.

Random Questions

Random Questions for Challenge/Response. SSPR presents some of these questions to the user during forgotten password - the number set in the **Minimum Password Required** setting. You might require the users to supply answers to all or some of these questions when setting up their responses, you control this by the **Minimum Random Challenges Required During Setup** setting.

Click on challenge questions to edit questions and policy settings.

Required Questions

Required Questions for Challenge/Response. The users must provide answers for all of these questions when setting up their responses. Additionally, the users must provide the answers to these questions during forgotten passwords.

To add a new question, perform the following steps.

1. Click **Add Question**.
2. Click on challenge questions to edit questions and policy settings.
3. Specify the new question in **Question**.
4. Select the option from following:
   - Admin Defined
   - User Defined
5. Specify the minimum length of the question in **Min Length**.
6. Specify the maximum length of the question in **Max Length**.
7. Specify the maximum question characters in **Max Question Characters**.
8. Click **OK**.

Minimum Random Required

Specify the minimum number of random questions required at the time of forgotten password recovery.

Minimum Random Challenges Required During Setup

Specify the minimum number of random questions for the users to complete during the Response Setup. If this number is higher than the available randoms or lower than the minimum required, SSPR adjusts it accordingly. Set the value to zero to force the users to configure all available random questions at the time of setup.

Help Desk Random Questions

Specify additional random questions to present to the help desk users. SSPR might require the users to supply answers to all or some of these questions when setting up their responses, as controlled by the **Minimum Help Desk Random Challenges Required During Setup** setting. The questions and answers are visible to Help Desk users but are not used for forgotten password recovery.

To add a new question, perform the following steps.

1. Click **Add Question**.
2. Click on challenge questions to edit questions and policy settings.
3. Specify the new question in **Question**.
4. Select the option from following:
   - Admin Defined
   - User Defined
5. Specify the minimum length of the question in **Min Length**.
6. Specify the maximum length of the question in **Max Length**.
7. Specify the maximum question characters in **Max Question Characters**.
8. Click **OK**.

Help Desk Required Questions

Add the questions which the users must provide answers for when setting up their responses. The questions and answers are visible to Help Desk users but are not used for forgotten password recovery.

To add a new question, perform the following steps.

1. Click **Add Question**.
2. Click on challenge questions to edit questions and policy settings.
3. Specify the new question in **Question**.
4. Select the option from following:
   - Admin Defined
   - User Defined
5. Specify the minimum length of the question in **Min Length**.
6. Specify the maximum length of the question in **Max Length**.
7. Specify the maximum question characters in **Max Question Characters**.
8. Click **OK**.

Minimum Help Desk Random Challenges Required During Setup

Specify the minimum number of Help Desk random questions for the users to complete during the Response Setup. If this number is higher than the available randoms or lower than the minimum required, the system adjusts it accordingly. Set this option to zero to force the users to configure all available randoms Challenge/ Response questions at the time of setup.

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

Configuring password policies

You configure your password policy to increase your network security by enforcing rules about how users create their passwords. Apply Self Service Password Reset password policy in one the following ways:

- Apply only the Self Service Password Reset policy
- Apply only the LDAP policy
- Merge the Self Service Password Reset policy with the LDAP policy

When you merge the Self Service Password Reset policy with the LDAP policy, Self Service Password Reset reads both policies. If both policies conflict with each other, Self Service Password Reset chooses the most restrictive policy.

Self Service Password Reset checks the text that a user set as their password and does not allow if that is available in the predefined password dictionary word list. The word list is a ZIP file containing one or more plain text files with one word per line.

Self Service Password Reset allows storing the shared password history for all users, which provides more security. You can also configure profile specific password policy, which means setting password policies for a different group of users who are part of different profiles.

To configure a password policy you must create a profile and configure two different sets of settings in Self Service Password Reset.

- "Configuring a profile for a password policy" on page 83
- "Configuring the word list settings" on page 90

Configuring a profile for a password policy

You can configure the password policies for specific groups of users by using the password policy profile. You can create different profiles for different user groups so that the system applies the specified password policy to each user group for each profile. For more information, see "Configuring profiles" on page 26.

Based on the policy specified for users, Self Service Password Reset generates the text to display in the change password policy. To customize this text, use the **Password Rule Text** setting, which overwrites the Self Service Password Reset auto-generated text.

Self Service Password Reset allows you to define the requirements for the password. You can specify if the password is required to have numbers, letters, and special characters. You can also define the minimum and the maximum number of uppercase and lowercase letters. Along with how many unique characters are required.

You can also define if groups of characters are allowed by using regular expressions. For example, the following two character groups of:

```
[a-zA-Z]+
[0-9]+
```

This regular expression requires that the users have a lowercase or uppercase letter or a number in their passwords.

To configure a password policy for the default profile:

1. Log in to Self Service Password Reset at `https://dns-name/sspr` as an administrator.
2. In the toolbar, click your name.
3. Click **Configuration Editor**.
4. Click **Polices** > **Password Policies > default**.
5. Configure the following password policy settings:

Password Policy Profile Match

Specify a query to determine if this password policy applies to a given user. During login, if the system has not assigned a previous policy to the user, it considers the matches here, and if positive, it assigns the user to this policy.

1. Click **Add Filter**.
2. Select the filter for profiles in **LDAP Profile.**
3. Specify the valid LDAP filter in **LDAP Search Filter**.
4. Specify the LDAP base DN in **LDAP Base DN (Optional)**.
5. Click View Matches.

You can add a new group of users to the Challenge Profile Match.

1. Click **Add Group**.
2. Select the filter for filtering the profiles in **LDAP Profile**.
3. Specify the LDAP base DN in **LDAP Group DN**.
4. Click **View Matches**.

Minimum Length

Specify the minimum length of the password. A value of zero disables this setting.

Maximum Length

Specify the maximum length of the password. A value of zero disables this check. Although, you can set this limit to large values, the LDAP directory is used may have fixed limitations on the supported password length.

Maximum Repeat

Specify the maximum amount of times the users can repeat any character throughout the password. A value of zero disables this setting.

Maximum Sequential Repeat

Specify the maximum times the users can sequentially repeat any character throughout the password. A value of zero disables this setting.

Allow Numeric Characters

Enable this option to allow numeric characters in the password.

Allow Last Character Numeric

Enable this option to allow the last character of the password to be numeric. This setting is applied only if the **Allow Numeric Characters** is enabled.

Maximum Numeric

Specify the maximum number of numeric characters which can be added in the password. A value of zero disables this check. This setting is applied only if the **Allow Numeric Characters** is enabled.

Minimum Numeric

Specify the minimum number of numeric characters which can be added in the password. A value of zero disables this check. This setting is applied only if the **Allow Numeric Characters** is enabled.

Allow Special Characters

Enable this option to allow special characters in the password.

Allow First Character Special

Enable this option to allow the first character of the password to be a special character. This setting is applied only if the **Allow Special Characters** is enabled.

Allow Last Character Special

Enable this option to allow the last character of the password to be a special character. This setting is applied only if the **Allow Special Characters** is enabled.

Maximum Special

Specify the maximum number of special characters which can be added in the password. A value of zero disables this setting. This setting is applied only if the **Allow Special Characters** is enabled.

Minimum Special

Specify the minimum number of special characters which can be added in the password. A value of zero disables this setting. This setting is applied only if the **Allow Special Characters** is enabled.

Maximum Alphabetic

Specify the maximum number of alphabetic characters which can be added in the password. A value of zero disables this setting.

Minimum Alphabetic

Specify the minimum number of alphabetic characters which can be added in the password. A value of zero disables this setting.

Allow Non-Alphabetic Characters

Enable this option to allow non-alphabetic characters in the password.

Maximum Non-Alphabetic

Specify the maximum number of non-alphabetic characters which can be added in the password. A value of zero disables this setting. This setting is applied only if the Allow Non-Alphabetic Characters is enabled.

Minimum Non-Alphabetic

Specify the minimum number of non-alphabetic characters which can be added in the password. A value of zero disables this setting. This setting is applied only if the Allow Non-Alphabetic Characters is enabled.

Maximum Uppercase

Specify the maximum number of uppercase characters which can be added in the password. A value of zero disables this setting.

Minimum Uppercase

Specify the minimum number of uppercase characters which can be added in the password. A value of zero disables this setting.

Maximum Lowercase

Specify the maximum number of lowercase characters which can be added in the password. A value of zero disables this setting.

Minimum Lowercase

Specify the minimum number of lowercase characters which can be added in the password. A value of zero disables this setting.

Minimum Unique Characters

Specify the minimum number of unique characters which can be added in the password. A value of zero disables this setting.

Maximum Characters From Previous Password

Specify the maximum number of characters from the previous password allowed in the new password. A value of zero disables this setting.

Minimum Lifetime

Specify the minimum number of time that must pass between password changes. Value is in seconds. A value of zero disables this setting.

Enable Word List

Enable this option to check the password against the configured Word List.

For more information about uploading Word List, see Configuring the word list settings.

For more information about Word List setting, see "Word lists" on page 114

Enabling Breach Database Check

To increase the security of the password you must enable **Breach Database Check**. When enabled, the Self Service Password Reset performs an online validation for the user entered password against `HaveIBeenPwned` database, and allows only if it is not available in the database.

Active Directory Password Complexity

Select the Microsoft Active Directory style password complexity rules.

Active Directory 2008 Password Complexity Maximum Violations

Specify the number of maximum Active Directory 2008 Level Complexity category violations. This setting does not affect unless the **Active Directory Password Complexity** is set to **AD 2008 Level Complexity**.

Required Regular Expression Matches

Specify a Regular Expression pattern which the password must match for the system to allow it. You can list multiple patterns. A pattern must match the entire password for the system to apply it. SSPR ignores a partial match. You can use macros. Click **Add Value** to add a new value.

Disallowed Regular Expression Matches

Specify a Regular Expression pattern which the password must not match for the system to allow it. You can list multiple patterns. A pattern must match the entire password for the system to apply it. SSPR ignores a partial match. You can use macros. Click **Add Value** to add a new value.

Disallowed Values

Specify a case insensitive list of values SSPR does not allow the users to use as passwords. Click **Add Value** to add a new value.

Disallowed Attributes

Specify a list of attributes not allowed to be used as passwords. SSPR reads the values for a given user and does not permit the users to use them as part of the password value. This check is case-insensitive.

For example: "Language:4" indicates the password cannot contain: "Engl", "ngli", "glis", or "lish", for English speaking users.

NOTE: Specifying a number after the attribute name restricts how many consecutive characters SSPR disallows in the value.

1. Click **Add Value** to add a new value.

Minimum Password Strength

Specify the strength of the passwords. SSPR examines the password strengths on a scale of 0 to 100 irrespective of other password policy settings. This setting requires that the users have a password that meets the minimum strength level specified here, regardless of other password policy rules. "Good" is 45 or better while 70 or better is considered "strong." A value of 0 disables this setting.

Maximum Consecutive Characters

Specify the maximum amount of characters in a sequence, such as 0123456789 or abcdefghijk. SSPR defines a more specific character sequence by the Unicode character order of each character after it converts the entire value to lowercase. A value of 0 disables this setting.

Password Change Message

Specify a message SSPR displays to the users during password changes. Might include HTML markup. You can override this setting by adding a change password message read as part of an LDAP password policy. Click **Add Value** to add a new value.

Password Rule Text

When blank, SSPR displays an automatically generated rule list to the user. The automated rule list may not be inclusive of all settings in the password policy. Some of the more esoteric or difficult to communicate rules do not appear in the automatically generated list. This is done in an attempt to not overwhelm the users with having to read and parse the rules before attempting to change their passwords. Should the user type a password that conflicts with such a rule - the per-keystroke rule checker provides direct feedback to the user on how to correct the problem.

If you do not want the automatically generated rule list, you can override it by setting a value here. The field permits HTML tags. Click **Add Value** to add a new value

Disallow Current Password

Enable this option to prevent the current password from being used as a new password.

NOTE: SSPR can only enforce this if the login method permits the user's password to be known.

Minimum Character Groups Required

Specify the number of regular expression matches defined in the setting **Policies > Password Policies > [profile] > Character Group Definitions**.

Character Group Definitions

Add an LDAP filter that contains a list of regular expression character matches. Along with the setting **Policies > Password Policies > [profile] > Minimum Character Groups Required**, this setting allows creating a complex list of requirements that the user only needs to partially match. For example, you can use this type of policy to replicate the Active Directory "3 out of 5" rules, but with more flexibility and customization.

1. Click **Add Value** to add a new value.

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

Configuring the word list settings

To increase the security of the passwords you must define a word list. A word list is a predefined password dictionary that Self Service Password Reset checks against the text that users set as their passwords. Self Service Password Reset does not allow a password if that text is available in the word list. The word list is a ZIP file containing one or more plain text files with one word per line. Regular expressions are not allowed in the word list file.

To configure the word list:

1. Log in to Self Service Password Reset at `https://dns-name/sspr` as an administrator.
2. In the toolbar, click your name.
3. Click **Configuration Editor > Policies > Password Policies > default**.
4. Ensure that **Enable Word List** is selected.
5. Upload the word list in one of the following ways:
   - **5a** Using a web server
   - **5b** Using the user interface
6. Click **Save changes** in the toolbar.

To verify the size of the word list, click **Configuration Manager > Wordlist**. The **Word Count** displays the size of the word list available in the text file.

For more information to add or remove words from the word list to view the updated word count, see Word lists.

Updating the word list

You can add few more words that you do not want to allow as password to the word list. To update the word list, perform one of the following:

- Customize the existing word list
- Create a word list

Customize the existing word list

1. Navigate to the `wordlist.zip` file from one of the following paths according to your setup:
   - **Appliance**: `/var/lib/docker/overlay2/c25d96dc05d02d3f3159889fa78d9e2e2fe44393b67a1ca257e14079d84d6d36/merged/root/.sspr-workpath/work-sspr-8443/war/WEB-INF/`
   - **Linux**: `/srv/tomcat/webapps/sspr/WEB-INF/`
   - **Windows**: `C:\Program Files\NetIQ Self Service Password Reset\apache-tomcat-9\webapps\sspr\WEB-INF`
2. Extract the `wordlist.zip` folder and open the `wordlist.txt` file.
3. Add the words that you do not want to allow as password in the text file. Ensure that one word is specified per line.
4. Save the text file and compress the wordlist folder to the `.zip` format.
5. Continue with Uploading the word list.

Create a word list

1. Create the **wordlist.txt** file.
2. Add the words that you do not want to allow as password in the text file. Ensure that one word is specified per line.
3. Save the text file within the folder wordlist.
4. Compress the word list folder to the `.zip` format.
5. Continue with Uploading the word list.

Uploading the word list

NOTE: It is recommended to save the `wordlist.zip` on an HTTP server, and configure URL of the file location in SSPR. This will restore the word list as per your requirement even after the upgrade.

You can upload the updated or new word list in one of the following ways:

- Using a web server
- Using the user interface

Using a web server

You can save the `wordlist.zip` file in any of the web server and save the file location URL for further reference. Perform the following steps to set the word list file URL in SSPR:

1. Click **Configuration Editor > Settings > Word Lists**.
2. Specify the URL of the text file in **Word List File URL**.
3. Click **Save changes** in the toolbar.

Using the user interface

To upload the `wordlist.zip` file through the user interface, perform the following steps:

1. Click **Configuration Manager > Word Lists**.
2. Click **Upload Word List**.
3. Click **Choose File** and select the `wordlist.zip` from your local drive.
4. Click **Upload**.

8 Configuring settings

Self Service Password Reset allows you use settings to customize the users' experience with Self Service Password Reset. You can change the user interface, the policy for passwords, email notification, and many more options.

- "Customizing the theme of Self Service Password Reset" on page 93
- "Customizing user interface features" on page 97
- "Customizing the text of Self Service Password Reset" on page 98
- "Customizing email masking regular expression" on page 98
- "Configuring CAPTCHA" on page 99
- "Configuring email notification settings" on page 99
- "HTTPS server" on page 101
- "Configuring password settings" on page 102
- "Configuring SMS notification settings" on page 102
- "Configuring Self Service Password Reset for Single Sign-On client" on page 106
- "Configuring token settings" on page 110
- "Sending notifications for expiring passwords" on page 112
- "Word lists" on page 114
- "Enabling Self Service Password Reset proxy user for accessing the RESTful web services" on page 116

Customizing the theme of Self Service Password Reset

Self Service Password Reset includes a flexible theme mechanism that allows for maximum customization of the look and feel of Self Service Password Reset for your users. Through customization you can change the look and feel by:

- Use one of the provided themes instead of the default theme
- Embed a cascading style sheet
- Embed a mobile cascading style sheet
- Embed JavaScript
- Upload a custom bundle (include graphics)

To make the customization you must be a web developer and have a good understanding of the following topics:

- **Cascading style sheets:** You must know how to create and use cascading style sheets. For more information, see the *CSS Introduction* section on the *w3schools portal*.
- **JavaScript:** You must understand and know how to write JavaScript. For more information, see the *JavaScript Tutorial* on the *w3schools* website.

NOTE: The Self Service Password Reset JavaScript environment is not documented and might change from version to version. Using this feature should be done only in an environment where development resources are available to maintain the custom JavaScript over time. If you do need help writing JavaScirpt, please contact consulting services. For more information, see NetIQ Consulting.

Use the following information to create and implement a custom theme.

- "Creating the Self Service Password Reset resource bundle" on page 94
- "Implementing the custom resource bundle" on page 94
- "Example of customizing a home page" on page 95
- "Reference for Self Service Password Reset CSS syntax" on page 96

Creating the Self Service Password Reset resource bundle

The custom resource bundle is a ZIP file that contains a specific directory structure, style sheets for desktops and laptops, and any graphics you want to use in the theme. You must create the directory structure with specific folder names for the custom resource bundle to work.

The custom resource bundle must always be `themes.zip`. It must contain one or more subdirectory that is the name of your custom theme. In this example, it is pony. Each theme sub-folder contains a minimum of two files:

- **style.css:** The style sheet that defines the custom theme for desktop and laptop computers.
- **mobileStyle.css:** The style sheet that defines the custom theme for mobile devices.

The custom theme subdirectory might contain additional files if the style sheets require these files. For example, if you want to add a graphic to the theme, you must include that file in the custom theme subdirectory.

For detailed instructions, watch How to Create a Custom Theme in Self Service Password Reset. For an example of the contents of the style sheet, see "Reference for Self Service Password Reset CSS syntax" on page 96.

After you have created the custom theme subdirectory and all supporting files, you must zip up the themes directory so you can import the custom themes in the Configuration Editor.

Implementing the custom resource bundle

After you have created the custom resource bundle and have the `themes.zip` file created, you must upload the file in the Configuration Editor and set a value for the custom theme to become global.

To implement the custom resource bundle:

1. Log in to Self Service Password Reset at `https://dns-name/sspr` as an administrator.
2. In the toolbar, click your name.
3. Click **Configuration Editor**.
4. Click **Settings** > **User Interface** > **Look & Feel**.
5. Under **Custom Resource Bundle**, click **Upload File**.

6 Under **Interface Theme**, click **Set Value**.

7 Specify the name of the custom theme subdirectory.

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

Self Service Password Reset takes you to the applications page and you can see the new custom theme.

If you have more than one custom theme, you can specify the URL parameter theme. For example, `https://www.example.com:@PwmContextPath@?theme=pony`

You can also embed style sheets or a JavaScript to customize the theme. Follow the help for details on how to customize those options.

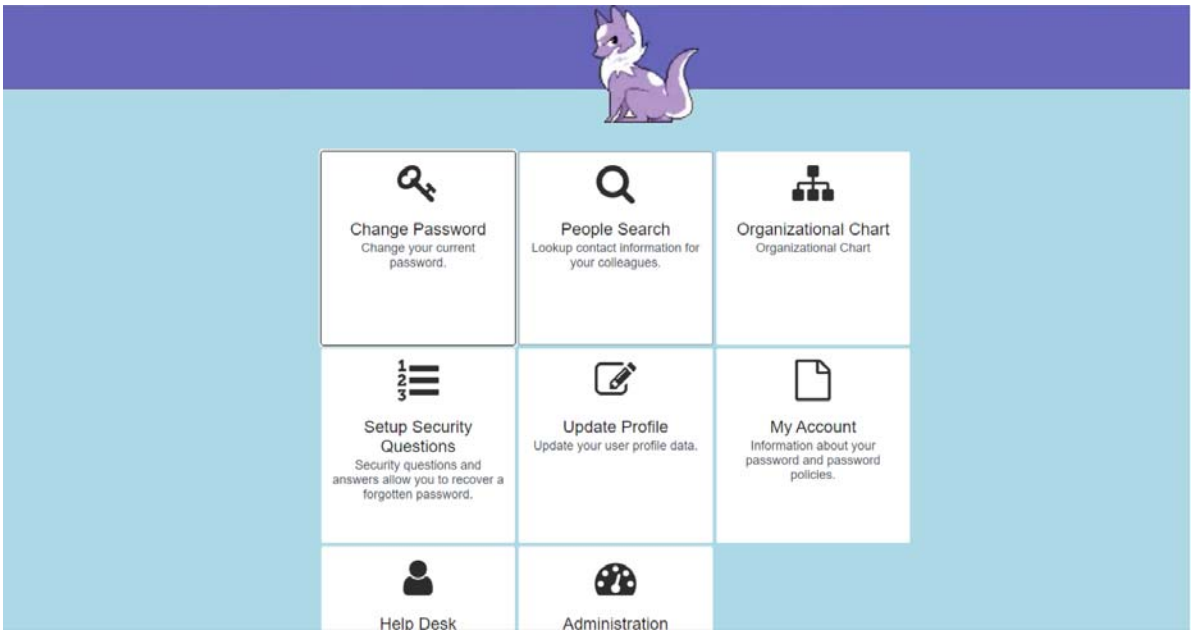
Example of customizing a home page

In this example, the ANME Group company wants to customize the home page for the banner background color, position of tiles, and company logo.

To achieve the customized login page in the Figure 8-1 for Anme Group of company, you can perform the following:

- "Create a custom SSPR resource bundle" on page 96
- "Customize the background color and tile position" on page 96
- "Customize the company logo and banner background color" on page 96

Figure 8-1



Create a custom SSPR resource bundle

The resource bundle contains the custom logo and custom style.css file that will override the default SSPR files.

To create a resource bundle, perform the following steps:

1. Create a folder for a directory named `themes`.
2. Create another folder for a subdirectory named pony. The custom theme subdirectory folder might contain additional files if the style sheets require these files.

   NOTE: You can create multiple subdirectories for each custom theme you create.

3. Create a custom `style.css` file and add the required graphics in the folder pony.
4. Zip up the themes directory to these.zip so you can import the custom themes in the **Configuration Editor**.

Customize the background color and tile position

You can change the background color of the complete login page and add a background image. Also, you can change the tile position and style the heading of the tiles.

In this example, to change the background color to blue and move the tiles to the center, add the following parameter:

```
body {background-color: lightblue;} h1 {color:white; text-align: center;}
```

Customize the company logo and banner background color

You can edit the logo displayed on the login page. In this example, to edit the logo of the login page and banner background color, add the below parameter in the style.css file:

```
#header {background: #6666BB; /*Light purple header. */
}
#header-company-logo {
Background: url ("pony.png") no-repeat scroll 0 0 rgba (0, 0, 0, 0);
position: center center;
width: 100px;
height: 100px;
margin: 0 auto;
}
```

Reference for Self Service Password Reset CSS syntax

The following is an example of the default `style.css` file. We provide this for reference so you can understand the `style.css` file.

```
#header-company-logo {
background: url("banner-220x60.jpg") no-repeat scroll 0 0 rgba(0, 0, 0, 0);
background-position: center center;
width: 220x;
height: 60px;
margin: 0 auto;
}
```

Here is the explanation for the different ID selectors for the CSS file.

```
#header
Common Style Attributes:
   background
Example:
   #header  {
        background: #6666BB;       /* Light purple header. */
}
#header-company-logo
Common Style Attributes:
   background
       Example: background: url("picture.ipg") no-repeat scroll 0 0
rgba(0,0,0,0):
   background-position
       Example: background-position: center center;
   width
       Example: width 220px;
   height
       Example: height: 60px;
   margin
       Example margin:0 auto;
```

Customizing user interface features

Self Service Password Reset allows you to customize the user interface features on the users' pages. This allows you to change Self Service Password Reset to behave as you want. For example, you can decide to mask password fields or not, you can show cancel buttons or not, or you can show logout buttons or not.

Self Service Password Reset allows you to change the user experience to what you need. The Configuration Editor allows you to change these UI features for the users.

To customize the UI features for the user pages:

1. Log in to Self Service Password Reset at `https://dns-name/sspr` as an administrator.
2. In the toolbar, click your name.
3. Click **Configuration Editor**.
4. Click **User Interface > UI Features**.
5. Change the appropriate options for your environment. By default, Self Service Password Reset enables all of the options.
6. In the toolbar, click **Save changes**.

Customizing the text of Self Service Password Reset

Self Service Password Reset allows you to customize the text of fields, buttons, and information the users see when they interact with Self Service Password Reset. For example, if you want to customize the name of the verification methods displayed to the users when they are logging in to Self Service Password Reset, you can do that.

It also allows you to customize the messages users see, whether they are error messages or success messages.

To customize the text of Self Service Password Reset:

1. Log in to Self Service Password Reset at `https://dns-name/sspr` as an administrator.
2. In the toolbar, click your name.
3. Click **Configuration Editor**.
4. Click **Display Text**, then click **Display**, **Error**, or **Message** depending on what you want to change.
5. Search for the item you want to change, then click on it to change the text.
6. (Conditional) You can also configure the customized text in other languages for some options. Click **Add Locale**, then select the required language from the list.
7. In the toolbar, click **Save changes**.

Customizing email masking regular expression

Self-Service Password Reset masks the email characters while sending an email token to the user for updating their profile, activating their account, or resetting a forgotten password to secure user data.

Masking an email address character helps to ensure the privacy and security of the user's information and protects against potential security threats such as email harvesting or phishing attacks. Additionally, masking the email address also helps to prevent the accidental disclosure of sensitive information.

By default, the SSPR masks the email address in the below format:

s**********@m*********.com

Self-Service Password Reset allows you to mask the required characters of an email address by customizing the regular expression in the configuration settings.

To customize email masking regular expression:

1. Log in to Self Service Password Reset at `https://dns-name/sspr` as an administrator.
2. In the toolbar, click your name.
3. Click **Configuration Editor**.
4. Click **Settings > Application > Application > App Property Overrides**.
5. Click **Add Value**.
6. Specify the new value to override the default value of email masking in the below format:

   ```
   token.mask.email.regex=<regular expression as preferred>
   ```

The default value is

```
token.mask.email.regex=(?<=.).(?=[^@]*?@)|(?:(?<=@.)|(?!^)\G(?=[^@]*$)
).(?=.*\.)
```

7 Click **OK** to add the value.

8 Click **Save changes**.

Configuring CAPTCHA

Self Service Password Reset supports reCAPTCHA version 2 and invisible reCAPTCHA. This provides advanced security protection for the Self Service Password Reset websites. CAPTCHA prevents an automated attack and ensures that humans are logging in to applications, not computers. For more information, see the *Googlr reCAPTCHA Documentation*.

Self Service Password Reset uses the online reCAPTCHA service for CAPTCHA generation and validation. You must configure a reCAPTCHA account to use this service. Registration at the reCAPTCHA site provides a public and private key that you must use to configure Self Service Password Reset for the reCAPTCHA support.

NOTE: By default, reCAPTCHA is disabled. Before enabling this feature, verify your privacy statement. Some regions may consider it a privacy issue.

To configure the CAPTCHA settings:

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

2 In the toolbar, click your name.

3 Click **Configuration Editor**.

4 Click **Settings > Captcha**.

5 Use the help to configure CAPTCHA for your deployment of Self Service Password Reset.

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

Configuring email notification settings

Self Service Password Reset lets you specify the email server and customize the templates for email notifications. You can configure Self Service Password Reset to send an automated email to users when required.

Self Service Password Reset supports both plain text and HTML formats. For each configured setting and locale, you should configure both plain text and HTML email bodies. Self Service Password Reset sends email in both formats and the email client can choose the display format.

When you configure the email body in HTML, ensure that you use the proper HTML tags and supported characters.

You can configure macros for the body (plain text or HTML), subject, and from values of email. Email templates offer language support. For more information about macros, see "Configuring macros for messages and actions" on page 22.

- "Configuring email settings" on page 100
- "Configuring email templates" on page 100

Configuring email settings

You must have an SMTP server installed and configured for the email notifications in Self Service Password Reset to work. It is best to use a local SMTP server to your Self Service Password Reset system. The email settings allow you to configure Self Service Password Reset to communicate with your SMTP server.

If your environment requires it, Self Service Password Reset supports configuring multiple SMTP servers to send emails.

To configure the email settings:

1. Log in to Self Service Password Reset at `https://dns-name/sspr` as an administrator.
2. In the toolbar, click your name.
3. Click **Configuration Editor**.
4. Click **Settings > Email > Email Settings**.
5. Use the help to configure the SMTP server to communicate and work with Self Service Password Reset.
6. (Optional) To configure SSL support:
   - **6a** Click **SMTP Email Advanced Settings > Add Value**.
   - **6b** In the field, specify `mail.smtp.ssl.enable=true`, then click **OK**.
7. In the toolbar, click **Save changes**.

Configuring email templates

Self Service Password Reset contains many different email templates for you to configure. You must decide which templates you want to configure to have the emails automatically sent to your users. If email is not required, you must delete or blank the email templates.

For example, when the system creates new users, you can configure Self Service Password Reset to automatically send them emails with their login credentials by configuring the **New User Email** template.

To configure the email templates:

1. Log in to Self Service Password Reset at `https://dns-name/sspr` as an administrator.
2. In the toolbar, click your name.
3. Click **Configuration Editor**.
4. Click **Settings > Email > Email Templates**.
5. Configure the appropriate templates to automatically send emails to users by using the help.

NOTE: You can also configure all of the email template settings in a different language. Click **Add Locale**, then select the required language from the list.

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

HTTPS server

In HTTPS Server, you can Import the private key and certificate used by the SSPR HTTPS web server, select the HTTPS TLS protocols supported by the SSPR HTTPS web serve, and specify the HTTPS TLS ciphers accepted by the SSPR HTTPS web server.

NOTE: Any changes to HTTPS Server setting require a server restart.

Perform the following steps to configure HHPS Server:

1. Log in to Self Service Password Reset as an administrator.
2. In the top-right corner of the Dashboard screen, click the user name.
3. Click **Configuration Editor**.
4. Navigate to **Settings > HTTP Server**.
5. Configure the following settings:

HTTPS Private Key & Certificate

Import the private key and certificate used by the SSPR HTTPS web server.

If this setting does not have a value, the SSPR HTTPS web server uses an auto-generated value based on **Settings > Application > Application > Site URL** and other current configuration data. Changes to this setting require a server restart.

Perform the following steps to upload Private key or Certificate:

1. Click **Import Private Key & Certificate**.
2. Select the file format.
3. Specify the password of the file if any.
4. Specify the name of the file in **Alias**.
5. Click **Choose file** and select the certificate from the local drive.
6. Click **Upload**.
7. Restart the server.

TLS Protocols

Select the HTTPS TLS protocols supported by the SSPR HTTPS web server. Changes to this setting require a server restart.

TLS Ciphers

Specify the HTTPS TLS ciphers accepted by the SSPR HTTPS web server. The value for this setting is an ordered, comma separated list of Java SSE provided cipher names. Changes to this setting require a server restart.

6 Click **Save**.

Configuring password settings

After you create the password profile you must configure the settings for the password policy. The password policy settings allow you to define the source of the password policy if you want to share the password history among all users to discourage similar passwords, or control if the passwords are case sensitive.

To configure a password policy:

1 Log in to Self Service Password Reset at `https://dns-name/sspr` as an administrator.
2 In the toolbar, click your name.
3 Click **Configuration Editor**.
4 Click **Settings > Password Settings**.
5 Configure the password policy settings using the help.
6 In the toolbar, click **Save changes**.

Configuring SMS notification settings

Self Service Password Reset sends SMS notifications many different user actions. For example, Self Service Password Reset sends SMS messages for password recovery and new user account verification.

You must have an SMS gateway to send SMS messages to the users and you must configure Self Service Password Reset to communicate to the SMS gateway service for SMS messages to be sent to the users. By default, Self Service Password Reset does not contain any configured SMS messages. You must configure the SMS messages to have the messages automatically sent to the users. If you do not configure both items, the system cannot send SMS messages.

- "Configuring the SMS gateway" on page 102
- "Configuring the SMS messages" on page 105

Configuring the SMS gateway

For Self Service Password Reset to send SMS notifications, you must have access to an HTTP or HTTPS based SMS gateway service. You must configure Self Service Password Reset to communicate to the SMS gateway service before you can send SMS messages.

Self Service Password Reset allows you to configure multiple SMS gateway services. You would do this if the first service is not available for any reason.

For security reasons, we recommend that you always use an HTTPS bases SMS gateway. Self Service Password Reset imports the trusted certificate for the SMS gateway for you through the **SMS Gateway Certificates** setting in the Configuration Editor.

To configure the SMS gateway:

1. Log in to Self Service Password Reset at `https://dns-name/sspr` as an administrator.
2. In the toolbar, click your name.
3. Click **Configuration Editor**.
4. Click **Settings > SMS > SMS Gateway**.
5. Specify the following details:

Parameter	Description
SMS Gateway	Specify the SMS gateway URL in the following format: `https://<api-of-sms-provider>/<api-doc-creation-date>/Accounts/<account-SID>/Messages.xml` For example: `https://api.twilio.com/2019-07-01/Accounts/AMwqeiu0283749cabgg81283/Messages.xml`
SMS Gateway Certificates	After providing the valid URL in **SMS Gateway**, click **Import From Server** to automatically fetch the certificate's details.
SMS Gateway User	Specify the account SID of your account from the SMS provider.
SMS Gateway Password	Click **Store Value** and specify the auth token of your account and confirm it.
HTTP(S) Method	By default, **POST** is set for secured connection.
SMS Gateway Authentication Method	By default, **HTTP - Use HTTP basic connection** is set as the authentication method.

SMS Request Data	Specify the following details in SMS Request Data using the following parameters:
	`To=%user's mobile number%&`
	`From=%sender id or mobile number%&`
	`Body=%Message body that you want to deliver%&`
	`USER=%authentication user name(account id)%&`
	`PASS=%authentication password%`
	NOTE: The ampersand symbol (&) is used as the separator between parameters.
	For example:
	`To=%+911234567890%&From=%+19876543210%&Body=%Hi {user}, This is to notify that your corporate password expires in 7 days.%&USER=%AMwqeiu0283749cabgg81283%&PASS=%aj437987349857jlkfj%`

SMS Data Content Type	By default, the value `application/x-www-form-urlencoded` is set as the Data Content Type. You can retain the same value.
SMS Data Content Encoding	Select the encoding format to transmit the SMS content. By default, **URL - recommended for GET requests and POST with form data** is set as the encoding format.
SMS Gateway HTTP Request Headers	Specify the SSPR host address in the format - https://*dns-name*/sspr

Parameter	Description
Maximum SMS Text Length	Specify the number of characters in the SMS. By default, 140 is set as the maximum text length
SMS Sender ID	Specify the sender ID that is displayed as from address in SMS. Include the country code if required.
SMS Phone Number Format	Select the phone number format for both sending and receiving the SMS. **Zeros - Same as plain, but prefixed with double zero: 00112312345** is set as the default format.
Default SMS Country Code	Specify the default country code of the receiver's phone number. Set to 0 if you want to disable the country code.
Request ID Characters	Specify the request ID characters required for SMS transmission.
Request ID Length	Specify the length of the request ID.
Response Regular Expression	Specify the regular expression to determine whether SSPR sent the SMS successfully to the gateway. If the response matches any of the expressions, SSPR considers the transmission successful. If you do not specify any expressions, SSPR assumes that all transmissions are successful.
Successful HTTP Result Codes	HTTP result status codes indicate whether a specific HTTP request has been successfully completed. You can define the following result codes: ◆ 201: Represents that the request has succeeded and SMS is delivered successfully. This is typically the response sent after POST requests, or some PUT requests. ◆ 400: Represents that the SMS transmission is not successful due to invalid configuration. ◆ 404: Represents that the SMS is not delivered due to the invalid number of the recipient.
Maximum SMS Queue Age	Specify the maximum age (in seconds) an SMS can wait in the queue. If an SMS is in the send queue longer than the specified time, the system discards it.

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

Configuring the SMS messages

After you have configured the SMS gateway service to communicate with Self Service Password Reset, you must configure the SMS messages to be sent to the users. You must configure the SMS text for each setting and locale you want to use.

For example, you can configure Self Service Password Reset to automatically send SMS when a user changes the password by configuring the **Change Password SMS text** template.

Before configuring the SMS messages, ensure to add your SSPR setup meets the following prerequisites:

- Configure SMS gateway details to deliver SMS.
- Set **SMS Destination Address LDAP Attribute** to **telephoneNumber** in **Configuration Editor > LDAP > LDAP Directories > default > User Attributes**.

To configure the SMS messages:

1. Log in to Self Service Password Reset at `https://dns-name/sspr` as an administrator.
2. In the toolbar, click your name.
3. Click **Configuration Editor**.
4. Click **Settings > SMS > SMS Messages**.

   NOTE: You can also configure all of the SMS message settings in a different language. Click **Add Locale**, then select the required language from the list.

5. Use the help to configure the SMS messages to send to your users.
   - **Change Password SMS Text**: Displays the default SMS text sent to users on changing their password. Click the Edit icon to customize the SMS text as per your requirement.
   - **Update Profile SMS Text**: Displays the default SMS text sent to users on updating their profile. Click the Edit icon to customize the SMS text as per your requirement.
6. In the toolbar, click **Save changes**.

Configuring Self Service Password Reset for Single Sign-On client

Self Service Password Reset can integrate with different systems to provide a single sign-on (SSO) experience for your users. Self Service Password Reset supports basic authentication (basic auth), HTTP SSO, and OAuth.

- "Configuring basic authentication for Single Sign-On" on page 106
- "Configure HTTP for Single Sign-On" on page 107
- "Configuring OAuth Single Sign-On" on page 107

Configuring basic authentication for Single Sign-On

Self Service Password Reset allows you to use HTTP basic authentication for a single sign-on experience for your users. By default, Self Service Password Reset uses basic authentication.

To configure basic authentication:

1. Log in to Self Service Password Reset at `https://dns-name/sspr` as an administrator.
2. In the toolbar, click your name.
3. Click **Configuration Editor**.
4. Click **Settings > Single Sign On (SSO) Client > Basic Authentication**.
5. Configure the following Application Security settings:

Field	Description
Enable Basic Authentication	Check **Enabled** to enable basic authentication.
Force Basic Authentication	Check **Enabled** to force basic authentication. If it is disabled, then the system presents the form page for unauthenticated users. However, if a basic authentication header is present, the system always uses it.

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

Configure HTTP for Single Sign-On

Self Service Password Reset allows you to create a single sign-on experience using an HTTP header. Self Service Password Reset uses the HTTP header to log users into an application with a user name automatically.

To configure the HTTP header for single sign-on:

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

2 In the toolbar, click your name.

3 Click **Configuration Editor**.

4 Click **Settings > Single Sign On (SSO) Client > HTTP SSO**.

5 Configure the following Application Security settings:

Field	Description
SSO Authentication Header Name	Specify the name of the HTTP header that configures SSPR to use an upstream server to allow automatic logins with only a user name, and a password is not required. This setting controls the name of the HTTP header. When used, SSPR prompts users for their passwords to access certain functionality.

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

Configuring OAuth Single Sign-On

Self Service Password Reset allows you to create a single sign-on experience for your users using OAuth. You must have a basic understanding of OAuth to complete the configuration because you must obtain OAuth-specific information from the application to complete the configuration. For more information, see the *OAuth 2.0 documentation*.

You must gather the following information from the OAuth Identity Server of your application before you can complete the configuration:

❒ URL for the OAuth login

- ❒ OAuth code resolve service URL
- ❒ OAuth profile service URL
- ❒ OAuth web server certificate
- ❒ OAuth client ID
- ❒ OAuth shared secret
- ❒ Attribute you want the OAuth server to use to identify the user names

Use the information you gathered to create an OAuth single sign-on experience for your users:

To configure OAuth SSO:

1. Log in to Self Service Password Reset at `https://dns-name/sspr` as an administrator.
2. In the toolbar, click your name.
3. Click **Configuration Editor**.
4. Click **Settings > Single Sign On (SSO) Client > OAuth**.
5. Configure the following Application Security settings:

Field	Description
OAuth Login URL	Specify the OAuth server login URL. This is the URL to redirect the user for authentication. For example, `https://oauthserver.example.com/osp/a/idm/auth/oauth2/grant`
OAuth Scope	Specify the optional OAuth scope. The OAuth identity service provider (IdP) provides this value. The content provided, if any, must contain the user attribute to be read for authentication. For example, `email`
OAuth Token / Code Resolve Service URL	Specify the OAuth Code Resolve Service URL. The system uses this web service URL to resolve the artifact returned by the OAuth identity server. For example, `https://oauthserver.example.com/osp/a/idm/auth/oauth2/authcoderesolve`
Skip Authorization header in Oauth Code Resolve request.	Check **Enabled** to skip the authorization header in the OAuth Code Resolve request.
OAuth Profile/UserInfo Service URL	Specify the URL of the web service provided by the identity server to return attribute data about the user. For example, `https://oauthserver.example.com/osp/a/idm/auth/oauth2/getattributes`
OAuth Server Certificate	Import the certificate for the OAuth web service server.
OAuth Client ID	Specify the OAuth client ID. The OAuth identity service provider (IdP) provides this value.

OAuth Shared Secret	Specify the OAuth shared secret. The OAuth identity service provider (IdP) provides this value.
	
	1. Click **Store Value**.
	2. In **Store Password - OAuth Shared Secret**, specify the following details:
	  ◆ New Password
	  ◆ Confirm Password
	3. Click **Store Password**

OAuth User Name/DN Login Attribute	Specify the attribute to request from the OAuth server SSPR uses as the user name for local authentication. The SSPR resolves this value the same as if the user had typed the password at the local authentication page.

Field	Description
Add login hint optional parameter to oauth authorization request	Specify the username as a macro to add the login hint optional parameter to an OAuth authorization request, you can follow the OAuth specification for including optional parameters in the request. When the user is redirected to the Authorization Server for authentication, the Login Hint parameter provides a hint about the user's identity or account, which makes the login process smoother and pre-fills the username field on the login page.
OAuth Profile / UserInfo Service Method Type	Select the HTTP method to invoke the Identity Server’s OAuth Profile/UserInfo Service URL. The HTTP method returns the user-related attribute data for Single Sign-on and Forgotten Password modules. By default, the HTTP method is set to POST. However, the administrator can select GET method for making a request to the Identity server's OAuth Profile/ UserInfo Service. Selecting HTTP method enhances the flexibility and security of SSPR and allows the administrators to customize the application’s interaction with the Identity server's web service in order to retrieve the user attribute information.

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

Configuring token settings

Self Service Password Reset sends tokens through email and SMS for secure user authorization. You can configure the Self Service Password Reset to send a random token during a new user registration, forgotten password recovery, etc. For example, when users try to reset their passwords, Self Service Password Reset prompts them to specify answers to the challenge-responses and sends a token through an email or SMS to the email ID or phone number specified by the user. The user must enter this token into the Password Change form. When the token matches with the token sent by Self Service Password Reset, the system changes the user's password.

Self Service Password Reset also sends tokens for new user registration confirmation.

NOTE: The Self Service Password Reset session is specific to the browser used. If the users copy the email verification link provided in the email manually, it is recommended that the users paste the email verification link into the same browser session in which they initiated the Self Service Password Reset process.

To configure token settings:

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

2 In the toolbar, click your name.

3 Click **Configuration Editor**.

4 Click **Settings > Tokens**.

5 Use the help to configure the settings for tokens.

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

Verifying the email token in a different browser session

This feature enables the users to verify an email token from a different browser session than the one from which they initiated the user activation process. Verifying email tokens across sessions ensures seamless transition from one session to another without losing progress or encountering authentication issues.

NOTE: This feature is only available for the **User Activation** module.

If users starts the user activation process but later switches to a different browser session (e.g., due to a browser crash or intentionally opening a new tab), they should be able to continue where they left off.

Additionally, you can force users to verify that whether they are humans or a robots using the Google reCAPTCHA after user activation email token verification in different browsers.

The following example scenarios describe how this feature works:

Scenario 1: Maria initiates Self Service Password Reset User Activation process in a Chrome browser on the system. However, Maria copies the email verification link provided in the email manually and pastes the email verification link into the Firefox browser session window. If the **Allow Token Verification in a Different Browser Session** feature is enabled, Maria can verify that email token in the Firefox browser.

Scenario 2: Paul starts the Self Service Password Reset User Activation process on his home laptop but realizes he needs to leave. Later, he continues the process on his tablet to verify the email token. If the **Allow Token Verification in a Different Browser Session** feature is enabled, he can verify that email token through his tablet.

By default, Self Service Password Reset does not allow users to verify their email token in a different browser than the one from which they initiated the user activation process. To use a different browser for the user activation email token verification, perform the following steps:

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

2 In the toolbar, click your name.

3 Click **Configuration Editor**.

4 Click **Settings > Tokens**.

5 Enable the **Allow Token Verification outside the Browser Session** option.

6 Enable the **Verify ReCaptcha Post Token Verification** option, if you want to force users to verify that they are humans or robots. If this option is enabled, it stops the bots from completing the user Activation process.

   NOTE: This option is applicable if the **Allow Token Verification in a different Browser Session** option is enabled.

   ---

7 Navigate to **Settings > Captcha**.

8 Select the **User Activation** page in the **CAPTCHA Protected Pages** to protect user activation page using CAPTCHA after token verification in another browser.

NOTE:

- If the **Verify ReCaptcha Post Token Verification** option is not enabled and the **User Activation** page is selected in the **CAPTCHA Protected pages** option, then email token verification in a different browser will be unsuccessful.
- Ensure to configure **reCAPTCHA Site Key** and **reCAPTCHA Secret**.

---

9 Select the required **reCAPTCHA Mode** from the list.

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

Sending notifications for expiring passwords

Self Service Password Reset has the ability to send emails to users warning them their passwords are about to expire. In Self Service Password Reset 4.4 or later, you can use an LDAP director or a remote database to send the password expiration notifications. Prior release of Self Service Password Reset only supported an external database.

To enable these email notifications for your users, you must properly configure Self Service Password Reset to enable and send the password expiration notifications. Use the following information to configure Self Service Password Reset to send the email notifications.

- "Configuring Self Service Password Reset for password expiration notifications" on page 112
- "Enabling the emails for password expiration notifications" on page 114
- "Verifying the password expiration notification configuration" on page 114

Configuring Self Service Password Reset for password expiration notifications

The steps for configuring Self Service Password Reset for password expiration notification are different depending on if you store the users' information on a remote database or an LDAP directory Use the following information to configure password exploration notifications.

- "Configuring Self Service Password Reset for password expiration notifications with a remote database" on page 112
- "Configuring Self Service Password Reset for password expiration notifications with an LDAP directory" on page 113

Configuring Self Service Password Reset for password expiration notifications with a remote database

If you use a remote database to store the users' information for Self Service Password Reset, you must use the following steps to configure password expiration notifications for users.

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

2 In the toolbar, click your name.

3 Click **Configuration Editor**.

4 Click **Settings > Password Expiration Notification > Storage Mode.**

5 Select **Remote Database**.

6 Click **Settings > Application > Session Management > Node Service Enabled**.

7 Select **Enabled (True)**.

8 Click **Settings > Application > Session Management > Node Service Storage Mode**.

9 Select **Remote Database**.

10 Click **Save changes**.

11 Configure the email password notification settings in the Configuration Editor. For more information, see "Enabling the emails for password expiration notifications" on page 114.

Configuring Self Service Password Reset for password expiration notifications with an LDAP directory

If you use an LDAP directory to store the users' information for Self Service Password Reset, you must use the following steps to configure password expiration notifications for users.

1 (Conditional) If you have upgraded to Self Service Password Reset 4.4, ensure that you extend the schema. For more information, see "Configuring the LDAP directories" in the *Self Service Password Reset 4.8 Installation Guide*.

2 Ensure that you have a functional LDAP test user configured. For more information, see "Configuring LDAP directory profile" on page 39.

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

4 In the toolbar, click your name.

5 Click **Configuration Editor**.

6 Click **Settings > Password Expiration Notification > Storage Mode.**

7 Select **LDAP Directory**,

8 Click **Settings > Application > Session Management > Node Service Enabled**.

9 Select **Enabled (True)**.

10 Click **Settings > Application > Session Management > Node Service Storage Mode**.

11 Select **LDAP Directory**.

12 Click **Save changes**.

13 (Conditional) If you do not want to use the default attribute of `pwdData` to store the user data, you can use on the of the other attributes in your LDAP directory. To change the default attribute:

   13a In the toolbar, click your name.

   13b Click **Configuration Editor**.

   13c Click **LDAP > LDAP Directories > *default* > User Attributes > Application Data Attribute**.

   13d Click **Add Value**.

13e Specify the appropriate attribute, then click **OK**.

13f Click **Save changes**.

14 Configure the email password notification settings in the Configuration Editor. For more information, see "Enabling the emails for password expiration notifications" on page 114.

Enabling the emails for password expiration notifications

After you have configured Self Service Password Reset to use a remote database or an LDAP directory for password expiration notification, you must configure the setting to send the emails to the users. Use the following steps to send password expiration notifications to your users.

1 Ensure that you have enabled email notifications in the Configuration Editor. For more information, see "Configuring email notification settings" on page 99.

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 **Settings > Password Expiration Notification**.

6 Enable this option, define one or more filters to find the users that will receive the notification emails, and then define when to send the email.

7 Click **Settings > Email > Email Templates > Password Expiration Notification Email**.

8 Define the content of the email template that your users receive when their passwords are about to expire.

9 In the toolbar, click **Save changes**, then close the Configuration Editor.

Verifying the password expiration notification configuration

After you have configured Self Service Password Reset for password expiration notifications, you can verify that the configuration is working. You can view the job that runs that sends the emails to your users.

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

2 In the toolbar, click the **Home**.

3 On the Home page, click **Administration**.

4 Click **Data Analysis > Directory Reporting > Report Engine Status**.

5 Click **Start** to view the report.

6 Click **Summary** to view the information about the job that ran to send the emails to the users.

7 (Conditional) If you are using a remote database and you have clustered Self Service Password Reset, ensure the password notification service runs on the master node of the cluster.

Word lists

To strengthen the security of the passwords you must define a word list. A word list is a prepared password dictionary that Self Service Password Reset checks against the text that users set as their passwords. Self Service Password Reset does not allow a password if that text is available in the word

list. The word list is a ZIP file containing one or more plain text files with one word per line. The Word List setting enables you to add the details of Word List files, identify whether to use case sensitivity in Word List, minimum number of character match, etc.

For more details to upload Word List, see Configuring the word list settings.

For more information about enabling Word List, see Configuring password policies

1. Log in to Self Service Password Reset at `https://dns-name/sspr` as an administrator.
2. In the toolbar, click your name.
3. Click **Configuration Editor**.
4. Click **Settings > Word List**.
5. Configure the following settings:

Word List File URL

Specify the URL of a file containing a word list for dictionary checking to prevent users from using common words as passwords.

The first time a startup happens with a new word list configuration, the word list must be compiled into a database. For progress details, consult the status screen and logs. The word list file format consists of one or more text files with a single word per line, enclosed in a ZIP file. The Tether! #comment: at the start of a line indicates a comment.

The value must be a valid URL, using the protocol "file" (local file system), "http", or "https".

1. Click **Add Value**.
2. Specify the valid URL in **Edit Value - Word List File URL**.

Word List Case Sensitivity

Enable this option to make all matches using the word list case-sensitive. Changing this value recompiles the word list in SSPR.

Word List Word Size Check

Specify the minimum number of characters required for SSPR to compare a password to the Word List dictionary. If this value is set to zero or the password to be checked is less than the value indicated here, the system verifies the complete password against the Word List, but not smaller portions of it.

For instance, if the system-checked password is **wordlist** and this parameter is set to 6, the combinations of following words are all verified against the configured dictionary. If any of these values correspond to a term in the Word List dictionary, the system rejects the password as a match to the Word List.

- wordli
- wordlis
- wordlist
- ordlis
- rdlist

Seed List File URL

Provide a valid URL containing the location of the seed list. When SSPR creates random passwords, it can provide users with friendly password suggestions. It accomplishes this by taking a seed word or words and then randomly changing that term until it is sufficiently complicated and fits the user's configured rules.

The value must be a valid URL, using the protocol "file" (local file system), "http", or "https".

1. Click **Add Value**.
2. Specify the valid URL in **Edit Value - Seed List File URL**.

Enabling Self Service Password Reset proxy user for accessing the RESTful web services

A proxy user is a trusted individual with permissions to perform tasks on behalf of other users without revealing their identity, enhancing security and access control.

Self-Service Password Reset integrates with any REST-supporting product, allowing for external web authentications through REST.

Administrators can configure proxy user settings in the Self Service Password Reset application and grant LDAP permissions to the proxy user based on roles for accessing RESTful Web Services using REST APIs. This setup restricts direct access to user information and password management functions from anonymous users or external systems, adding an extra layer of security against unauthorized access.

When the administrator configures the LDAP proxy user with the required permissions, the proxy user can invoke the below Self Service Password Reset REST APIs to access the RESTful Web Services:

NOTE: When invoking the SSPR REST APIs on behalf of another user, you must provide the `username` parameter in the API call. This ensures that the API functions in the context of a specified user instead of a proxy user.

If you do not provide a `username` parameter, then the API will execute the operation for the proxy user.

- Challenges
- Check Password
- Health
- Profile
- Password Policy
- Random Password
- Set Password

  NOTE: To execute this API, make sure the LDAP proxy user has permission to set the user password.

- Signing Form
- Statistics
- Status
- Verify One-Time-Password
- Verify Responses

For more information about REST API, see SSPR REST API (https://www.netiq.com/documentation/self-service-password-reset-46/references/SSPR/).

To enable the LDAP proxy user to access the RESTful Web Services, perform the below steps:

IMPORTANT: Create a user in your LDAP directory that Self Service Password Reset uses to access the LDAP directory. The user must have the following rights:

- Browse users and manage password attributes of the user object
- Create object rights in the new user container (if enabled)

For more information about how to assign the user rights, see Proxy user rights.

1. Log in to Self Service Password Reset at `https://dns-name/sspr` as an administrator.
2. In the toolbar, click your name.
3. Click **Configuration Editor**.
4. Navigate to **LDAP > LDAP Directories > default > Connection > LDAP Proxy User**.
5. Click **Add Value** to add the LDAP proxy user that SSPR uses to access the LDAP directory.
6. Click **Store Value** in **LDAP Proxy Password**.
7. Specify the LDAP proxy user password and click the **Store Password** button.
8. Navigate to **Settings > Web Services > REST Services > Use LDAP Proxy User for Accessing RESTful Web Services**.

9 Check the **Enabled (True)** check-box.

10 Click **Save changes**.

II Configuring integrations

9 Integrating Self Service Password Reset with NetIQ access manager

Access Manager is a comprehensive access management solution that provides secure access to web and enterprise applications. Access Manager also provides seamless single sign-on across technical and organizational boundaries.

Integration of Self Service Password Reset with Access Manager provides a comprehensive and secure access management solution. For this integration, you must configure settings in Access Manager and Self Service Password Reset.

- "Configuring access manager to integrate with Self Service Password Reset" on page 121
- "Configuring Self Service Password Reset to integrate with access manager" on page 127
- "Additional integration options with access manager" on page 132

Configuring access manager to integrate with Self Service Password Reset

Integrating Self Service Password Reset with Access Manager provides single sign-on to your users.For the integration to work, ensure that you are running Access Manager 4.4. SP4 or later.

This integrations allows you to:

- Create a proxy service for Self Service Password Reset.
- Create Self Service Password Reset as a protected resource in Access Manager.
- Provide single sign-on access to the users and administrations.
- Provider single sign-on access with OAuth2 tokens.

Use the following information to properly configure Access Manager and Self Service Password Reset to work together.

- "Configuring proxy service for Self Service Password Reset" on page 122
- "Configuring protected resources for Self Service Password Reset" on page 122
- "Configuring Single Sign-On to Self Service Password Reset" on page 123
- "Configuring Single Sign-On to Self Service Password Reset when password is not available" on page 124
- "Configuring single sign-on with OAuth2 tokens" on page 125

Configuring proxy service for Self Service Password Reset

You can configure Self Service Password Reset as path-based multi-homing or domain based multi-homing proxy service on Access Manager. For more information about these proxy services, see "Using Multi-Homing to Access Multiple Resources" in the *NetIQ Access Manager Administration Guide*.

The following is a list of the values for a sample configuration for path-based multi-homing in Access Manager:

Proxy service type

Self Service Password Reset uses path based multi-home. For example: `Published DNS Name = intranet.company.com`

Ports

Specify the port of the web server.

- **Appliance:** 443
- **Linux:** 8443 (Default)
- **Windows:** 8443 (Default)

Configured multi-homing path

Specify `/Self Service Password Reset`

Remove path on fill

Disable this option.

Host header

Specify the Self Service Password Reset web server hostname.

Rewriter configuration

Use the default setting for this option.

Configuring protected resources for Self Service Password Reset

Some modules of Self Service Password Reset, such as Forgotten Password and New User Registration must be publicly accessible. To support this, configure URLs as public or restricted by using your proxy or Access Gateway configuration.

For example, assume that Self Service Password Reset is set up so that the user enters the following URL to access:

`http://password.example.com/sspr`

You can configure the URL to be public or restricted as follows:

URL	Mode
password.example.com/*	Public
password.example.com/sspr/private/*	Restricted
password.example.com/sspr/private/admin/*	Restricted
password.example.com/sspr/private/config/*	Restricted

In the table, you can create a protected resource for the `password.example.com/sspr/private/*` URL. The `/private/*` URL includes both the `/admin/*` and `/config/*` URLs so you do not have to create three separate protected resources. If you want to restrict access to the `/admin/*` and `/config/*` URLs separately, you must create separate protected resources for these URLs and not the `/private/*` URL.

Though Self Service Password Reset has built-in protection for configuration and administrative pages, configure authorization policy in Access Manager to protect `/config` and `/admin` paths to allow only administrators to access these parts of the Self Service Password Reset application.

Configuring Single Sign-On to Self Service Password Reset

Self Service Password Reset, by default, performs an HTML form-based authentication when an unauthenticated user tries to access restricted web pages. However, it always uses the basic authorization header if available in the HTTP request. You can configure an Identity Injection policy in Access Manager to perform single sign-on (SSO) to Self Service Password Reset for the authenticated user in the Access Manager Identity Server.

Configure the Identity Injection policy you must enable this policy for restricted URL paths. For more information, see "Configuring protected resources for Self Service Password Reset" on page 122.

Configuration	Value
Action for Identity Injection	Inject into Authentication Header
Auth Header – User Name	Credential Profile (LDAP Credentials: LDAP User DN)
Auth Header – Password	Credential Profile (LDAP Credentials: LDAP Password)
DN Format	LDAP format (default)

For more information about Identity Injection policies, see "Identity Injection Policies" in the *NetIQ Access Manager Administration Guide*.

Configuring Single Sign-On to Self Service Password Reset when password is not available

When Access Manager uses a non-password authentication mechanism such as Kerberos or x509 certificates, the user password is not available to use for single sign-on (SSO).

You can configure Self Service Password Reset to accept only the user name during SSO. In this partially authenticated state, users can perform some functions without providing their passwords. For example, the `CommandServlet` actions can be invoked without any user interaction.However, if users must interact with Self Service Password Reset, such as to change a password or to configure responses, they must provide their passwords before proceeding.

To configure SSO for Self Service Password Reset using access manager:

1. Log in to Self Service Password Reset at `https://dns-name/sspr` as an administrator.
2. In the toolbar, click your name.
3. Click **Configuration Editor**.
4. Click **Settings > Single Sign On (SSO) Client > HTTP SSO**.
5. In **SSO Authentication Header Name**, set the value to `ssoAuthUsername`.
6. In the toolbar, click **Save changes**.
7. In Access Manager, create the following identity injection policy for the Self Service Password Reset protected resources:
   - **Action for identity injection:** Select the option **Injection into Custom Header**.
   - **Custom header name:** Specify `ssoAuthUsername`.
   - **Value:** Select **Credential Profile (LDAP Credentials: LDAP User DN)**.

     NOTE: If Self Service Password Reset is using the LDAP directory and **Read User Password** is enabled (**Settings > LDAP > LDAP Settings > NetIQ eDirectory > eDirectory Settings > Read User Passwords**), and the LDAP Proxy user has permission to read the user passwords, then the user is not prompted for their passwords when authenticated to Self Service Password Reset by using this method.

   - **DN format:** Select **LDAP format (default)**.

Configuring single sign-on with OAuth2 tokens

You can provide single sign-on access to Self Service Password Reset with OAuth2 tokens generated in Access Manager. To provide single sign-on access requires configuring components in Access Manager and in Self Service Password Reset. You must understand OAuth2 and Access Manager to complete the integration. For more information, see "Implementing OAuth in Access Manager" in the *NetIQ Access Manager 4.4 Administration Guide*.

Use the following information to perform the steps in Access Manager. For the Self Service Password Reset steps, see "Configuring Self Service Password Reset to access the OAuth2 application" on page 130.

You must enable OAuth2 and create an OAuth2 application in Access Manager that Self Service Password Reset uses to obtain the OAuth2 tokens for the users authentications. If you have multiple Identity Provider clusters that you want Self Service Password Reset to reference, you must perform the following steps for each Access Manager Identity Provider cluster

Use the following information to enable OAuth2, create an OAuth2 application, and assign the proper rights in Access Manager.

1. Choose an attribute to use for Self Service Password Reset to identify the user. The attribute must have a value that uniquely identifies the user when authenticating. Self Service Password Reset reads this attribute value from the user and use it to identify the user in the LDAP directory user store for Self Service Password Reset.
2. Ensure that you enable OAuth2 in Access Manager.
   - **2a** Log in to the Access Manager Administration Console.
   - **2b** Click **Devices > Identity Servers > Edit**.
   - **2c** In the **Enabled Protocols** section, select **OAuth & OpenID Connect**.
   - **2d** Click **OK**.
   - **2e** Update the Identity Server.
3. Ensure that you have a resource server created in Access Manager or create a resource server. For more information, see "Adding a Resource Server" in the *NetIQ Access Manager 4.4 Administration Guide*.
4. Use an existing scope or create a new scope for the OAuth application with a claim type of **User Attributes**. This allows Self Service Password Reset to identify the user. The attribute must have a value that uniquely identifies the user when authenticating. Self Service Password Reset reads this attribute value from the user and use it to identify the user in the LDAP directory configured for Self Service Password Reset. For more information, see "Defining Scopes for a Resource Server" in the *NetIQ Access Manager 4.4 Administration Guide*.
5. Select the identification attribute from the LDAP profile or create a new attribute set that contains the identification attribute you determined in Step 1. This lists the user attributes in the attribute set. For more information, see "Configuring Attribute Sets" in the *NetIQ Access Manager 4.4 Administration Guide*.
6. (Conditional) Define the global settings. You might have already configured the global settings for other OAuth2 applications. For more information, see "Defining Global Settings" in the *NetIQ Access Manager 4.4 Administration Guide*.

7 Create an OAuth2 client application.

7a Click **Devices > Identity Servers > Edit > OAuth & OpenID Connect > Client Applications > Register New Client**.

7b Use the following information to create the OAuth2 application.

Name

Specify a name for the application. For example, SSPR.

Client Type

Select **Web Based** as the client type.

Redirect URL

Specify the Self Service Password Reset URL. For example:

`https://sspr.example.com/sspr/public/oauth`

Grants Required

Select all of the options except **SAML 2.0 Assertion**.

Token Types

Select **Always Issue New Token**.

7c Click **Register Client**.

7d Record the **Client ID** and **Secret** of the newly created client application so you can use them later in the Self Service Password Reset configuration.

8 Grant administrative roles to an Access Manager administrator.

8a In the Access Manager Administration Console, click **Policies > Policies**.

8b Locate a role policy to use.

or

Create a new role to use. For more information, see "Creating Roles" in the *NetIQ Access Manager 4.4 Administration Guide*.

8c In the **Actions** section, select **Activate Role**, then add the following two roles:

- `NAM_OAUTH2_DEVELOPER`
- `NAM_OAUTH2_ADMINs`

8d (Conditional) If you created a new policy, click **Edit IDP > Roles > *Select the new policy* > Enable**.

9 Update all Identity Servers with the configuration changes.

9a In the Access Manager Administration Console, click **Identity Servers**.

9b Click **Update All** to reconfigure all of the nodes in the cluster for the Identity Servers.

10 View and record the Endpoint URLs for the OAuth2 applications.

10a Click **Devices > Identity Servers > Edit > OAuth & OpenID Connect > Endpoint Summary**.

10b Record the Endpoint URLs to use in the Self Service Password Reset configuration.

11 Proceed to "Configuring Self Service Password Reset to access the OAuth2 application" on page 130 to configure Self Service Password Reset to accept the OAuth2 tokens from Access Manager.

Configuring Self Service Password Reset to integrate with access manager

Self Service Password Reset provides various options for integration with Access Manager including configurable redirection URLs, servlet command options, and support for HTTP basic authentication. The following are important configurations:

- "Configuring redirection URLs" on page 127
- "Configuring Self Service Password Reset parameters for access manager" on page 127
- "Using request parameters" on page 128
- "Using a command servlet" on page 129
- "Configuring Self Service Password Reset to access the OAuth2 application" on page 130

Configuring redirection URLs

The following are two important redirection URLs:

- **forwardURL:** By default, the user is redirected to the forwardURL site.
- **logoutURL:** If the password has been modified and the **Logout After Password Change** setting is set to **True**, then the user is redirected to the logoutURL site instead of the forwardURL site.

NOTE: These URLs are configured as part of the Self Service Password Reset general configuration. However, they can be overridden for any particular session by including the forwardURL or continueURL HTTP parameters on any request during the session.

You must force the user to log out from Self Service Password Reset and Access Manager after a user completes the password change operation. Otherwise, users might experience authentication failures and intruder lockout if they continue to use the same Access Manager session. For more information about how to configure session enforcement, see "Configuring the change password module" on page 51. The following are two instances when users are not immediately redirected to forwardURL:

- When **Check Expiration During Authentication** is selected and the user's password is about to expire. The user is redirected to the Change Password page instead of the forwardURL site. After changing the password, the user is redirected to forwardURL or logoutURL.
- When **Force Setup of Challenge Responses** is selected, the user matches **Challenge Response Query Match** and the user does not have valid Self Service Password Reset responses configured. In this case, the user is redirected to the Setup Responses module. After completing the response setup, the user is redirected to forwardURL or logoutURL.

Configuring Self Service Password Reset parameters for access manager

You must configure Self Service Password Reset to integrate with the Access Manager. The following steps help you define a password policy in Self Service Password Reset to define the groups or users that will use Access Manager with Self Service Password Reset.

To configure Self Service Password Reset to integrate with access manager:

1. Log in to Self Service Password Reset at `https://dns-name/sspr` as an administrator.
2. In the toolbar, click your name.
3. Click **Configuration Editor**.
4. Add a custom message to notify users about re-logging into their portal after a password change:
   - **4a** Click **Policies > Password Policies**.
   - **4b** Select the appropriate password policy. If you only have one password policy, click **default**.
   - **4c** In the **Password Change Message** field, add the custom message.
   - **4d** In the toolbar, click **Save changes**.
5. Add a URL where to forward users after completing any activity except for password changes:
   - **5a** In the toolbar, click your name.
   - **5b** Click **Configuration Editor**.
   - **5c** Click **Settings > Application > Application**.
   - **5d** In the **Forward URL** option, click **Add Value**.
   - **5e** Specify the URL where to forward users. For example:

     ```
     intranet.company.com
     ```

   - **5f** In the **Logout URL** option, add an Access Manager logout URL.
   - **5g** Click **Add Value**, then specify the Access Manager logout URL. For example:

     ```
     intranet.company.com/AGLogout
     ```

   - **5h** In the toolbar, click **Save changes**.
6. Enable Self Service Password Reset to log out users after a password change:
   - **6a** In the toolbar, click your name.
   - **6b** Click **Configuration Editor**.
   - **6c** Click **Modules > Authenticated > Change Password**.
   - **6d** Enable the **Logout After Password Change** option.
   - **6e** In the toolbar, click **Save changes**.

Using request parameters

You can specify various parameters on URLs. These parameters are case-sensitive. You can place these request parameters on any link that accesses Self Service Password Reset.

For example, `http://password.example.com/sspr/private/changepassword?passwordExpired=true&forwardURL=http://www.example.com`

Parameter	Description	Example
passwordExpired	Setting this parameter makes Self Service Password Reset override the state of the user's password expiration.	`passwordExpired=true`
forwardURL	Sets the forward URL. For example, http://www.example.com/main.html. The value must be URL encoded.	`forwardURL=http%3A%2F%2Fwww.example.com%2Fmain.html`
logoutURL	Sets the logout URL to Self Service Password Reset. The value must be URL Encoded.	`logoutURL=%2Fsspr`
locale	When a valid browser locale code is provided, Self Service Password Reset switches to the given locale to display all localized text.	`locale=en`

Using a command servlet

Command Servlet allows you to redirect a user to Self Service Password Reset and have it perform some specific command. You can use Command Servlet functions during a user's login sequence to a portal or another landing point.

Use Command Servlet functions with a proxy service, Access Gateway, or devices that automatically authenticate users. Otherwise, Self Service Password Reset requires that the user authenticates during each login.

You can combine Command Servlet calls with request parameters such as forwardURL.

The following table lists an example of the user login redirect sequence:

URL Example	Description
http://portal.example.com	Initial request from the browser.
http://portal.example.com/Login	Access Gateway redirects the user to the login page.
http://portal.example.com/	Access Gateway redirects the user to the portal root.
http://portal.example.com/index.html	Web server redirects the user to `index.html`.
http://password.example.com/sspr/private/CommandServlet?processAction=checkAll&forwardURL=http%3A%2F%2Fportal.example.com%2Fportalpage.html	`index.html` has meta redirect to the Self Service Password Reset checkAll CommandServlet with a URLEncoded forwardURL value.
http://portal.example.com/portal/main.html	Self Service Password Reset redirects the user to the actual portal URL.

The `index.html` file contains the following content:

```
<html> <head> <meta http-equiv="REFRESH" content="0; URL=http://
password.example.com/sspr/private/CommandServlet?
processAction=checkAll&forwardURL=http%3A%2F%2Fportal.example.com%2Fportal
page.html"/> </head> <body> <p>If your browser doesn't automatically load,
click <a href="http://password.example.com/sspr/private/CommandServlet?
processAction=checkAll&forwardURL=http%3A%2F%2Fportal.example.com%2Fportal
page.html">here</a>. </p> </body> </html>
```

The following table lists various useful commands:

Command	URL	Description
checkExpire	http://password.example.com/sspr/private/CommandServlet?processAction=checkExpire	Checks the user's password expiration date. If the expiration date is within the configured threshold, the user is required to change their password.
checkResponses	http://password.example.com/sspr/private/CommandServlet?processAction=checkResponses	Checks the user's challenge-responses. If no responses are configured, the user requires to set them up.
checkProfile	http://password.example.com/sspr/private/CommandServlet?processAction=checkProfile	Checks the user's profile. If the user's attributes do not meet the configured requirements, Self Service Password Reset requires that the user sets profile attributes.
checkAll	http://password.example.com/sspr/private/CommandServlet?processAction=checkAll	Calls checkExpire, checkResponses, and checkProfile consecutively.

Configuring Self Service Password Reset to access the OAuth2 application

To enable Self Service Password Reset to use the OAuth2 token Access Manager generates, you enter the DNS Name of the Identity Provider or Identity Provider clusters from Access Manager and you must use the scope, Client ID, Secret, and Endpoint URLs you recorded to complete the configuration.

1. Ensure that you have enabled OAuth and created an OAuth applications in Access Manager. For more information, see "Configuring single sign-on with OAuth2 tokens" on page 125.
2. Log in to the Self Service Password Reset Configuration Editor.
   - **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 Editor**.

2d (Conditional) Enter the configuration password.

3 Click **Settings > SSO Clients > OAuth**.

4 Define the following settings:

OAuth Login URL

Click **Add Value** and specify the Access Manager **Authorization Endpoint** you recorded in Step 10 on page 126, then click **OK**.

OAuth Scope

Click **Add Value** and specify the name of the scope you added the unique attribute to in Step 4 on page 125, then click **OK**.

OAuth Token / Code Resolve Service URL

Click **Add Value** and specify the Access Manager **Token Endpoint** you recorded in Step 10 on page 126, then click **OK**.

Skip Authentication header in OAuth Code Resolve Request.

Check **Enabled** to skip the authorization header in the OAuth Code Resolve request.

OAuth Profile/UserInfo Service URL

Click **Add Value** and specify the Access Manager **UserInfo Endpoint** you recorded in Step 10 on page 126, then click **OK**.

OAuth Server Certificate

Ensure that the Access Manager Endpoints you enter are valid and that Self Service Password Reset can communicate with Access Manager, then click **Import From Server** to import the Access Manager certificate in to Self Service Password Reset.

OAuth Client ID

Click **Add Value** and specify the Access Manager **Client ID** you recorded in Step 7d on page 126, then click **OK**.

OAuth Shared Secret

Click **Store Value** and define a password to protect the Access Manager **Secret**, then specify the **Secret** your recorded in Step 7d on page 126 and click **Store Password**.

OAuth User Name/DN Login Attribute

Click **Add Value** and specify the unique attribute that you defined in Step 1 on page 125, then click **OK**.

Add login hint optional parameter oauth authorization request

Specify the Username as a macro to add the login hint optional parameter to an OAuth authorization request and specify the username as a macro, you can follow the OAuth specification for including optional parameters in the request.

OAuth Profile / UserInfo Service Method Type

Select the HTTP method to invoke the Identity Server’s OAuth Profile/UserInfo Service URL. This method returns the user-related attribute data for Single Sign-on and Forgotten Password module. By default, the HTTP method is set to POST, but the administrator can select the GET method for making a request to the Identity server's OAuth Profile/UserInfo Service.

5 In the Configuration Editor, click **Settings > Application > Application > Site URL** and ensure that the Self Service Password Reset **Site URL** matches exactly the Access Manger **Redirect URL** you defined in Step 7b on page 126.

6 Click **Save changes** in the toolbar.

Additional integration options with access manager

Access Manager provides many different access solutions and you can integrate many different aspects of Access Manager with Self Service Password Reset and the reverse is true as well. The following sections contain some common use case configuration options for you to use. All of these use cases are optional.

- "Integrating the forgotten password module with access manager" on page 132
- "Deleting user accounts in access manager from the delete account module" on page 133
- "Creating accounts for social users in Self Service Password Reset using the new user registration module" on page 134
- "Adding the device management link to the update profile page" on page 134

Integrating the forgotten password module with access manager

Self Service Password Reset contains many different modules that provide different functionality. You can integrate the Forgotten Password module with Access Manager so that the Forgotten Password link on the User Portal page.

To add the Forgotten Password link to the User Portal page you must perform configuration steps in Self Service Password Reset and in Access Manager.

- "Configure Self Service Password Reset forgotten password module to work with access manager" on page 132
- "Configuring password expiration servlet in access manager" on page 133
- "Integrating the forgotten password URL" on page 133

Configure Self Service Password Reset forgotten password module to work with access manager

To have the Access Manager users to see the Forgotten Password link on the User Portal page, you must first ensure that you configure the Forgotten Password module. For more information, see "Configuring forgotten password module" on page 61.

You must also add the Access Manager logout URL to the redirected whitelist in Self Service Password Reset.

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

2 In the toolbar, click your name.

3 Click **Configuration Editor**.

4 Click **Security > Web Security > Redirect Whitelist**.

5 Click Add Value, then specify the Access Gateway logout URL. For example:

`https://intranet.yourcompany.com/AGLogout`

6 Click **OK**, then in the toolbar, click **Save changes**.

Configuring password expiration servlet in access manager

To allow your Access Manager users to use the Forgotten Password link on the user portal in Access Manager, you must configure the Access Gateway to redirect users to Self Service Password Reset when their password expires.

1 Log in to the Access Manager administration console.

2 Click the identity server cluster you want to modify.

3 Click **Local** > **Contracts** > ***Contract Name*** > **Password Expiration Servlet**.

   Select the type of contract you are using in your Access Manager environment.

4 Set the URL option to the Self Service Password Reset **Change Password URL**. For example:

```
http://password.example.com/sspr/private/
changepassword?passwordExpired=true
```

5 Click **OK** twice, then click **Close**.

This URL specifies that if the authenticated user's password has expired and there are grace logins remaining, then the user must be redirected to the Self Service Password Reset change password portal.

Integrating the forgotten password URL

You can configure the Access Manager user portal page to include the Forgotten Password URL for Self Service Password Reset. On the Identity Server, add the following HTML code in the `login.jsp` file (`/opt/novell/nids/lib/webapp/jsp/login.jsp`) above the last two </body></html> tags:

```
<CENTER> <a href="https://intranet.company.com/sspr/public/
forgottenpassword? forceAuth=TRUE&logoutURL=https://intranet.company.com/
AGLogout" target="_top"> Forgot Password - Self Service Password Reset</
a></CENTER>
```

Deleting user accounts in access manager from the delete account module

Self Service Password Reset allows to you do further integration with Access Manager by deleting user account information from Access Manager when a user deletes their own accounts using the Delete Account module. For more information, see "Configuring the delete account module to delete accounts from integrated products" on page 53.

Creating accounts for social users in Self Service Password Reset using the new user registration module

Access Manager allows users to use their social networking accounts to login and access resources. The Access Manager configuration for protected resources determines what users have access to use. You must have Access Manager configured to support social logins for this to work. For more information, see "Social Authentication" in the *NetIQ Access Manager 4.4 Administration Guide*.

Self Service Password Reset usually does not allow new users to access resources without specifying a password. Self Service Password Reset allows you to by pass the password requirement and redirect the users (behind the scenes) back to Access Manager to access any protected resources define in Access Manager.

To configure the new registration module to allow social logins:

1. Log in to Self Service Password Reset at `https://dns-name/sspr` as an administrator.
2. In the toolbar, click your name.
3. Click **Configuration Editor**.
4. Click **Modules > Public > New User Registration > New User Profiles**.
5. Create a new profile for the group of users you want to all to login in with social networking identities.
   - **5a** In **New User Form** section, change the **mail** field from **email** to **text** to allow Self Service Password Reset to accept hyphens and colons as part of the email address.

     Salesforce accounts contain hyphens and Google uses colons when passing information through OAuth for single sign-on.
   - **5b** Disable the **Prompt User for Password**. This allows the social users to login using their social identities without creating a new password.
   - **5c** In the **After Registration Redirect URL** field, specify the Access Manager URL where you want the users redirected to access the protected resources.

     You must specify `http://` or `https://` in the field or it is appended to the Self Service Password Reset site URL. This fields supports macros. For more information, see "Configuring macros for messages and actions" on page 22.
   - **5d** Define the remaining options using the embedded help.
6. In the toolbar, click **Save changes**.

Adding the device management link to the update profile page

Access Manager allows users to manage their own devices if they are ever lost or stole, when the users have MobileAccess installed. Self Service Password Reset allows you to add a link to the Access Manager manage devices page. This gives the users one location to access to perform multiple tasks. It simplifies the user's experience and adds another point of integration between Self Service Password Reset and Access Manager. For more information about MobileAccess, see "Enabling Mobile and Web Access" in the *NetIQ Access Manager 4.4 Administration Guide*.

To add a custom link to the update profile page:

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

2 In the toolbar, click your name.

3 Click **Configuration Editor**.

4 Click **Modules > Authenticated > Update Profile > Update Profile Profiles > default** or the profile you have created for the Access Manager users.

5 In the **Custom Links** field, click **Add Item**, then use the following information to define the custom link to add to the Update Profile page.

   5a Specify a descriptive name that appears in LDAP for the new custom link. For example, devices.

   NOTE: This field cannot accept any special characters including space, underscores, or hyphens.

   5b Click **Options** to define the link.

   5c Add a description to the link for your users by:

      5c1 In the **Description field**, click the edit icon.

      5c2 Specify a name for the link that appears on the Update Profile page for the users.

      5c3 (Optional) Click **Add Locale**, then select the correct language for your users.

      5c4 Click **OK** to save the description.

   5d In the **Link URL** field, specify the custom link where you want to redirect the users.

   5e (Optional) Select whether you want the link to open in a new window.

   5f Click **OK** to save the changes.

6 Click **Save changes** in the toolbar to have this take effect.

Users can now access the new link on the Update Profile page. You can add as many different links as required for your users.

10 Integrating Self Service Password Reset with advanced authentication

Advanced Authentication provides required flexibility to an organization to secure the authentication to the level of protection that is required. Advanced Authentication lets organizations efficiently use as many different devices as required, or continue to use old devices while phasing in the new devices. All the devices can be under the same management and control.

You can integrate Self Service Password Reset with Advanced Authentication and use multifactor authentication methods to provide secure access for customers, contractors, and employees. It provides fast and easy identity verification.

You integrate Advanced Authentication with Self Service Password Reset by configuring the Forgotten Password module to use an OAuth2 verification method. This requires you to configure and enable the Forgotten Password module. For more information, see "Configuring forgotten password module" on page 61.

Self Service Password Reset 4.0 or earlier integrated with Advanced Authentication through Endpoints. Now, Self Service Password Reset ingrates with Advanced Authentication through a Forgotten Password identification method. The old method is still in place and you do not have to make any changes. However, we recommend using this new method. For more information about the old method, see Self Service Password Reset 4.0 documentation.

To integrate Self Service Password Reset with Advanced Authentication, you must configure few settings in Self Service Password Reset and Advance Authentication. The following sections describe the prerequisites and the required configuration:

- "Prerequisites" on page 137
- "Configuring advanced authentication to integrate with Self Service Password Reset" on page 138
- "Configuring Self Service Password Reset for advanced authentication" on page 139

Prerequisites

When using Advanced Authentication for the Forgotten Password module, you must ensure the following:

❒ Install and configure the Advanced Authentication server version 6.3.7 or later.

For more information about configuring the Advanced Authentication server, see the *Advance Authentication Server Administration Guide (https://www.netiq.com/documentation/advanced-authentication-64/server-administrator-guide/data/part_config_applnc.html)*.

- ❒ Create and configure the Advanced Authentication repositories. For more information, see "Adding a Repository (https://www.netiq.com/documentation/advanced-authentication-64/server-administrator-guide/data/add_repo.html)" in the *Advance Authentication Server Administration Guide (https://www.netiq.com/documentation/advanced-authentication-64/server-administrator-guide/data/bookinfo.html)*.
- ❒ A good understanding of OAuth2. For more information, see the *OAuth 2.0 Documentation*.

Configuring advanced authentication to integrate with Self Service Password Reset

To integrate Self Service Password Reset and Advanced Authentication, you must create an Event type of OAuth2 to create the integration between the two products. You must create the Event type in Advanced Authentication before configuring Self Service Password Reset. The Event type contains information you must use in Self Service Password Reset to create the OAuth2 connection.

To configure advanced authentication to connect to Self Service Password Reset:

1. Log in to the Advanced Authentication Administrative Portal as an administrator.

   `https://dns-name-advanced-authentication/admin`

2. Open **Policies > Web Authentication**.

   NOTE: You only need to configure the policies during the initial setup of Advanced Authentication while integrating with Self Service Password Reset.

   ---

3. Specify the Identity Provider URL in **Identity Provider URL**. For more information, see Configuring the Identity Provider (https://www.netiq.com/documentation/advanced-authentication-64/server-administrator-guide/data/t4gadzfldq6t.html).
4. Click **Save**, to save the change. For more information, see Web Authentication (https://www.netiq.com/documentation/advanced-authentication-64/server-administrator-guide/data/web_auth.html).
5. Click **Event**, then click **Add** to create a new Event for Self Service Password Reset.

   5a Use the following information to create an OAuth 2 Event type for Self Service Password Reset:

   Name

   Specify a unique name for this Event type. Ensure that you know this Event is for Self Service Password Reset.

   Is enabled

   Ensure that this option is set to **ON** so that the Event functions.

   Event type

   Select **OAuth2** as the Event type. This must be set to OAuth2 or the connection to Self Service Password Reset does not work.

Chains

Select the appropriate authentication chains you want to use in your environment, then move the authentication option to the **Used** panel. An authentication chain is a chain of authentication methods a user must complete to authenticate to Self Service Password Reset.

OAuth2 settings > Client ID

Copy this client ID to use later in the Self Service Password Reset configuration.

OAuth2 settings > Client secret

Copy this client secret to use later in the Self Service Password Reset configuration.

Redirect URIs, One URI per line

Specify the Self Service Password Reset site URL with /public/oauth at the end of the URL. For example:

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

NOTE: You can see what the Self Service Password Reset URL is by accessing the **Site URL** setting in the Configuration Editor here: **Configuration Editor > Settings > Application > Application**.

5b Click **Save**, to save the OAuth2 Event type in Advanced Authentication. For more information, see OAuth2 event (https://www.netiq.com/documentation/advanced-authentication-64/server-administrator-guide/data/create_custom_evnt.html#create_oauth_20_evnt)

You must now configure Self Service Password Reset using the client ID and client secret to create the OAuth2 connection between the two products.

Configuring Self Service Password Reset for advanced authentication

To integrate Self Service Password Reset, you must enable the Forgotten Password module and create an identification method of OAuth2 for Forgotten Password. OAuth 2 is an authentication framework Self Service Password Reset uses to create a secure connection to Advanced Authentication for your users. You also create an Oauth2 event in Advanced Authentication.

Ensure that you have created an Event type in Advanced Authentication before configuring Self Service Password Reset. You must obtain information from the Event type configuration to complete the Self Service Password Reset configuration. For more information, see "Configuring advanced authentication to integrate with Self Service Password Reset" on page 138.

To configure the forgotten password module with an OAuth 2 verification method to advanced authentication:

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

4 Configure a Forgotten Password profile for the group of users that will use Advanced Authentication to access Self Service Password Reset with the following specific configuration.

4a Click **Modules > Public > Forgotten Password > Profiles > *default* > Definition > Verification Method**.

Define the default profile for your users or create a new profile.

4b Set **OAuth** to **Optional** and **Challenge/Response Answers** to **Optional**.

4c (Optional) After the validation of OAuth, you can set this option to **Mandatory** instead.

4d Change **Minimum Optional Required** to a value of 1 to display the menu to users for selection of either Challenge/Response or an external Advanced Authentication server.

4e Use the help and the documentation to finish configuring the profile definition for your users. For more information, see "Configuring the forgotten password profile" on page 62.

5 Click **Modules > Public > Forgotten Password > Profile > *default* > OAuth**.

5a In **OAuth Login URL**, click the **Edit** icon , then specify the Identity Provider URL, which is added in Advanced Authentication.

For example, `https://<advanced-authentication-Idp-domain>osp/a/TOP/auth/oauth2/grant`.

5b In **OAuth Code Resolve Service URL**, click **Add Value** to specify the Advanced Authentication Resolve Service URL.

For example, `https://dns-name-advanced-authentication/osp/a/TOP/auth/oauth2/authcoderesolve`.

5c In **OAuth Profile Service URL**, click **Add Value** to specify the web service URL provided by the Advanced Authentication to return attribute data about the user.

For example, `https://dns-name-advanced-authentication/osp/a/TOP/auth/oauth2/getattributes`.

5d Click **Import From Server** in **OAuth Web Service Server Certificate** to import the certificate from the Advanced Authentication server.

NOTE: To import the certificate, you must resolve the domain name within the Serf Service Password reset docker's host file.

5e In the **OAuth Client ID** field, click **Add**, then copy the **Client ID** from Advanced Authentication.

5f In the **OAuth Shared Secret** field, click **Store Value**, then copy the **Client secret** from Advance Authentication.

5g In the **OAuth User Name/DN Login Attribute** field, click **Add Value**, then add the Advanced Authentication attribute that represents the user name. For Advanced Authentication the attribute is `user_name`.

5h In the **OAuth Inject User Name Value** field, click **Add Value**, then add your Advanced Authentication repository name with a macro appended containing the user name. The Advanced Authentication repository is the LDAP directory that contains your users. For example:

```
AADirectory\@LDAP:cn@
```

5i You must specify the Identity Provider URL, which is added in Advanced Authentication to complete the configuration. Here is an example of what the URLs are:

```
https://<advanced-authentication-Idp-domain>osp/a/TOP/auth/oauth2/
grant
https://dns-name-advanced-authentication/osp/a/TOP/auth/oauth2/
authcoderesolve
https://dns-name-advanced-authentication/osp/a/TOP/auth/oauth2/
getattributes
```

Use the help and the documentation to finish configuring the profile for the OAuth options. For more information, see "Configuring the OAuth2 verification method for the forgotten password module" on page 74.

6 Ensure that you have defined the Forgotten Password Settings for this module. For more information, see "Configuring the forgotten password settings" on page 68.

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

11 Integrating Self Service Password Reset with NetIQ identity manager

Identity Manager is a comprehensive Identity management solution that provides secure access to web and enterprise applications. Identity Manager also provides seamless single sign-on across technical and organizational boundaries.

Self Service Password Reset integrates with Identity Manager to manage passwords for all the users who access the identity applications. This integration is possible if Self Service Password Reset is installed with Identity Manager by using Integrated Installer, or if Self Service Password Reset is installed as a standalone product and configured with Identity Manager. When a user enters the credentials to access an identity application, the request is sent to Self Service Password Reset and the user is allowed to access the web pages depending on the password policy that is defined for the user.

There are two different ways to integrate Self Service Password Reset with Identity Manager: use the integrated installer or integrate a standalone Self Service Password Reset deployment with Identity Manager. If you use the integrated installer for Identity Manager there are fewer configuration steps to complete.

- "Supported versions" on page 143
- "Installing Self Service Password Reset with the identity manager integrated installer" on page 144
- "Integrating a standalone Self Service Password Reset with identity manager" on page 144
- "Enabling Self Service Password Reset proxy users to read passwords from edirectory" on page 147

Supported versions

Self Service Password Reset ships as part of Identity Manager and you install it with the integrated installer. All of the releases of Self Service Password Reset have not synchronized with the Identity Manager release.

The Identity Manager integrated installers installs Tomcat for you. Self Service Password Reset supports the version of Tomcat installed with the integrated installer if you use the integrated installer to install Self Service Password Reset. If you install Self Service Password Reset as a standalone deployment, you must meet the Self Service Password Reset requirements. For more information, see "Installing Self Service Password Reset" in the *Self Service Password Reset 4.8 Installation Guide*.

Installing Self Service Password Reset with the identity manager integrated installer

If you install Self Service Password Reset by using the Identity Manager integrated installer, ensure that you follow the Identity Manager documentation and complete all prerequisites before installing Self Service Password Reset. For more information, see "Installing the Password Management Component" in the *NetIQ Identity Manager Setup Guide*.

If you install Self Service Password Reset by using Identity Manager Integrated Installer, it automatically defines the configuration settings in the Self Service Password Reset configuration file. However, there is a Self Service Password Reset **NetIQ Identity Manager/ OAuth Integration** template that includes all of the default settings that you must configure for your Identity Manager users. For more information, see "Configure OAuth settings for Self Service Password Reset" on page 144.

Integrating a standalone Self Service Password Reset with identity manager

If you have installed Self Service Password Reset as a standalone product and want to utilize the Self Service Password Reset password management functionality for identity applications then, you can provide the configurable values for the required settings by using the Self Service Password Reset Configuration Editor page and configuring the template for Identity Manager.

Complete the following sections to use Self Service Password Reset as the password management tool for Identity Manager:

- "Configure OAuth settings for Self Service Password Reset" on page 144
- "Set the Self Service Password Reset theme to match the identity manager theme" on page 146
- "Configure syslog audit server" on page 146

NOTE: Ensure that you have selected **Password Management Provider** as **Self Service Password Reset** in the Roles Based Provisioning Module Configuration utility of Identity Manager. For more information about configuring settings in Roles Based Provisioning Module Configuration utility, see "Configuring the Settings for the Identity Applications" in the *NetIQ Identity Manager Setup Guide.*

Configure OAuth settings for Self Service Password Reset

This section discusses various settings that enable Self Service Password Reset to integrate with OAuth Identity Server for a single sign-on. The Identity Manager Roles Based Provisioning Module configuration utility includes OAuth settings under **Self Service Password Reset** in the **SSO clients** tab. The OAuth settings that are defined in the Roles Based Provisioning Module configuration utility must be included in the Self Service Password Reset OAuth settings. For more information about configuring or viewing the settings in the Roles Based Provisioning Module configuration utility, see "Configuring the Settings for the Identity Application" in the *NetIQ Identity Manager Setup Guide*.

To configure the identity manager OAuth settings in Self Service Password Reset:

1. Log in to Self Service Password Reset at `https://dns-name/sspr` as an administrator.
2. In the toolbar, click your name.

3 Click **Configuration Editor**.

4 Configure Self Service Password Reset to communicate to Identity Manager.

   4a Click **Default Settings > LDAP Vendor Default Settings**.

   4b Select **NetIQ IDM / OAuth Integration**.

5 Click **Settings > Single Sign On (SSO) Client > OAuth**.

6 Configure the following settings:

OAuth Login URL

Specify the URL for OAuth server login. This is the URL to redirect the user for authentication. For example:

```
https://IP address of the Identity Manager server:8543/osp/a/idm/
auth/oauth2/grant
```

OAuth Scope

Specify the optional OAuth scope. The OAuth identity service provider (IdP) provides this value. The content provided, if any, must contain the user attribute to be read for authentication.

OAuth Token / Code Resolve Service URL

Specify the URL for OAuth Code Resolve Service. This web service URL is used for resolving the artifact that the OAuth identity server returns. For example:

```
https://IP address of the Identity Manager server:8543/osp/a/idm/
auth/oauth2/authcoderesolve
```

Skip Authentication header in OAuth Code Resolve Request.

Check **Enabled** to skip the authorization header in the OAuth Code Resolve request.

OAuth Profile / UserInfo Service URL

Specify the URL for the web service that the Identity Server provides that returns attribute data about the user. For example:

```
https://IP address of the Identity Manager server:8543/osp/a/idm/
auth/oauth2/getattributes
```

OAUTH Server Certificate

Import the certificate from the Identity Manager server for the OAuth web service server.

OAuth Client ID

Specify SSPR as the client ID of the OAuth client. This value is provided by the OAuth identity service provider.

OAuth Shared Secret

Specify the OAuth shared secret. This value is provided by the OAuth identity service provider.

OAuth User Name/DN Login Attribute

Specify the attribute to request from the OAuth server that is used as the user name for local authentication. This value is then resolved as the same password the user had typed at the local authentication page. For example, `cn` would be the attribute that contains the OAuth User Name or the DN Login Attribute.

Add login hint optional parameter oauth authorization request

Specify the Username as a macro to add the login hint optional parameter to an OAuth authorization request and specify the username as a macro, you can follow the OAuth specification for including optional parameters in the request.

OAuth Profile / UserInfo Service Method Type

Select the HTTP method to invoke the Identity Server's OAuth Profile/UserInfo Service URL. This method returns the user-related attribute data for Single Sign-on and Forgotten Password module. By default, the HTTP method is set to POST, but the administrator can select the GET method for making a request to the Identity server's OAuth Profile/UserInfo Service.

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

Set the Self Service Password Reset theme to match the identity manager theme

Self Service Password Reset includes an option to use the Identity Manager theme for the Self Service Password Reset password management page. To set the theme of the Self Service Password Reset web page to match the Identity manager theme, perform the following in the Self Service Password Reset Configuration Editor page:

To configure the Self Service Password Reset user interface to match identity manager:

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

2 In the toolbar, click your name.

3 Click **Configuration Editor**.

4 Click **Settings** > **User Interface > Look & Feel**.

5 Select **IDM** (Identity Manager) from the list of themes in the **Interface Theme** setting.

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

Configure syslog audit server

Self Service Password Reset provides logging and auditing functionality to send event alerts. To configure Self Service Password Reset audit server with the Identity Manager server you must configure the **Syslog Audit Servers** setting in the Configuration Editor page. **Settings > Auditing > Audit Forwarding > Syslog Audit Server**.

When this value is set, all the audit events are sent to the specified syslog server. For more information about configuring the audit server, see "Auditing for Self Service Password Reset" on page 161.

Enabling Self Service Password Reset proxy users to read passwords from edirectory

An administrator can configure the password policy settings for eDirectory and provide a Self Service Password Reset proxy user the permission to read the password from eDirectory. During Single Sign-On process for the Forgotten Password module, this permission allows Self Service Password Reset to provide details on behalf of the user. Also, the user is not prompted to enter credentials or to set a temporary password on the user account.

Proxy users play a role in SSPR for scenarios where users face account lockout or are unable to reset their passwords. It adds an additional layer of security by ensuring that only authorized individuals can perform password resets on behalf of others. Users with generic proxy user rights perform operations such as pre-authentication.

Use the following steps for an integrated deployment of Self Service Password Reset or a standalone deployment to allow users to read password by using the Self Service Password Reset proxy user.

To provide a Self Service Password Reset proxy user permission to read the password from edirectory, perform the following steps:

1. Log in to Self Service Password Reset at `https://dns-name/sspr as an administrator`.
2. In the toolbar, click your name.
3. Click **Configuration Editor**.
4. Click **Settings > LDAP > LDAP Settings > NetIQ eDirectory > eDirectory Settings**.
5. Ensure to enable the **Read User Passwords**.
6. Click **Save changes** in the toolbar.

To configure the password policy settings for edirectory, perform the following steps:

1. Log in to iManager.
2. Select **Roles and Tasks** from the header icons.
3. Select **Passwords** > **Password Policies.**
4. Select the appropriate password policy.
5. Click the **Password** tab, and then click **Configuration Options** tab.
6. Enable the **Allow the following to retrieve passwords** check box.
7. Click **Insert** and select the Self Service Password Reset proxy user.
8. Click **OK**.

12 Integrating Self Service Password Reset with client login extension

Self Service Password Reset provides your users with the ability to reset their own passwords and perform other self-service activities. Integrating Self Service Password Reset with the Client Login Extension increases the self-service password reset activities that your users can perform. This helps reduce calls to the help desk and makes users more productive.

By integrating Self Service Password Reset and the Client Login Extension, it solves the following problems for your users. When users are using Microsoft Windows workstation, but they encounter a locked Windows login screen and the users must reset a forgotten password, activate an account, or register as a new user account and they cannot do it.

The user must be able to log in to their workstations to access Self Service Password Reset to reset their passwords, activate an account, or register as a new user account, but they cannot access Self Service Password Reset because the workstation is locked. This is a problem and causes many help desk calls.

The solution to this problem is when you integrate the two products, Client Login Extension allows users to access Self Service Password Reset without logging into their workstations so they can reset their passwords, activate an account, or register as a new user without calling the help desk.

This occurs because when you integrate the two products Client Login Extension adds a component to the Windows login environment, known as a credential provider on modern (Windows 7+) workstation operating systems. When you complete the integration, Client Login Extension now contains a restricted web browser that allows the user to access only the Self Service Password Reset application and no other websites.

- "Prerequisites" on page 149
- "Configuring Self Service Password Reset for client login extension" on page 150
- "Configuring client login extension" on page 150

Prerequisites

To integrate Self Service Password Reset with Client Login Extension, you must meet the following prerequisites:

	Prerequisites	Description
❑	Self Service Password Reset	It must be installed and configured to integrate with Client Login Extension. For more information, see *Self Service Password Reset 4.8 Installation Guide*.

	Prerequisites	Description
❑	Secure HTTPS	Self Service Password Reset must be configured to use secure HTTPS. For more information, see ""Importing certificates to create an HTTPS connection to browsers" on page 34".
❑	HTTPS certificates must be trusted by the workstation	You must not have any certificate errors between Internet Explorer and Self Service Password Reset. To ensure this happens the certificates used by the workstation must be signed by a commercial Certificate Authority (CA) or because you imported the CA into the workstation trust.

Configuring Self Service Password Reset for client login extension

Self Service Password Reset communicates to Client Login Extension through REST. You must enable Self Service Password Reset to communicate through REST to start the integration process.

1. Log in to Self Service Password Reset at `https://dns-name/sspr` as an administrator.
2. In the tool bar, click your name.
3. Click **Configuration Editor**.
4. Click **Settings > Web Services > REST Services**.
5. Ensure to enable the **Enable Web Services** and **Allow Challenge Services to Read Answer** options.
6. Click **Save changes** in the tool bar.

Configuring client login extension

Client Login Extension is an application that you install on each Windows workstation in your environment. Client Login Extension contains a Configuration Utility that allows you to modify the installation settings for Client Login Extension so each Windows workstation contains the information required to connect to Self Service Password Reset. The Configuration Utility modifies the Client Login Extension MSI file so the changes occur during the installation of Client Login Extension.

Client Login Extension allows you to deploy these files in an enterprise environment without having to manually run the installation on each workstation. For more information, see "Configuring the Client Login Extension Configuration Utility" in the *Client Login Extension Administration Guide*.

To use the configuration utility:

1. Download Client Login Extension from Patch Finder.
   - **1a** Access Patch Finder (https://download.microfocus.com/patch/finder/).
   - **1b** In the **Select a Product** field, select Self Service Password Reset, then click **Search**.

1c Click the appropriate version of Self Service Password Reset to access the Client Login Extension file.

1d Click the Client Login Extension file, then follow the prompts to download the file.

2 Find the `ClientLoginExtensionConfigurationUtility.exe` file that is part of the Client Login Extension.

3 Run the **ClientLoginExtensionConfigurationUtility.exe** file.

4 Configure the following options that are specific to Self Service Password Reset:

Link URL

Specify the URL that the Client Login Extension restricted browser uses to connect to Self Service Password Reset. You can redirect your users to the Forgotten Password page or to the main Self Service Password Reset page.

For example:

Main Self Service Password Reset Page

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

Forgotten Password Page

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

Link Text

Specify the text the restricted browser displayed on the link for users to access Self Service Password Reset. For example: `Forgotten Password`.

Enable SSPR Configuration

Select this option to enable the Self Service Password Reset configuration with Client Login Extension.

REST URI

Specify the REST URI for Self Service Password Reset. For example:

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

(Optional) Change Password through SSPR

Select this option if you want users to be able to change their passwords through Self Service Password Reset.

Password Policy Link Text

Specify the text that the Client Login Extension displays to the users about the password policy. The default value is Password Policy.

The password policies are the restrictions you define in Self Service Password Reset. For example, a password policy requires one capital letter, one number, and no special characters.

(Optional) Challenge Response

If you want your users to use the Challenge-Response feature in Self Service Password Reset, select this option. Next, you must specify the text users see informing them they must configure their Challenge-Responses before they can log in to the system.

IMPORTANT: There are other options you can configure in the Configuration Utility that are not part of the Self Service Password Reset integration with Client Login Extension. View the Client Login Extension documentation for information about the additional options. For more information, see "Configuring Client Login Extension Configuration Utility" in the *Client Login Extension Administration Guide*.

5 Click **Configure Installer** to make the changes to the MSI file for Client Login Extension.

6 Install Client Login Extension on each Windows workstations to implement the integration.

III Maintaining Self Service Password Reset

13 Managing Self Service Password Reset

Self Service Password Reset provides tools to back up configuration information and to view the activity throughout the system. You can back up the configuration information if you are going to migrate to new hardware or you need to recover from a hardware failure.

- "Backing up configuration information" on page 155
- "Importing configuration information" on page 155
- "Viewing LDAP permissions recommendations" on page 156
- "Uploading the seed list" on page 157
- "Configuring data analysis" on page 158
- "Configuring logging" on page 159
- "Auditing for Self Service Password Reset" on page 161
- "Adding a patch update" on page 163

Backing up configuration information

Self Service Password Reset allows you to back up and store the configuration information for Self Service Password Reset in an XML file. You use this information if you are migrating to new hardware or if you had a hardware failure.

To back up the configuration information:

1. Log in to Self Service Password Reset at `https://dns-name/sspr` as an administrator.
2. In the toolbar, click your name.
3. Click **Configuration Manager**.
4. Click **Download Configuration** and save the configuration information somewhere safe.
5. (Conditional) To download local database information:
   - **5a** Click the **LocalDB** tab.
   - **5b** Click **Download LocalDB** and save the information somewhere safe.

If you must restore the information, see "Importing configuration information" on page 155.

Importing configuration information

Self Service Password Reset allows you to import configuration information from other Self Service Password Reset systems. You would want to do this when you are moving to new hardware, upgrading Self Service Password Reset, recovering from a disaster or configuring Self Service Password Reset for high availability and load balancing.

IMPORTANT: Ensure that you export your Self Service Password Reset configuration settings anytime you change your settings.

To import Self Service Password Reset configuration information:

1. Ensure that you have created a backup of the current Self Service Password Reset configuration by backing up the configuration information. For more information, see "Backing up configuration information" on page 155.
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 Manager**.
5. Click **Import Configuration**, then browse to and select the `SSPRConfiguration.xml` file you created earlier.
6. (Conditional) To import the local database information:
   - **6a** Click the **LocalDB** tab.
   - **6b** Click **Import (Upload) LocalDB Archive File**, then browse to and select the local database archive file you created earlier.

     NOTE: Self Service Password Reset provides the local database for testing purposes only. For production environments, you must use an external database or an LDAP directory.

     The local database storage limit is 102,400 bytes (1024 * 100 bytes).

The new deployment now contains all of the configuration settings of the old system.

Viewing LDAP permissions recommendations

Self Service Password Reset contains an LDAP Permissions tool that displays all of the required rights specific to the LDAP directory you are using and what Self Service Password Reset modules you enable. Anytime you enable new modules, you must run the LDAP Permissions tool to ensure that you have the correct LDAP rights assignments for the module to work.

Here is a video demonstrating how to use the LDAP Permissions tool.

The LDAP Permissions tool is available when you run the Configuration Guide and it is also available in the Configuration Manager.

To access the LDAP permissions tool:

1. Log in to Self Service Password Reset at `https://dns-name/sspr` as an administrator.
2. In the toolbar, click your name.
3. Click **Configuration Manager**.
4. Click **LDAP Permissions**.
5. Review the LDAP Permissions Recommendations report and change the rights according to the information in the report.

WARNING: Changing rights in your LDAP directory might permanently change the LDAP directory. Ensure that your LDAP directory administrator performs any required rights changes. If the LDAP directory is not healthy or there are communication problems in your network, changing the schema can cause problems.

Uploading the seed list

Self Service Password Reset generates a random password for the test user to give useful password suggestions. The random password will be generated by using words from the seed list, which are then randomly changed until they are sufficiently complex and comply with the user's configured requirements.The word list and seed list are ZIP files containing one or more plain text files with one word per line.

Updating seed list

You can add few more words that you want to allow as password to the seed list. To update the seed list, perform one of the following:

- Customize the existing seed list
- Creating a seed list

Customize the existing seed list

1. Navigate to the `seedlist.zip` file from one of the following paths according to your setup:
   - **Appliance**: `/var/lib/docker/overlay2/c25d96dc05d02d3f3159889fa78d9e2e2fe44393b67a1ca257e14079d84d6d36/merged/root/.sspr-workpath/work-sspr-8443/war/WEB-INF/`
   - **Linux**: `/srv/tomcat/webapps/sspr/WEB-INF/`
   - **Windows**: `C:\Program Files\NetIQ Self Service Password Reset\apache-tomcat-9\webapps\sspr\WEB-INF`
2. Extract the `seedlist.zip` folder and open the `seedlist.txt` file.
3. Add the words that you want to allow as password in the text file. Ensure that one word is specified per line.
4. Save the text file and compress the seedlist folder to the `.zip` format.
5. Continue with Uploading the seed list.

Creating a seed list

1. Create the **seedlist.txt** file.
2. Add the words that you want to allow as password in the text file. Ensure that one word is specified per line.
3. Save the text file within the folder seedlist.
4. Compress the seed list folder to the `.zip` format.
5. Continue with Uploading the seed list.

Uploading the seed list

NOTE: It is recommended to save the `seedlist.zip` on an HTTP server, and configure URL of the file location in SSPR. This will restore the seed list as per your requirement even after the upgrade.

You can upload the updated or new seed list in one of the following ways:

- Using a web server
- Using the user interface

Using a web server

You can save the `seedlist.zip` file in any of the web server and save the file location URL for further reference. Perform the following steps to set the seed list file URL in SSPR:

1. Click **Configuration Editor > Settings > Word Lists**.
2. Specify the URL of the text file in **Seed List File URL**.
3. Click **Save changes** in the toolbar.

Using the user interface

To upload the `seedlist.zip` file through the user interface, perform the following steps:

1. Click **Configuration Manager > Word Lists**.
2. Click **Upload Seed List**.
3. Click **Choose File** and select the `seedlist.zip` from your local drive.
4. Click **Upload**.

   To verify the seed list file is uploaded, check the **Word Count** that displays the number of words in the seed list available in the text file.
5. If you want to clear the uploaded seed list file and restore the old file, click **Clear Seed List**.

To verify the size of the seed list, check the **Word Count** that displays the number of words in the seed list available in the text file.

Configuring data analysis

Self Service Password Reset helps analyzes the data passing through the system to create reports. You view the reports through the Administration module on the Dashboard, but you configure all of the settings in the Configuration Editor. If you do not enable **Directory Reporting**, the **Data Analysis** tab in the Dashboard does not display any information.

- "Configuring reporting" on page 159
- "Viewing the reports" on page 159

Configuring reporting

The reports that Self Service Password Reset provides are a summary report and a detailed report on password change status, what validation methods users have registered for, plus additional reports on the other password self-service fields. The report does not work by default. You must enable **Directory Reporting** to see and access the reports.

After you have configured reporting, Self Service Password Reset maintains the reports in the local cache until the time that you specified during the configuration.

To configure reporting:

1. Log in to Self Service Password Reset at `https://dns-name/sspr` as an administrator.
2. In the toolbar, click your name.
3. Click **Configuration Editor**.
4. Click **Settings > Reporting**.
5. Use the help to configure reporting for Self Service Password Reset.
6. In the toolbar, click **Save changes**.

Viewing the reports

Self Service Password Reset maintains and displays the reports through the Administration module. You must enable **Directory Reporting** to see the reports. If you have the proper privileges, you can see and use the reports to help manage your environment.

You can view password changes, validation methods users have registered for, what hash method was used to store responses and much more date. You must configure reporting to return the data you want to see.

To view reports:

1. Log in to Self Service Password Reset at `https://dns-name/sspr` as an administrator.
2. Click **Administration**.
3. On the Dashboard, click **Data Analysis**.
4. View the reports you configured.

Configuring logging

Self Service Password Reset provides logs for your to troubleshoot any issues that might occur. The system uses Apache log4j for logging. Apache log4j is a Java-based logging utility that allows logging to a variety of outputs such as files, syslog, NT event log, databases, and so forth.

You configure the logging settings in the Configuration Editor and you view the logs through the administration console for Self Service Password Reset. The system also outputs a number of logs to the file system depending on the options you configure.

- “Configuring logging settings” on page 160
- “Viewing logs” on page 160

Configuring logging settings

You configure the setting for logging in the Configuration Editor. A number of settings use the same log levels. Depending on what you must see, you set a different level of severity for the logs. The following list includes available log levels for all settings in order of severity:

6 - Trace

Most detailed information. Use this level during initial configuration.

5 - Debug

Detailed information on the flow through the system.

4 - Info

Informational messages that highlight the progress of the application at coarse-grained level. Use this level for normal operations. This is the default log level for `StdOut`.

3 - Warn

Potentially harmful situations.

2 - Error

Runtime errors or unexpected conditions.

1 - Fatal

Severe errors that cause premature termination.

To configure logging:

1. Log in to Self Service Password Reset at `https://dns-name/sspr` as an administrator.
2. In the toolbar, click your name.
3. Click **Configuration Editor**.
4. Click **Settings > Logging**.
5. Use the help to configure logging for Self Service Password Reset.
6. In the toolbar, click **Save changes**.
7. (Conditional) To log all LDAP events to the Trace logging level:
   - **7a** In the Configuration Editor, click **LDAP** > **LDAP Settings** > **Global**.
   - **7b** Select **Enable LDAP Wire Trace**. For more information, see "Configuring LDAP settings" on page 41.
   - **7c** In the toolbar, click **Save changes**.

Viewing logs

Self Service Password Reset allows you to view the logs through the administration console. The option you set in "Configuring logging settings" on page 160 determines what the log shows. You can also change the log level through the viewer.

To view the log:

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

2 In the toolbar, click your name.
3 Click **View Log**.
4 Select the appropriate log level, then click **Refresh** to see that level.
5 (Conditional) To save the information to a file, right click and select **Save page as**.
6 Close the separate browser window to return to the administration console.

Auditing for Self Service Password Reset

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.

- "Configuring auditing" on page 161
- "Forwarding auditing information" on page 161
- "Configuring auditing for user history" on page 162
- "CEF audits and customization" on page 162

Configuring auditing

Self Service Password Reset allows you to enable and configure event alerts such as intruder alerts and fatal event alerts.

To configure the logging and auditing options, perform the following steps:

1 Log in to Self Service Password Reset at `https://dns-name/sspr` as an administrator.
2 In the toolbar, click your name.
3 Click **Configuration Editor**.
4 Click **Settings > Auditing > Audit Configuration**.
5 Select the type of events to audit. Use the help for more information.
6 In the toolbar, click **Save changes**.

Forwarding auditing information

You can forward auditing events to external systems to analyze the information. Self Service Password Reset supports forwarding audit information to Sentinel, ArcSight, and syslog servers. You forward the audit events to the external systems for further analysis.

NOTE: In SSPR 4.6, if you have configured the Sentinel Syslog server to collect the audit events in the CEF format, there might be a parsing error. The Parsing error occurs because the CEF audit events are routed to the Universal CEF collector instead of the NetIQ SSPR collector.

If you require to get the CEF audit events on the Sentinel Syslog server, it is recommended to remove the SSPR collector so that the events are stored and managed in the Universal CEF collector.

Before removing the NetIQ SSPR collector, ensure that the audit configuration is not set to JSON format, else there can be loss of audit events data.

1. Log in to Self Service Password Reset at `https://dns-name/sspr` as an administrator.
2. In the toolbar, click your name.
3. Click **Configuration Editor**.
4. Click **Settings > Auditing > Audit Forwarding**.
5. Use the help to configure the audit service for Self Service Password Reset.

   NOTE: Self Service Password Reset allows specifying multiple syslog servers for fail-over purposes. If you only have one syslog server and it is not available, Self Service Password Reset queues the audit events until the syslog server is available again.

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

Configuring auditing for user history

Self Service Password Reset allows you to store the user history in different locations. Use the following settings to configure that storage.

1. Log in to Self Service Password Reset at `https://dns-name/sspr` as an administrator.
2. In the toolbar, click your name.
3. Click **Configuration Editor**.
4. Click **Settings > User History**.
5. Use the help to configure the audit settings for the user history.
6. Click **Save changes**.

CEF audits and customization

Self Service Password Reset can be configured to send information about the system events and actions in logs in the CEF format to any Syslog sever. The CEF format log message is sent in the format:

```
<date> <host> CEF:0|<vendor>|<product>|<version>|<event code>|<time
stamp>|<message>|<perpetrator ID>|<perpetrator DN>|<source
address>|<source host>|<target ID>|<target DN>
```

Before customizing CEF audits, ensure to that **Syslog Output Format** is set to **CEF** in **Configuration Editor > Settings > Auditing > Audit forwarding**.

1. Log in to Self Service Password Reset (https://*dns-name*/sspr) as an administrator.
2. In the toolbar, click your name.
3. Click **Configuration Editor > Settings > Application > Application**.
4. To customize the fields in the CEF message, use **App Property Overrides**. It is advisable to contact the SSPR Support team for further assistance.

   For example, specify the following customized log message to include the outcome information along with default message:

```
audit.syslog.cef.extensions=type,cat:eventCode,act:timestamp,rt:narrat
ive,msg:message,reason:perpetratorID,suid:perpetratorDN,suser:sourceAd
dress,src:sourceHost,srchost:targetID,duid:targetDN,duser:xdasOutcome,
outcome
```

Following is the message that gets generated with the above customized log:

```
Jan 23 08:49:19 host1-Latitude-7480 SSPR CEF:0|Micro Focus|SSPR|v b0
r0|AUTHENTICATE|Authentication|2| dvchost=localhost dtz=Zulu cat=USER
act=AUTHENTICATE rt=2020-01-23T03:19:19Z msg=admin
(cn\=admin,o\=novell) has authenticated reason=type\=AUTHENTICATED,
source\=LOGIN_FORM suid=admin suser=cn\=admin,o\=novell src=127.0.0.1
srchost=127.0.0.1 outcome=XDAS_OUT_SUCCESS
```

5 Click **Save changes**.

Adding a patch update

We regularly release patch updates for Self Service Password Reset that contains fixes for the product. The patch updates contain fixes for bugs and security updates. We recommend that you apply the latest patch update. The steps to install the patch update are different depending on the platform running Self Service Password Reset.

- "Adding a patch update to the Appliance" on page 163
- "Adding a patch update to Linux" on page 163
- "Adding a patch update to Windows" on page 164

Adding a patch update to the Appliance

If you are running the Self Service Password Reset appliance, the appliance notifies you that there are updates to apply. To apply the updates, see "Performing an online update" on page 172.

Ensure that you back up your configuration information before applying any updates. For more information, see "Backing up configuration information" on page 155.

Adding a patch update to Linux

If Self Service Password Reset is running on Linux platforms, use the following information to install the patch update. Self Service Password Reset is a web application. Since it is a web application, you deploy a new version of the application to add a patch update.

To add a patch update to Linux:

1 Download the most recent patch update from the Patch Finder (https://sldlogin.microfocus.com/nidp/idff/sso?id=5&sid=5&option=credential&sid=5).

2 (Conditional) If you have not deployed Self Service Password Reset, deploy the patch update as a new installation of Self Service Password Reset. For more information, see "Deploying the WAR file on Linux" in the *Self Service Password Reset 4.8 Installation Guide*.

3 (Conditional) If you have an existing installation of Self Service Password Reset, upgrade the current version to the patch update version.

   3a Back up the current configuration information. For more information, see "Backing up configuration information" on page 155.

   3b Stop the Tomcat service. In the *Tomcat_Home*/bin/ directory, execute the catalina.sh script file:

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

   3c Delete the existing sspr folder and sspr.war file from the *Tomcat_home*/webapps directory.

   3d Delete the catalina folder from the ../*apache-tomcat-xxx*/work directory.

   3e Copy the sspr.war file from the current patch update to the *Tomcat_home*/webapps directory.

   3f Restart the Tomcat service. In the *Tomcat_Home*/bin/ directory, execute the catalina.sh script file:

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

   3g Restore the backup configuration information. For more information, see "Importing configuration information" on page 155.

Adding a patch update to Windows

If Self Service Password Reset is running on Windows servers, use the following information to install the patch update. Self Service Password Reset is a web application. Since it is a web application, you deploy a new version of the application to add a patch update.

To add a patch update to Windows servers:

1 Download the most recent patch update from the Patch Finder (https://sldlogin.microfocus.com/nidp/idff/sso?id=5&sid=5&option=credential&sid=5).

2 (Conditional) If you have not deployed Self Service Password Reset, deploy the patch update as a new installation of Self Service Password Reset. For more information, see "Installing Self Service Password Reset on Windows" in the *Self Service Password Reset 4.8 Installation Guide*.

3 (Conditional) If you have an existing installation of Self Service Password Reset, upgrade the current version to the patch update version. For more information, see "Upgrading the Self Service Password Reset Appliance" in the *Self Service Password Reset 4.8 Installation Guide*.

14 Managing the Appliance

You can deploy Self Service Password Reset as an appliance. You use the appliance management console to change certain configuration settings for the appliance, such as administrative passwords for the vaadmin user and the `root` user, network settings, and certificate settings. You should perform these tasks only from the appliance management console, because native Linux tools are not aware of the configuration requirements and dependencies of the Self Service Password Reset services.

IMPORTANT: NetIQ delivers and updates the Self Service Password Reset appliance as a single unit including the operating system, the Self Service Password Reset application, and associated runtime components. NetIQ does not recommend adding any additional software components to the appliance. Any support issues that arise with customer supplied components might require removal before support issues can be resolved.

To access the appliance management console:

1. In a web browser, specify the DNS name or the IP address for the appliance with the port number 9443. For example:

   `https://10.10.10.1:9443`

   or

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

2. Specify the administrative user name and password for the appliance, then click **Sign in**.The default users are `vaadmin` and `root`.
3. Continue manage the appliance.

The appliance management console displays the following options:

- Setting administrative passwords
- Configuring network setting
- Adding additional hosts to the hosts file
- Configuring time settings
- Accessing system services
- Managing Appliance certificates
- Configuring the firewall
- Sending information to support
- Adding a field patch to the Appliance
- Performing an online update
- Performing a product upgrade
- Using the administrative commands

- Rebooting or shutting down the Appliance
- Logging out

Setting administrative passwords

Use the Administrative Passwords page to modify the passwords and SSH access permissions for the appliance administrators: the `vaadmin` user and the `root` user. You might need to modify passwords periodically in keeping with your password policy, or if you reassign responsibility for the appliance management to another person.

The `vaadmin` user can use the Administrative Passwords page to perform the following task:

- Modify the `vaadmin` user password. To change a password, you must be able to provide the old password.
- The vaadmin user automatically has permissions necessary to remotely access the appliance with SSH instead of using a VMware client. The SSH service must be enabled and running to allow SSH access.

NOTE: The SSH service is disabled and is not running by default. For information about how to start SSH on the appliance, see "Accessing system services" on page 168.

The `root` user can use the Administrative Passwords page to perform the following tasks:

- Modify the `root` user password. To change a password, you must be able to provide the old password.
- Enable or disable the `root` user SSH access to the appliance.

  When this option is selected, the `root` user is able to SSH to the appliance. If this option is deselected, only the `vaadmin` user can SSH to the appliance and the root user cannot SSH even if the `sshd` service is running.

To manage the administrative access as the `vaadmin` user:

1. Log in to the appliance management console as the `vaadmin` user.
2. Click **Administrative Passwords**.
3. Specify a new password for the `vaadmin` administrator. You must also specify the current `vaadmin` password.
4. Click **OK**.

To manage the administrative access as the `root` user:

1. Log in to the appliance management console as the `root` user.
2. Click **Administrative Passwords**.
3. Specify a new password for the `root` administrator. You must also specify the current `root` password.
4. (Optional) Select or deselect **Allow root access to SSH**.
5. Click **OK**.

Configuring network setting

Use the Network tool to configure settings for the DNS servers, search domains, gateway, and NICs for the appliance. You might need to modify these settings after the initial setup if you move the appliance VM to a new host server, or move the host server to a new domain in your network environment. You can also optionally restrict the networks that are allowed to access the appliance.

To configure network settings for the appliance:

1. Log in to the appliance management console as the `vaadmin` user.
2. Click **Network**.
3. In the **DNS Configuration** section, you can modify the DNS name servers, search domains, and gateway settings for your appliance network.

   If the **Search Domains** field is left blank, it is auto-populated with the domain of the appliance hostname. For example, if the hostname of the appliance is `ptm.mycompany.com`, the domain is auto-populated with `mycompany.com`.
4. In the **NIC Configuration** section, you can modify the IP address, hostname, and network mask of any NIC associated with the appliance.
   - **4a** Click the ID of the NIC.
   - **4b** Edit the IP address, hostname, or network mask for the selected NIC.
   - **4c** Click **OK**.
   - **4d** Repeat these steps for each NIC that you want to configure.
5. (Optional) In the **Appliance Management UI (port 9443) Access Restrictions** section, do one of the following:
   - Specify the IP address of each network for which you want to allow access to the appliance. Only the listed networks are allowed.
   - Leave this section blank to allow any network to access the appliance.

   NOTE: After you configure the appliance, changes to your appliance network environment can impact the appliance communications.
6. Click **OK**.

Adding additional hosts to the hosts file

You can add additional entries to the `hosts` file for the Self Service Password Reset appliance. You must add the entry to the `/etc/opt/novell/base/hosts.appliance` file. This is a manual process. If you try to change the host entries through any other means it will not work.

1. Access the command line console of the appliance.
2. Navigate to `/etc/opt/novell/base/hosts.appliance`.
3. Open the file in a text editor, then add the additional entries to the `hosts` file.
4. Save and then close the file.
5. Reboot the appliance to have the change take effect.

Configuring time settings

Use the Time tool to configure the Network Time Protocol (NTP) server, the geographic region, and the time zone where you have deployed the appliance.

To configure time parameters for the appliance:

1. Log in to the appliance management console as the `vaadmin` user.
2. Click **Time**.
3. Change the following time configuration options as appropriate:

   NTP server: Specify the NTP server that you want to use for time synchronization.

   Region: Select the geographic region where your appliance is located.

   Time zone: Select the time zone where your appliance is located.
4. Click **OK**.

Accessing system services

Use the System Services tool to view the status of services running on the appliance, or performs on them. System services include the following:

- SSH
- SSPR Application (Self Service Password Reset)

To access the system services page:

1. Log in to the appliance management console as the `vaadmin` user.
2. Click **System Services**.

You can start, stop, or restart any of the system services.

To start, stop, or restart a service on the appliance:

1. Click **System Services**.
2. Select the service that you want to start, stop, or restart.
3. Click **Action**, then select **Start**, **Stop**, or **Restart**.
4. Click **Close** to exit System Services.

You can change the system services to be automatic or manual.

To change the system services:

1. Click **System Services**.
2. Select the service that you want to make automatic or manual.
3. Click **Options**, then select either **Set as Automatic** or **Set as Manual**.
4. Click **Close** to exit System Services.

Managing Appliance certificates

Use the Appliance Certificates page to add and activate certificates for the appliance. You can use the digital certificate tool to create your own certificate and then have it signed by a CA, or you can use an existing certificate and key pair if you have one that you want to use.

IMPORTANT: This section is only for managing certificates for the Self Service Password Reset appliance (port 9443). To change the certificates for the Self Service Password Reset application (port 443), use the **Configuration Editor**.

The appliance ships with a self-signed digital certificate. Instead of using this self-signed certificate, It is recommended that you use a trusted server certificate that is signed by a trusted certificate authority (CA) such as VeriSign or Equifax.

Complete the following sections to change the digital certificate for your appliance:

- "Creating or signing the digital certificates" on page 169
- "Using an existing certificate and key pair" on page 170
- "Activating the certificate" on page 171

Creating or signing the digital certificates

- "Creating a new self-signed certificate" on page 169
- "Getting your certificate officially signed" on page 170

Creating a new self-signed certificate

1. Log in to the appliance management console as the `vaadmin` user.
2. Click **Appliance Certificates**.
3. In the **Key Store** drop-down list, ensure that **Web Application Certificates** is selected.
4. Click **File** > **New Certificate (Key Pair)**, then specify the following information:

   4a General

   Alias: Specify a name that you want to use to identify and manage this certificate.

   Validity (days): Specify how long you want the certificate to remain valid.

   4b Algorithm details

   Key algorithm: Select either **RSA** or **DSA**.

   Key size: Select the desired key size.

   Signature algorithm: Select the desired signature algorithm.

   4c Owner information

   Common name (CN): This must match the server name in the URL in order for browsers to accept the certificate for SSL communication.

   Organization (O): (Optional) Large organization name. For example, My Company.

Organizational unit (OU): (Optional) Small organization name, such as a department or division. For example, Purchasing.

Two-letter country code (C): (Optional) Two-letter country code. For example, US.

State or province (ST): (Optional) State or province name. For example, Utah.

City or locality (L): (Optional) City name. For example, Provo.

5 Click **OK** to create the certificate.

After the certificate is created, it is self-signed.

6 Make the certificate official, as described in "Getting your certificate officially signed" on page 170.

Getting your certificate officially signed

1 On the Appliance Certificates page, select the certificate that you just created, then click **File** > **Certificate Requests** > **Generate CSR**.

2 Complete the process of emailing your certificate to a certificate authority (CA), such as Verisign.

The CA takes your Certificate Signing Request (CSR) and generates an official certificate based on the information in the CSR. The CA then emails the new certificate and certificate chain back to you.

3 After you have received the official certificate and certificate chain from the CA:

3a Revisit the Appliance Certificates page.

3b Click **File** > **Import** > **Trusted Certificate**. Browse to the trusted certificate chain that you received from the CA, then click **OK**.

3c Select the self-signed certificate, then click **File** > **Certification Request** > **Import CA Reply**.

3d Browse to and upload the official certificate to be used to update the certificate information.

On the Appliance Certificates page, the name in the **Issuer** column for your certificate changes to the name of the CA that stamped your certificate.

4 Activate the certificate, as described in "Activating the certificate" on page 171.

Using an existing certificate and key pair

When you use an existing certificate and key pair, use a `.P12` key pair format.

1 Log in to the appliance management console as the `vaadmin` user.

2 Click **Appliance Certificates**.

3 In the **Key Store** drop-down menu, select **JVM Certificates**.

4 Click **File** > **Import** > **Trusted Certificate**. Browse to and select your existing certificate, then click **OK**.

5 Click **File** > **Import** > **Trusted Certificate**. Browse to and select your existing certificate chain for the certificate that you selected in Step 4, then click **OK**.

6 Click **File** > **Import** > **Key Pair**. Browse to and select your `.P12` key pair file, specify your password if needed, then click **OK**.

7 Continue with "Activating the certificate" on page 171.

Activating the certificate

1 On the Appliance Certificates page, in the **Key Store** drop-down menu, select **Web Application Certificates**.

2 Select the certificate that you want to make active, click **Set as Active**, then click **Yes**.

3 Verify that the certificate and the certificate chain were created correctly by selecting the certificate and clicking **View Info**.

4 When you successfully activate the certificate, click **Close** to exit the page.

Configuring the firewall

Use the Firewall page to view your current firewall configuration directly from the appliance. By default, all ports are blocked except those needed by the appliance. For example, the Login page for the appliance management console uses port 9443, so this port is open by default.

NOTE: To have a seamless experience with the appliance, ensure that you do not block the ports with your firewall settings. For more information, see "Default Ports for Self Service Password Reset" in the *Self Service Password Reset 4.8 Installation Guide*.

To view firewall settings for the appliance:

1 Log in to the appliance management console as the `vaadmin` user.

2 Click **Firewall**.

The Firewall page lists port numbers with the current status of each port number. The page is for informational purposes and is not editable.

3 Click **Close** to exit the Firewall page

Sending information to support

Use the Support tool to send configuration information to Technical Support (https://www.netiq.com/support/) by uploading files directly to FTP, or by downloading the files to your management workstation and sending them by an alternative method.

To send configuration files to technical support:

1 Log in to the appliance management console as the `vaadmin` user.

2 Click **Support**.

3 Use one of the following methods to send the appliance's configuration files to Technical Support (https://www.netiq.com/support/):
   - Select **Automatically send the configuration to Micro Focus using FTP** to initiate the FTP transfer of configuration information.
   - Select **Download and save the configuration file locally, then send it to Micro Focus manually** to download configuration information to your management workstation. You can then send the information to Technical Support (https://www.netiq.com/support/) using a method of your choice.
4 Click **OK** to complete the process.

Adding a field patch to the Appliance

Use the **Field Patch** option to add patches provided by engineering or technical support. A field patch is not a full patch and should only be used until a full patch is released. When you apply a field patch, you must disable all other updates for the appliance or the field patch can be overwritten.

To manage patch updates:

1 Create a backup of the configuration information for the appliance. For more information, see "Backing up configuration information" on page 155.
2 Log in to the appliance management console as the `vaadmin` user.
3 Click **Browse** and browse to and select the field patch file you received from engineering or technical support, then click **Open**.
4 Click **Install** and follow the prompts to install the patch.
5 (Conditional) If you need to uninstall the patch update, select the patch you want to uninstall, then click **Uninstall Latest Patch** and follow the prompts.
6 Download a log file that includes details about the patch update installation.
   6a Click **Download Log File** for the appropriate patch update.
7 Click **Close** to exit the Field Test Patch page.
8 To disable online updates and automatic updates until you apply a full patch, click **Online Updates**, then click **Schedule > Manual**, then exit out of the Field Patch page.

Performing an online update

Use the **Online Update** page to register for the online update service from the Customer Center (https://www.netiq.com/customercenter). You can install updates automatically or manually to the Self Service Password Reset appliance. You must be connected to the internet to use this feature.

If you need to manage access to the internet and your corporate policy does not allow for the Self Service Password Reset appliance to have internet access, you can still provide updates to the appliance through a local Subscription Management Tool (SMT).

A Subscription Management Tool (SMT) is a feature provided in SUSE Linux Enterprise Server 11. SMT allows you to download the updates to a single SMT server in your network that must have an internet connection. All Self Service Password Reset appliances receive their updates from this

server. For more information, see *Subscription Management Tool Guide*. To obtain the proper credentials to use the SMT server, see "Mirroring Credentials" in the *Subscription Management Tool Guide*.

NOTE: You must use SUSE Linux Enterprise Server 11 to have the updates work. The SUSE Linux Enterprise Server 12 does not support SMT updates to the Self Service Password Reset appliance.

You can disconnect the SMT server from the internet but we recommend that you connect the SMT server often to receive the operating system updates. Operating system updates occur daily. By using the SMT server you control when the updates are applied to the Self Service Password Reset appliance.

You must have the license key for Self Service Password Reset to activate the Update Channel. You obtain the license key from the Customer Center. If the key is not available, contact the Customer Center through an email from within the Customer Center (https://www.netiq.com/customercenter).

If you have clustered the Self Service Password Reset appliance, you must log in to each appliance in the cluster and add the license key to each appliance to enable updates. You can schedule updates or manually perform updates on each appliance.

To register for the online update service:

1. Log in to the appliance management console as the `vaadmin` user.
2. Click **Online Update**.
3. If the Registration dialog does not open automatically, click the **Register** tab.
4. Specify the **Service Type**:
   - Local SMT (Proceed to Step 5.)
   - Customer Center (Skip to Step 6.)
5. (Local SMT) Specify the following information for the SMT server, then continue with Step 7.
   - Hostname such as `smt.example.com`
   - (Optional) SSL certificate URL that communicates with the SMT server
   - (Optional) Namespace path of the file or directory
6. (Customer Center) Specify the following information about the Customer Center (https://www.netiq.com/customercenter) account for this Self Service Password Reset Appliance:
   - Email address of the account in Customer Center
   - Activation key (the same Full License key that you used to activate the product)
   - Allow data send (select any of the following)
     - Hardware Profile
     - Optional information
7. Click **Register**.

   Wait while the appliance registers with the service.
8. Click **OK** to dismiss the confirmation.

After you have registered the appliance, you can view a list of the needed updates, or view a list of installed updates. You can use manual or automatic options to update the appliance.

To perform other actions after registration:

- **Update now:** Click **Update Now** to trigger downloaded updates.
- **Schedule:** Configure the type of updates to download and whether toautomatically agree to the licenses.

  To schedule online update:

  1. Click the **Schedule** tab.
  2. Select a schedule for download updates (**Manual**, **Daily**, **Weekly**, **Monthly**).
- **View info:** Click **View Info** to display a list of installed and downloaded software updates.
- **Refresh:** Click **Refresh** to reload the status of updates on the appliance.

Performing a product upgrade

The difference between an product update and a product upgrade is that the product upgrades contain new features and functionality while a product update contains bug fixes. The upgrades also increase the major or minor version of the product. For example, an upgrade changes the version from 4.2.0.6 to 4.3.0.

Self Service Password Reset provides two different ways for you to upgrade the appliance. You can manually upgrade the appliance or use this option to automatically upgrade the appliance. If you choose to use this option, there are some important considerations to think about.

IMPORTANT: There are some items you must consider before performing the automated upgrade:

- You must apply the latest updates to perform the upgrade. If you do not have the latest updates applied, the upgrade fails.
- The upgrade takes twice the disk space as a new deployment of Self Service Password Reset.
- The upgrade takes an hour or longer to complete.

If you decide not to perform an automated upgrade, you can perform a manual upgrade.

The instructions for how to use both options for upgrading the appliance are in the Installation Guide. For more information, see "Upgrading the Self Service Password Reset Appliance" in the *Self Service Password Reset 4.8 Installation Guide*.

Using the administrative commands

Self Service Password Reset appliance does not allow you full access to the command line of the operating system. There are some administrative tasks that you perform from the command line. You can perform these administrative tasks by issuing the administrative commands. Here are different administrative commands you can perform.

Lock and unlock configuration

If you are using an LDAP directory to store the user accounts, and you cannot login to the LDAP directory, you can use the lock and unlock configuration options to allow you access the Self Service Password Reset Configuration Editor without authenticating to the LDAP directory. For more information, see "Configuring locked and unlocked modes" on page 177.

Delete configuration

If the Self Service Password Reset configuration become corrupted, this option allows you to delete the configuration file. If you delete the configuration file, the appliance is set back to the default configuration. It is important to ensure that you create a backup of the configuration file anytime you make configuration changes in Self Service Password Reset. If you have a backup configuration file, you can import the file to restore the appliance. For more information, see "Backing up configuration information" on page 155.

Reset HTTPS settings

Use this option to reset the HTTPS settings to the default values. You would use this option if your certificates expired.

Show version

Use this option to display the version of the appliance.

Rebooting or shutting down the Appliance

You might need to initiate a graceful shutdown or to restart the appliance for maintenance. Using the appliance management console options is preferred over using a Power Off/On option in the hypervisor's VM management tool.

1. Log in to the appliance management console as the `vaadmin` user.
2. In the upper right corner of the appliance management console, click **Reboot** or click **Shutdown**.

Logging out

For security reasons, you should sign out to exit your management session with the appliance, then close your web browser. Your session terminates automatically when you close your web browser.

To sign out of the appliance management console:

1. In the upper-right corner of the appliance management console, next to the user name, click **Logout**.
2. Close the web browser.

15 Troubleshooting Self Service Password Reset

Self Service Password Reset provides tools that check the health of your connections to LDAP directories and database to help troubleshoot connection issues. This section explains how to use the tools and how to work around known issues.

- "Configuring locked and unlocked modes" on page 177
- "Troubleshooting connections" on page 181
- "Troubleshooting Self Service Password Reset with the provided tools" on page 182
- "Accessing the configuration editor and configuration manager directly" on page 184
- "Troubleshooting user issues with Self Service Password Reset" on page 184
- "Troubleshooting the challenge set policy" on page 187
- "Troubleshooting error codes" on page 187
- "Troubleshooting Single Sign-On issue with OAuth" on page 187
- "Self Service Password Reset throws 404 error when upgrading WAR file to 4.7 version" on page 188
- "An error while upgrading the Self Service Password Reset Appliance to 4.7 version" on page 189
- "Issue with Self Service Password Reset site URL after online upgrade" on page 190
- "Server utilization reaches 100%" on page 190

Configuring locked and unlocked modes

Best practice for managing Self Service Password Reset administrators is to create an LDAP group that contains the proper administrative privileges and then add the administrators as a member of this LDAP group. This allows you to assign the LDAP policies and restrict who has access to what resource. For more information, see "Configuring the administrators module" on page 50.

Sometimes, there are circumstances when an LDAP defined Self Service Password Reset administrator cannot perform various Self Service Password Reset configuration operations. For this reason, Self Service Password Reset has two configuration modes:

Locked configuration: In this mode, configuration operations require the authentication of a Self Service Password Reset administrator, who is a member of the LDAP Self Service Password Reset administration group.

Unlocked configuration: In this mode, Self Service Password Reset allows:

- Configuration operations without an LDAP authentication from the administration group.

- End-user services are unavailable such as **Change Password**, **Setup Security Questions**, and **My Account** modules.
- Self Service Password Reset administrative users can perform additional administrative operations such as importing the Self Service Password Reset configuration file.

IMPORTANT: While in production use, and **accessible by untrusted network entities**, you must always keep Self Service Password Reset in the locked configuration mode to preserve the security integrity of Self Service Password Reset.

Changing the configuration mode from a locked configuration mode to an unlocked configuration mode is a security sensitive operation, and must not be accessible by standard Self Service Password Reset access channels. Rather, Self Service Password Reset implements the unlock configuration operation using various side-band channels available for each deployment type of Self Service Password Reset.

- "When to run Self Service Password Reset in the unlocked configuration mode" on page 178
- "How to lock and unlock the Self Service Password Reset configuration" on page 179

When to run Self Service Password Reset in the unlocked configuration mode

There are two uses cases for running Self Service Password Reset in the unlocked mode. Those use cases are: you have lost the configuration password or the connection to the LDAP directory became corrupt.

Lost configuration password

During the Self Service Password Reset installation, you specify a **Configuration Password**. Self Service Password Reset requires the **Configuration Password** prior to any modifications of its configuration. In the unlocked configuration mode, it is possible to delete the current Self Service Password Reset configuration, and then reconfigure Self Service Password Reset as if it is a new installation, including specifying a new **Configuration Password**.

Corrupted configuration for the LDAP Connection

Self Service Password Reset interfaces with LDAP directories that contain your users. If the LDAP directory becomes unavailable or corrupted you must run Self Service Password Reset in the unlocked configuration mode to fix the connection. Also, if you modify the Self Service Password Reset configuration for the LDAP connection in such a way that you severe the connection, you must run Self Service Password Reset in the unlocked configuration mode.

How to lock and unlock the Self Service Password Reset configuration

Each platform deployment of Self Service Password Reset requires different steps to lock or unlock the Self Service Password Reset configuration. Use the platform-specific steps for your environment to unlock the configuration.

- "How to lock and unlock the Self Service Password Reset configuration for the Appliance" on page 179
- "How to lock and unlock the Self Service Password Reset configuration on Windows" on page 180
- "How to lock and unlock the Self Service Password Reset configuration on Linux" on page 181

How to lock and unlock the Self Service Password Reset configuration for the Appliance

Use the following information if you have deployed the Self Service Password Reset appliance to lock and unlock the Self Service Password Reset configuration.

The Self Service Password Reset appliance has two user interface ports:

- **Port 443:** The public interface port for the Self Service Password Reset application.
- **Port 9443:** The private interface for maintenance of Self Service Password Reset.

Only the appliance version of Self Service Password Reset uses the port 9443 interface. We recommend that only administrators access this interface and that you protect this interface behind a firewall to limit access to administrators. This interface allows for the overall appliance maintenance. It also provides a convenient side-band interface to specific Self Service Password Reset administrative operations.

To lock or unlock the Self Service Password Reset configuration for the appliance:

1. Log in to the appliance administration interface as the appliance `root` user.

   `https://dns-name-sspr-appliance:9443`

2. Click **Administrative Commands**.
3. Specify the appropriate command.

   Lock configuration: Prevents anyone from editing the configuration without an LDAP authentication.

   Unlock configuration: Allows anyone to edit the configuration without an LDAP authentication.

   Delete configuration: Deletes the product configuration of Self Service Password Reset, if it exists.

   Reset HTTPS settings: Resets the HTTPS settings to the default values.

   Show version: Displays the current Self Service Password Reset product version.
4. Ensure to lock the configuration for normal Self Service Password Reset functionality.

When the appliance is in the unlocked configuration mode, locking the Self Service Password Reset configuration through the appliance administrative commands accomplishes the same this as clicking **Restrict Configuration** in the **Configuration Manager** `https://dns-name-appliance/sspr`.

How to lock and unlock the Self Service Password Reset configuration on Windows

Use the following information if you have deployed Self Service Password Reset on Windows using the `.msi` file.

The Self Service Password Reset version for Windows implements a `.bat` command-line utility to facilitate various Self Service Password Reset administrative operations. You must have access to the Windows file system where you installed Self Service Password Reset to access and use the `.bat` command-line utility.

To lock and unlock the Self Service Password Reset configuration on Windows:

1. Log in to the Windows server as an administrator with file system access to where you installed Self Service Password Reset.
2. Access the `.bat` file here:

   `x:\ProgramFiles\NetIQ Self Service Password Reset\sspr.cmd`

3. From the command line, enter **sspr.cmd**.
4. Specify the appropriate commands:

   help: Lists all available commands from the `.bat` file.

   ConfigDelete: Deletes the Self Service Password Reset configuration file.

   ConfigLock: Locks the Self Service Password Reset configuration file, and prevents administrators from editing the configuration file without LDAP authentication.

   ConfigResetHttps: Resets the Self Service Password Reset HTTPS settings to the default values.

   ConfigSetPassword *password*]: Sets the configuration password for Self Service Password Reset.

   ConfigUnlock: Unlocks the Self Service Password Reset configuration file and allows administrators to edit the configuration file without LDAP authentication.

   Version: Lists the current version of the Self Service Password Reset deployment.

   Exit: Exits the command line shell for the `.bat` file.

5. Ensure to lock the configuration for normal Self Service Password Reset product activity.

When the Windows version of Self Service Password Reset configuration is in the unlocked configuration mode, locking the Self Service Password Reset configuration with the `.bat` file accomplishes the same this as clicking **Restrict Configuration** in the **Configuration Manager** `https://dns-name-appliance/sspr`.

How to lock and unlock the Self Service Password Reset configuration on Linux

Use the following information if you have deployed Self Service Password Reset on Linux using the WAR file.

The Linux version of Self Service Password Reset implements a shell script command-line utility to facilitate various Self Service Password Reset administrative operations. You must have file system access to where you installed Self Service Password Reset to run the shell script command-line utility.

To lock or unlock the Self Service Password Reset configuration on Linux:

1. Log in to the Linux server as a user with file system access to where you installed Self Service Password Reset.
2. Access the shell script command-line utility here:

   `/Tomcat_home/webapps/sspr/WEB-INF/command.sh`

3. Specify the appropriate command:

   Lock: `./command.sh configLock`

   Unlock: `./command.sh configUnlock`

   NOTE: Ensure that the command.sh shell script has executable permissions.

   If you do not have the execute permission, add it using the below chmod command:

   `chmod u+x command.sh`

   ---

4. Ensure to lock the configuration for normal Self Service Password Reset product activity.

When the Linux version of Self Service Password Reset configuration is in the unlocked configuration mode, locking the Self Service Password Reset configuration with the shell script command-line utility accomplishes the same this as clicking **Restrict Configuration** in the **Configuration Manager** `https://dns-name-appliance/sspr`.

Troubleshooting connections

Self Service Password Reset provides tools to help troubleshoot connections to the LDAP directories and the external databases. There are also log files you can download and send to technical support for further help.

To troubleshoot connections:

1. Log in to Self Service Password Reset at `https://dns-name/sspr` as an administrator.
2. Click **Administration**.
3. Click the **Health** tab, then review the health for the following components:

   Configuration

   Displays the health of the configuration of Self Service Password Reset. If there is something configured incorrectly, the **Configuration** entry changes color.

LDAP

Displays that Self Service Password Reset can connect to all configured LDAP servers. If there is a problem with the connection, the **LDAP** entry changes color.

Configuration

Displays that the LDAP test user account can connect to the LDAP directory and that the password policy functions. If there is a problem with the connection or the password policy, the **LDAP** entry changes color.

LocalDB/External Database

Displays that Self Service Password Reset can connect to the local database or the external database. If there is a problem with the connection, the **LocalDB** or **External Database** entry changes color.

NOTE: Self Service Password Reset provides the local database for testing purposes only. For production environments, you must use an external database or an LDAP directory.

The local database storage limit is 102,400 bytes (1024 * 100 bytes).

Platform

Java platform is operating normally. If there is something wrong with the Java platform, the Platform entry changes color.

4 Click **Troubleshooting Bundle** and download the file to obtains logs files and other information.

5 Click **Home** to exit the **Configuration Manager**.

Troubleshooting Self Service Password Reset with the provided tools

Use the following information to troubleshoot the tools provided with Self Service Password Reset.

- "Troubleshooting with the dashboard" on page 182
- "An unexpected LDAP error for the test user in the configuration manager" on page 183
- "One or more responses is not correct error for users on mobile devices" on page 183
- "No automated emails from the SMTP server" on page 184

Troubleshooting with the dashboard

Self Service Password Reset provides a Dashboard to help you see the health of your system and troubleshoot many different issues. Use the Dashboard to help understand URL references, to see if tokens are not working, to see the health of the system, and many more things. For more information, see "Using the dashboard" on page 20.

An unexpected LDAP error for the test user in the configuration manager

Issue: When you open the Configuration Manager page, Self Service Password Reset displays a warning message for LDAP stating LDAP Test User error. This issue occurs because Self Service Password Reset generates a random password for the test user and Active Directory does not allow frequent changes to the test user password. This might result in new user registration failure.

Workaround: This happens when you have configured a user distinguished name (dn) for a test user during the Self Service Password Reset configuration and specified **TESTUSER** in the **Password Policy Template** setting, under **New User Registration**. As you require different password policies for different profiles, it is recommended that you skip specifying the test user dn during Self Service Password Reset configuration. You can provide a user dn, whose password policy can be used for a specific profile, by using the **Password Policy Template** setting.

This issue can also happen if you have not specified any test user during the Self Service Password Reset configuration and the **Password Policy Template** setting is set as **TESTUSER**. You must specify the user dn in the **Password Policy Template** setting to resolve this issue.

One or more responses is not correct error for users on mobile devices

Issue: Mobile users see the error of `one or more responses is not correct` when using Self Service Password Reset.

Solution: This error is caused by time not being in synchronized in your network. You must synchronize the time between the LDAP and the Self Service Password Reset servers by using the same NTP source.

The error occurs in the following conditions:

- The time (in seconds) set in the LDAP server, the Self Service Password Reset server, and the mobile device are not synchronized
- A difference of more than 5 seconds occurs between the LDAP server and the Self Service Password Reset server
- A difference of more than 5 seconds occurs between the Self Service Password Reset server and the mobile device
- A difference of more than 5 seconds occurs between the LDAP server and the mobile device

To use the same NTP source:

1. Log in to the appliance administration tool.
2. Use the **Time** settings in the appliance management tool to specify the same NTP source as your LDAP servers are using. For more information, see "Configuring time settings" on page 168.
3. Ensure that time is synchronized on the LDAP servers and they are using the same NTP time source. For more information, see:
   - **Active Directory:** Refer the *How the Windows Time Service Works* section in the *Microsoft Documentation*.
   - **eDirectory:** "Synchronizing Network Time" in the *NetIQ eDirectory Administration Guide*

No automated emails from the SMTP server

Issue: Users do not receive any automated emails from the SMTP server even after you have configured Self Service Password Reset to send emails. You receive the error `Unable to send Email: No From Address` in the logs. Self Service Password Reset displays this message only when it is installed on a SUSE Linux Enterprise Server and the computer name is not defined in the `/etc/hosts` file.

Solution: On the SUSE Linux Enterprise Server where Self Service Password Reset is installed, include the computer name in the `/etc/hosts` file. Replace `127.0.0.1 localhost` with `127.0.0.1` *`name of the computer`* `localhost`.

Accessing the configuration editor and configuration manager directly

Sometimes an installation might not complete or you cannot authenticate to the LDAP directory, but you must have access to the Configuration Editor and Configuration Manager to make Self Service Password Reset functional. Self Service Password Reset provides a way to access these tools directly without authenticating.

Use the following URLs to access the tools:

Configuration Editor

```
http://Self-Service-Password-Reset-IP-Address:port/sspr/private/
config/ConfigEditor
```

Configuration Manager

```
http://Self-Service-Password-Reset-IP-Address:port/sspr/private/
config/ConfigManager
```

Troubleshooting user issues with Self Service Password Reset

Use the following information to troubleshoot users' issue when using Self Service Password Reset.

- "Obtaining the user debug information" on page 185
- "Users in Active Directory see delays in accessing the user website" on page 185
- "Users did not complete the forgotten password process" on page 186
- "Helping users change the default language of Self Service Password Reset" on page 186
- "How to enable Windows desktop to support forgotten password reset" on page 186
- "How to make Self Service Password Reset honor the Active Directory password history policy" on page 187

Obtaining the user debug information

Self Service Password Reset provides a tool that allows you to see a list of detailed information about a user to help troubleshoot many different issues. The User Debug tool displays the following information about a specific user account:

- Profiles
- Assigned modules
- Permissions
- Password policy defined in Self Service Password Reset
- Password policy defined in the LDAP directory
- Where the response information is stored
- Challenge profile

This information helps you troubleshoot when users cannot log in or when users do not see the modules you have assigned to them.

To access the user debug tool:

1. Log in to Self Service Password Reset at `https://dns-name/sspr` as an administrator.
2. Click the **Administration** module.
3. Click **More Options > User Debug**.
4. Specify the name of the user account you want to debug.
5. View the information about the user to help troubleshoot issues.
6. (Optional) Click **Download** to download a JSON file with the information to give to technical support.

Technical support might ask for this information to help troubleshoot issues. The troubleshooting bundle that you download for support contains a debug report for a couple of the last users that logged into Self Service Password Reset.

Users in Active Directory see delays in accessing the user website

Issue: When the LDAP identity source is Active Directory, sometimes users see a delay when accessing the user website for Self Service Password Reset.

Solution: One of the major performance issues in an Active Directory network is the reverse DNS resolution. Disable **Settings > Security > Application Security > Enable Reverse DNS**. If the performance increases, then there are DNS issues in your network you must resolve to enable the reverse DNS resolution again.

If turning off the reverse DNS resolution does not work, access the logs and look at the timestamps and ensure time is synchronized between your Active Directory servers and the server running the Self Service Password Reset application.

Users did not complete the forgotten password process

Issue: A user started the forgotten password process and did not complete the process. The user cannot log in to Self Service Password Reset any longer.

Solution: When a user starts the password change process by clicking **Forgotten password**, a random password is generated and if the user cancels the process without completing it, the user cannot use the old password. This happens because Self Service Password Reset recognizes the random password that was created when the user clicked on **Forgotten password**.

To resolve this issue perform the following:

- For Active Directory, you can enable the **Use Proxy When Password Forgotten** setting in the Configuration Editor under **LDAP** > **LDAP Settings** > **Microsoft Active Directory**.
- For eDirectory and Oracle Directory Server, have the user start the forgotten password process again and complete the process. The forgotten password process forces the users to reset their passwords.

Helping users change the default language of Self Service Password Reset

There are two different options for you to have the users change the default language. The first option allows the users to change the default language and the second option is that you provide a URL that automatically displays the desired language.

- Users click language option at the bottom of the Self Service Password Reset screen and select the desired locale. The language option displays the language that the page is currently using.
- As an administrator, you can override the default language through the locale parameter by using a link to Self Service Password Reset. For example, `http://sspr.example.com/sspr/?locale=sv`.

This sets the locale to Swedish and overrides the browser locale settings.

How to enable Windows desktop to support forgotten password reset

Integration of Self Service Password Reset with Novell Client Login Extension (CLE) enables Windows desktop to support forgotten password reset.

CLE facilitates password self-service by adding a link to the Microsoft Credential Provider (MSCP), and Microsoft GINA login clients. When users click the **Forgot Password** link in their login client, CLE launches a restricted browser to access the Password Self-Service feature on the login clients. For more information about how to integrate CLE with Self Service Password Reset, see Client Login Extension User Guide.

How to make Self Service Password Reset honor the Active Directory password history policy

Forgotten Password recovery or reset is generally performed by using a proxy or administrator's account in Self Service Password Reset. However, you can configure it to use the user's account while setting the forgotten password by disabling **Use Proxy When Password Forgotten** in the Configuration Editor under **LDAP**> **LDAP Settings** > **Microsoft Active Directory**. In this scenario, the Active Directory policy is disabled while changing the password.

However, this does result in a temporary password being set on the user's account just before they set a new password. This can cause issues if there is a minimum lifetime set for the password policy.

Troubleshooting the challenge set policy

There was a change made to the challenge set policy options when Self Service Password Reset 3.3 was released. The changes impact how you manage the challenge set policy options. The changes are to the following options:

- Word List (dictionary) checks answers
- eDirectory Challenge Set Minimum Randoms During Setup
- eDirectory Challenge Set Maximum Question Characters in Answer

With the Self Service Password Reset-defined challenge sets, these policy options have been changed from per-policy settings to per-challenge policies. If these policy settings were previously modified from their defaults, administrators must reapply the appropriate settings to each challenge question in the Configuration Editor of Self Service Password Reset 3.3 or above. The upgrade process does not migrate the old settings.

In the case of the eDirectory and NMAS defined challenge sets (Challenge Sets defined and managed using iManager), Self Service Password Reset 3.2 applied these policy settings based on their values in the Self Service Password Reset defined challenge set policies, often resulting in confusing policy assignments for users. As of Self Service Password Reset 3.3, this process has been changed to use eDirectory specific policy settings. The new settings at **LDAP** > **LDAP Settings** > **NetIQ eDirectory** > **eDirectory Challenge Sets** are applied to all challenge set policies read from eDirectory. Administrators should review these settings to ensure they are appropriate for their environment.

Troubleshooting error codes

Self Service Password Reset contains the error codes in the internal REST documentation located here `https://SSPR-IP-ADDRESS/sspr/public/reference/tables.jsp#error`. The REST documentation is also available on the documentation website.

Troubleshooting Single Sign-On issue with OAuth

Issue: Self Service Password Reset fails to create a Single Sign-On experience using OAuth.

Reason: This issue may occur due to several reasons. The exact solution depends on the Identity Provider used or the SSPR/OAuth configuration.

However, if you find the following error message in the SSPR logs, it may be due to an incorrect HTTP method used in the OAuth userinfo request to the Identity server:

```
2022-10-10T18:26:58Z, DEBUG, http.PwmResponse, {10083} forcing logout due
to error 5071 ERROR_OAUTH_ERROR (unexpected HTTP status code (400) during
OAuth userinfo request to https://sso.fed.dev.aws.swacorp.com/idp/
userinfo.openid) [10.9.136.83]
```

```
2022-10-10T18:26:58Z, ERROR, http.PwmResponse, {10083} 5071
ERROR_OAUTH_ERROR (unexpected HTTP status code (400) during OAuth userinfo
request to https://sso.fed.dev.aws.swacorp.com/idp/userinfo.openid)
[10.9.136.83]
```

```
2022-10-10T18:26:58Z, FATAL, servlet.AbstractPwmServlet, {10083}
unexpected error: 5071 ERROR_OAUTH_ERROR (unexpected HTTP status code (400)
during OAuth userinfo request to https://sso.fed.dev.aws.swacorp.com/idp/
userinfo.openid) [10.9.136.83]
```

```
2022-10-10T18:26:58Z, TRACE, client.PwmHttpClient, {10083} received
response (id=102) in 158ms: HTTP response status 400 Bad Request
[10.9.136.83]
```

Solution: Ensure to use the correct HTTP method (GET or POST) is used to make the OAuth UserInfo request to the Identity Provider. To select the HTTP method, navigate to **Settings > Single Sign On (SSO) Client > OAuth > > OAuth Profile / UserInfo Service Method Type**.

Self Service Password Reset throws 404 error when upgrading WAR file to 4.7 version

When you attempt to deploy the Self Service Password Reset 4.7 WAR file on the Java version below 11.x:

- The following error is displayed:

- Self Service Password Reset 4.7 does not work as expected.
- Self Service Password Reset logs display the below error:

  ```
  Log 1:: catalina.out31-Jul-2023 07:50:37.577 SEVERE [main]
  org.apache.catalina.core.StandardContext.startInternal One or more
  listeners failed to start. Full details will be found in the appropriate
  ```

```
container log file31-Jul-2023 07:50:37.581 SEVERE [main]
org.apache.catalina.core.StandardContext.startInternal Context [/sspr]
startup failed due to previous errors
```

```
Log 2:: localhost.yyyy-mm-dd.log
java.lang.UnsupportedClassVersionError: password/pwm/http/
HttpEventManager has been compiled by a more recent version of the Java
Runtime
```

Perform the following steps to resolve this issue:

1. Install the required version of Java and Tomcat. For more information on how to install Java and Tomcat, see Prerequisites for deploying the WAR file in the Self Service Password Reset 4.8 Installation Guide.
2. Upgrade the Self Service Password Reset WAR deployment. For detailed procedure, see Upgrading Self Service Password Reset on Linux in the Self Service Password Reset 4.8 Installation Guide.

An error while upgrading the Self Service Password Reset Appliance to 4.7 version

Issue: While upgrading the SSPR appliance to 4.7 version, the below error is displayed:

```
The Update process has reported a warning or error. Review the returned
text below:
```

Workaround: This issue may occur due to the `xorg-x11` rpm package.

To check whether the problem is caused because of `xorg-x11` rpm package or not, run the below command in the terminal and try to upgrade from the user interface:

```
tail -f /var/log/zypper.log
```

If the above rpm package is causing the issue, then perform the below steps to resolve this issue:

1. Run the following command:

   ```
   zypper -n remove xorg-x11-server-{version that is causing issue}
   ```

   NOTE: While removing the `xorg-x11` rpm package, the `yast2-vabase-vainit` package is being removed automatically.

2. Run the command to install the latest version of this rpm package:

   ```
   zypper -n install xorg-x11-server-*
   ```

3. Add the removed package by using the below command:

   ```
   zypper in yast2-vabase-vainit
   ```

4. Make sure to select the below solution always:

   ```
   Solution 2: break yast2-vabase-vainit-15.1.2-33.1.noarch by ignoring
   some of its dependencies.
   ```

Issue with Self Service Password Reset site URL after online upgrade

Issue: After upgrading the Self Service Password Reset, the Self Service Password Reset site URL fails to load.

Workaround: This issue may occur if the docker engine is not running.

To check whether docker is the cause of this issue, run the below command in the terminal:

```
docker info
```

Verify whether you encounter the following error or not:

```
ERROR: Cannot connect to the Docker daemon at unix:///var/run/docker.sock.
Is the docker daemon running?
```

If the above error message is displayed, perform the below steps to resolve this issue:

1. Run the following command:

   ```
   vi /usr/lib/systemd/system/docker.service.d/custom.conf
   ```

2. Go to insert mode and add the below details in the `custom.conf` file:

   ```
   [Service]
   ExecStart=
   ExecStart=/usr/bin/dockerd --storage-driver=overlay2
   ```

3. Save this file.
4. Reboot the system.

Server utilization reaches 100%

Issue: When using the word list, the server utilization reaches 100%.

Workaround: This issue may occur due to the word list URL, which is configured in the configuration editor.

To resolve this issue, perform the following:

1. Log in to Self Service Password Reset at `https://dns-name/sspr as an administrator`.
2. In the toolbar, click your name.
3. Click **Configuration Editor**.
4. Navigate to **Settings > Word List > Word List File URL**.
5. Remove the URL of a file containing a word list.
6. In the toolbar, click **Save changes**.
7. Perform the steps mentioned in Using the user interface under Uploading the word list.