# Self Service Password Reset 4.1

## Administration Guide

**April 2017**

NetIQ

## Legal Notice

# Contents

# 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.

**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).

# About NetIQ Corporation

We are a global, enterprise software company, with a focus on the three persistent challenges in your environment: change, complexity, and risk—and how we can help you control them.

## Our Viewpoint

**Adapting to change and managing complexity and risk are nothing new**

In fact, of all the challenges you face, these are perhaps the most prominent variables that deny you the control you need to securely measure, monitor, and manage your physical, virtual, and cloud computing environments.

**Enabling critical business services, better and faster**

We believe that providing as much control as possible to IT organizations is the only way to enable timelier and cost effective delivery of services. Persistent pressures like change and complexity will only continue to increase as organizations continue to change and the technologies needed to manage them become inherently more complex.

## Our Philosophy

**Selling intelligent solutions, not just software**

In order to provide reliable control, we first make sure we understand the real-world scenarios in which IT organizations like yours operate — day in and day out. That's the only way we can develop practical, intelligent IT solutions that successfully yield proven, measurable results. And that's so much more rewarding than simply selling software.

**Driving your success is our passion**

We place your success at the heart of how we do business. From product inception to deployment, we understand that you need IT solutions that work well and integrate seamlessly with your existing investments; you need ongoing support and training post-deployment; and you need someone that is truly easy to work with — for a change. Ultimately, when you succeed, we all succeed.

## Our Solutions

- Identity & Access Governance
- Access Management
- Security Management
- Systems & Application Management
- Workload Management
- Service Management

# Contacting Sales Support

For questions about products, pricing, and capabilities, contact your local partner. If you cannot contact your partner, contact our Sales Support team.

| | |
|---|---|
| **Worldwide:** | www.netiq.com/about_netiq/officelocations.asp |
| **United States and Canada:** | 1-888-323-6768 |
| **Email:** | info@netiq.com |
| **Website:** | www.netiq.com |

# Contacting Technical Support

For specific product issues, contact our Technical Support team.

| | |
|---|---|
| **Worldwide:** | www.netiq.com/support/contactinfo.asp |
| **North and South America:** | 1-713-418-5555 |
| **Europe, Middle East, and Africa:** | +353 (0) 91-782 677 |
| **Email:** | support@netiq.com |
| **Website:** | www.netiq.com/support |

# Contacting Documentation Support

Our goal is to provide documentation that meets your needs. The documentation for this product is available on the NetIQ website in HTML and PDF formats on a page that does not require you to log in. If you have suggestions for documentation improvements, click **Add Comment** at the bottom of any page in the HTML version of the documentation posted at www.netiq.com/documentation. You can also email Documentation-Feedback@netiq.com. We value your input and look forward to hearing from you.

# Contacting the Online User Community

NetIQ Communities, the NetIQ online community, is a collaborative network connecting you to your peers and NetIQ experts. By providing more immediate information, useful links to helpful resources, and access to NetIQ experts, NetIQ Communities helps ensure you are mastering the knowledge you need to realize the full potential of IT investments upon which you rely. For more information, visit http://community.netiq.com.

# 1 Self Service Password Reset Overview

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

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

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

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


- "Self Service Password Reset Key Features" on page 13
- "Self Service Password Reset Architecture" on page 14
- "Understanding Challenge-Response Storage Methods" on page 15


## Self Service Password Reset Key Features

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

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

- **Simplify Help Desk Support:** The Help Desk Module simplifies administrative tasks, such as resetting passwords, clearing intruder lockout, unlocking user accounts, and debugging user information.
- **Create Password Policies:** Administrators can use password policies to enforce restrictions on the types of passwords that users can create.
- **Generate Usage and Lockout Reports:** Administrators can generate reports for intruder lockout, daily usage statistics, and online log information for debugging purposes.
- **Supports Localization:** Self Service Password Reset provides an easy way to add new languages. Self Service Password Reset provides default localization support for English, Catalan, Chinese Simplified, Chinese Traditional, Danish, Dutch, French, German, Italian, Japanese, Polish, Portuguese (Brazilian), Russian, Spanish, and Swedish.
- **Easily Customized:** Administrators can easily customize Self Service Password Reset to integrate with external web authentication methods as well as integrate with 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 15, 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.

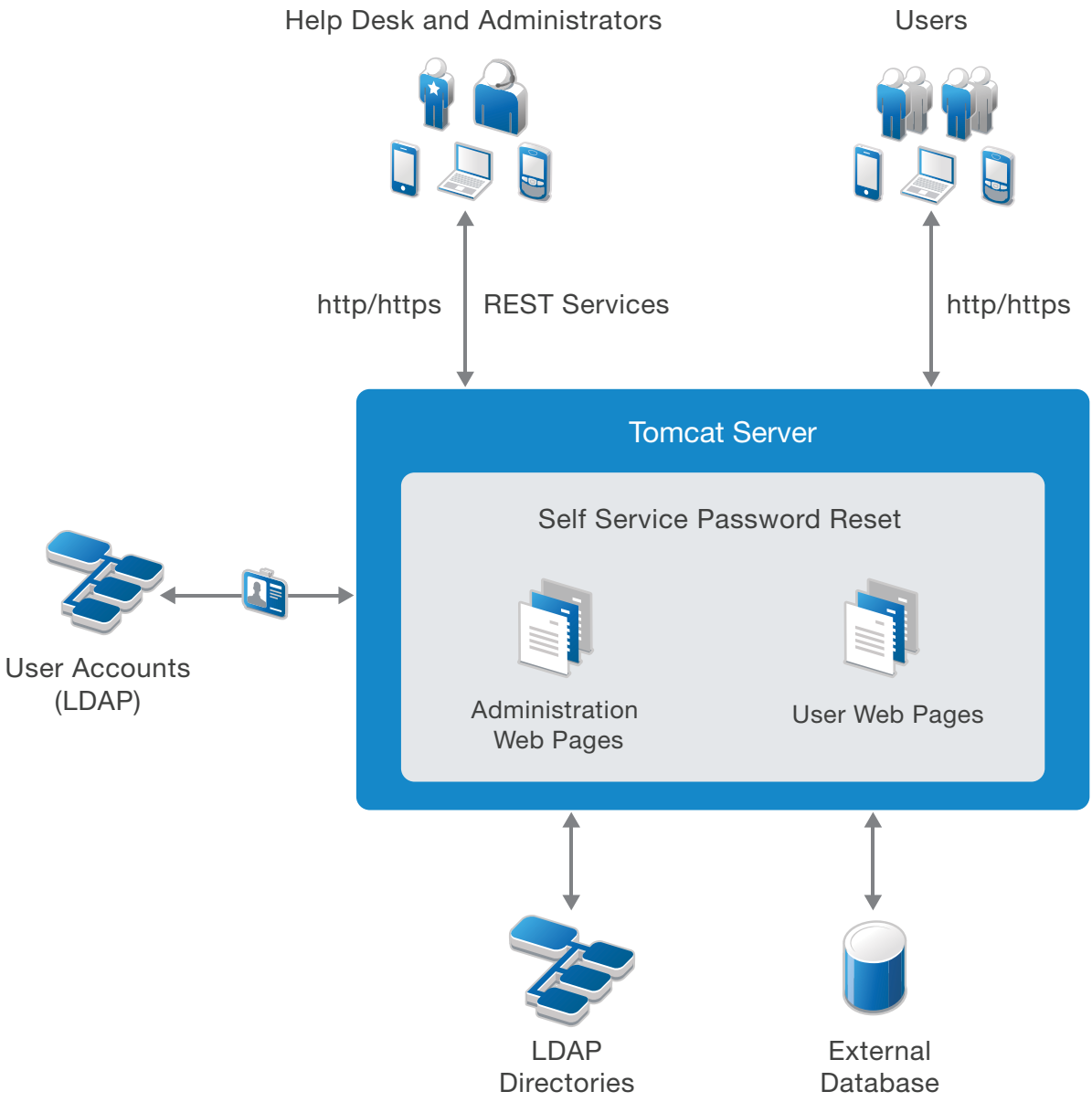
---

**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 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.

---

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 PBKDF2WithHmacSHA1 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 13, “Managing the Appliance,” on page 131.

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

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.
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 149.

# 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 4.1 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 30.
- **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.

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 149.

# 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 126.

**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 123.

**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 146.

**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.

**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

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



### Configuring Application Settings

These setting help you define the URL your users access, what happens to users after they log out, and other similar 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. Configure the following fields:

   **Site URL**

   Specify the URL to access Self Service Password Reset. The system uses this URL in emails and other user communications. For example, `https://password.example.com/sspr`.

   Include the context path in the URL. For example, `/SSPR`.

   If blank, the system attempts to auto-detect the URL, however, some network configurations prevent Self Service Password Reset from accurately determining the URL.

**Forward URL**

After completing any activity, which does not need a logout, users are forwarded to this URL.

You can override this URL for any user session by adding a `forwardURL` parameter to the HTTP request. If blank, the system forwards the user to the application menu.

**Logout URL**

Specify a URL that Self Service Password Reset redirects users to after logout. If the user accesses the site through a web authentication gateway, configure this URL to match the gateway's logout URL to prevent authentication errors, intruder lockouts, and other issues.

You can set Logout URL to any relative or absolute URL. When the user's browser requests this URL, the Self Service Password Reset session already is invalidated.

You can override this URL for any user session by adding a `logoutURL` parameter to any HTTP request during the session.

**Home URL**

Specify the URL to redirect users to upon clicking the home button. If blank, the home button returns the user to the application context URL.

**Instance Name**

Specify the name of this application instance. If blank, the system uses a persistent, randomly generated value. The recommended value is blank.

**Idle Timeout Seconds**

Specify the duration of an authenticated session in seconds after which the session times out.

**Hide Configuration Health Warnings**

Enable this option to hide health warnings about configuration issues from the health status monitors.

**HTTP Proxy**

Specify the URL of the HTTP proxy server. If you do not provide a value, then the system does not use a proxy server.

For an HTTP proxy server, use the `http://serverame:3128` format.

For an authenticated proxy server, use the `http://username:password@servername:3128` format.

**App Property Overrides**

---

**IMPORTANT:** Use this setting only when a technical support expert asks you to change the properties of the application.

---

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

# 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 simply 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 Configure the following fields:

**Locales (Languages) and Flags**

Select the appropriate localizations for your users to use. The table displays the list of available locales. The code is in two parts separated by two colons. The first part is the browser locale code and the second part is the ISO country code. The flag value is the ISO code.

**Locales Cookie Age**

Specify the duration of time to remember a user's locale preferences. Anytime Self Service Password Reset overrides a browser's default locale setting, it stores a cookie in the browser remembering that setting for the duration of this setting.

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.

**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 Configure the following fields:

**Login Session Mode**

Select the mode Self Service Password Reset uses to manage the login session state. Local mode is the most secure and reliable, but it does not allow for server fail-over.

**Module Session Mode**

Select the mode Self Service Password Reset uses to manage the module session state. Local mode is the most secure and reliable, but it does not allow for server fail-over.

6 In the toolbar, 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 26


## 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 Configuration Editor 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 and 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 the Application" on page 27
- "Configuring Web Security" on page 28


## Configuring Security for the Application

The following settings help increase the security for Self Service Password Reset.

**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 settings:

**Security Key**

The system uses a security key for tokens and other crypto functions. This setting is applicable if you have configured **Crypto Token Storage Method**.

You must set a random security value for the tokens to function.

Select **Set Password** to configure. This value must be at least 32 characters. The longer and more random this value, the more secure it is. If multiple instances are in use, you should configure each instance with the same value.

**Enable Reverse DNS**

If you set this option to true, the system uses its reverse DNS to record the hostname of the client. In some cases, this can cause performance issues so you can disable it if it is not required.

**Show Detailed Error Message**

Select this option to show detailed error messages. This setting is useful for administrators especially during configuration.

**Maximum Session Duration**

The maximum duration of a session (in seconds). Having a maximum session lifetime prevents certain types of long-term session fixation attacks.

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

# Configuring Web Security

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 settings:

**Enable Back Button Detection**

Select this option to detect the use of the back button or other browser navigation irregularities. This option prevents duplicate HTTP form submissions.

**Enable Form Nonce**

Select this option to ask for a form nonce (a unique key) for each form in Self Service Password Reset to prevent certain types of cross-site scripting (XSS) attacks.

**Sticky Session Verification**

If you enable this option, browser sessions are verified using an HTTP redirect and verification code. This verification proves that the browser can correctly establish a session with the server. Verification proves the browser either supports cookies or URL sessions (if enabled) and the communication channel between browser and application server is 'sticky' when there are multiple server instances. Additionally, it helps prevent some types of XSS attacks.

The pre-load browser cache shows a “please wait” screen to the user during the verification. This has the added benefit that many of the HTTP resources (Javascript, CSS, images, and so forth) are “pre-cached” by the browser before any actual pages are loaded.

**Disallowed HTTP Inputs**

Specify the input value. If any input value (on any HTTP parameter) matches these patterns, the matching portion is stripped from the input.

**Require HTTPS**

Enable this option to require HTTPS (instead of cleartext HTTP) traffic to the Self Service Password Reset server. While non-secure connections are useful during testing, production servers must always have this setting enabled. By default, this setting is disabled to simplify the configuration of Self Service Password Reset.

**Use X-Forwarded-For Header**

Use the X-Forwarded-For HTTP header value as the client IP address instead of the source IP address of the HTTP connection. X-Forwarded-For header is typically added by upstream proxies or firewalls and is a reliable way to identify the user's source IP address.

**Allow Roaming Source Network Address**

Select this check box to allow a single HTTP session to be accessed from different source IP addresses. Some load balancing and proxy network infrastructures need this setting, but in most cases, you must deselect this option.

**Required HTTP Headers**

Specify the required HTTP header name and value pairs. If specified, any HTTP request sent to the server must have these headers. This feature is useful if you have a security gateway and want to allow sessions from the gateway.

The format of this setting must be `name=value`.

**Permitted IP Network Addresses**

Specify the IP address ranges that permits only the connections that originated from those addresses. If you do no specify a value, the system permits any source address.

**Page Leave Notice Timeout**

When a user navigates away from any page, the server receives a notice. The next time a user requests a page, the system checks the timeout to determine if the last page leave time was greater than the timeout and if so, the system invalidates the user's session. This has the effect of logging out users that navigate away from the application without explicitly logging out. Specify 0 to disable this feature.

**Prevent HTML Framing**

Deselect this option to allow users to view Self Service Password Reset in an inline frame for any application that includes the iFrame HTML source code.

If you select this option, the specified iFrame does not include Self Service Password Reset for the application.

**Redirect Whitelist**

Specify the list of URL fragments. These URL fragments are allowed for URL forwarding. In an application, you can provide a link to redirect the user to a particular web page with the URL fragment that is defined in the whitelist. The URL forwarding follows the criteria of:

- The forwarding URL from a web page must match the complete URL fragment that is listed in the whitelist.
- The forwarding URL is decoded and processed before it is matched against the whitelist.
- The forwarding URL must have the fragment with the same spelling, wildcards, and case, as it is mentioned in the URL fragments listed in the whitelist.
- If a fragment has the prefix regex, the remaining part of the fragment is treated as a regular expression and it 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.

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

# Importing Certificates to Create an HTTPS Connection to Browsers

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. Configure the following settings:

   **HTTPS Private Key & Certificate**

   Import the X.509 certificate that you generated.

   **TLS Protocols**

   Select one or more TLS protocols that the certificate supports. Changes to this setting require a server restart.

   **TLS Cipher**

   Specify the HTTPS TLS ciphers accepted by Self Service Password Reset. 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.
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 might provide. Because Self Service Password Reset can be exposed directly to the internet, this additional layer of detection helps protect against direct attacks. Self Service Password Reset always honors the internal intruder detection (if enabled) of the LDAP directory.

The goal for this intruder detection system is not to watch for human intruders, but it is designed to stop robotic or automatic attacks. Set the triggers to be sufficiently high so that normal user usage does not cause an application-level intruder detection. The help desk or administrator cannot unlock accounts due to this 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. Configure the following settings:

   **Enable Intruder Detection**

   Enable the Self Service Password Reset intruder detection system. Your LDAP directory intruder detection settings function independently of this setting.

   **Intruder Record Storage Location**

   Select the location of where to store the data for intruder records. Select any one of the following from the list:

   - **Database:** Allows you to store the data in the external database. All application instances share a common view for intruder status.
   - **LocalDB:** Stores data in the local database. If you use the local database, Self Service Password Reset determines an intruder status with each instance of the application.

   **Enable Bad Password Simulation**

   Enable this option to have Bad Password Simulation activity occur when users add information to a forgotten password field. When an identified user attempts to recover a forgotten password but uses incorrect data, the application attempts to authenticate to the directory using a known bad password value. This is done to allow the LDAP directory to trigger its own defense mechanisms against intruders.
6. Click **Settings > Intruder Detection > Intruder Timeouts**.
7. Configure the following settings:

   **Intruder User Reset Time**

   Specify the time in seconds after which a user account recovers from the intruder lockout automatically. The user lockout table contains logs for a failed attempt to authenticate, recover a password, or activate a user account.

   The default value is 1800 seconds or 30 minutes. Specify 0 if you want to disable the user lockout functionality.

**Intruder User Maximum Attempts**

Specify the maximum number of attempts a user can make during the login process. When a user exceeds this value, the user cannot perform any activities until the reset time interval has passed or a help desk user has reset the password.

The default value is 10 attempts. Specify 0 if you want to disable the user lockout functionality.

---

**NOTE:** Ensure that the maximum attempts specified in this setting is always greater than what is specified in the LDAP directory. This avoids the denial of service (DOS) attacks.

---

**Intruder User Check Time**

Specify the maximum time period between each intruder attempt. When this time period is exceeded, the intruder attempt count is reset to zero. The default value is 300 seconds or 5 minutes.

**Intruder Attribute Reset Time**

Specify the time period, in seconds, after which Self Service Password Reset clears a bad attempt from the lockout table.

The default value is 1800 seconds or 30 minutes. Specify 0 to disable the attribute lockout functionality.

**Intruder Attribute Maximum Attempts**

Specify the maximum number of attempts a user can make. Self Service Password Reset uses this setting to limit the number of times a user can provide incorrect attribute values. When a user exceeds this value, the user cannot perform any activities until the reset time interval has passed.

The default value is 10 attempts. Specify 0 if you want to disable the attribute lockout functionality.

**Intruder Attribute Check Time**

Specify the maximum time period between each attempt a user can make for the attributes. When users exceed this time period, Self Service Password Reset resets the intruder attempt count is to zero. The default value is 300 seconds or 5 minutes.

**Intruder Token Destination Reset Time**

Specify the time period (in seconds) after which a bad attempt is cleared from the lockout table. The attribute lockout table is marked for a user when a token is sent, and it is cleared when the token is used.

The default value is 1800 seconds or 30 minutes. Specify 0 to disable the attribute lockout functionality.

**Intruder Token Destination Attempts**

Specify the maximum number of attempts a user can make before a lockout occurs. When this value exceeds the limit, the user cannot perform any activities until the reset time interval has passed.

The default value is 10 attempts. Specify 0 to disable the user lockout functionality.

**Intruder Token Destination Check Time**

Specify the maximum time period between each intruder attempt. When this time period exceeds the limit, the intruder attempt count is reset to zero. The default value is 300 seconds or 5 minutes.

**Intruder Address Reset Time**

Specify the time in seconds after which Self Service Password Reset removes an intruder attempt from the lockout table. The default value is 1800 seconds or 30 minutes. Specify 0 if you want to disable the lockout functionality.

The address lockout table contains logs for the source IP address of the user who had a failed attempt to authenticate, recover a password, or activate a user account from that address.

**Intruder Address Maximum Attempts**

Specify the maximum number of attempts any user can make using a particular address. When this value is exceeded, no user from that address can perform any activities until the reset time interval has passed.

The default is 30 attempts. Specify 0 if you want to disable the address lockout functionality.

**Intruder Address Check Time**

Specify the maximum time between each intruder attempt. When this period is exceeded, the intruder attempt count is reset to zero.

The default is 300 seconds or 5 minutes. Specify 0 if you want to disable the address lockout functionality.

**Maximum Intruder Attempts Per Session**

Specify the maximum amount of invalid password reset attempts that are allowed for the users. When this limit exceeds, the session gets “locked”, and the user cannot perform any more requests by using that session.

The default is 8 attempts. Specify 0 to disable the session lockout functionality.

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

# Configuring External Web Services Extensions

This section discusses various settings that enable integrating Self Service Password Reset with external web authentication methods. You can integrate Self Service Password Reset with Access Manager. These settings are intended for the developers and the component integrators to integrate Self Service Password Reset with other external source and keep the session more secure for the users.


- “Configuring REST Clients” on page 33
- “Configuring REST Services” on page 34


## Configuring REST Clients

If you want to configure the web services for an external application, 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 Click **Settings > Web Services > REST Clients**.

5 Configure the following settings:

**External Token Destination Server URLs**

Specify a valid URL for the RESTful client API to allow flexibility in reading and in displaying the destination token addresses to the user.

**External Password Check REST Server URLs**

Specify the URLs for the RESTful client API to allow additional password rules validation for an application.

**External Macro REST Server URLs**

Specify the URLs for the RESTful client API to provide additional macro functions.

The format of this setting must be @External*number*:*value* where, number can be any number representing the order of the URL and value is the URL. For example, @External1:value@ corresponds to the first URL, @External2:value@ corresponds to the second URL and so on.

**External Remote Responses REST Server URL**

Specify the URL for the RESTful client API to allow a remote service to provide challenge-response-validation during forgotten password.

This setting is applicable when the setting, verification method is set for **Remote Responses**. You can navigate to the setting from **Forgotten Password > Forgotten Password Profiles > [profile name] > Verification Methods**.

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

# Configuring REST Services

To configure Self Service Password Reset web services, 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 > Web Services > Rest Services**.

5 Configure the following settings:

**Enable External Web Services**

Select this option to allow public use of web services. The form nonce is not required to invoke the web services after enabling this feature.

When this option is disabled, the form nonce is required to invoke all web services. The form nonce is difficult to retrieve programmatically.

**Allow Web Services to Read Answers**

Select this option to allow web services to read stored challenge-response answers of users. The read responses are available in the hashing method format that is being used.

**Enable Public Health and Statistics Web Services**

Select this option to allow public use of the Health and Statistics web services. These services require authentication to retrieve the data.

This option allows the use of web services without authenticating the user. This setting is required for the public (non-authenticated) page at `/public/health.jsp` to be functional.

**External Web Services Permissions**

Specify the LDAP query for the users who are allowed to execute the REST web services. You can also query for the users in a specific LDAP group.

The query for user search can be added by using **Add Filter**, or **Add Group** options.

**NOTE:** If you want specific users to use the Self Service Password Reset REST services then you must specify the LDAP query for those users. But if you are using the **NetIQ Identity Manager/ OAuth Integration** template, all the users are allowed to execute the REST web services.

**Web Services Third Party Permissions**

Specify the query for users who are permitted to execute REST web services and are allowed to specify a third party by using the **user name** parameter.

**External Web Services Secret Key**

If you need the external web service client to provide a password when requesting for Self Service Password Reset web services, specify the password by using **Store Value**.

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

# 4 Configuring LDAP Profiles and Settings

Self Service Password Reset help manage your users' credentials if you store the users' credentials in an LDAP directory. Self Service Password Reset supports Active Directory, eDirectory, and the 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

Self Service Password Reset allows you to configure multiple LDAP directory profiles depending on your environment. During the Configuration Guide process, it 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.

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 25. The following steps explain how to edit or create the **default** profile.

Before configuring the default LDAP profile or creating a new profile, you must export the corresponding LDAP server certificates. The profile configuration requires that you import the LDAP server certificates. For more information, see "Exporting LDAP Certificates" in the *Self Service Password Reset 4.1 Installation Guide*.

**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. Click **Configuration Editor**.
4. To define the connection to the LDAP directory:
   - **4a** Click **LDAP > LDAP Directories > default > Connection**.
   - **4b** Use the following information:

     **LDAP URLs**

     Specify the URLs of LDAP servers.

The system uses these servers in configuring failover in the same order as these appear in this list. If the first server is unavailable, the system uses the next available server in the list. Self Service Password Reset checks unavailable servers periodically to check their availability.

For secure SSL, use the `ldaps://servername:636` format. For plain text servers, use the `ldap://serverame:389` format (not recommended). When using secure connections, the Java virtual machine (JVM) must trust the directory server in either of these scenarios:

- It has a valid commercial certificate.
- You have manually added the public key certificate from the tree to the Java keystore.

---

**IMPORTANT**

- Do not use a non-secure connection for anything but the most basic testing purposes (Many LDAP servers will reject password operations on non-secure connections)
- Do not use a load-balancing device for LDAP high availability, instead use the built-in LDAP server fail-over functionality
- Do not use a DNS round-robin address.
- Avoid using the network address, use the proper fully-qualified domain name address for the server.

---

**LDAP Certificates**

Import the LDAP server certificates to create a secure connection between Self Service Password Reset and the LDAP directory. After you have imported the certificate, this setting displays details of LDAP server certificates. Click **Import From Server** to import the certificates from the server. Self Service Password Reset stores these certificates in the configuration file and it uses the certificates to validate the identity of the LDAP server.

**LDAP Proxy User**

Configure an LDAP proxy user using the LDAP distinguished name format. For example, `cn=admin,o=example` or `cn=administrator,cn=users,dc=subdomain,dc=domain,dc=net`

You can gain access to the LDAP directory through the LDAP proxy user. This 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 Proxy Password**

Set the password for the LDAP proxy user.

**LDAP Contextless Login Roots**

Specify the base context to search for user names during authentication and other operations. This is the top level LDAP container where your users exist.

You can add multiple contexts. Self Service Password Reset searches each context until it finds a single match. To improve search performance, do not add large numbers of contexts because Self Service Password Reset searches each context serially.

**LDAP Test User**

Specify an LDAP test user account that Self Service Password Reset uses to validate the health of the LDAP server. Create a new test user account with the same privileges and policies as any other users in the system.

Using a test user account increases the ability to detect and alert you to any configuration or health issues. Use a test user to test the following:

- Authentication
- Read password policy
- Set password
- Set challenge-responses
- Load challenge-responses

This is an important setting. You can configure an LDAP Test User at any time.

**Auto Add GUID Value**

Select this option to create a unique GUID value and assign it to any user who does not have a GUID value and is attempting to authenticate. The system writes this value to the attribute named in the **LDAP GUID Attribute** setting.

**LDAP Profile Enabled**

Select **Enabled** if you want to enable this profile. When you deselect this option, the system disables the profile but does not delete the configuration details of the settings. This setting is helpful when you do not want to remove all the configuration settings for a particular profile but keep the profile for future use.

**4c** Click **Test LDAP Profile** to test if Self Service Password Reset is able to read the data of the users in this LDAP profile.

**5** To configure the login setup:

**5a** Click **LDAP > LDAP Directories > default > Login Setup.**

**5b** Use the following information:

**User Name Search Filter**

Specify the user name search query in the following format:

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

Replace the value `%USERNAME%` with the actual user name value. Self Service Password Reset uses this filter for the contextless login and for finding users in the LDAP directories.

**User Selectable Login Contexts**

Specify the values in this format: `display value:::context`. For example,

- `ou=sf,ou=ca,o=example:::San Francisco`
- `ou=lon,ou=uk,o=example:::London`
- `ou=nyc,ou=ny,o=example:::New York`

This is an optional setting. If you configure this, the system adds a field to the form-based login screen and other user search screens. This field allows users to select a specific context.

**LDAP Profile Display Name**

Specify the name of the LDAP profile that you have configured. Self Service Password Reset displays this name to the users.

6 To configure the user attributes for the LDAP directory:

6a Click **LDAP > LDAP Directories > default > User Attributes.**

6b Use the following information:

**Attribute to use for User Name**

Specify an attribute to allow pages to display other details such as the user name of a user instead of the **LDAP Naming Attribute** value.

**LDAP GUID Attribute**

Specify an attribute to identify and reference unique users in the LDAP directory. You can set any string readable attribute as the GUID, as long as the directory can be trusted to the uniqueness. You can also use a custom attribute and enable **Auto-Add GUID Value**. The application-defined schema includes the attribute `pwmGUID` for this usage.

The default value is `VENDORGUID`. For the default value, the system attempts to read the vendor-specific LDAP GUID.

**LDAP Naming Attribute**

Specify an attribute name that the system can use as the naming attribute on LDAP user entries. This attribute is the first part of the distinguished name of a user. This name is constant depending on the directory vendor type even if you use a different attribute for the login search filter. Typically, the naming attribute is `cn` or `uid`.

**Last Password Update Attribute**

Specify an attribute to record when users update their passwords and when the system uses the password during replication checks and other processes.

**User Group Attribute**

Specify the attribute for a user entry that you specified as a group entry in the directory.

**User Email Attribute**

Specify the attribute that contains the users' email address.

**SMS Destination Address LDAP Attribute**

Specify the users' LDAP attribute containing the users' mobile phone numbers for SMS.

**Response Storage Attribute**

Specify the attribute to use for response storage when storing responses in an LDAP directory. If blank, Self Service Password Reset does not store responses in the LDAP directory. If configured, it stores the responses in the LDAP directory in addition to any other configured storage repositories.

**User History LDAP Attribute**

Specify the attribute Self Service Password Reset uses to write a user event attribute in LDAP. The user event log attribute holds an XML document with the users' event history. Leave blank to disable logging event history in LDAP.

**Web Service User Attributes**

Add the user attributes that the various web services use and Self Service Password Reset presents as part of the users' data sets.

**Auto Add Object Classes**

Specify the LDAP object classes to automatically add users who are authenticated using the password servlet. This is an auxiliary LDAP class that contains attributes used to store password self-service data. If you extended the schema to store the challenge-response information, this setting is required This is not required for Active Directory even with schema extension

7 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:

- eDirectory
- 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 115 and Chapter 9, “Integrating Self Service Password Reset with NetIQ Access Manager,” on page 103.

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

- “Configuring the Global LDAP Settings” on page 41
- “Configuring NetIQ eDirectory Settings” on page 43
- “Configuring Microsoft Active Directory Settings” on page 44
- “Configure the Oracle Directory Settings” on page 45

## Configuring the Global LDAP Settings

The Global settings control the interaction with an LDAP directory. These settings are not applicable for the user's LDAP profile. For more information about configuring LDAP for a profile see, “Configuring LDAP Directory Profile” on page 37.

**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** Configure the following settings:

**LDAP Idle Timeout**

Specify the amount of time an LDAP session can remain inactive before the session times out and the user must authenticate again. If you specify 0 (the number), the LDAP connection does not time out in the HTTP session unless you close it.

**User Object Class**

Specify object classes of user entries in your LDAP directory.

**Follow LDAP Referrals**

Select this option if you want Self Service Password Reset to follow the LDAP referrals.

**LDAP Duplicate Mode**

Select the appropriate mode that provides a solution for searching the appropriate user from the list of multiple users. For multiple user matches found, you can control the user authentication. Select any of the following options from the list:

- **No duplicates permitted**: Select this option if you want the application to fail whenever duplicate users are found in any context or profile.
- **Match first LDAP profile**: Select this option if you want the application to use the first user that the system discovers in the first profile that has only a single match.
- **Match first user**: Select this option if you want the application to authenticate the first user that the system discovers in any context or profile. This option ignores any duplicate user in the search result.

**User Selectable LDAP Context/Profile**

Select appropriate option from the following list to control the use of LDAP profiles and LDAP contexts during identification such as login, the Forgotten Password process, and so on:

- Show the LDAP profile
- Show the LDAP profile and LDAP contexts
- Do not show

**Ignore Unreachable LDAP Profiles**

Select this option if you want to ignore the profiles that are unreachable. The system uses this option when there are multiple LDAP profiles.

The system displays a directory unavailable error message for the user when there is only a single configured LDAP Profile or all LDAP Profiles are unreachable.

**Enable LDAP Wire Trace**

Select this option to log all LDAP events to the TRACE logging level.

**WARNING:** Enabling this option might allow user passwords and other sensitive data to be written to the log files.

**9** 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 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. Configure the following settings:

   **Read eDirectory Challenge Sets**

   Select this option if you want Self Service Password Reset to read the challenge set configuration from the eDirectory universal password policy and apply it to users.

   If you want Self Service Password Reset to use challenge sets configured in NAMAS only, do not configure the required and forgotten questions in Self Service Password Reset, else Self Service Password Reset uses these if no eDirectory policy exists.

   **eDirectory Challenge Set Minimum Randoms During Setup**

   Specify the number of random questions that a user is required to answer from NMAS at the time of saving challenge/response answers.

   **eDirectory Challenge Set Apply Word List**

   Enable this option if you do not want the users to use any of the words mentioned in the word list dictionary for the challenge/response answers.

   **eDirectory Challenge Set Maximum Question Chars in Answer**

   Specify the maximum number of characters of the question text that are allowed in answers when saving challenge/response answers in NMAS.
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 the following settings:

   **Save NMAS Responses**

   Select this option if you want to save the user responses to the NMAS response storage container. This storage is in addition to any other configured response storage methods.

   **Enable NMAS Responses for Forgotten Password**

   Select this option to use NMAS stored responses during forgotten password recovery. Self Service Password Reset tries all other configured storage methods before evaluating.

   **Read User Passwords**

   Select this option if you want Self Service Password Reset to read the user's password from eDirectory before changing it.

   This prevents an extra password change from being set to a temporary random password during the forgotten password sequence. If the proxy user does not have rights to read the password, then Self Service Password Reset generates a temporary random password for the user.
7. 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 following settings:

   **Use Proxy When Password Forgotten**

   If you select this option, when users forget their passwords, the system uses the LDAP proxy account for LDAP to work. This is because an LDAP connection is not possible to Active Directory without the passwords for the users. When authenticated in this condition, the system forces the users to change their passwords immediately.

**Allow Authentication When “Must Change Password On Next Login” Is Set**

Active Directory fails an LDAP login attempt when the **Must Change Password On Next Login** flag is set. If you enabled this option, the system allows login even though the LDAP bind has failed. The user is only able to set a new password when this condition occurs. No other functions are available until the password has been set (and this flag is cleared).

**Allow Authentication When Password Expired**

Active Directory fails an LDAP login attempt when the current date is after the user's password expiration date. If you enabled this option, the system allows login even though the LDAP bind has failed. The user is only able to set a new password when this condition occurs. No other functions are available until the password has been set (and this flag is cleared).

**Enforce Password Policy During Forgotten Password**

Enforce password policy during forgotten password when the option **Use Proxy When Password Forgotten** is also set to true. This setting that the Active Directory servers support the LDAP_SERVER_POLICY_HINTS_OID (1.2.840.113556.1.4.2066) LDAP modification control.

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

# Configure the Oracle Directory 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 following settings:

**Allow Manipulation of PasswordAllowChangeTime**

If select this option, during the forgotten password recovery sequence, allow manipulation of the `allowPasswordChangeTime` attribute. This allows forgotten password functionality, with expected behavior, when the system enforces a policy of minimum time between password changes.

**Allow Authentication When “Require Password Change at First Login and After Reset” Is Set**

Oracle Directory Server normally fails an LDAP login attempt when the user's `pwdReset` attribute is set due to an administrator password set. If you enabled this option, the system allows login even though the LDAP bind has failed. The user can only set a new password when this condition occurs. No other functions are available until the password has been set (and this flag is cleared).

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

# 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 75.

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 63.

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

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 a **My Account** tile after the users log in to Self Service Password Reset. The **My Account** tile allows users to view the history of 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. Configure the following settings:

   **Enable Account Information**

   Displays the **My Account** tile on the web page for users.

**Show Password Event History**

Displays the password history for the user in the My Account page under the **Password History** tab.

**Viewable Status Fields**

Select the options you want users to see when they click the **My Account** tile.

**LDAP Display Attributes**

Specify the LDAP attributes to show to users on the account information page.

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 begging 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. For example, users must provide their current passwords before they can change their passwords.

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 from 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 79.

**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. Configure the following settings:

   **Change Password Permission**

   Specify the query for the users that Self Service Password Reset allows to change their passwords. 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.

   **Logout After Password Change**

   Enable this option to forces users to log out (and send them to the logout URL) after a password change. For security reasons, enable this feature for all users especially if a user is using a single sign-on service. By default, Self Service Password Reset enables this option.

   **Change Password Required Values Form**

   Specify the values Self Service Password Reset requires the users to enter before changing their passwords.

   **Require Current Password During Change**

   Select whether you want Self Service Password Reset to require the users to provide their current passwords on the Change Password page. You must enable this option if users are using a single sign-on service. In most cases, this is not required because the single sign-on service authenticates the users prior to accessing the Change Password page.

   **Password Change Agreement Message**

   Specify the message to display to users before Self Service Password Reset allows them to change their passwords. The message can include HTML tags. If you leave this field blank, the Change Password Agreement page is not visible to users. You can use macros in this setting. For more information, see "Configuring Macros for Messages and Actions" on page 21.

   You can also configure this setting in a different language. Click **Add Locale**, then select the required language from the list.

   **Password Change Completion Message**

   Specify the message that Self Service Password Reset displays to users when users complete the password change process. If you leave this setting blank, the user does not see the change password completion page. This message might include HTML tags. You can also use macros. For more information, see "Configuring Macros for Messages and Actions" on page 21.

   You can also configure this setting in a different language. Click **Add Locale**, then select the required language from the list.

**Password Guide Text**

Specify the text (in HTML) Self Service Password Reset displays for the Password Guide page. This shows up as a **password guide** link in a pop-up dialog. Leave blank to not show the password guide link. You can use macros for this setting. For more information, see "Configuring Macros for Messages and Actions" on page 21.

You can also configure this setting in a different language. Click **Add Locale**, then select the required language from the list.

**Password Sync Enable Replication Checking**

Enable this option to have Self Service Password Reset perform a replica sync that polls all of the configured replicas on the users' LDAP Profile to determine if the LDAP directory updated the password change time. The particular method to determine the last password change time varies per LDAP vendor type.

You can choose to display the progress of the replica check to the users or not depending on the option you select.

**Password Change Minimum Wait Time**

Specify the minimum wait time (in seconds), during a password change, Self Service Password Reset waits for a password change to take effect. The system uses this time for background synchronization processes.

**Password Change Maximum Wait Time**

Specify the maximum time, in seconds, the system waits for the password to be synchronized to all configured LDAP servers during a password change action. This setting prevents the page from timing out when the synchronization takes a longer time.

**Password Pre-Expire Time**

Specify the number of seconds before the users' passwords expire, which forces the users to change their passwords. If the users' passwords expire within this time frame, the system behaves as if the users' passwords had already expired.

Setting this value to a day prevents most cases when the users' passwords expire while they are logged in. The recommend setting for this value is 86400 (1 day).

**Password Expire Warn Time**

Specify the time in seconds that Self Service Password Reset sends the password expiry notification before the users' passwords expire. If the users' passwords expire within this time frame, the system warns the users during a `CommandServlet`, `checkExpire`, or `checkAll` operation.

To disable this feature set the time to 0 or less than `expirePreTime`. The recommended value for this setting is 432000 seconds (5 days).

**Check Expire During Authentication**

Enable this option to have the system verify whether the users' passwords are expired or about to expire while the users authenticate. If the password is expired, the system forwards the user to the Expired Password page.

**Post Password Change Actions**

Specify the actions to be taken when a user changes a password. The system invokes the configured actions immediately after the user changes the password. You can use macros within the action. For more information, see "Configuring Macros for Messages and Actions" on page 21.

When you add an action, following are the services available to set the actions:

**webservice**

You can select the HTTP method, add headers and specify the web service URL.

**LDAP**

You can specify the LDAP attribute name, attribute value, and the type of the operation that is performed. The operation types are:

**Replace**

Replaces the existing values and include the new ones in the output.

**Add**

Adds the new values along with the existing values in the output.

**Remove**

Removes the specified value in the output.

**Show Auto Generate Random**

Enable this option to have the user web page display a link to users during the change password process that displays a list of auto-generated sample passwords that the configured password policies allow. The users have the option to select and use one of the values in the list. If you enable this option, Self Service Password Reset does not force the users to choose a password from the list.

**Show Strength Meter**

Enable this option to display the strength meter, for the password strength, on the Change Password page. By default, Self Service Password Reset enables this option.

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.

**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 for the Delete Account module with the following information.

**Delete Account Profile Match**

Specify a query to search for the users that you want to be able to delete their own accounts. 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.

**Delete Account Agreement**

Specify a message to display to the users before allowing them to delete their accounts. If blank, SSPR does not display the delete account user agreement page to the users. This message can include HTML tags.

You can also configure this setting in a different language. Click **Add Locale**, then select the required language from the list.

**Delete LDAP Entry**

Select whether you want Self Service Password Reset to delete the LDAP entry for the user account when the users delete their accounts. Self Service Password Reset has this option disabled by default.

**Pre-Delete Actions**

Define any pre-delete actions you want Self Service Password Reset to perform prior to deleting the user accounts. You can use these actions to disable the LDAP accounts instead of deleting the LDAP accounts. Specify a descriptive name for the action, then click **OK** to display the available options.

**Next URL**

Specify a URL where to direct the users after they delete their own accounts. If blank, the normal logout handling occurs.

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 70.

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 25.

# 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 on.

You can create required number of help desk profiles and configure appropriate settings for each profile. For more information, see “Configuring Profiles” on page 25.

Self Service Password Reset allows help desk administrators to search user details by using the wildcard search. 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.

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.

**To 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 with the following information:

   **Help Desk Profile Match**

   Specify the set of users for a profile, so that the configuration setting that you specify for the profile is applicable for that set of users.

   You can use LDAP Group or LDAP filters to query the LDAP directory for users.

   **Add Filter**

   Select the appropriate profile from the list, then select the LDAP search filter. For example:

   ```
   (&(objectClass=Person)(|((cn=*%USERNAME%*)(uid=*%USERNAME%*)(sAMAccoun
   tName=*%USERNAME%*)(userprincipalname=*%USERNAME%*)(givenName=*%USERNA
   ME%*)(sn=*%USERNAME%*))))
   ```

   **Add Group**

   Select the appropriate profile from the list, then specify the LDAP Group DN. For example:

   ```
   cn=admins,o=company or cn=administrators,cn=builtin,dc=example,dc=com
   ```

   **Help Desk Search Form**

   Specify the user attributes that you want to display to help desk administrators in the search result. You can also add a new form field by clicking **Add Item**.

   **Help Desk Search Filter**

   Specify an LDAP search filter to query the directory. Substitute `%USERNAME%` for a user-supplied user name. If not specified, the system auto calculates a search filter based on the **Help Desk Search Form**. For example:

   **Active Directory**

   ```
   (&(objectClass=Person)(|((cn=*%USERNAME%*)(uid=*%USERNAME%*)(sAMAccoun
   tName=*%USERNAME%*)(userprincipalname=*%USERNAME%*)(givenName=*%USERNA
   ME%*)(sn=*%USERNAME%*))))
   ```

   **eDirectory**

   ```
   (&(objectClass=Person)(|((cn=*%USERNAME%*)(uid=*%USERNAME%*)(givenName
   =*%USERNAME%*)(sn=*%USERNAME%*))))
   ```

   **LDAP Search Base**

   Specify the LDAP search base. If you leave this field blank, the system uses the default LDAP search bases.

**Help Desk Detail Form**

Specify the user attributes that you want to display to help desk administrators for an individual user. You can add, delete, and add new fields that the help desk administrators see.

**Help Desk Search Result Limit**

Specify the limit of the search result for the help desk user.

**Send Password to User**

Select this option to send the reset password to users. You set the method of sending the password under **Forgotten Password** > **New Password Send Method**.

**Post Set Password Actions**

Specify the actions that the system executes after a help desk administrator modifies a user's password. You can use macros. Specify a descriptive name for the action, then click **OK** to display the available options.

**Help Desk Actor Actions**

Specify the actions that a help desk administrator can perform. You can use macros. Specify a descriptive name for the action, then click **OK** to display the available options.

**Idle Timeout Seconds for Help Desk Users**

Specify the number of seconds after which an authenticated help desk administrator’s session requires re-authentication.

**Enforce User Password Policy**

Select this option if you want the help desk administrators to follow the same password policies that a user does while setting their passwords.

**Clear Responses on Password Set**

Select a mode to allow help desk administrators to clear responses after setting passwords, which a user provides during password change request. The available options include:

**Ask**

Asks whether to remove the user’s secret questions and answers.

**False**

Neither removes nor asks for removing the user’s secret questions and answers.

**True**

Automatically removes the user’s secret questions and answers.

**Force Password Expiration On Password Set**

Enable this setting if you want the password to expire when the user logs in with the new password that the help desk administrator has set.

**Use Proxy Connection**

Select this option to use the application proxy connection for all the actions that you initiated in the help desk module.

If deselected, the system initiates the actions using the LDAP connection of the logged in user. The user must have appropriate privileges in the LDAP directory.

**User Detail Display Name**

Specify the display name that identifies the user on the user detail screen. You can use macros to display the name of the user.

**Token Send Method**

Select a method for sending token code the user. The available methods include:

**None**

Self Service Password Reset does not perform the token verification.

**Email Only**

Self Service Password Reset sends the token to the user's email address.

**SMS Only**

Self Service Password Reset send the token through SMS.

**Both**

Self Service Password Reset sends the token to both the user's email and SMS.

**Email First**

Self Service Password Reset tries to send token through email; if no email address is available, it sends the token through SMS.

**SMS First**

Self Service Password Reset tries to send token through SMS; if no SMS number is available, it sends the token to the user's email.

**Operator choice**

If both mobile number and email address are available, the help desk operator can decide which method to use.

5 Click **default > Options** to configure the options for the Help Desk module with the following information:

**Viewable Status Fields**

Select the fields that are available to help desk administrators to view. The fields display the status of the users.

**Set Password UI Mode**

Select a mode from the list to allow help desk administrators to set passwords. This is applicable for the users who have proper LDAP permissions. The options include:

**None**

Help desk administrators cannot change passwords for users.

**Type new password**

Requires the help desk administrators to type a new password to change the password for a user.

**Auto generate a list of random passwords to choose from**

Help desk administrators can select a password from the automatically generated passwords list and assign it to the user.

**Auto generate a list of random passwords and allow typing on new password**

Help desk administrators can set a password by selecting an automatically generated password or by typing it.

**Set the password to a random value unknown to the Help Desk operator**

The help desk administrator cannot view or provide the new password to the user. However, the system sets passwords for users to a random value and sends the value to the users through the specified send method.

**Enable Unlock**

Enable this option to enable help desk administrators to unlock an intruder locked account.

**Enable Clear Responses Button**

Enable this option to allow the help desk operator to use a button for clearing the stored responses of the user.

**Enable Clear One Time Password Settings Button**

Enable this option to allow the help desk operator to click a button and clear the stored one-time password settings of the user.

**Enable Delete User Button**

Enable this option to allow help desk operator to delete the user account from the LDAP directory.

**Mask Password Value**

Enable this option if you want to mask the password that the help desk user types for changing the user's password.

6 Click **default > Verification** to configure the verification options for the Help Desk module with the following information:

**Verification Methods**

Select the appropriate help desk verification methods. You can use LDAP attributes, SMS and email token verification, and OTP (mobile device) verification.

**Help Desk Verification Form**

Define a verification form for the help desk.

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 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 you enable the People Search module and configure it, anyone can 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).

**To 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 Configure the following settings:

**Enable People Search**

Enable this option to enable the People Search module.

**Permitted Users**

Specify an LDAP search filter or an LDAP group and an existing LDAP profile to control the users who access People Search. The user must match this query to use this feature.

You can add multiple LDAP search filters and add multiple groups or LDAP profiles for the query. However, Self Service Password Reset ORs the items in the search. So a user must match the LDAP search filter or the LDAP group.

**Search Attributes**

Add the list of LDAP attributes that Self Service Password Reset must search when the system generates an automatic search for the setting **People Search LDAP Filter**. The system also uses the search attributes to determine which fields in the user detail form displays the **Like** search option.

**Search Result Attributes**

Specify the LDAP attributes that Self Service Password Reset displays in the search result for a user during searches.

**Search Detail Attributes**

Specify the LDAP attributes that Self Service Password Reset displays during the detail view of an individual person's record.

**Search Result Limit**

Specify the maximum number of records that the People Search module displays in the search results.

**Use Proxy Account**

Enable this option to use the LDAP proxy account to perform searches. For proper security in most environments, do **not** enable this setting.

**UserDN Name Display**

Specify the configuration value that People Search module displays for the user's name. Specify the value for this setting in the `@LDAP:name@` format. For example, if you want the People Search module to display the user's first and last names then you can provide the following configuration value: `@LDAP:givenName@ @LDAP:sn@`.

**Person Detail Display Labels**

Specify the details that the People Search module must display in the details on the organizational chart for each user.

**LDAP Photo Attribute**

Specify the name of the LDAP attribute that includes the photo of the LDAP users. When you specify the LDAP attribute name, Self Service Password Reset uploads the photos from the LDAP directory.

This is an optional field. If you do not specify an LDAP attribute, the People Search module does not display a photo of the user during the user search.

**Photo URL Override**

Specify a URL of an external system to show the photos if you do not store the user photos in the LDAP directory. If you specified this setting, the People Search module does not load the photo from the LDAP directory.

For example: `http://photos.example.com/employee/@LDAP:workforceID@.jpg`

**Search Maximum Cache Seconds**

Specify the interval, in seconds, to store the search information in cache.

**Photo Display Permission**

Specify the query for the users that the People Search module allows to view the photo of other users in the organizational chart.

**People Search LDAP Filter**

Specify the LDAP search filter to query the directory with Substitute `%USERNAME%` for the user-supplied user name. If blank, the system auto-generates the search filter based on the values in the setting **Search Attributes**.

For example:

```
(&(objectClass=Person)(|(givenName=*%USERNAME%*)(sn=*%USERNAME%*)(mail=*%U
SERNAME%*)(telephoneNumber=*%USERNAME%*)))
```

**LDAP Search base**

Specify the LDAP search base. If you leave this field blank, the system uses the default LDAP search bases.

**Enable People Search Public (Non-Authenticated) Access**

Enable this option to allows access to the People Search module for unauthenticated users. The URL the unauthenticated users access to view the People Search module is: *ipaddress*`/sspr/public`.

**Idle Timeout Seconds**

Specify the number of seconds after which an authenticated session expires. There is no timeout for users using the People Search module without authenticating.

**Organizational Chart Parent Attribute**

Specify the LDAP attribute that contains the LDAP DN of the manager. If this setting is blank, then the People Search module does not display the organizational chart view.

**Organizational Chart Child Attribute**

Specify the LDAP attribute that contains the LDAP DN of the users who directly report to the user.

6 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 25.

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 following settings:

**Enable Setup Responses**

Enable this option to display the save responses page for users.

**Force Response Setup**

Select this option to redirect users to configure the challenge-response when they log in. This setting allows users to save responses if they do not have stored responses yet.

**Show Response Confirmation**

Enable this option to show the responses to the user after they configure responses. This gives users an opportunity to read and review their responses before submitting.

**Case Insensitive Responses**

Enable this option to make the responses case-insensitive. The setting does not affect or apply to users who have already configured their responses prior to modifying this setting.

**Allow Duplicate Responses**

Enable this option to allows users to use duplicate responses. That is not a good security practice. Ensure that you do not select this option if you want users to enter a unique value for each response.

**Save Challenge Permission**

Specify an LDAP search filter or add an LDAP group or LDAP profile to determine if you permit the users to configure challenges. The LDAP query must return the user or else Self Service Password Reset does not permit the user to configure challenges.

To view the list of users that match the query, click **View Matches**.

**Check Responses Match**

Specify the LDAP search filter or specify an LDAP group and LDAP profile.

If the query calls the command servlet with the `checkResponses` command (`/private/CommandServlet?processAction=checkResponses`), the system first checks the users to see if they match the specified LDAP query before checking the password responses of the users. If users do not match this query, then the system does not check the responses for the users and redirects the users to the forward URL.

To view the list of users that match the query, click **View Matches**.

**Enforce Minimum Password Lifetime**

Determine when the users authenticate through ForgottenPassword should have the **Password Minimum Lifetime** (if set) setting enforced. If you enable this setting, the users cannot change their passwords if the **Minimum Lifetime** has not passed. If not enabled, the system permits the users to change their passwords when authenticated through Forgotten Password even if the **Minimum Lifetime** has not changed.

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 following settings to enable the module:

   **Enable Shortcuts**

   Enable this option to enable the Main Menu for users on the Self Service Password Reset web page.

   **Shortcut Items**

   Specify the shortcuts you want to make available to users in this format: `label::url::ldapQuery::description`

   **label**

   The label of the shortcut that users see.

   **ldapQuery**

   Valid LDAP syntax style query. If the user matches this query, then the shortcut is shown to the user.

   **url**

   The HTTP shortcut where the users are directed.

   **description**

   The long description of the shortcut.

   You can also configure this setting in a different language. Click **Add Locale**, then select the required language from the list.

   **Shortcut Headers**

   Specify HTTP headers to control the list of visible shortcuts. The values must correspond to the label values specified as part of the shortcut items. When this header is present, the system does not use the `ldapQuery` part of the shortcut items and displays shortcuts only if the label is present in the header.

   You can set the values separately or by comma separating the values. A blank value disables this feature.

   **Launch Shortcuts in New Window**

   Enable this option to launch the shortcuts in a new window (or tab).
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. Ensure that the attributes you configure in the Update Profile module have the required rights in the LDAP directory.

You can create required number of profiles for the Update Profile module and configure appropriate settings for each profile. For more information, see “Configuring Profiles” on page 25.

**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 following settings for the default profile:

**Update Profile Match**

Specify a query to define a Profile Match that only allows users who match this query to update their profiles. You add an LDAP profile to match as well as an LDAP search filter.

Click **View Matches** to see the result of the filter.

**Update Profile Actions**

Add actions to execute after Self Service Password Reset populates the users' attributes. Specify a descriptive name for the action, then click **OK** to display the available options.

**Force Update Profile**

Enable this option to present the Update Profile module to the users upon login if the users do not satisfy the form configuration conditions. Specifically, the system checks the **Required and Regular Expression** conditions against the current LDAP form values. The user cannot perform other functions until they update the form values to values that match the form configuration.

**Update Profile Agreement Message**

Specify the message you want to display to users before allowing them to update their profile. You can include HTML tags in the message.

Leave this field blank if you do not want to display any agreement message to users.

You can also configure this setting in a different language. Click **Add Locale**, then select the required language from the list.

**Update Profile Form**

Specify attributes that users can view and update.

For example:

- givenName: First Name:text:1:40:false:false
- sn: Last Name:text:1:40:false:false
- facsimileTelephoneNumber:Fax Number 2:text:3:25:false:false

---

**NOTE:** The user must have read and write privilege to these attributes to save the changes.

---

**Show Update Profile Confirmation**

Enable this option to show users the profile update confirmation message before they submit changes. This provides users an opportunity to read and review their attributes before submitting changes.

**Enable Email Verification**

Enable this option to have the system send an email to the user's email address before updating the account. The user must verify receipt of the email before the system can update the account.

**Enable SMS Verification**

Enable this option to have the system sends an SMS message to the user's mobile phone number before updating the account. The user must verify receipt of the SMS before the system updates the account.

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 75.

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 47.

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 the Forgotten Password Module

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

The Forgotten Password module uses challenge-response authentication to let users recover their passwords. This feature enables prompting for challenge set or a one-time password (OTP) that allows a password change. Requiring a user to answer challenge questions, or entering an OTP before receiving the forgotten password provides an additional level of security.

To correctly configure the Forgotten Password module, you must define a Forgotten Password profile and configure the Forgotten Password settings.

# Configuring the Forgotten Password Profile

You can configure a Forgotten Password profile and the users of that group can reset their passwords by using the method that you define in the settings for that profile. This section helps you define the default Forgotten Password profile. 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 25.

The users can use the challenge-response and also use the one-time password (OTP) during forgotten password process, depending on the verification method that you define in the profile. For more information about one-time password, see “Configuring One-Time Password” on page 97.

**To configure the Forgotten Password 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 **Modules > Public > Forgotten Password > Profiles > default > Definition.**
5. Configure the following settings for the Forgotten Password profile:

   **Forgotten Password Profile Match**

   Specify the set of users for a profile, so that the configuration setting that you specify for the profile is applicable for that set of users.

   You can use LDAP Group or LDAP filters to query the LDAP directory for users.

   **Add Filter**

   Select the appropriate profile from the list, then select the LDAP search filter. For example:

   ```
   (&(objectClass=Person)(|((cn=*%USERNAME%*)(uid=*%USERNAME%*)(sAMAccoun
   tName=*%USERNAME%*)(userprincipalname=*%USERNAME%*)(givenName=*%USERNA
   ME%*)(sn=*%USERNAME%*))))
   ```

   **Add Group**

   Select the appropriate profile from the list, then specify the LDAP Group DN. For example:

   ```
   cn=admins,o=company or cn=administrators,cn=builtin,dc=example,dc=com
   ```

   **Verification Methods**

   Select one or more verification methods used during the forgotten password process. The users must satisfy each option set at **Required**, then the users select any of the remaining **Optional** methods until the users complete the minimum number of **Optional** methods. For more information, see “Understanding the Verification Methods” on page 67.

   **Token Send Method**

   Select the methods used for sending the token code or new password to the user. You can send the password through only email, only SMS messages, both, emails first, SMS messages first, or the users can choose the method.

   You must perform additional configuration to send emails and SMS messages. For more information, see:

   - “Configuring Email Notification Settings” on page 91
   - “Configuring SMS Notification Settings” on page 94

**Allow Unlock**

Enable this option to allow users to unlock locked accounts during the Forgotten Password process. If **Enabled**, and if the users' accounts are locked due to too many invalid login attempts and the users' passwords are not expired, then the Forgotten Password process allows the users to unlock their accounts instead of resetting their passwords. This only works if the users have populated the Self Service Password Reset challenge set.

If you are using the NMAS challenge set, you must enable the **Enable NMAS Responses for Forgotten Password** option to have the same functionality for the NMAS challenge set. For more information, see "Configuring the LDAP eDirectory Settings" on page 44.

**Forgotten Password Recovery Mode**

Select an action to take when the users complete the Forgotten Password process.

**Allow user to set new password**

Allows users to set a new password, after answering the challenge questions to prove their identity. The users can change their passwords without the Forgotten Password process requiring them to provide their current passwords because the users authenticated through answering the challenge questions. To use this option, you must require a challenge set and the user must have set up challenge-response by answering the challenge questions. For more information, see "Configuring the Setup Security Questions Module" on page 58.

**Send new password**

Select this option to send the password through the chosen **Token Send Method**.

**Send new password and mark as expired**

Select this option to send the password through the chosen **Token Send Method** and to expire the old password.

**New Password Send Method**

Select the method to send new passwords to users when the **Forgotten Password Success Action** is set to **Send new password**. You can send the password through email only, SMS messages only, both, emails first, or SMS messages first.

**Required LDAP Attributes**

Specify the required LDAP attributes for Forgotten Password authentication. The users must specify these attributes as part of the Forgotten Password authentication process. The LDAP Proxy User requires LDAP compare permission to these attributes.

**Allow Forgotten Password when Locked**

Allows the 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 to store responses.

6 (Conditional) Configure the OAuth2 connection to an external application if you selected OAuth2 as a verification method. For more information, see "Configuring the OAuth2 Verification Method for the Forgotten Password Module" on page 68.

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

# Configuring the Forgotten Password Settings

To complete the configuration of the Forgotten Password module, you must also configure the Forgotten Password settings. The settings allows 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 considers 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 change the password through the email token to the password history.

**To configure the Forgotten 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 > Public > Forgotten Password > Settings**.
5. Configure the following settings:

   **Enable Forgotten Password**

   Enable this option to allow the users to recover forgotten passwords.

   **Forgotten Password User Search Form**

   Specify the attributes that users specify to authenticate, such as name or email. Ideally, the information the users specify is not publicly known.

   The system uses these values internally to search for the users who request the Forgotten Password recovery action.

   **Forgotten Password User Search Filter**

   Specify a filter to find users. Include each attribute configured in the **Forgotten Password User Search Form** in the search filter. Strings encoded with a percent sign (%) are replaced with values supplied by the user.

   For example, if the **Forgotten Password User Search Form** includes `email` and `sn` attributes, then the filter would be:

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

   **Response Read Location**

   Specify the location where the system stores the challenge-responses. If you select an option with multiple locations, the system reads each location until it finds a stored response.

   **Response Write Location**

   Specify the location where the system writes the responses. If you select an option with multiple locations, the system stores responses in each location when users configure their response answers.

   **Response Storage Attribute**

   Specify an attribute the system uses for storing responses when you want to store responses in the LDAP directory. The system stores responses in the LDAP directory in addition to any other configured storage repositories.

   **Response Storage Hashing Method**

   Select a hashing method the system uses to store responses from the list. By default, Self Service Password Reset uses PBKDF2WithHmacSHA1. The available options are:

   - None (Plaintext)
   - MD5
   - SHA1
   - SHA-1 with Salt

- SHA-256 with Salt
- SHA-512 with Salt
- PBKDF2WithHmacSHA1
- PBKDF2WithHmacSHA256
- PBKDF2WithHmacSHA512
- BCrypt
- SCrypt

Storing the responses as plain text facilitates synchronization or migration to other systems.

---

**NOTE:** If an administrator changes this setting and uses the same browser to store the responses, then the changes are not effective. The administrator needs to start a new browser session for the changes to be made effective.

---

**Forgotten Password Post Actions**

Specify the name of the actions and define the following services to set the actions that the Forgotten Password module must execute after a user successfully completes the Forgotten Password process and the user's password is modified.

You can also use macros. For more information, see “Configuring Macros for Messages and Actions” on page 21. Specify a descriptive name for the action, then click **OK** to display the available options.

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

# Understanding the Verification Methods

The verification method that you require the users to use must be set to **Required** (placing the vertical bar to extreme right). You can also include any number of the optional method 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 during forgotten password process the system requires that the users answer the challenge-response or to skip it using the one-time password for verification.

The following are the verification methods that can be used during a forgotten password process:

- **Previous Authentication:** This verification method 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:** This verification method requires the user to specify the values for all the 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:** This verification method requires the users to answer the challenge-responses. For more information, see “Configuring the Setup Security Questions Module” on page 58.
- **SMS/Email Token Verification:** This verification method allows the user 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**.

- **OTP (Mobile Device) Verification:** This verification method requires the user to use the one-time password (OTP) during forgotten password process. For more information about OTP, see "Configuring One-Time Password" on page 97.
- **External Responses:** This verification method 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:** This verification method allows you to create an OAuth2 connection between Self Service Password Reset and any application that supports OAuth2. For more information, see "Configuring the OAuth2 Verification Method for the Forgotten Password Module" on page 68.
- **Advanced Authentication:** Self Service Password Reset deprecated this method of connecting to 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. For more information, see Chapter 10, "Integrating Self Service Password Reset with Advanced Authentication," on page 111.

In a scenario where the verification method is challenge-response and OTP is optional, users can choose to skip enrolling for OTP. But during forgotten password process, if you enabled the OTP with the **Force Setup-but allow user to skip** setting, the login page prompts the 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 a password is reset.

You can customize the text and descriptions for these verification methods that the users see through the **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. For more information, see Chapter 3, "Configuring Self Service Password Reset," on page 23.

# Configuring the OAuth2 Verification Method for the Forgotten Password Module

If you selected to use 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.

To properly configure the OAuth2 verification method you must obtain information from the application you are connecting to through this method. For example, if are using Advanced Authentication as the application for the OAuth2 verification method, you must obtain information from the application, this case Advanced Authentication to complete the configuration. Plus you must perform configuration steps in the connected application to complete 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 Forgotten Password profile.
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 > Public > Forgotten Password > Profiles > OAuth**.

6 Use the following information to configure the OAuth settings:

**OAuth Login URL**

Specify the OAuth server login URL for the connected application. SSPR uses this is the URL to redirect the user to for authentication. For example:

`https://advanced-authentication.example.com/osp/a/TOP/auth/oauth2/grant`

**OAuth Code Resolve Service URL**

Specify the OAuth Code Resolve Service URL for the connected application. Self Service Password Reset uses this web service URL to resolve the artifact returned by the OAuth identity server. For example:

`https://advance-authentication.example.com/osp/a/TOP/auth/oauth2/authcoderesolve`

**OAuth Profile Service URL**

Specify the web service URL provided by the identity server to return attribute data about the user. This is the identity server from the connected application. For example:

`https://advanced-authentication.example.com/osp/a/TOP/auth/oauth2/getattributes`

**OAuth Web Service Server Certificates**

Import the certificate for the OAuth web service server. This is the connected application's OAuth web service server.

**OAuth Client ID**

Specify the OAuth client ID from the connected application. The OAuth identity service provider gives you this value.

**OAuth Shared Secret**

Specify the OAuth shared secret from the connected application. The OAuth identity service provider gives you this value.

**OAuth User Name/DN Login Attribute**

Specify the attribute to request from the OAuth server that Self Service Password Reset uses as the user name for local authentication. Self Service Password Reset then resolves this value the same as if the user had typed the password at the local authentication page.

**OAuth Inject User Name Value**

(Conditional) Specify the user name value to send as part of the grant or redirect request. The remote OAuth server must support the sign endpoint for this to work.

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/oath` at the end of the URL. For example:

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

# 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 following settings:

   **Enable Forgotten User Name**

   Enable this option to allow users to recover their user name based on the configured search filter and attributes.

   **Forgotten User Name Form**

   Specify the fields that the users use to search for their users names.

   **Forgotten User Name Search Filter**

   Specify the search filter query to find user name. Include each attribute configured in **Forgotten User Name Form**. Strings encoded with a percent sign (%) are replaced with values supplied by the user.

   For example, if **Forgotten User Name Form** includes `mail` and `sn` attributes, the filter would be:

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

   **Forgotten User Name Message**

   Edit the message to show to a user upon a successful forgotten user name action.

   **User Name Send Method**

   Select a method to send a new password to the user. This setting is applicable when **Forgotten Password Recovery Mode** is set to **Send new password**.
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. 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 25.

When a new user registration is complete, 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 4.1 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 following settings:

   **Creation Context**

   Specify an LDAP context where Self Service Password Reset creates the new users.

   **New User Agreement Message**

   Specify a message to display to the users before allowing them to register as a new user. You can include HTML tags in this message.

   You can also configure this setting in a different language. Click **Add Locale**, then select the required language from the list.

   **New User Form**

   Specify attributes that the users must enter while registering as a new user.

   **New User Actions**

   Specify the actions the system takes when it creates a user. Specify the value in the name=value pair format. You can specify multiple attributes by separating with a comma. You can also use macros. Specify a descriptive name for the action, then click **OK** to display the available options.

   **Delete On Creation Failure**

   Enable this option to have Self Service Password Reset delete the new user account if the creation fails for some reason. It deletes the (potentially partially-created) “broken” account in the LDAP directory.

   **LDAP Entry ID Definition**

   Specify the entry ID of the newly created LDAP entry. In some directories, this is often used as the user name, though many directories separate the concepts and values of entry ID and user name.

   Values can (and usually do) include macros. In case the first value already exists in the directory, Self Service Password Reset tries each successive value until it finds a free value. Though Self Service Password Reset has not yet created the user when it evaluates the macros, the LDAP macros use the data provided on the new user form. Other macros might not be useful as there no data yet available on the user. For more information about macros, see “Configuring Macros for Messages and Actions” on page 21.

If you leave this field blank, the system does not generate a random user name or entry ID.

For example, in the LDAP directory, specify the value as `@User:Email@` to display the display name or entry ID as the email address for the new registered user.

**Enable New User Email Verification**

Enable this option to send an email to the new user's email address before Self Service Password Reset creates the account. The new user must verify receipt of the email to complete the account creation.

---

**NOTE:** You must configure and enable the **Email** settings to make this option work. For more information about how to configure email settings, see "Configuring Email Notification Settings" on page 91.

---

**Enable New User SMS Verification**

Enable this option to send an SMS to the new user's mobile phone number before Self Service Password Reset creates the account. The new user must verify receipt of the SMS to complete the account creation.

---

**NOTE:** You must configure and enable the **SMS** settings to make this option work. For more information about how to configure the SMS settings, see "Configuring SMS Notification Settings" on page 94.

---

**Password Policy Template**

Specify a user Self Service Password Reset uses as a template for the new user password policy. If the value is TESTUSER, Self Service Password Reset uses the configured test user's password policy.

**New User Minimum Wait Time**

Specify a delay time during a new user creation. SSPR delays the creation of the user for at least this amount of time before forwarding the user to the next activity.

Specify the value in seconds.

**Profile Display Name**

Specify the publicly viewable display name of this profile.

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 accounts and set a temporary password. When users create accounts that do not have an established channel to send the passwords to the users, this feature helps the users activating their accounts. Configure the settings to allow only those users to activate their accounts that have never been authenticated. This behavior might differ depending on the configuration and directory type.

**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 following settings:

   **Enable User Activation**

   Enable this option allows users to activate their accounts by clicking **Activate Account** on the login page.

   **Unlock User During Activation**

   Enable this option to allow users to try to unlock their user accounts during activation. If true, and if the users' accounts are locked Self Service Password Reset unlocks the users' accounts.

   **Token Send Methods**

   Select a method for sending the token code to the user. The available methods include:

   - **None**: The system does not perform a token verification
   - **Email Only**: Send to email address
   - **SMS Only**: Send through SMS
   - **Both**: Send token to both email and SMS
   - **Email First**: Try to send token through email; if no email address is available, send through SMS
   - **SMS First:** Try to send token through SMS; if no SMS number is available, send through email

   **Activate User Agreement Message**

   Specify a message to display to users before they activate their account. You can include HTML tags in the message.

   If you leave this field blank, the system does not display the Activate User Agreement message.

   You can also configure this setting in a different language. Click **Add Locale**, then select the required language from the list.

   **Activate User Form**

   Specify the attributes Self Service Password Reset requires a user to provide during user activation.

   **Activate Search Filter**

   Specify a filter to find users during user activation. Include each attribute configured in **Activate User Form** in the search filter. Strings encoded with a percent sign (%) are replaced with values supplied by the user.

   For example, if **Activate User Form** includes `cn` and `sn` attributes, the filter is:

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

   **Activation Permission**

   Specify and LDAP filter that only allows Self Service Password Reset to active users who match this query. Generally, you only allow users who have never been authenticated and are not disabled to activate. The default example uses the last login time attributes on the

user object to determine if the user has never logged in. It is the responsibility of the administrator to ensure this activation feature works correctly. Misconfiguration could potentially result in unintended activations occurring.

**Activation Actions (Before Password Change)**

Specify the actions that the system executes before the user configures a password post-activation. You can use macros. Specify a descriptive name for the action, then click **OK** to display the available options.

**Post-Activation Actions (After Password Change)**

Specify the actions that the system executes after users activate their accounts and set their initial passwords. You can use macros. Specify a descriptive name for the action, then click **OK** to display the available options.

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 25.

This chapter includes the following:



## Configuring a Profile for a Challenge Response 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 25.

A Self Service Password Reset administrator can configure the random and required questions for the users to use for resetting their password. 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.
- Enable word list dictionary so that the users do not use an answer that is present in the word list.

**To configure the default 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:

   **Challenge Profile Match**

   Specify the query that matches users with the specified profile.

   **Random Questions**

   Configure random questions for Challenge/Response. Some of these questions are presented to the user during forgotten password. Additional settings control what questions are presented to users.

   - The number of questions presented to users is set in the **Minimum Password Required** setting.
   - The number of answers Self Service Password requires the users to answer is controlled by the **Minimum Random Challenges Required During Setup** setting.

The Configuration Editor displays the default questions in different languages. When you click on the questions, you can specify different requirements for the different questions. The requirements are:

**Admin Defined:**

Select this option if you want to define the question here. Deselect this option to allow users to define their own questions.

**Min Length**

Specify the minimum length the of the answer to the challenge question.

**Max Length**

Specify the maximum length of the answer to the challenge question.

**Max Question Characters**

Specify the maximum number of characters allowed in the response that are the same in the challenge question.

**Apply Word List**

Select this option to ensure that none of the responses to the challenge questions are contained in the word list.

**New Questions**

If you do not want to use any of the default questions, you can add your own questions when you click **Add Value** at the end of the page. You specify your own questions for the users.

**Required Questions**

Define the required questions for the challenge-response. The users must answer all of these questions while setting up their responses. The users must provide answers to these questions during the resetting process of forgotten password.

When you click **Add Value**, you can specify different requirements for the different questions. The requirements are:

**Admin Defined**

Select this option if you want to define the question here. Deselect this option to allow users to define their own questions.

**Min Length**

Specify the minimum length the of the answer to the challenge question.

**Max Length**

Specify the maximum length of the answer to the challenge question.

**Max Question Characters**

Specify the maximum number of characters allowed in the response that are the same in the challenge question.

**Apply Word List**

Select this option to ensure that none of the responses to the challenge questions are contained in the word list.

**New Questions**

If you do not want to use any of the default questions, you can add your own questions when you click **Add Value** at the end of the page. You specify your own questions for the users.

You can also configure this setting in a different language. Click **Add Locale**, then select the required language from the list.

**Minimum Random Required**

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

---

**NOTE:** If you modify this setting after the users have answered the challenge-response then, the users are prompted to answer the same number of challenge questions during the Forgotten Password process instead of answering the modified number of challenge-responses. But if the users clear the responses and answer the challenge-responses again then users are prompted to answer the modified number of challenge-responses.

---

**Minimum Random Challenges Required During Setup**

Specify the minimum number of random questions the user is required to answer during the response setup.

If the specified number is higher than the available random questions, or lower than the **Minimum Random Required** value, this setting is adjusted accordingly.

The random challenge questions are shown to users during initial setup and during forgotten password recovery.

Specify 0 to force all available random questions to be configured at the time of setup.

**Help Desk Random Questions**

Specify the help desk random questions for challenge-response in this field.

Users must answer all or some of these questions when setting up their responses. This setting is controlled by the **Minimum Help Desk Random Challenges Required During Setup** setting.

The help desk users can access the questions and its responses. These questions are not used for forgotten password recovery. When you click **Add Value**, you can specify different requirements for the different questions. The requirements are:

**Admin Defined:**

Select this option if you want to define the question here. Deselect this option to allow users to define their own questions.

**Min Length**

Specify the minimum length the of the answer to the challenge question.

**Max Length**

Specify the maximum length of the answer to the challenge question.

**Max Question Characters**

Specify the maximum number of characters allowed in the response that are the same in the challenge question.

**Apply Word List**

Select this option to ensure that none of the responses to the challenge questions are contained in the word list.

**New Questions**

If you do not want to use any of the default questions, you can add your own questions when you click **Add Value** at the end of the page. You specify your own questions for the users.

You can also configure this setting in a different language. Click **Add Locale**, then select the required language from the list.

**Help Desk Required Questions**

Set up help desk required questions for challenge-response. Users must supply answers for all of these questions when setting up their responses.

The help desk users can access the questions and its responses. These questions are not used for forgotten password recovery. When you click **Add Value**, you can specify different requirements for the different questions. The requirements are:

**Admin Defined**

Select this option if you want to define the question here. Deselect this option to allow users to define their own questions.

**Min Length**

Specify the minimum length the of the answer to the challenge question.

**Max Length**

Specify the maximum length of the answer to the challenge question.

**Max Question Characters**

Specify the maximum number of characters allowed in the response that are the same in the challenge question.

**Apply Word List**

Select this option to ensure that none of the responses to the challenge questions are contained in the word list.

**New Questions**

If you do not want to use any of the default questions, you can add your own questions when you click **Add Value** at the end of the page. You specify your own questions for the users.

You can also configure this setting in a different language. Click **Add Locale**, then select the required language from the list.

**Minimum Help Desk Random Challenges Required During Setup**

Specify the minimum number of help desk random questions the users are required to answer while setting up the response.

If this number is higher than the available help desk random questions, or lower than the required questions, the setting is adjusted accordingly.

Specify 0 to force all available help desk random questions to be configured at the time of setup

6 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 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 79
- "Configuring Password Settings" on page 83
- "Configuring the Word List Settings" on page 84


# 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 25.

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.

**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 settings:

   **Password Policy Profile Match**

   Specify the query that matches specific users for the specified profile. You can query by using **Add Filter** that includes the object class, and by using **Add Group** that includes the LDAP group.

   **Minimum Length**

   Specify the minimum length of the password. Specify 0 to disable this feature.

   **Maximum Length**

   Specify the maximum length of the password. Specify 0 to disable this feature.

   **Maximum Repeat**

   Specify the maximum number of times a character can be repeated in the password. This is case-insensitive. Specify 0 to disable this feature.

   **Maximum Sequential Repeat**

   Specify the maximum number of times a character can be repeated sequentially in the password. This is case-insensitive. Specify 0 to disable this feature

   **Allow Numeric Characters**

   Select this option to allow numeric characters in the password.

**Allow First Character Numeric**

Select this option to allow the first character of the password to be numeric. This setting is applicable when only numeric characters are allowed in the password.

**Allow Last Character Numeric**

Select this option to allow the last character of the password to be numeric. This setting is applicable only when numeric characters are allowed in the password.

**Maximum Numeric**

Specify the maximum number of numeric characters you want to allow in the password. This setting is applicable when you allow numeric characters in the password. Specify 0 to disable this feature.

**Minimum Numeric**

Specify the minimum number of numeric characters you want to allow in the password. This setting is applicable when you allow numeric characters in the password. Specify 0 to disable this feature.

**Allow Special Characters**

Select this option to allow non-alphanumeric characters in the password.

**Allow First Character Special**

Select this option to allow the non-alphanumeric character to be the first character of the password. This setting is applicable when you allow the special characters in the password.

**Allow Last Character Special**

Select this option to allow the non-alphanumeric character to be the last character of the password. This setting is applicable when you allow the special characters in the password.

**Maximum Special**

Specify the maximum number of special characters allowed in the password. This setting is applicable when you allow the special characters in the password. Specify 0 to disable this feature.

**Minimum Special**

Specify the minimum number of special characters required in the password. This setting is applicable when you allow the special characters in the password. Specify 0 to disable this feature.

**Maximum Alphabetic**

Specify the maximum number of alphabetic characters allowed in the password. Specify 0 to disable this feature.

**Minimum Alphabetic**

Specify the minimum number of alphabetic characters required in the password. Specify 0 to disable this feature.

**Maximum Non-Alphabetic**

Specify the maximum number of non-alphabetic characters allowed in the password. Specify 0 to disable this feature.

**Minimum Non-Alphabetic**

Specify the minimum number of non-alphabetic characters required in the password. Specify 0 to disable this feature.

**Maximum Uppercase**

Specify the maximum number of uppercase characters allowed in the password. Specify 0 to disable this feature.

**Minimum Uppercase**

Specify the minimum number of uppercase characters required in the password. Specify 0 to disable this feature.

**Maximum Lowercase**

Specify the maximum number of lowercase characters allowed in the password. Specify 0 to disable this feature.

**Minimum Lowercase**

Specify the minimum number of lowercase characters required in the password. Specify 0 to disable this feature.

**Minimum Unique Characters**

Specify the minimum number of unique characters required in the password. Specify 0 to disable this feature.

**Maximum Characters From Previous Password**

Specify the maximum number characters that a user can reuse from the previous password in the new password. Specify 0 to disable this feature.

**Minimum Lifetime**

Specify the minimum amount of time that must pass between password changes. Value is in seconds. Specify 0 to disable this feature.

**Enable Word List**

Select this check box to enable users to check the password against the configured word list.

**Active Directory Password Complexity**

Select the Microsoft Active Directory style password complexity rules from the list:

**Active Directory 2003 Level Complexity**

Select this setting to use the following password complexity rule:

- Cannot contain the user's account name or parts of the user's full name that exceeds two consecutive characters
- Contain at least six characters in length
- Contain characters from three of the following four categories:
  - English uppercase characters (A through Z)
  - English lowercase characters (a through z)
  - Base 10 digits (0 through 9)
  - Non-alphabetic characters (for example, !, $, #, %)

**Active Directory 2008 Level Complexity**

Select this setting to use the following password complexity rule:

- Cannot contain the user's account name or parts of the user's full name that exceeds two consecutive characters
- Minimum 6 characters
- Maximum 512 characters
- Must contain following category of characters. You specify the exact number of categories by setting the **Policies > Password Policies > [profile] > Active Directory 2008 Password Complexity Maximum Violations** option.
  - European language uppercase alphabetic characters

- European language lowercase alphabetic characters of Base 10 digits (0 through 9)
- Non-alphabetic characters (for example, !, $, #, %)
- Other alphabetic characters not included in the other categories

**None**

Select this setting if you do not require any of the Active Directory password complexity rule.

---

**NOTE:** Self Service Password Reset considers the password policy that is a combination of Self Service Password Reset and Active Directory complexity. Hence, the change password page displays the policies that are a combination of Self Service Password Reset and Active Directory complexity.

If you require the exact policy of Active Directory complexity, then ensure to make changes to minimum and maximum character specifications in Self Service Password Reset policy settings as specified in the Active Directory complexity.

---

**Active Directory 2008 Password Complexity Maximum Violations**

Specify the maximum number of Active Directory 2008 Level Complexity category violations that is allowed for users.

This setting is applicable if the **Active Directory Password Complexity** setting is set to **Active Directory2008 Level Complexity**.

**Required Regular Expression Matches**

Add a Regular Expression pattern the password must match in order to be allowed. Multiple patterns can be listed. A pattern must match the entire password to be applied. The system ignores a partial match. You can use Macros.

**Disallowed Regular Expression Matches**

Specify a Regular Expression pattern the password must not match in order to be allowed. Multiple patterns can be listed. A pattern must match the entire password to be applied. The system ignores a partial match. You can use Macros.

**Disallowed Values**

Specify the list of case-insensitive values that you do not want to allow in the password. For example, password, user name, and the name of the organization.

**Disallowed Attributes**

Specify the list of attributes not allowed to be used as passwords. For a given user, the system reads the values and does not permit it to be used as part of the password value. This check is case-insensitive.

---

**NOTE:** Specifying a number after the attribute name restricts how many consecutive characters in the value are disallowed. For example, `Language:4` means the password cannot contain: `Engl`, `ngli`, `glis`, or `lish`, for English speaking users.

---

**Minimum Password Strength**

Specify the minimum password strength level required. 45 to 69 are good and above 69 are strong. A value of 0 disables this check.

**Maximum Consecutive Characters**

Specify the maximum amount of characters in a sequence such as `0123456789` or `abcdefghijk`. You can define a more specific character sequence by a Unicode character order of each character after the entire value is converted to lowercase. To disable this check set the value to 0.

**Password Change Message**

Specify the message to be displayed to the user during password changes. You can include HTML tags in messages.

---

**NOTE:** A change password message read as part of an LDAP password policy might overwrite this setting.

---

**Password Rule Text**

When blank, the system displays an automatically generated rule list to the user. The automated rule list might 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 user with having to read and parse the rules before attempting to change the password. 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.

To override the automatically generated rule list, set a value in this option. The option permits HTML tags.

**Disallow Current Password**

Prohibits the current password from being used as the new password.

---

**NOTE:** This can only be enforced if the login method permits the user's password to be known.

---

**Minimum Character Groups Required**

Specify the minimum number of defined character groups users must have in their passwords.

**Character Group Definitions**

Define a character group that users must have in their password. A character group is a regular expression character matches. For example, the following two character groups of:

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

Requires that the users have a letter or a number in their passwords. If you use the setting **Polices > Password Policies > [profile] > Minimum Character Groups Required** with this setting, you can create 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.

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

# Configuring Password Settings

After you create the password profile you must configure the settings for the password policy.

**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 > Policies > Password Settings**.

5 Configure the following settings:

**Password Policy Source**

Select any one of the following:

**LDAP**

Self Service Password Reset reads the LDAP password policies. If you select this option, Self Service Password Reset ignores some of the Self Service Password Reset password policy settings.

**Local**

Self Service Password Reset reads the Self Service Password Reset policies. If you select this option, Self Service Password Reset ignores any policy settings of the LDAP directory.

**Merge Local and LDAP**

Self Service Password Reset reads both policies. If any conflict between these policies, Self Service Password Reset chooses the most restrictive value of the policy.

**Enable Shared History**

Select this option if you want to enable a global shared password history for all users on **Main Menu**. If enabled, all users share a common password history. This helps prevent usage of common organizational words in passwords. The system stores passwords as a salted and encrypted hash in the local database.

**Shared History Age**

Specify the maximum age of the shared history storage in seconds. The default value is four weeks (2419200 seconds).

**Password is Case Sensitive**

Select the required option from the following list that controls the use of case-sensitive password:

- **Read from Directory**
- **True (Case Sensitive)**
- **False (Case Sensitive)**

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.

**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**.

4 Click **Settings > Word Lists**.

5 Configure the following settings:

**Word List File URL**

Specify a word list file URL for dictionary checking to prevent users from using commonly used words as passwords. Using word lists is an important part of password security. Word lists are used by intruders to guess common passwords. The default word list included contains commonly used English passwords.

The first time a startup occurs with a new word list setting, it will take some time to compile the word list into a database. See the status screen and logs for progress information. The word list file format is one or more text files containing a single word per line, enclosed in a ZIP file. The String `!#comment:` at the beginning of a line indicates a comment.

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

**Word List Case Sensitivity**

Select this option if you want to use the word list as case-sensitive for all matches. Changing this value causes a word list re-compilation.

**Word List Word Size Check**

Specify the number of characters in a word that Self Service Password Reset checks against the configured word list.

For example, if the word to be checked is word list and this setting is set to 6, then the system checks these combinations wordli, ordlis, and rdlist against the configured dictionary. If any of these values match, then the entire value is a match to the word list. If you specify 0 (the number) or the password to check is smaller than the value specified here, then the system checks the entire password against the word list by not any smaller parts of the password.

**Seed List File URL**

Specify the URL for the seed list. The value must be a valid URL, using the protocol `file` (local file system), `http`, or `https`.

When passwords are randomly generated, the system can generate friendly random password suggestions to users. It does this by using a seed word or words, and then modifying that word randomly until it is sufficiently complex and meets the configured rules computed for the user.

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

# 8 Configuring the User Experience

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 Branding of Self Service Password Reset

Self Service Password Reset includes a flexible theme mechanism that allows for maximum customization of look and branding of the Self Service Password Reset application for your users. You can make the following changes:

- Change the look and feel of the Self Service Password Reset user interface. Self Service Password Reset provides several standard themes. Each theme is an extension or modification of the default theme.
- Determine whether to display or hide certain options, buttons, and messages on the user interface.
- Customize the password guide text.
- Determine the theme's language.

You customize Self Service Password Reset through the **Configuration Editor**. You can also view a video about how to customize the theme for Self Service Password Reset. To view the video, see How to Create a Custom Theme in Self Service Password Reset.

**To configure user interface 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** > **User Interface** > **Look & Feel**.
5. Configure the following settings:

   **Interface Theme**

   Select an appropriate theme from the list.

If you select **Embedded**, the system uses the Embedded CSS style sheet and the Embedded Mobile CSS style sheet to manage the custom CSS tags. Self Service Password Reset expects the themes to be available at the URL paths:

- `@PwmContextPath@/public/resources/[theme]/style.css`
- `@PwmContextPath@/public/resources/[theme]/mobileStyle.css`

You can add additional themes using the **Custom Resource Bundle** option. You can also overwrite the default theme by specifying the URL parameter of **the theme**. For example:

```
https://www.example.com:@PwmContextPath@?theme=sterile
```

**Embedded CSS Stylesheet**

Specify the contents of the custom CSS style sheet.

To implement this setting, you must set **Embedded** as theme under **User Interface** > **Theme**. The contents of this setting can be served from the URL of `/public/resources/themes/embed/ssprStyle.css`.

**Embedded Mobile CSS Stylesheet**

Specify the contents of the custom mobile CSS style sheet.

To implement this setting, you must set **Embedded** as theme under **User Interface** > **Theme**. The contents of this setting can be served from the URL of `/public/resources/themes/embed/ssprMobileStyle.css`.

**Embedded JavaScript**

Provide a Javascript to include a particular content in all pages inside an HTML tag near the bottom of the page.

**Custom Resource Bundle**

Select **Custom** to upload a custom ZIP file containing static HTTP resources that Self Service Password Reset serves from the HTTP path `/public/resources/` that it adds to the configuration.

The maximum ZIP file size is 10MB. Files included are types of HTML, text, images, and so forth. Self Service Password Reset does not perform any server-side processing when serving these files.

6 Click **Settings > User Interface > UI Features**.

7 Configure the following settings:

**Enable Showing Masked Fields**

Enable this option if you want to allow users to toggle the **Show/ Hide** button wherever required. This setting applies to all HTML masked password fields, regardless of the actual data type.

**Mask Password Fields**

Enable this option to hide the input fields with a standard password masking.

**Mask Response Fields**

Enable this setting to mask the challenge-response answers with standard password masking. This setting applies to both setup responses and forgotten password response entry screens.

**Show Cancel Button**

Enable this option to display the **Cancel** button to users wherever applicable.

When users click **Cancel**, the system sends users to the forward URL (or logout URL if the password has been modified). The **Cancel** button does not appear on the Change Password screen if:

- The password is expired
- JavaScript is not enabled in the browser

**Show Success Pages**

Select this option to enable Self Service Password Reset to display success messages when an activity completes successfully.

**Show Login Page Options**

Select this option to display the **Forgotten Password** and other options on the Login page.

**Show Logout Button**

Select this option to display the **Log Out** button to an authenticated user.

**Show Home Button**

Select this option to display the **Home** button to an authenticated user.

**Show Idle Timeout Counter**

Select this option to display the user's remaining idle time. When that time reaches zero, the system redirects the user to the logout page.

8 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 the 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 in 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**.

# Configuring CAPTCHA

Self Service Password Reset has integrated support for the CAPTCHA protection. CAPTCHA prevents from automated attack. Self Service Password Reset uses the online re CAPTCHA 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 configure in Self Service Password Reset for the reCAPTCHA support.

**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. Configure the following settings:

   **reCAPTCHA Public Key**

   Specify the public reCAPTCHA key. Leave this field blank if you do not want to perform CAPTCHA verification.

   **reCAPTCHA Private Key**

   Specify the private reCAPTCHA key. Leave this field blank if you do not want to perform CAPTCHA verification.

   **CAPTCHA Protected Pages**

   Select the pages that must be CAPTCHA protected. Self Service Password Reset only requires the CAPTCHA validation for the first instance of a session. If during the same session the users visit all those selected pages, then they do not have to perform the CAPTCHA validation on each page.

   **Captcha Skip Parameter Value**

   Specify the parameters and include the `skipCaptcha` key for the parameters that you want to skip the CAPTCHA request. This setting is useful for internal clients and links where CAPTCHA is not required.

   For example, if “Forgotten Password” is checked, Self Service Password requires CAPTCHA validation to access the “Forgotten Password” page.

   **Captcha Skip Cookie**

   Specify the browser cookies. that you want Self Service Password Reset to skip the CAPTCHA request.

   **Captcha Intruder Attempt Trigger**

   Specify the number of intruder attempts before Self Service Password Reset requires CAPTCHA. If set to 0, Self Service Password Reset ignores the intruder attempt count and it always requires CAPTCHA. Self Service Password Reset considers intruder attempts for the current session and for the source network address.

   The recommended value for this setting is 0. However, determined network attackers might be able to bypass the CAPTCHA verification altogether if you use this setting.
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. 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 21.



## 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.

**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. Configure the following settings:

   **SMTP Email Server Address**

   Specify the SMTP server address for sending emails. This is a mandatory setting. Ensure that the server you specify here allows relaying. For best results, use a local SMTP server.

   **SMTP Email Server Password**

   Specify the password that Self Service Password Reset uses to access the SMTP server.

   **SMTP Email Server Port**

   Specify the port number of the SMTP server.

   **Default From Address**

   Specify the email address that is the default from email address for all emails.

   **SMTP Email Server User Name**

   Specify the user name for the SMTP server. Only this user can log into the SMTP server to send an email. If you do not specify any user here, the system sends SMTP messages without authentication.

   **Maximum Email Queue Age**

   Specify the maximum time (in seconds) an email can wait in the send queue. If an email is in the send queue longer than this time, the system discards it. An email persists in the send queue if there is any input error, output error, or network error to the SMTP server while sending the email.

**SMTP Email Advanced Settings**

Specify the name/value settings to control the behavior of the mail agent. You define the available settings as part of the JavaMail API. The settings must be in the `name=value` format, where name is the key value of a valid JavaMail API setting.

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

# Configuring Email Templates

Self Service Password Reset contains many different email templates for you to configure. The system does not send out any emails until you configure the templates. You must decide which templates you want to configure to have the emails automatically sent to your users.

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:

---

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

---

**Change Password Email**

Configure the email format that they system sends to users when they change their passwords. For example, the sender's address, subject, format, and text of the email body.

**Help Desk Change Password Email**

Configure the email format that the system sends to users when the help desk changes their passwords. For example, the sender's address, subject, format, and text of the email body.

**Update Profile Email**

Configure the email format that the system sends to users when they update their profiles. For example, the sender's address, subject, format, and text of the email body.

**Update Profile Email Verification**

Configure the email format that the system sends to users during profile email validation. For example, the sender's address, subject, format, and text of the email body.

**New User Email**

Configure the email format that they system sends to new users. For example, the sender's address, subject, format, and text of the email body.

**New User Verification Email**

Configure the email format that the system sends to new users after they register with links to verify the registration. For example, the sender's address, subject, format, and text of the email body.

Use `%TOKEN%` to insert the token value into the email.

**Activation Email**

Configure the email format that the system sends to new users after they successfully activate their account. For example, the sender's address, subject, and format and text of the email body.

**Activation Verification Email**

Configure the email format that the system sends to new users during the activation verification process. For example, the sender's address, subject, and text of the email body including the verification link.

Use `%TOKEN%` to insert the token value into the email.

**Forgotten Password Verification Email**

When users request for the password reset, they receive a verification email. Users must click the link available in the email to authenticate the request.

Configure the email format and other details such as sender's address, subject, and text of the email body including the verification link.

Use `%TOKEN%` to insert the token value into the email.

**Help Desk Verification Email**

Configure the email format that the system sends to users for verification of the help desk changes. For example, the sender's address, subject, and text of the email body including the verification link.

Use `%TOKEN%` to insert the token value into the email.

**Send Password Email**

The system sends an email to the user with the new password during forgotten password reset process. This setting is valid if you enabled the send password functionality.

Configure the email format and other details such a sender's address, subject, and text of the email body.

**Send User Name Email**

The system sends an email to the user with the new user name during forgotten password reset process.

Configure the email format and other details such a sender's address, subject, and text of the email body.

**Intruder Notice Email**

When a user or any intruder attempts to reset the password with incorrect responses that locks the user account, the user receives an email to notify them that the system disabled the account due to the lockout.

Configure the email format and other details such a sender's address, subject, and text of the email body.

**Delete Account Email**

The system sends an email to the user after the Account Delete action.

Configure the email format and other details such a sender's address, subject, and text of the email body.

**Help Desk Unlock Account Email**

The system sends an email to the user when the account is unlocked by the help desk.

Configure the email format and other details such a sender's address, subject, and text of the email body.

**Unlock Account Email**

The system sends an email to the users who unlock their own accounts.

Configure the email format and other details such a sender's address, subject, and text of the email body.

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 94
- "Configuring the SMS Messages" on page 96


## 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.

**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 Configure the following settings:

**Maximum SMS Queue Age**

Specify the maximum age (in seconds) an SMS can wait in the local send queue. If an SMS is in the send queue longer than this time, the system discards it. SMS messages only persist in the send queue if there is an IO or network error to the SMS gateway server while sending the message.

**SMS Gateway**

Specify the URL of the SMS service provider.

**SMS Gateway User**

Specify the user name of the SMS gateway.

**SMS Gateway Password**

Specify the password for the SMS gateway user.

**HTTP(S) Method**

Specify the HTTP or HTTPS protocol method that you want to use for sending SMS messages. It is either POST or GET.

**SMS Gateway Authentication Method**

Select a method from the list that the SMS gateway uses for authentication.

**SMS Request Data**

Specify the details required to send an SMS message. You can use the following codes:

- **%USER%:** authentication user name
- **%PASS%:** authentication password
- **%SENDERID%:** sender's identification
- **%TO%:** recipient's phone number
- **%REQUESTID%:** randomly generated request identifier
- **%MESSAGE%:** the SMS message

Example format: `user=%USER%&pass=%PASS%&to=%TO%&msg=%MESSAGE%`

**SMS Data Content Type**

Specify the content type of the POST data. This is the mime type for the content. This only applies if the **HTTP(S) Method** is POST.

Common values include:

- **application/x-www-form-urlencoded:** HTTP form data
- **text/plain:** Plain ASCII data
- **text/xml:** XML document

You can also append a character set. For example, `application/x-www-form-urlencoded; charset=utf-8: HTTP form data in UTF-8 encoding`

**SMS Data Content Encoding**

Select the type of encoding for the SMS data. The SMS data might need encoding or escaping.

**SMS Gateway HTTP Request Headers**

Specify any additional HTTP request headers for the SMS request. For example, `SOAPAction` for SOAP messages.

**Maximum SMS Text Length**

Specify the maximum length of the SMS text. Some services allow texts longer than one message (generally 140 bytes). If the text is longer than the configured maximum, the system makes multiple requests.

**Response Regular Expressions**

Specify the regular expression that you can use to determine whether the system sent the SMS successfully to the gateway. If the response matches any of the expressions, Self Service Password Reset considers the transmission successful. If you do not specify any expressions, Self Service Password Reset assumes that all transmissions are successful.

If the response matches none of the expressions, Self Service Password Reset retries the SMS later (default 30 seconds). Use the **Maximum SMS Queue Age** option to limit the number of retries.

---

**NOTE:** The string must match an entire line. Use `.*` to match anything after the required texts.

---

**SMS Sender ID**

Specify the ID of the sender for the SMS message. You can use alphanumerical values in this identification. If you leave this field blank, the provider uses a default or anonymous sender identification. SMS provider validates the sender ID. Contact your SMS provider for values that you can use as sender identification.

**SMS Phone Number Format**

Select a phone number format from the list that Self Service Password Reset uses while sending SMS.

**Default SMS Country Code**

Specify the default country code for SMS phone numbers. Set to 0 to disable.

For a list of country codes, see (http://countrycode.org/).

**Request ID Characters**

Specify the characters that you want to be included in the random string generated by **SMS Request Data**.

**Request ID Length**

Specify the length of the random string generated by **SMS Request Data**.

**Use URL Shortener**

Select this option to use a URL shortener service such as `tinyurl.com`, `bit.ly`, and `goo.gl`. This enables searching the SMS text for HTTP and HTTPS URLs and replaces them with a shortened version.

**Successful HTTP Result Codes**

Specify the HTTP result codes that are considered successful send attempts.

**Enable URL Shortening Service Class**

Specify the URL Shortening Service class name. This is the Java full class name that implements a short URL service. The corresponding JAR or ZIP file must be included in the classpath, typically in the `WEB-INF/lib` directory or the `lib` directory of the application server.

**Configuration Parameters for URL Shortening Service**

Specify the `Name/Value` settings used to configure the selected URL shortening service. For example, use an API key, a user name, a password or a domain name. The settings must be in `name=value` format, where `name` is the key value of a valid service setting.

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.

**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.

**Forgotten Password SMS Text**

Specify the text of the SMS message Self Service Password Reset sends during the forgotten password token process.

**Forgotten Password New Password SMS Text**

Specify the text of SMS message Self Service Password Reset sends when the users create new passwords during forgotten password process.

**New User Verification SMS Text**

Customize the text of the SMS messages Self Service Password Reset sends during the new user verification process.

**Help Desk Verification SMS Text**

Specify the text of SMS message Self Service Password Reset sends during the Help Desk token verification process.

**Activation Token SMS Text**

Customize the text of the SMS message that contains the token Self Service Password Reset sends during the activation process.

**Activation SMS Text**

Customize the text of the SMS message that Self Service Password Reset sends after a successful activation.

**Forgotten User Name SMS Text**

Specify the text of the SMS message Self Service Password Reset sends upon a successful forgotten user name sequence, if you configured the **Forgotten User Name** setting.

**Update Profile SMS Verification Text**

Specify the text of the SMS message Self Service Password Reset sends during a profile update of the SMS phone number verification.

5 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:** The time (in seconds) for LDAP server, Self Service Password Reset server and mobile device must be 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 the Forgotten Password Module” on page 63.

**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 **Settings > One Time Password**.
5. Configure the following fields:

   **Enable One Time Passwords**

   Enable this option if you want to enable and configure the one-time password settings.

   **Force Setup of One Time Passwords**

   Select the appropriate option from the list.

   **Force Setup**

   Select this option if you want the user to configure one-time password when they log in for the first time.

   **Force Setup - but allow user to skip**

   Select this option if you want to provide option to the user to either configure one-time password or skip the configuration for the one-time password when they log in for the first time.

   If the verification method specified in the forgotten password policy is set to challenge-response as required and OTP as optional, then users are prompted to enroll for OTP but have an option to skip enrolling.

   **Do not force setup**

   Select this option if you do not want to force the user to configure the one-time password when they log in.

   Self Service Password Reset forces the user to configure one-time password if they do not have a current valid secret stored, even if you select **Do not force setup**.

   **OTP Secret Read Location**

   Select where to read the OTP secret. If you select an option with multiple values, each location is read in turn until the system finds a stored response.

   **OTP Secret Write Location**

   Select the location where to write the OTP secret. Self Service Password Reset writes to all storage methods when the users configure their response answers.

   **Token Storage Method**

   Select the storage format that must be used to save the one-time password secrets.

   **PWM JSON**

   Select this option to store the secret, descriptions, and recovery codes in PWM native (JSON) format.

   **Base32 secret**

   Select this option to store only the TOTP secret as a base32 encoded string. This format does not support recovery codes or counter based tokens.

   **OTP URL**

   Select this option to store only the TOTP secret as a base32 encoded string. This format does not support recovery codes or counter based tokens.

**PAM text**

Select this option to store the secret, descriptions, and recovery codes in the text file format, which the Google Authenticator PAM module uses.

**Encrypt OTP secret**

Enable this option to encrypt the OTP secret. Self Service Password Reset uses the Security Key for encrypting and decrypting token information. Different application instances must use the same Security Key. If you change the Security Key, Self Service Password Reset cannot use the stored OTP password.

**OTP Secret LDAP Attribute**

Specify the LDAP attribute for storing the OTP secret. Only use this setting when the storage method is set to **LDAP**.

**OTP Secret Setup Permission**

Set an LDAP search filter query for the users who are allowed to set up an OTP secret. You can add multiple filters by providing the object class. You can also search users by providing the LDAP group name.

You can add multiple filters, and groups. To view the list users who match the query click **View Matches**.

**OTP Secret Identifier**

Specify the user identifier that must be linked to the secret stored. You can use macros such as `@User:Email@`

**OTP Recovery Codes**

Specify the number of OTP recovery codes to supply to users. Users can use recovery codes one-time each to authenticate and are intended for occasions when the users lose access to their OTP devices. Specify 0 to disable recovery codes. Not all storage formats support recovery codes.

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

# Configuring Self Service Password Reset for Single Sign-On Clients

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 99
- “Configure HTTP for Single Sign-On” on page 100
- “Configuring OAuth Single Sign-On” on page 100


## 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 settings:

**Enable Basic Authentication**

Enable this option to enable basic authentication for Self Service Password Reset. By default, this option is enabled.

**Force Basic Authentication**

Enable this options to force basic authentication. If false, then the system presents the form page for unauthenticated users, however, if a basic auth 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 automatically log users into an application with a user name only.

**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 setting:

**SSO Authentication Header Name**

Specify the name of the HTTP header that configures Self Service Password Reset to use an upstream server to allow automatic logins with only a user name, a password is not required. This setting controls the name of the HTTP header. When used, Self Service Password Reset 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 https://oauth.net/2/.

Use the following information to create an OAuth single sign-on experience for your users. You must gather information from the OAuth Identity Server of your application.

**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 settings:

**OAuth Login URL**

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

**OAuth Code Resolve Service URL**

Specify the URL for OAuth Code Resolve Service. Self Service Password Reset uses this web service URL for resolving the artifact that the OAuth identity server returns.

**OAuth Profile Service URL**

Specify the URL for the web service that the Identity Server provides to return attribute data about the user.

**OAUTH Web Service Server Certificate**

Import a certificate for the OAuth web service server.

**OAuth Client ID**

Specify the client ID of the OAuth client. The OAuth Identity Service provider gives you this identity.

**OAuth Shared Secret**

Specify a password for the OAuth shared secret. The OAuth Identity Service provider gives you this value.

**OAuth User Name/DN Login Attribute**

Specify the attribute that you want the OAuth server to identify as the user name for local authentication. Self Service Password Reset then resolves this value as the same password that the users type at the local authentication page.

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 Self Service Password Reset to send a random token in different scenarios such as during a new user registration and forgotten password recovery. 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.

**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 Configure the following settings:

**Token Storage Method**

You can configure the storage method used to save tokens. Self Service Password Reset supports the following methods:

**LocalDB**

Use this method to store tokens in the local database. If you select this method, tokens do not work across multiple application instances.

**Database**

Use this method to store tokens in an external database. If you select this method, tokens work across multiple application instances.

**Crypto**

Use this method to create and read tokens. Tokens are not stored locally and work across multiple application instances if they have the same security key.

---

**NOTE:** When you select **Crypto**, ensure that you have configured a security key, otherwise, tokens do not work. For more information about how to configure a security key, see "Configuring Security Settings" on page 27.

---

**LDAP**

Use this method to store tokens in the LDAP directory. Tokens work across multiple application instances. You cannot use LDAP tokens as new user registration tokens.

The system generates tokens by using the length and character configuration options (except when using the Crypto method). When you use the Crypto method, tokens are longer.

**Token Characters**

Specify the available characters for the email token.

**Token Length**

Specify the length of the token.

**Token Maximum Lifetime**

Specify the time in seconds for which a token is valid. Default value is one hour.

**Token LDAP attribute name**

Specify a name for the LDAP attribute token. Self Service Password Reset uses the LDAP attribute to store and search for tokens when you select this option.

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

# 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 few settings in the Access Gateway, a component of Access Manager. To enable Self Service Password Reset to integrate with Access Manager, configure the extensions settings. For more information, see Configuring External Web Services Extensions.

This chapter includes the following topics:



## Configuring Access Gateway for Self Service Password Reset

This section discusses the configuration required for the Access Gateway to integrate it with Self Service Password Reset.



### 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 need 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 104.

| 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)**.

# Integrating Self Service Password Reset with Access Manager

Self Service Password Reset provides various options for integration with Access Gateways including configurable redirection URLs, servlet command options, and support for HTTP basic authentication. The following are important configurations:

- **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 password change operation is completed. 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 48. 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

Configure the following Self Service Password Reset settings using 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. 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**.

## Configuring Password Expiration Servlet

You must configure the Access Gateway to redirect users to Self Service Password Reset when their password expires. You can configure this in Access Manager.

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**.

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 Forgotten Password URL

Administrators can configure the Access Manager Identity Server login 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>
```

# 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` |

# 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. |

| URL Example | Description |
|---|---|
| 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%2Fportalpage.htm
l"/>
 </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%2Fportalpage.htm
l">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 requires to change 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. |

# 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.

Prior releases of Self Service Password Reset integrated with Advanced Authentication through Endpoints. This release of 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, going forward 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

When using Advanced Authentication for forgotten password, you must ensure the following:

- ❒ Install and configure the Advanced Authentication server version 5.4 or later.

  For more information about configuring the Advanced Authentication server, see the *Advance Authentication Server Administration Guide*.
- ❒ Create and configure the Advanced Authentication repositories. For more information, see “Adding a Repository” in the *Advance Authentication Server Administration Guide*.
- ❒ A good understand of Oauth2. For more information, see https://oauth.net/2.

## 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-AdvancedAuthentication/admin`

2 Click **Event**, then click **Add** to create a new Event for Self Service Password Reset.

3 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**

Use the value of the Self Service Password Reset site URL with /public/oauth at the end of the URL for the value of this option. For example:

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

4 Click **Save**, to save the OAuth2 Event type in Advanced Authentication.

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 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.

**To configure an OAuth 2 connection 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 Click **Modules > Public > Forgotten Password > Profile > default > OAuth**.

5 Configure an OAuth 2 connection to Advanced Authentication. For more information, see “Configuring the OAuth2 Verification Method for the Forgotten Password Module” on page 68.

6 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

Self Service Password Reset ships as part of Identity Manager and is installed with the integrated installer. All of the releases of Self Service Password Reset have not synchronized with the Identity Manager release. The following table lists what versions of Self Service Password Reset shipped with what version of Identity Manager and what versions of Self Service Password Reset are supported with Identity Manager.

***Table 11-1*** *Support Matrix for Identity Manager and Self Service Password Reset*

| | **Supported** |
|---|---|
| Identity Manager 4.5 | Self Service Password Reset 3.3.*x* and 4.1.*x*. |
| Identity Manager 4.6 | Self Service Password Reset 4.1.*x* |

**IMPORTANT:** 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 4.1 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 116.

# 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 116
- “Set the Self Service Password Reset Theme to Match the Identity Manager Theme” on page 118
- “Configure Syslog Audit server” on page 118

**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 Identity Manager to Use Self Service Password Reset ” 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 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`

   **OAuth Profile 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 Web Service 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.

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 126.

# 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 or 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.

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 allow a user to read passwords by using Self Service Password Reset proxy user:**

1. Log in to iManager.
2. Select **Roles and Tasks** from the header icons.
3. Select **Passwords** > **Password Polices.**
4. Select the appropriate password policy.
5. Click the **Universal 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 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

Self Service Password Reset allows you to back up and store the configuration information for Self Service Password Reset. 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 need to restore the information, see “Importing Configuration Information” on page 121.

## 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 129.
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.

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.

---

# 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

The reports that Self Service Password Reset provide are a summary report and a detailed report on password change status, 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. This section discusses various settings that enable reporting for Self Service Password Reset.

**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. Configure the following settings:

   **Enable Directory Reporting**

   Select this option to enable directory reporting. You can maintain a local cache to store user data. To use this option you need additional disk space and Java heap memory.

   **Reporting Search Filter**

   Specify the LDAP search filter to generate the required report. If you do not provide a value, the system generates a filter based on the login query setting.

   **Maximum Cache Age**

   Specify the maximum time limit, in seconds, to keep a record of a cached report before discarding it. Records older than this time gets periodically purged from the local report data cache. The default value is 25,92,000 seconds (30 days).

   **Minimum Cache Age**

   Specify the minimum time limit, in seconds, to keep the record of a cached report until you want to re-read the cached report. For example, setting this value to one day (86400) would mean that a given cached report can be read for a day, regardless of how often the report is run.

   **Engine User Search Rest Time**

   Set the time interval, in milliseconds, that must be used between two searches.

   **Maximum LDAP Query Size**

   Specify the maximum number of records that can be read during a reporting query search. Setting this value to larger sizes require more Java heap memory.

**Reporting Job Time Offset**

Specify the number of seconds to process records after midnight (GMT). Setting the value to `-1` disables the nightly job processor.

**Reporting Summary Day Intervals**

Select the day intervals to include in report summary data.

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.

**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 through 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 124
- "Viewing Logs" on page 126


## 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 need to 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. Configure the following settings:

   **Console (StdOut) Log Level**

   Select the appropriate log level for `StdOut`. Most servlet containers redirect `StdOut` to a log file. For example, Tomcat logs `StdOut` output to the `tomcat/logs/catalina.out` file by default.

   **LocalDB Log Level**

   Select the appropriate log level for the local database. You view the log events written to the local database in the Administrator event log viewer. For more information, see "Viewing Logs" on page 126.

   **File Log Level**

   Select the appropriate log level to log events to the local file log. The system writes the log files to the `WEB-INF/logs` directory of the servlet.

   **Maximum LocalDB Events**

   Set the maximum log events stored in the local database. Each 100,000 log events consumes approximately 100 MB of disk space. The local database retains this number of events and uses these events to display in the log viewer. For more information, see "Viewing Logs" on page 126.

   This setting does not affect the normal log files configured in the `log4jconfig.xml` file or the log file settings for Tomcat.

   **Maximum Age LocalDB Events**

   Set the maximum age of events stored in the local database (seconds). The system periodically purges events older than the configured value. The default value is four weeks (60s * 60m * 24h * 7d * 4w = 2419200). The system does not remove events due to age if you specify a value of 0.

   **Daily Summary Alerts**

   Enable this option to send an email alert once a day (at 0:00 GMT) that contains a summary of the statistics and health for the day.
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 124 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

In order 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

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. Configure the following settings:

   **System Audit Event Types**

   Select the system event types to record and take action.

   **User Audit Event Types**

   Select the user audit event types to record and take action.

   **LocalDB Audit Events Storage Max Age**

   Specify the maximum age (in seconds) of the local audit event log. The default is 30 days.

   **LocalDB Audit Events Storage Max Events**

   Specify the maximum count of events in the local audit event log. The default is 1000000.
6. In the toolbar, click **Save changes**.

# Forwarding Auditing Information

You can forward auditing events to external systems to analyze the 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 Editor**.
4. Click **Settings > Auditing > Audit Forwarding**.
5. Configure the following settings:

   **System Audit Event Email Alerts**

   Specify the email address where you want to send the system audit events information. You can provide multiple email addresses.

   **User Audit Event Email Alerts**

   Specify the email address on which you want to send the user audit events information. You can provide multiple email addresses.

   **Syslog Audit Servers**

   Self Service Password Reset can send events to the Syslog service. Specify Syslog audit servers information as follows:

   - **Protocol**: TCP, UDP or TLS/ SSL
   - **Host**: Host name or IP address of the computer running the Syslog service
   - **Port**: Port number where the Syslog service is listening

   **Syslog Audit Server Certificates**

   Import the certificates from the Java keystore to configure TLS/SSL from the Syslog service.
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. Configure the following settings:

   **User History Storage Location**

   Select the data store location where to store the user-specific audit history. The options are **LDAP** and **Remote Database**.

   **Use History Event**

   Select the event types to store for the user audit history.

   **User History Maximum Events**

   Specify the maximum number of events to hold in the event history attribute for a user.
6. Select **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

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 139.

Ensure that you back up your configuration information before applying any updates. For more information, see "Backing Up Configuration Information" on page 121.

## 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 NetIQ Patch Finder (https://dl.netiq.com/patch/finder).
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 4.1 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 121.
   - **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 121.

# 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 NetIQ Patch Finder (https://dl.netiq.com/patch/finder).
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 Self Service Password Reset on Windows" in the *Self Service Password Reset 4.1 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 Self Service Password Reset on Windows" in the *Self Service Password Reset 4.1 Installation Guide*.

# 13 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 Console, because native Linux tools are not aware of the configuration requirements and dependencies of the Self Service Password Reset services.

**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 using the Appliance Configuration tools.

The Appliance System Configuration page displays the following options:

- Setting Administrative Passwords
- Configuring Network Setting
- Configuring Time Settings
- Accessing System Services
- Managing Digital Certificates
- Configuring the Firewall
- Using the Ganglia Configuration and Monitoring
- Sending Information to Support
- Adding a Field Patch to the Appliance
- Performing an Online Update
- Performing a Product Upgrade
- Rebooting or Shutting Down the Appliance
- Logging Out

## Setting Administrative Passwords

Use the Administrative Passwords tool 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 administration 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 133.

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 Administration 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**.

# 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 perform the following actions:

- Starting, Stopping, or Restarting System Services
- Making System Services Automatic or Manual

## Starting, Stopping, or Restarting System Services

You might want to start, stop, or restart the SSH or the Self Service Password Reset service.

**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.

## Making System Services Automatic or Manual

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 Digital Certificates

Use the Digital Certificates tool 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:


- "Using the Digital Certificate Tool" on page 134
- "Using an Existing Certificate and Key Pair" on page 136
- "Activating the Certificate" on page 136


## Using the Digital Certificate Tool


- "Creating a New Self-Signed Certificate" on page 134
- "Getting Your Certificate Officially Signed" on page 135


### Creating a New Self-Signed Certificate

1. Log in to the Appliance Management Console as the `vaadmin` user.
2. Click **Digital 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 135.

## Getting Your Certificate Officially Signed

1 On the Digital Certificates page, select the certificate that you just created, then click **File** > **Certificate Requests** > **Generate CSR**.

2 Complete the process of emailing your digital 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 Digital 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 Digital Certificates page, the name in the **Issuer** column for your certificate changes to the name of the CA that stamped your certificate.

4 Activate the certificate, as described in "Activating the Certificate" on page 136.

## 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 **Digital 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 136.

## Activating the Certificate

1. On the Digital 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 Digital Certificates.

# Configuring the Firewall

Use the Firewall tool 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 4.1 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

# Using the Ganglia Configuration and Monitoring

Ganglia is a scalable, distributed monitoring system that allows you to gather important information about your appliance. The default metrics that you can monitor are CPU, disk, load, memory, network, and process.



## Configuring Ganglia

Use the Ganglia Configuration tool to configure monitoring for the appliance. The Ganglia `gmond` daemon uses UDP port 8649 for communications. The `gmetad` daemon uses TCP port 8649 for metrics data. You can also enable or disable non-secure HTTP viewing of the metrics on port 9080.

1. Log in to the Appliance Management Console as the `vaadmin` user.
2. Click **Ganglia Configuration**.
3. As appropriate, change the following Ganglia configuration options:

   **Monitoring Services**

   - **Enable Full Monitoring Services:** Select this option to receive and store metrics from other appliances, and to allow the Ganglia Web Interface to run on the appliance. This option is enabled by default.

     You might want to disable Ganglia monitoring by deselecting this option:

     - If you already have a monitoring system that you plan to use for the appliance.
     - If you plan to configure a dedicated appliance for viewing monitoring information.

       You specify a dedicated appliance by selecting **Unicast** under Monitoring Options, and then specifying the DNS name or IP address of the appliance that collects the monitoring information.

   **Monitoring Options**

   - **Enable monitoring on this appliance:** Select this option to enable Ganglia monitoring on this appliance.
     - **Multicast:** Select this option to send monitoring information to other appliances on the network. This option is selected by default.
     - **Unicast:** (Recommended) Select this option to send monitoring information to a single destination.

       ---

       **NOTE:** Unicast mode is recommended for improving performance of the system.

       ---

       **Publish to:** Specify the URL where Ganglia sends monitoring information when it is running in Unicast mode.

   **Monitoring Tool Options**

   - **Enable direct http port 9080 access:** Select this option to enable the Ganglia Monitoring dashboard to be available directly at the following URL using the non-secure http protocol and port 9080:

     http://*ptm_dns_server_name*:9080/gweb/

4. (Optional) Click **Reset Database** to remove all existing Ganglia metrics from the Ganglia database on this appliance.
5. Click **OK**.
6. Click **Close** to exit Ganglia Configuration.

## Viewing Ganglia Metrics Using the Appliance Management Console Port 9443 (Secure)

Use the Ganglia Monitoring tool to securely view the Ganglia Dashboard in the Appliance Management Console using port 9443. The dashboard displays the health and status metrics for the appliance.

1. Log in to the Appliance Management Console as the `vaadmin` user.
2. Click **Ganglia Monitoring**.

   The Ganglia Dashboard opens in a new tab to the following web page:

   https://*ptm_dns_server_name*:9443/gweb/
3. When you are done viewing information, close the Ganglia tab in your web browser.

## Viewing Ganglia Metrics Directly Using Port 9080 (Not Secure)

1. Ensure that you have enabled **Monitoring Tool Options > Enable direct http port 9080 access.**
2. In a web browser, access the following URL:

   http://*ptm_dns_server_name*:9080/gweb/

   No login is required.
3. When you are done viewing information, close your web browser.

# Sending Information to Support

Use the Support tool to send configuration information to Technical Support (https://www.netiq.com/support/) by uploading files directly with 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 manage Self Service Password Reset appliance software updates and security updates for the software and operating system. You can install new patch updates, view currently installed patch updates, and uninstall patch updates. You download patch updates from NetIQ Patch Finder (https://dl.netiq.com/patch/finder/).

**To manage patch updates:**

1. Log in to the Appliance Management Console as the `vaadmin` user.
2. Click **Field Patch**, then follow the prompts to install the patch update.
3. (Conditional) Install a downloaded patch update:
   - **3a** Download the Self Service Password Reset patch update file from the Patch Finder website to your management computer.
   - **3b** On the Field Patch page in the **Install a Downloaded Patch** section, click **Browse**.
4. (Conditional) Uninstall a patch update:

   You might not be able to uninstall some patch updates.
   - **4a** In the **Patch Name** column of the Field Patch list, select the patch update that you want to uninstall.
   - **4b** Click **Uninstall Latest Patch**.
5. (Conditional) Download a log file that includes details about the patch update installation.
   - **5a** Click **Download Log File** for the appropriate patch update.
6. Click **Close** to exit the Field Test Patch page.

# Performing an Online Update

Use the **Online Update** option to register for the online update service from the Customer Center (https://www.netiq.com/customercenter). You can install updates automatically or manually to update the Self Service Password Reset appliance. You must be connected to the internet to use this feature.

To activate the Update Channel, you obtain the key from the Customer Center. If the key is not available, contact the Customer Center through an email from within the Customer Center.

**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 to automatically agree with the licenses.

  **To schedule online update:**

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

This option does not work in the Self Service Password Reset 4.1 release. If you use this option to try and upgrade from Self Service Password Reset 4.0 to 4.1, it will break the appliance. The correct steps 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 4.1 Installation Guide*.

This option will work in a future release of Self Service Password Reset.

# 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 Configuration pane, 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 page, next to the user name, click **Logout**.
2. Close the web browser.

# 14 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

Self Service Password Reset administrators belonging to an LDAP Self Services Password Reset group that usually performs configuration operations. For more information, see "Configuring the Administrators Module" on page 48. However, 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 to each deployment type of Self Service Password Reset.

# 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 144
- “How to Lock and Unlock the Self Service Password Reset Configuration on Windows” on page 145
- “How to Lock and Unlock the Self Service Password Reset Configuration on Linux” on page 146

## 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`

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.

**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

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 19.

## 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 random password for 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 133.
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:** “How the Windows Time Service Works”
   - **eDirectory:** “Synchronizing Network Time” in the *NetIQ eDirectory Administration Guide*
   - **Oracle:** “Understanding the Oracle Directory Synchronization Service”

## 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 away 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.


- "Users in Active Directory See Delays in Accessing the User Website" on page 149
- "Users Did Not Complete the Forgotten Password Process" on page 150
- "Helping Users Change the Default Language of Self Service Password Reset" on page 150
- "How to Enable Windows Desktop to Support Forgotten Password Reset" on page 150
- "How to Make Self Service Password Reset Honor the Active Directory Password History Policy" on page 151


## 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 Server 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 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 the 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.

# A Documentation Updates

These sections contains a list of the changes made to the documentation.



## April 2017

| Location | Change |
|---|---|
| “Customizing the Branding of Self Service Password Reset” on page 87 | Added a link for a how to video on custom themes. |

## March 2017

| Location | Change |
|---|---|
| “Supported Versions” on page 115 | Added this new section. |