Legal Notice

For information about legal notices, trademarks, disclaimers, warranties, export and other use restrictions, U.S. Government rights, patent policy, and FIPS compliance, see https://www.netiq.com/company/legal/.

Copyright © 2016 NetIQ Corporation. All Rights Reserved.
## Contents

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>About NetIQ Corporation</td>
<td>9</td>
</tr>
<tr>
<td>About this Book</td>
<td>11</td>
</tr>
<tr>
<td><strong>1 Self Service Password Reset Overview</strong></td>
<td>13</td>
</tr>
<tr>
<td>Self Service Password Reset Key Features</td>
<td>13</td>
</tr>
<tr>
<td>Self Service Password Reset Architecture</td>
<td>14</td>
</tr>
<tr>
<td>Understanding Challenge-Response Storage Methods</td>
<td>15</td>
</tr>
<tr>
<td><strong>2 Planning to Install Self Service Password Reset</strong></td>
<td>17</td>
</tr>
<tr>
<td>Security Considerations</td>
<td>17</td>
</tr>
<tr>
<td>Over-the-Wire Data Encryption</td>
<td>17</td>
</tr>
<tr>
<td>At-Rest Data</td>
<td>18</td>
</tr>
<tr>
<td>Best Practices for Self Service Password Reset Security</td>
<td>18</td>
</tr>
<tr>
<td>Best Practices for Password Policy</td>
<td>18</td>
</tr>
<tr>
<td>High Availability and Load Balancing</td>
<td>19</td>
</tr>
<tr>
<td>Selecting an Appropriate Configuration</td>
<td>19</td>
</tr>
<tr>
<td><strong>3 Installing Self Service Password Reset</strong></td>
<td>21</td>
</tr>
<tr>
<td>Obtaining Self Service Password Reset</td>
<td>21</td>
</tr>
<tr>
<td>Downloading the Full Version</td>
<td>21</td>
</tr>
<tr>
<td>Downloading the Trial Version</td>
<td>21</td>
</tr>
<tr>
<td>Default Ports for Self Service Password Reset</td>
<td>22</td>
</tr>
<tr>
<td>Installing Self Service Password Reset</td>
<td>23</td>
</tr>
<tr>
<td>Deploying the Self Service Password Reset Appliance</td>
<td>23</td>
</tr>
<tr>
<td>Deploying Self Service Password Reset on Windows</td>
<td>25</td>
</tr>
<tr>
<td>Deploying the WAR File on Linux</td>
<td>27</td>
</tr>
<tr>
<td><strong>4 Upgrading Self Service Password Reset</strong></td>
<td>31</td>
</tr>
<tr>
<td>Upgrading the Self Service Password Reset Appliance</td>
<td>31</td>
</tr>
<tr>
<td>Upgrading Self Service Password Reset on Linux</td>
<td>32</td>
</tr>
<tr>
<td>Upgrading Self Service Password Reset on Windows</td>
<td>33</td>
</tr>
<tr>
<td>Upgrading the Identity Manager Deployment of Self Service Password Reset</td>
<td>34</td>
</tr>
<tr>
<td><strong>5 Configuring Your Environment for Self Service Password Reset</strong></td>
<td>37</td>
</tr>
<tr>
<td>Self Service Password Reset Configuration Worksheet</td>
<td>37</td>
</tr>
<tr>
<td>Using the Configuration Guide</td>
<td>40</td>
</tr>
<tr>
<td>Manually Configuring Self Service Password Reset</td>
<td>40</td>
</tr>
<tr>
<td>Exporting LDAP Certificates</td>
<td>41</td>
</tr>
<tr>
<td>Configuring the LDAP Directories</td>
<td>42</td>
</tr>
<tr>
<td>Creating an LDAP Profile for Your Environment</td>
<td>46</td>
</tr>
<tr>
<td>Configuring Databases</td>
<td>46</td>
</tr>
<tr>
<td>Configuring Self Service Password Reset to Work with the External Database</td>
<td>47</td>
</tr>
<tr>
<td>Integrating with Other NetIQ Products</td>
<td>48</td>
</tr>
<tr>
<td>Chapter</td>
<td>Title</td>
</tr>
<tr>
<td>---------</td>
<td>-------</td>
</tr>
<tr>
<td>6</td>
<td>Configuring Self Service Password Reset</td>
</tr>
<tr>
<td></td>
<td>Working with Configuration Editor</td>
</tr>
<tr>
<td></td>
<td>Defining the Criteria for Administrators</td>
</tr>
<tr>
<td></td>
<td>Configuring Macros for Messages and Actions</td>
</tr>
<tr>
<td></td>
<td>Configuring Basic Settings</td>
</tr>
<tr>
<td></td>
<td>Configuring LDAP Settings</td>
</tr>
<tr>
<td></td>
<td>Configuring the Global LDAP Settings</td>
</tr>
<tr>
<td></td>
<td>Configuring NetIQ eDirectory Settings</td>
</tr>
<tr>
<td></td>
<td>Configuring Microsoft Active Directory Settings</td>
</tr>
<tr>
<td></td>
<td>Configure the Oracle Directory Settings</td>
</tr>
<tr>
<td></td>
<td>Configuring Security Settings</td>
</tr>
<tr>
<td></td>
<td>Configuring Security for the Application</td>
</tr>
<tr>
<td></td>
<td>Configuring Web Security</td>
</tr>
<tr>
<td></td>
<td>Configuring External Web Services Extensions</td>
</tr>
<tr>
<td></td>
<td>Configuring REST Clients</td>
</tr>
<tr>
<td></td>
<td>Configuring REST Services</td>
</tr>
<tr>
<td>7</td>
<td>Configuring the User Experience</td>
</tr>
<tr>
<td></td>
<td>Customizing the Branding of the User Interface</td>
</tr>
<tr>
<td></td>
<td>Configuring Password Policy</td>
</tr>
<tr>
<td></td>
<td>Configuring Password Settings</td>
</tr>
<tr>
<td></td>
<td>Configuring the Word List Settings</td>
</tr>
<tr>
<td></td>
<td>Configuring Challenge-Response Authentication</td>
</tr>
<tr>
<td></td>
<td>Configuring Email Notification Settings</td>
</tr>
<tr>
<td></td>
<td>Configuring Email Settings</td>
</tr>
<tr>
<td></td>
<td>Configuring Email Templates</td>
</tr>
<tr>
<td></td>
<td>Configuring SMS Notification Settings</td>
</tr>
<tr>
<td></td>
<td>Configuring the SMS Gateway</td>
</tr>
<tr>
<td></td>
<td>Configuring the SMS Messages</td>
</tr>
<tr>
<td></td>
<td>Configuring CAPTCHA</td>
</tr>
<tr>
<td></td>
<td>Configuring Intruder Detection</td>
</tr>
<tr>
<td></td>
<td>Configuring Token Settings</td>
</tr>
<tr>
<td></td>
<td>Configuring One-Time Password</td>
</tr>
<tr>
<td></td>
<td>Configuring OAuth SSO</td>
</tr>
<tr>
<td>8</td>
<td>Configuring Modules</td>
</tr>
<tr>
<td></td>
<td>Configuring the Account Information Module</td>
</tr>
<tr>
<td></td>
<td>Configuring the Change Password Module</td>
</tr>
<tr>
<td></td>
<td>Configuring the Forgotten Password Settings</td>
</tr>
<tr>
<td></td>
<td>Configuring Forgotten User Name</td>
</tr>
<tr>
<td></td>
<td>Enabling User Activation</td>
</tr>
<tr>
<td></td>
<td>Configuring the Update Profile Module</td>
</tr>
<tr>
<td></td>
<td>Enabling Shortcut Menu</td>
</tr>
<tr>
<td></td>
<td>Enabling the People Search Module</td>
</tr>
<tr>
<td>9</td>
<td>Configuring LDAP and Policy Profiles</td>
</tr>
<tr>
<td></td>
<td>Configuring LDAP Directory Profile</td>
</tr>
<tr>
<td></td>
<td>Configuring a Profile for Password Policy</td>
</tr>
<tr>
<td></td>
<td>Configuring a Profile for Forgotten Password Policy</td>
</tr>
<tr>
<td></td>
<td>Configuring a Profile for New User Registration</td>
</tr>
<tr>
<td></td>
<td>Configuring a Profile for a Challenge Response Policy</td>
</tr>
<tr>
<td></td>
<td>Configuring a Profile for a Help Desk Policy</td>
</tr>
<tr>
<td>Chapter</td>
<td>Title</td>
</tr>
<tr>
<td>---------</td>
<td>-------</td>
</tr>
<tr>
<td>10</td>
<td>Integrating Self Service Password Reset with NetIQ Access Manager</td>
</tr>
<tr>
<td></td>
<td>Configuring Access Gateway for Self Service Password Reset</td>
</tr>
<tr>
<td></td>
<td>Configuring Proxy Service for Self Service Password Reset</td>
</tr>
<tr>
<td></td>
<td>Configuring Protected Resources for Self Service Password Reset</td>
</tr>
<tr>
<td></td>
<td>Configuring Single Sign-On to Self Service Password Reset</td>
</tr>
<tr>
<td></td>
<td>Configuring Single Sign-On to Self Service Password Reset When Password Is Not Available</td>
</tr>
<tr>
<td></td>
<td>Integrating Self Service Password Reset with Access Manager</td>
</tr>
<tr>
<td></td>
<td>Configuring Self Service Password Reset Parameters for Access Manager</td>
</tr>
<tr>
<td></td>
<td>Configuring Password Expiration Servlet</td>
</tr>
<tr>
<td></td>
<td>Integrating Forgotten Password URL</td>
</tr>
<tr>
<td></td>
<td>Request Parameters</td>
</tr>
<tr>
<td></td>
<td>Command Servlet</td>
</tr>
<tr>
<td>11</td>
<td>Integrating Self Service Password Reset with NetIQ Advanced Authentication</td>
</tr>
<tr>
<td></td>
<td>Prerequisite</td>
</tr>
<tr>
<td></td>
<td>Configuring Advanced Authentication Settings for Forgotten Password</td>
</tr>
<tr>
<td>12</td>
<td>Integrating Self Service Password Reset with NetIQ Identity Manager</td>
</tr>
<tr>
<td></td>
<td>Configuring Self Service Password Reset Settings for Identity Manager</td>
</tr>
<tr>
<td></td>
<td>Configure OAuth Settings for Self Service Password Reset</td>
</tr>
<tr>
<td></td>
<td>Set the Self Service Password Reset Theme to Match the Identity Manager Theme</td>
</tr>
<tr>
<td></td>
<td>Configure Syslog Audit server</td>
</tr>
<tr>
<td></td>
<td>Enabling Self Service Password Reset Proxy Users to Read Passwords from eDirectory</td>
</tr>
<tr>
<td>13</td>
<td>Managing Self Service Password Reset</td>
</tr>
<tr>
<td></td>
<td>Backing Up Configuration Information</td>
</tr>
<tr>
<td></td>
<td>Importing Configuration Information</td>
</tr>
<tr>
<td></td>
<td>Uninstalling Self Service Password Reset</td>
</tr>
<tr>
<td></td>
<td>Removing the Self Service Password Reset Appliance</td>
</tr>
<tr>
<td></td>
<td>Uninstalling on Linux</td>
</tr>
<tr>
<td></td>
<td>Uninstalling on Windows</td>
</tr>
<tr>
<td></td>
<td>Viewing LDAP Permissions Recommendations</td>
</tr>
<tr>
<td></td>
<td>Using the Dashboard</td>
</tr>
<tr>
<td></td>
<td>Configuring Data Analysis</td>
</tr>
<tr>
<td></td>
<td>Configuring Reporting</td>
</tr>
<tr>
<td></td>
<td>Viewing the Reports</td>
</tr>
<tr>
<td></td>
<td>Configuring Logging</td>
</tr>
<tr>
<td></td>
<td>Configuring Logging Settings</td>
</tr>
<tr>
<td></td>
<td>Viewing Logs</td>
</tr>
<tr>
<td></td>
<td>Auditing for Self Service Password Reset</td>
</tr>
<tr>
<td></td>
<td>Configuring Auditing</td>
</tr>
<tr>
<td></td>
<td>Forwarding Auditing Information</td>
</tr>
<tr>
<td></td>
<td>Configuring Auditing for User History</td>
</tr>
<tr>
<td></td>
<td>Adding a Patch Update</td>
</tr>
<tr>
<td></td>
<td>Adding a Patch Update to the Appliance</td>
</tr>
<tr>
<td></td>
<td>Adding a Patch Update to Linux</td>
</tr>
<tr>
<td></td>
<td>Adding a Patch Update to Windows</td>
</tr>
<tr>
<td>14</td>
<td>Managing the Appliance</td>
</tr>
<tr>
<td></td>
<td>Setting Administrative Passwords</td>
</tr>
<tr>
<td></td>
<td>Configuring Network Setting</td>
</tr>
<tr>
<td></td>
<td>Configuring Time Settings</td>
</tr>
</tbody>
</table>

Contents
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accessing System Services</td>
<td>143</td>
</tr>
<tr>
<td>Starting, Stopping, or Restarting System Services</td>
<td>144</td>
</tr>
<tr>
<td>Making System Services Automatic or Manual</td>
<td>144</td>
</tr>
<tr>
<td>Downloading Log Files for System Services</td>
<td>144</td>
</tr>
<tr>
<td>Managing Digital Certificates</td>
<td>145</td>
</tr>
<tr>
<td>Using the Digital Certificate Tool</td>
<td>145</td>
</tr>
<tr>
<td>Using an Existing Certificate and Key Pair</td>
<td>146</td>
</tr>
<tr>
<td>Activating the Certificate</td>
<td>146</td>
</tr>
<tr>
<td>Configuring the Firewall</td>
<td>147</td>
</tr>
<tr>
<td>Using the Ganglia Configuration and Monitoring</td>
<td>147</td>
</tr>
<tr>
<td>Configuring Ganglia</td>
<td>147</td>
</tr>
<tr>
<td>Viewing Ganglia Metrics Using the Appliance Management Console Port 9443 (Secure)</td>
<td>148</td>
</tr>
<tr>
<td>Viewing Ganglia Metrics Directly Using Port 9080 (Not Secure)</td>
<td>148</td>
</tr>
<tr>
<td>Sending Information to Support</td>
<td>149</td>
</tr>
<tr>
<td>Adding a Field Patch to the Appliance</td>
<td>149</td>
</tr>
<tr>
<td>Performing an Online Update</td>
<td>150</td>
</tr>
<tr>
<td>Rebooting or Shutting Down the Appliance</td>
<td>151</td>
</tr>
<tr>
<td>Logging Out</td>
<td>151</td>
</tr>
<tr>
<td><strong>15 Troubleshooting Self Service Password Reset</strong></td>
<td>153</td>
</tr>
<tr>
<td>Troubleshooting Connections</td>
<td>153</td>
</tr>
<tr>
<td>Troubleshooting Self Service Password Reset with the Provided Tools</td>
<td>154</td>
</tr>
<tr>
<td>Troubleshooting with the Dashboard</td>
<td>154</td>
</tr>
<tr>
<td>An Unexpected LDAP Error for the Test User in the Configuration Manager</td>
<td>154</td>
</tr>
<tr>
<td>One or More Responses is Not Correct Error for Users on Mobile Devices</td>
<td>154</td>
</tr>
<tr>
<td>No Automated Emails from the SMTP Server</td>
<td>155</td>
</tr>
<tr>
<td>Troubleshooting User Issues with Self Service Password Reset</td>
<td>155</td>
</tr>
<tr>
<td>Users in Active Directory See Delays in Accessing the User Website</td>
<td>155</td>
</tr>
<tr>
<td>Users Did Not Complete the Forgotten Password Process</td>
<td>156</td>
</tr>
<tr>
<td>Helping Users Change the Default Language of Self Service Password Reset</td>
<td>156</td>
</tr>
<tr>
<td>How to Enable Windows Desktop to Support Forgotten Password Reset</td>
<td>156</td>
</tr>
<tr>
<td>How to Make Self Service Password Reset Honor the Active Directory Password History Policy</td>
<td>157</td>
</tr>
<tr>
<td>Troubleshooting the Challenge Set Policy</td>
<td>157</td>
</tr>
</tbody>
</table>

### A Documentation Updates

<table>
<thead>
<tr>
<th>Month</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>December 2016</td>
<td>159</td>
</tr>
<tr>
<td>November 2016</td>
<td>159</td>
</tr>
</tbody>
</table>
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.
About this Book


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. Enforce data security policy and integrate the advanced authentication framework. Integrate Identity and Access Manager.

Other Information in the Library

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

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

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_akvzAAjmlneyJXW1).
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 in to Self Service Password Reset, it prompts users to provide answers for 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 re-activate 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 Web Pages:** Self Service Password Reset contains a web-based configuration manager. Administrators use this configuration manager to configure Self Service Password Reset, to view recent log events, download the current XML configuration file, 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 intrude 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 back up the database.

Self Service Password Reset supports Microsoft SQL Server and Oracle.
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.
Planning to Install Self Service Password Reset

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

- “Security Considerations” on page 17
- “High Availability and Load Balancing” on page 19
- “Selecting an Appropriate Configuration” on page 19

Security Considerations

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

- “Over-the-Wire Data Encryption” on page 17
- “At-Rest Data” on page 18
- “Best Practices for Self Service Password Reset Security” on page 18
- “Best Practices for Password Policy” on page 18

Over-the-Wire Data Encryption

Self Service Password Reset is an endpoint for several communication traffic channels that send users’ credentials. Self Service Password Reset does not control the communication traffic channels.

Each channel requires its own security configuration settings. For example, ensure that all browser communication is HTTPS. However, you should encrypt all channels by using an end-to-end encryption protocol. Do not rely on private, secure networks. We recommend you use the encryption protocols listed below:

**HTTPS Browser to Self Service Password Reset**
Secure this channel by using SSL/TLS for HTTPS communication.

**Self Service Password Reset to the User Store (LDAP)**
Secure this channel by using SSL/TLS to LDAP by using LDAPS.

**Self Service Password Reset to the Database**
Secure this channel by using database specific security measures.
At-Rest Data

It is important to secure the data used in Self Service Password. You must secure the operating system where you have hosted Self Service Password Reset, the local database, and the LDAP directory by using the respective vendor’s best practices.

The Self Service Password Reset stores sensitive security data in several locations.

**Configuration Files**

Stored in Self Service Password Reset here: `SSPR-installation-directory/config/SSPRConfiguration.xml`.

**User Responses (Hashed)**

Stored in configurable locations of the local database, an external database, LDAP, or in NMAS. Self Service Password Reset stores the users answers as a one-way cryptographically hash using the configured hash algorithm. For more information, see “Understanding Challenge-Response Storage Methods” on page 15.

**Help Desk Response**

Stored in configuration locations of the local database, an external database, or LDAP.

**Shared Password History**

Stored in the local database.

Best Practices for Self Service Password Reset Security

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

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

For more information, see “Configuring Security Settings” on page 57.

Best Practices for Password Policy

To enhance security of password policies:

- Use a word list to prevent easily guessable passwords
- Use a shared word list to prevent organizational password value use from becoming common among many users
- Do not allow users to configure challenge questions
- Do not impose complex syntax rules on users; instead use a specific overall complexity level
- Use a long list of potential random question challenges that are unlikely to have similar answers among different users

For more information, see "Configuring Password Policy” on page 65.
**High Availability and Load Balancing**

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

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

1. Install an L4 switch and ensure you use session persistence.
2. Deploy two or more separate, yet identical, instances of Self Service Password Reset.
   a. Install and configure a Self Service Password Reset system.
   b. Back up the configuration information. For more information, see “Backing Up Configuration Information” on page 129.
   c. Install the second Self Service Password Reset system, then import the configuration information from the first system to the second system. For more information, see “Importing Configuration Information” on page 129.
   d. Repeat these steps for each additional system you want to add.
3. Ensure that the Self Service Password Reset computers and the L4 switch are in the same subnet.
4. Follow the L4 switch documentation to configure the L4 switch to provide load balancing for the Self Service Password Reset computers.

There are no additional configuration steps in Self Service Password Reset to make the load balancing and high availability work.

**Selecting an Appropriate Configuration**

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

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

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

There are two different versions of Self Service Password Reset: a full version and a trial versions. For more information, see “Obtaining Self Service Password Reset” on page 21.

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

Select the platform where you want to install Self Service Password Reset. The supported platforms are:

- An appliance of Self Service Password Reset for Hyper-V or VMware
- SUSE Linux Enterprise Server or Red Hat Enterprise Linux
- Microsoft Windows Server
- Oracle Directory Server with an attached Oracle database

For more information, see "Installing Self Service Password Reset" on page 23.
Where are your users? (User Store)

Select the LDAP directory that contains the users account that Self Service Password Reset manages. The supported LDAP directories are:

- Active Directory
- eDirectory
- Oracle Directory Server.

For more information, see “Installing Self Service Password Reset” on page 23.

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

Select where you want to save the users’ information, such as the challenge-response information. You can save the users’ information to the following locations:

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

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

- **External Database:** Best practice is to use an external database to store the users challenge-response information. The external database provides the ability to cluster to the database and easily backup the database. The supported databases are Microsoft SQL Server and the Oracle database. For more information, see “Installing Self Service Password Reset” on page 23.

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

- **LDAP:** You can securely store the users challenge-responses in any of the supported LDAP directories. For more information, see “Installing Self Service Password Reset” on page 23.

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

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

- "Obtaining Self Service Password Reset" on page 21
- "Default Ports for Self Service Password Reset" on page 22
- "Installing Self Service Password Reset" on page 23

Obtaining Self Service Password Reset

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

Downloading the Full Version

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

To access a full version of Self Service Password Reset:

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

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

Linux: Use tar. For example:

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

Windows: Unzip the .zip files.

Downloading the Trial Version

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

- After a 100 authentications, the system requires a restart to continue functioning.
- After 10,00 authentications, you must reinstall the system.

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

2. Click the Find Trial Download link.
3. Scroll down to find Self Service Password Reset, then click Download.
4. Enter your information to receive an email with the download link.

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

5. After you receive the email, click the link then download the appropriate version for your environment.

6. (Conditional) Extract the compressed file for the appliance.

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

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

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

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

**Linux:** Use `tar`. For example:

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

**Windows:** Unzip the .zip files.

### Default Ports for Self Service Password Reset

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

<table>
<thead>
<tr>
<th>Component</th>
<th>Port</th>
<th>Protocol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Inbound Traffic</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Appliance Management</td>
<td>9443</td>
<td>HTTPS</td>
<td>Appliance management for Self Service Password Reset. For more information, see Chapter 14, &quot;Managing the Appliance,&quot; on page 141.</td>
</tr>
<tr>
<td>Apache Tomcat</td>
<td>8080</td>
<td>HTTP</td>
<td></td>
</tr>
<tr>
<td>Apache Tomcat</td>
<td>8443</td>
<td>HTTPS</td>
<td></td>
</tr>
<tr>
<td><strong>Outbound Traffic</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SMTP</td>
<td>25</td>
<td>SMTP</td>
<td>SMTP messages to an email server.</td>
</tr>
</tbody>
</table>
Installing Self Service Password Reset

Before you install Self Service Password Reset, you must decide where you want to install it. You must select a platform specific installer to install the product. Use the following information to install the platform specific version that is appropriate for your environment.

- “Deploying the Self Service Password Reset Appliance” on page 23
- “Deploying Self Service Password Reset on Windows” on page 25
- “Deploying the WAR File on Linux” on page 27

Deploying the Self Service Password Reset Appliance

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

- “Deployment Requirements for the Appliance” on page 23
- “Deploying the Appliance” on page 24

Deployment Requirements for the Appliance

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

<table>
<thead>
<tr>
<th>Component</th>
<th>Port</th>
<th>Protocol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audit</td>
<td>514</td>
<td>UDP/IP</td>
<td>For more information, see the documentation for the Syslog server that you are using.</td>
</tr>
<tr>
<td>SMS</td>
<td></td>
<td>HTTP or HTTPS</td>
<td>For more information, see the documentation for the SMS gateway that you are using.</td>
</tr>
<tr>
<td>CAPTCHA</td>
<td></td>
<td></td>
<td>For more information, see <a href="http://www.captcha.net/">http://www.captcha.net/</a>.</td>
</tr>
<tr>
<td>Remote Database</td>
<td>Configurable</td>
<td></td>
<td>For more information, see the SQL Server documentation or the Oracle documentation.</td>
</tr>
<tr>
<td>LDAP</td>
<td>Configurable default 389</td>
<td></td>
<td>For more information, see the LDAP directory documentation that you are using.</td>
</tr>
<tr>
<td>LDAPS</td>
<td>Configurable default 636</td>
<td></td>
<td>For more information, see the LDAP directory documentation that you are using.</td>
</tr>
</tbody>
</table>
## Table 3-2  Self Service Password Reset Appliance Requirements

<table>
<thead>
<tr>
<th>Component</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Systems</td>
<td>✷ Hyper-V versions 4.0 and 3.0</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> When you are using Hyper-V, you must select Generation 1.</td>
</tr>
<tr>
<td></td>
<td>Generation 2 is currently not available.</td>
</tr>
<tr>
<td></td>
<td>✷ VMware ESX 5.5 or later</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> Your VMware license must be Enterprise or Enterprise Plus if</td>
</tr>
<tr>
<td></td>
<td>you want to use remote serial connections. For more information, please</td>
</tr>
<tr>
<td></td>
<td>refer to VMware support.</td>
</tr>
<tr>
<td></td>
<td>For more information, see the VMware documentation (<a href="https://www.vmware.com/support/pubs/">https://www.vmware.com/support/pubs/</a>).</td>
</tr>
<tr>
<td>Memory</td>
<td>2 GB of RAM</td>
</tr>
<tr>
<td>Hard disk space</td>
<td>40 GB</td>
</tr>
<tr>
<td>Browsers</td>
<td>✷ Mozilla Firefox 45.0.0 or later</td>
</tr>
<tr>
<td></td>
<td>✷ Google Chrome 49.0.2623.110 m or later</td>
</tr>
<tr>
<td></td>
<td>✷ Microsoft Internet Explorer 11 or later</td>
</tr>
<tr>
<td>IP Ports</td>
<td>Ensure that the default ports for the Self Service Password Reset appliance</td>
</tr>
<tr>
<td></td>
<td>are open in your firewall. For more information, see “Default Ports for</td>
</tr>
<tr>
<td></td>
<td>Self Service Password Reset” on page 22.</td>
</tr>
<tr>
<td>LDAP Directories</td>
<td>✷ NetIQ eDirectory 8.8.8 and 9.0</td>
</tr>
<tr>
<td></td>
<td>✷ Microsoft Active Directory 2012</td>
</tr>
<tr>
<td></td>
<td>✷ Oracle Directory Server 11g</td>
</tr>
<tr>
<td></td>
<td><strong>IMPORTANT:</strong> Self Service Password Reset does not support the Active</td>
</tr>
<tr>
<td></td>
<td>Directory Global catalog services. Instead, you can configure multiple</td>
</tr>
<tr>
<td></td>
<td>profiles for different domains to represent the data repository for each</td>
</tr>
<tr>
<td></td>
<td>domain. For more information about creating multiple profiles, see Chapter</td>
</tr>
<tr>
<td></td>
<td>9, “Configuring LDAP and Policy Profiles,” on page 95.</td>
</tr>
<tr>
<td>Remote Databases</td>
<td>✷ Microsoft SQL Server 2012</td>
</tr>
<tr>
<td></td>
<td>✷ Oracle Database 12c</td>
</tr>
</tbody>
</table>

## Deploying the Appliance

Before you deploy the appliance, ensure that you meet all of the appliance requirements and that you have downloaded and extracted the appropriate version of the appliance.

**To deploy the Self Service Password Reset appliance:**

1. Deploy the appliance to your virtual environment. For more information, see:
   - **Hyper-V:** Importing a Virtual Machine.
   - **VMware:** Deploy an OVF Template.
2. Power on the appliance.
3 Select the appropriate language, then read the license and click Accept.

4 Use the following information to configure the appliance:

   **root Password**
   Specify a password for the root user on the appliance.

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

   **Region and Time Zone**
   Select your region and time zone.

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

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

After you complete the deployment of the appliance, you must configure your environment to work with Self Service Password Reset. For more information, see Chapter 5, “Configuring Your Environment for Self Service Password Reset,” on page 37.

## Deploying Self Service Password Reset on Windows

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

- “Deployment Requirements for Self Service Password Reset on Windows” on page 25
- “Installing Self Service Password Reset with the .msi File on Windows” on page 26

### Deployment Requirements for Self Service Password Reset on Windows

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

<table>
<thead>
<tr>
<th>Component</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows Platforms</td>
<td>Microsoft Windows Server 2012 R2 (64-bit)</td>
</tr>
<tr>
<td>Memory</td>
<td>1 GB of RAM</td>
</tr>
<tr>
<td>Hard disk space</td>
<td>5 GB</td>
</tr>
<tr>
<td>Browsers</td>
<td>• Mozilla Firefox 45.0.0 or later</td>
</tr>
<tr>
<td></td>
<td>• Google Chrome 49.0.2623.110 m or later</td>
</tr>
<tr>
<td></td>
<td>• Microsoft Internet Explorer 11 or later</td>
</tr>
<tr>
<td>IP Ports</td>
<td>Ensure that the default ports for the Self Service Password Reset appliance are open in your firewall. For more information, see “Default Ports for Self Service Password Reset” on page 22.</td>
</tr>
</tbody>
</table>
Installing Self Service Password Reset with the .msi File on Windows

Ensure that you have met all of the installation requirements for installing Self Service Password Reset on Windows and that you have downloaded an extracted the .msi file before beginning the installation.

To install Self Service Password Reset on Windows:

1. Launch the `sspr.x.x.msi` file.
2. Read the notice for Self Service Password Reset, then click Next.
3. Read and accept the end user license, then click Next.
4. Specify the path for the installation of Self Service Password Reset, then click Next.
5. In Configure SSPR-Service URLs, specify the following:
   - **Shutdown Port**: Specify the port number for Apache Tomcat shutdown port.
   - **HTTPS Secure Port**: Specify the secure port for Self Service Password Reset service.
   - **Open Secure HTTPS Port**: Select the firewall setting for Self Service Password to use on the Windows server. The installer selects the open HTTPS Windows firewall port by default. The options for the firewall are:
     - **All**: This enables users to use Self Service Password Reset on a domain, private or public networks.
Domain
This enables users to use Self Service Password Reset on a domain network only.

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

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

6 Click Next, then click Install.
7 Click Install.
8 Record the HTTPS Secure URL, then click Finish.

After completing the installation, you must configure your environment to work with Self Service Password Reset. For more information, see Chapter 5, “Configuring Your Environment for Self Service Password Reset,” on page 37.

Deploying the WAR File on Linux

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

- “Deployment Requirements for Self Service Password Reset WAR File on Linux” on page 27
- “Prerequisites for Deploying the WAR File” on page 28
- “Setting Operating System Environment Variables” on page 29
- “Deploying the Self Service Password Reset WAR File” on page 29

Deployment Requirements for Self Service Password Reset WAR File on Linux

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

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

<table>
<thead>
<tr>
<th>Component</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Linux Platforms</td>
<td>• SUSE Linux Enterprise Server 12 SP1 or later (64-bit)</td>
</tr>
<tr>
<td></td>
<td>• Red Hat Enterprise Linux 7.2 or later (64-bit)</td>
</tr>
<tr>
<td>Memory</td>
<td>1 GB of RAM</td>
</tr>
<tr>
<td>Hard disk space</td>
<td>5 GB</td>
</tr>
<tr>
<td>Browsers</td>
<td>• Mozilla Firefox 45.0.0 or later</td>
</tr>
<tr>
<td></td>
<td>• Google Chrome 49.0.2623.110 m or later</td>
</tr>
<tr>
<td></td>
<td>• Microsoft Internet Explorer 11 or later</td>
</tr>
</tbody>
</table>
Prerequisites for Deploying the WAR File

You must have Java and Apache Tomcat installed and running on Linux before you deploy the WAR file. If you already have Java and Tomcat installed, proceed to “Setting Operating System Environment Variables” on page 29. Follow these steps to install and validate the installation of Java and Tomcat.

To install Java and Tomcat:

1 Install Java 8. For more information, see “JDK 8 and JRE 8 Installation”.
   Verify JAVA_HOME (or JRE_HOME) path is set appropriately by entering:
   
   ```
   echo $JAVA_HOME
   ```
   or
   ```
   echo $JRE_HOME
   ```

2 Install Tomcat 8. For more information, see “Tomcat Setup”.

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

4 Validate you can access http://localhost:port. The default port is 8080.
   Check the Tomcat_Home/logs/catalina.out file for any errors if you are unable to access the default Tomcat page.

IP Ports

Ensure that the default ports for the Self Service Password Reset appliance are open in your firewall. For more information, see “Default Ports for Self Service Password Reset” on page 22.

LDAP Directories

- NetIQ eDirectory 8.8.8 and 9.0
- Microsoft Active Directory 2012
- Oracle Directory Server 11g

**IMPORTANT:** Self Service Password Reset does not support the Active Directory Global catalog services. Instead, you can configure multiple profiles for different domains to represent the data repository for each domain. For more information about creating multiple profiles, see Chapter 9, “Configuring LDAP and Policy Profiles,” on page 95.

Remote Databases

- Microsoft SQL Server 2012
- Oracle Database 12c

Java

Java JDK 1.8

**IMPORTANT:** You must install this version of Java on the Linux server prior to deploying the WAR file. You must be familiar with the installation, configuration, and maintenance of this component.

Apache Tomcat

Apache Tomcat 8.0.x

**IMPORTANT:** You must install this version of Apache Tomcat on the Linux server prior to deploying the WAR file. You must be familiar with the installation, configuration, and maintenance of this component.

Component Requirements
Setting Operating System Environment Variables

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

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

- **SSPR_APPLICATIONPATH** *(Required)*: Specifies where Self Service Password Reset stores its configuration data file (`SSPRConfiguration.xml`). This file contains all of the Self Service Password Reset configuration data. The specified path must exist prior to starting Self Service Password Reset.
  
  For example: `export SSPR_APPLICATIONPATH="/etc/opt/microfocus/sspr"

- **CATALINA_OPTS**: Allows specification of additional options for the Java command that starts Apache Tomcat. The recommended Java options for the Self Service Password Reset Java servlet application running on Apache Tomcat include:
  
  - **-Xms**: Specifies the initial heap memory allocation pool.
  
  - **-Xmx**: Specifies the maximum heap memory allocation pool for a Java Virtual Machine (JVM). Setting the initial and maximum heap memory size to the same size is a best practice because the JVM does not increase heap memory size at runtime. The recommended SSPR heap memory size is 1 GB (1024 MB). For more information about how to set Java heap size, see the Apache Tomcat documentation.

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

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

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

Deploying the Self Service Password Reset WAR File

After you have installed Java and Apache Tomcat and they are running with the appropriate OS environmental variables set, you must deploy the Self Service Password Reset WAR file. Ensure that you have downloaded and extracted the file. For more information, see “Obtaining Self Service Password Reset” on page 21.

To deploy the WAR file on Linux:

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

   When Apache Tomcat discovers the `sspr.war` file in the `Tomcat_Home/webapps/` directory, Apache Tomcat auto-deploys Self Service Password Reset in an automatically created directory; `Tomcat_Home/webapps/sspr/`.

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

   `./catalina.sh stop`

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

   `./catalina.sh start`
After deploying the WAR file, you must configure your environment to work with Self Service Password Reset. For more information, see Chapter 5, “Configuring Your Environment for Self Service Password Reset,” on page 37.
Upgrading Self Service Password Reset

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

Since Self Service Password Reset is a web application, the steps to add a patch update are the same as when you upgrade Self Service Password Reset. For more information, see “Adding a Patch Update” on page 138.

- “Upgrading the Self Service Password Reset Appliance” on page 31
- “Upgrading Self Service Password Reset on Linux” on page 32
- “Upgrading Self Service Password Reset on Windows” on page 33
- “Upgrading the Identity Manager Deployment of Self Service Password Reset” on page 34

Upgrading the Self Service Password Reset Appliance

You can upgrade an existing Self Service Password Reset appliance installation to the latest version. For the Self Service Password Reset appliance, the upgrade steps and applying an Online Update are the same.

To upgrade the appliance:

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

      NOTE: This is for backup purposes only.

2. Back up the data stored in the local database:
   2a In the Configuration Manager, click LocalDB.
   2b Click Download LocalDB, then save the local database to a safe location.

      NOTE: This is for backup purposes only.

3. Register for online updates. For more information, see “Performing an Online Update” on page 150.

4. Click Update Now to upgrade to the latest version of the appliance, then follow the instructions.
5 (Optional) Restore any customizations.
6 Log in to Self Service Password Reset at https://dns-name/sspr as an administrator and verify that all of the configuration information is correct.

Upgrading Self Service Password Reset on Linux

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

Since Self Service Password Reset is a Java servlet application running Apache Tomcat, the steps to add a patch update are the same as upgrading Self Service Password Reset. For more information, see “Adding a Patch Update” on page 138.

To upgrade Self Service Password Reset on Linux:

1 Download the most recent version of Self Service Password Reset WAR file from the NetIQ Patch Finder download website.
2 Create a backup of your current configuration information.
   2a Log in to Self Service Password Reset at https://dns-name/sspr as an administrator.
   2b In the toolbar, click your name.
   2c Click Configuration Manager.
   2d Back up the configuration XML file:
      2d1 Under Configuration Activities, click Download Configuration.
      2d2 Save the SSPRConfiguration.xml file to a safe location.
3 Back up the data stored in the local database:
   3a In the Configuration Manager, click LocalDB.
   3b Click Download LocalDB, then save the local database to a safe location.
4 (Optional) If you have made any customization in Self Service Password Reset such as changes in the user interface, copy these for later reference.
   For more information, see “Customizing the Branding of the User Interface” on page 63.
5 Stop Apache Tomcat by running the catalina.sh script in the Tomcat_Home/bin directory.
   ./catalina.sh stop
6 Copy the updated sspr.war to the Tomcat_Home/webapps directory.

   NOTE: Ensure that you have set the SSPR_APPLICATION operating system environment variable in the setenv file. For more information, see “Setting Operating System Environment Variables” on page 29”.
7 Restart the Apache Tomcat service by running the catalina.sh script in the Tomcat_Home/bin directory.
   ./catalina.sh start
8 Import the configuration information you backed up prior to the upgrade. For more information, see “Importing Configuration Information” on page 129.”
9 Restore the local database information.
   9a Log in to the Configuration Manager as an administrator.
   9b Click LocalDB.
   9c Click Import (Upload) LocalDB Archive File, then browse to and select the file you saved before installing the new appliance.

10 (Optional) Copy any customization as required.

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

   10a Log in to Self Service Password Reset at `https://dns-name/sspr` as an administrator.
   10b In the toolbar, click your name.
   10c Select Configuration Editor.
   10d Click Settings > User Interface > Look & Feel > Custom Resource Bundle.
   10e Browse to and select the Custom Resource Bundle file, then click Upload File.

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

## Upgrading Self Service Password Reset on Windows

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

1 Download the most recent version of Self Service Password Reset `.msi` file from the NetIQ Patch Finder download website.

2 Create a backup of the current configuration information.

   2a Log in to Self Service Password Reset at `https://dns-name/sspr` as an administrator.
   2b In the toolbar, click your name.
   2c Click Configuration Manager.
   2d Back up the configuration XML file.
      2d1 Under Configuration Activities, click Download Configuration.
      2d2 Save the `SSPRConfiguration.xml` file to a safe location.

   **NOTE:** This is for backup purposes only.

3 Back up the data stored in the local database:

   3a In the Configuration Manager, click LocalDB.
   3b Click Download LocalDB, then save the local database to a safe location.

   **NOTE:** This is for backup purposes only.

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

   For more information, see "Customizing the Branding of the User Interface" on page 63.

5 Run the `.msi` file.
6 Follow the prompts to install the new version.
7 (Optional) Restore any customization.
8 Log in to Self Service Password Reset at https://dns-name/sspr as an administrator and verify that all of the configuration information is correct.

Upgrading the Identity Manager Deployment of Self Service Password Reset

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

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

1 Download the most recent version of Self Service Password Reset WAR file from the NetIQ Patch Finder download website.
2 Ensure that you have configured an administrator user for Self Service Password Reset.
   2a Log in to Self Service Password Reset at https://dns-name/sspr as an administrator.
   2b In the toolbar, click your name.
   2c Click Configuration Editor > Setting > Modules > Admin > Administrator Permission.
   2d Ensure that the LDAP filter you defined includes an administrator user.
3 Create a backup of your current configuration information.
   3a Log in to Self Service Password Reset at https://dns-name/sspr as an administrator.
   3b In the toolbar, click your name.
   3c Click Configuration Manager.
   3d Back up the configuration XML file:
      3d1 Under Configuration Activities, click Download Configuration.
      3d2 Save the SSPRConfiguration.xml file to a safe location.
4 Back up the data stored in the local database:
   4a In the Configuration Manager, click LocalDB.
   4b Click Download LocalDB, then save the local database to a safe location.
5 (Optional) If you have made any customization in Self Service Password Reset such as changes in the user interface, copy these for later reference.
   For more information, see “Customizing the Branding of Self Service Password Reset” on page 87.
6 Lock the Self Service Password Reset configuration file by accessing the Configuration Manager, then clicking Lock Configuration.
7 Stop Apache Tomcat by running the catalina.sh script in the Tomcat_Home/bin directory.
   ./catalina.sh stop
8 Delete the following directories:
   - Tomcat_home/webapps/sspr
   - Tomcat_home/work/Catalina/localhost
9 Copy the updated sspr.war to the Tomcat_Home/webapps directory.
NOTE: Ensure that you have set the `SSPR_APPLICATION` operating system environment variable in the `setenv` file. For more information, see “Setting Operating System Environment Variables” on page 29.

10 Restart the Apache Tomcat service by running the `catalina.sh` script in the `Tomcat_Home/bin` directory.

    ./catalina.sh start

11 Import the configuration information you backed up prior to the upgrade.
   11a Log in to Self Service Password Reset at `https://dns-name/sspr` as an administrator.
   11b In the toolbar, click your name.
   11c Click Configuration Manager.
   11d Click Import Configuration, then browse to and select the `SSPRConfiguration.xml` file you created earlier.

12 Restore the local database information.
   12a Log in to the Configuration Manager as an administrator.
   12b Click LocalDB.
   12c Click Import (Upload) LocalDB Archive File, then browse to and select the file you saved before installing the new appliance.

13 (Optional) Copy any customization as required.

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

   13a Log in to Self Service Password Reset at `https://dns-name/sspr` as an administrator.
   13b In the toolbar, click your name.
   13c Select Configuration Editor.
   13d Click Settings > User Interface > Look & Feel > Custom Resource Bundle.
   13e Browse to and select the Custom Resource Bundle file, then click Upload File.

14 Configure the setting that integrates Self Service Password Reset with Identity Manager.
   14a Log in to Self Service Password Reset at `https://dns-name/sspr` as an administrator.
   14b In the toolbar, click your name.
   14c Click Configuration Editor > Settings > Default Settings > LDAP Vendor Default Settings.
   14d Select NetIQ IDM / OAuth Integration.
   14e Select Save changes.

15 Verify that all of the configuration information is correct and if you imported the customization, that Self Service Password Reset restored all of the customizations.
Configuring Your Environment for Self Service Password Reset

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

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

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

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

- “Self Service Password Reset Configuration Worksheet” on page 37
- “Using the Configuration Guide” on page 40
- “Manually Configuring Self Service Password Reset” on page 40
- “Integrating with Other NetIQ Products” on page 48

Self Service Password Reset Configuration Worksheet

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

<table>
<thead>
<tr>
<th>Component</th>
<th>Gather the following information:</th>
</tr>
</thead>
<tbody>
<tr>
<td>LDAP Directory Information</td>
<td>Full DNS name or IP address and the port of the LDAP server</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> Do not use a virtual address or a proxy server address.</td>
</tr>
<tr>
<td></td>
<td>LDAP server certificates</td>
</tr>
<tr>
<td></td>
<td>Allow Self Service Password Reset to manage the certificates, or you must generate new certificates and import them into the Java keystore. For more information, see “Exporting LDAP Certificates” on page 41.</td>
</tr>
</tbody>
</table>
### Gather the following information:

<table>
<thead>
<tr>
<th>Component</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fully qualified LDAP distinguished name (DN)</td>
<td>For security reasons, create a proxy LDAP administrator that has sufficient rights to administer the users that log in to this system.</td>
</tr>
<tr>
<td>of the proxy administrator credentials</td>
<td></td>
</tr>
<tr>
<td>Fully qualified DN of the root container</td>
<td>You can add additional containers after the Configuration Guide completes.</td>
</tr>
<tr>
<td>of your LDAP users</td>
<td></td>
</tr>
<tr>
<td>Fully qualified DN of an LDAP administrators</td>
<td>A group in your LDAP directory to use to control administrative access to Self Service Password Reset.</td>
</tr>
<tr>
<td>group</td>
<td></td>
</tr>
<tr>
<td>Fully qualified DN of an LDAP test user</td>
<td>Self Service Password Reset uses this test user to periodically test the connection between the LDAP server and the system.</td>
</tr>
<tr>
<td>LDAP attribute permissions</td>
<td>You must change the LDAP attribute permissions to allow Self Service Password Reset to manage your users’ credentials. The Configuration Guide displays the specific permissions you must change for your environment.</td>
</tr>
<tr>
<td>Self Service Password Reset URL</td>
<td>If you perform a manual install, you must change these same attribute permissions for your environment. For more information, see “Configuring the LDAP Directories” on page 42.</td>
</tr>
<tr>
<td>Challenge-Response Storage</td>
<td><strong>NOTE:</strong> Select one of the locations to store the challenge-response information: local database, LDAP, or remote database.</td>
</tr>
<tr>
<td>Local Database</td>
<td></td>
</tr>
<tr>
<td>Local database - Testing Only</td>
<td>Use for testing only and nothing else must be done to your environment.</td>
</tr>
<tr>
<td>LDAP</td>
<td>You must extend the schema in your LDAP directory to allow Self Service Password Reset to manage the users. You can allow the Configuration Guide to extend the schema for you or you can manually extend the schema with the provided .ldif files. For more information, see “Configuring the LDAP Directories” on page 42.</td>
</tr>
</tbody>
</table>
Configuring Your Environment for Self Service Password Reset

**Challenge-Response Storage**

1. **Empty database**
   
   You must install an empty database that Self Service Password Reset supports. The configuration process adds the appropriate tables and schema to the database.

2. **Database driver**
   
   You must download the JDBC driver from the website of the database you are using. You upload the JAR or ZIP file during the configuration of Self Service Password Reset.

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

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

5. **Library Path - Microsoft SQL only**
   
   Set the appropriate values for JAVA_OPTS in catalina.bat in the `tomcat/bin` folder. For more information, see the [Tomcat documentation](#).

6. **Database user name**
   
   A user name that Self Service Password Reset uses to authenticate to the database.

7. **Database password**
   
   The password of the database user Self Service Password Reset uses to authenticate to the database.
Using the Configuration Guide

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

To use the Configuration Guide:

1. Ensure that you have gathered all of the information in the worksheet before proceeding. For more information, see “Self Service Password Reset Configuration Worksheet” on page 37.
2. Access the appropriate URL for your deployment.
   - Appliance
     https://dns-name/sspr
   - Windows
     https://localhost:8443/sspr
   - WAR File
     https://localhost:port/sspr
3. Click Start Configuration Guide.
4. Follow the instructions for your environment.

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

After you completed the Configuration Guide, you can now configure Self Service Password Reset for you environment. Proceed to Chapter 6, “Configuring Self Service Password Reset,” on page 49.

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

Manually Configuring Self Service Password Reset

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

1. Gather the information listed in the worksheet.
   For more information, see “Self Service Password Reset Configuration Worksheet” on page 37.
2. Manually configure your LDAP directory by extending the schema and assigning permissions.
   For more information, see “Configuring the LDAP Directories” on page 42.
3. Manually create an LDAP profile in the Self Service Password Reset Configuration Editor.
   For more information, see “Creating an LDAP Profile for Your Environment” on page 46.
4. Manually configure your external database to store the challenge-response information.
   For more information, see “Configuring Databases” on page 46.
5. Manually define the database settings in the Self Service Password Reset Configuration Editor. For more information, see “Configuring Self Service Password Reset to Work with the External Database” on page 47.

After you have completed the manual configuration of your environment, you can now configure Self Service Password Reset. Proceed to Chapter 6, “Configuring Self Service Password Reset,” on page 49.

Exporting LDAP Certificates

To create a secure channel of communication between LDAP and Self Service Password Reset, Self Service Password Reset must trust the LDAP server’s certificates to create a secure channel. You must export the LDAP server certificates to use during the manual configuration of Self Service Password Reset.

To export the LDAP server certificates:

1. Identify the certificates you want to use. You can use one of the following certificates:

   **A certificate issued by a recognized commercial certificate authority (CA):**
   
   The certificate of this type of CA must be present in the certificate database. If the server name in the LDAP URL is identical to the common name (CN) of the certificate, the certification process is complete.

   **A certificate issued by a private certificate authority such as Microsoft Active Directory:**
   
   In this case, the certificates of this CA must be imported into the Java certificate database.

   **A self-signed certificate:**
   
   In this case, import the self-signed certificate into the Java certificate database.

2. Export the certificates from the LDAP server.

   **eDirectory**
   
   To export certificates from eDirectory, see Exporting the SSL Certificate Using iManager.

   **Microsoft Active Directory**
   
   To export certificates from Microsoft Active Directory, see Exporting the LDAPS Certificates and Importing for Use with AD DS

   **Oracle Directory Server**
   
   To export certificate from Oracle Directory Server, see Managing Certificates.

3. Ensure that the exported certificate is accessible from a computer that you will use to configure Self Service Password Reset.

After you have your LDAP certificate, you must manually configure the LDAP directories to work with Self Service Password Reset. Proceed to “Configuring the LDAP Directories” on page 42.
Configuring the LDAP Directories

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

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

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

Self Service Password Reset contains an LDAP Permissions tool that reads your Self Service Password Reset configuration file. The LDAP Permissions tool lists all of the required rights for your environment depending on the components of Self Service Password Reset you have enabled. The rights listed in the tool change depending on the Self Service Password Reset modules you enable. The following steps are guidelines for what rights you need in your environment for Self Service Password Reset to work. It is best to use the LDAP Permissions tool to see all of the rights specific to your deployment of Self Service Password Reset. For more information, see “Viewing LDAP Permissions Recommendations” on page 131.

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

- “Configuring eDirectory” on page 42
- “Configuring Active Directory” on page 44
- “Configuring the Oracle Directory” on page 45

Configuring eDirectory

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

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

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

Use the following information to modify eDirectory:

- “Extending the eDirectory Schema” on page 43
- “Modifying eDirectory Rights to Grant Permissions” on page 43
Extending the eDirectory Schema

You must use eDirectory tools to extend the eDirectory schema with the edirectory-schema.ldif file. You can access this file here: https://sspr.server.com/sspr/public/reference. Depending on your platform, you must use a different eDirectory tool to extend the schema. The steps for extending the schema are in the eDirectory documentation. For more information, see “Manually Extending the Schema” in the NetIQ eDirectory Administration Guide.

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

- pwmEventLog
- pwmResponseSet
- pwmLastPwdUpdate
- pwmGUID
- pwmOTFsecret

Modifying eDirectory Rights to Grant Permissions

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

You must modify the edirectory-rights.ldif file before you use it in your environment.

Set up the following user rights:

- Proxy User Rights
- Authenticated User Rights
- Other Rights

Proxy User Rights

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

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

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

Authenticated User Rights

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

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

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

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

Configuring Active Directory

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

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

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

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

- “Extending the Active Directory Schema” on page 44
- “Assigning User Rights” on page 45

Extending the Active Directory Schema


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

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

- pwmEventLog
- pwmResponseSet
- pwmLastPwdUpdate
- pwmToken
- pwmOTPSecret

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

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

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

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

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

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

Configuring the Oracle Directory

You must extend the schema and assign permissions for the Oracle Directory Server to store the challenge-response information. This allows Self Service Password Reset to manage the passwords for the users.

- “Extending the Schema for the Oracle Directory Server” on page 45
- “Assigning Rights for the Oracle Directory Server” on page 45

Extending the Schema for the Oracle Directory Server

You must use Oracle tools to extend the schema. You use the OracleDS-schma.ldif file to extend the schema. The file is available here: https://sspr.server.com/sspr/public/reference/.

To extend the Oracle schema for Self Service Password Reset, use the Oracle documentation. For more information, see “Extending Directory Server Schema”.

The OracleDS.ldif file adds the following Self Service Password Reset attributes to the Oracle Directory Server schema:

- pwmEventLog
- pwmResponseSet
- pwmLastPwdUpdate
- pwmGUID
- pwmOTPsecret

Assigning Rights for the Oracle Directory Server

You must change the permission for the Oracle Directory attributes to store the following users’ data:

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

Secret questions and answers

The permission between the Oracle Directory Server and eDirectory are similar. The information for permission provided for eDirectory is the same as for the Oracle Directory Server.

Self Service Password Reset requires permission to perform operations in Oracle Directory. The following rights are required:

- Proxy User Rights
- Authenticated User Rights

Use the OracleDS-right.ldif file to make the permissions changes for your environment. You must modify this file for your environment for the file to work.

Creating an LDAP Profile for Your Environment

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

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

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

For instructions and more information, see “Configuring LDAP Directory Profile” on page 95.

Configuring Databases

Self Service Password Reset uses two types of databases:

- **Local Database**: Self Service Password Reset uses a local database for storing local data. The local database requires no administration or maintenance and the default values are sufficient.

- **External Database**: Self Service Password Reset uses an external database to store data for certain functions. Any standard JDBC database that supports a standard Java JDBC driver works. Self Service Password Reset connects to the database and creates the necessary tables. You can configure multiple Self Service Password Reset instances to the same database instance. Self Service Password Reset officially supports MS SQL database and Oracle database.

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

**To configure the database:**

1. Create a database.
   For more information about how to create a database, see the related product documentation.

2. Create a database administrator for that database. You must specify this administrator during Self Service Password Reset configuration.
3  Create a user and associate it with the database you created in Step 1.

4  (Conditional) If you are using the Microsoft SQL database, ensure that the user has enabled the SQL server authentication mode and has suitable rights to open the database, which is the SQL Server Authentication mode. For more information, see "Choosing an Authentication Mode."

Configuring Self Service Password Reset to Work with the External Database

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

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

1  Ensure that you have downloaded the JDBC driver from the vendor’s website.

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

3  In the toolbar, click your name.

4  Click Configuration Editor > Default Settings.

   4a  Select the LDAP directory type you are using.

   4b  Select where to store information as Remote Database

   4c  Click Save.

5  (Conditional) If you are using anything other than Active Directory to store challenge-response information in an external database, click Modules > Forgotten Password > Settings.

   5a  Set Response Read Location to Database.

   5b  Set Response Write Location to Database.

   5c  Click Save.

6  Click Settings > Database (Remote) > Connection.

7  Use the following information to configure the database connection:

   Database Driver

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

   Database Class

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

         •  Microsoft SQL: com.microsoft.sqlserver.jdbc.SQLServerDriver

         •  Microsoft SQL using jTDS: net.sourceforge.jtds.jdbc.Driver

         •  Oracle: oracle.jdbc.OracleDriver

   Database Connection String

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

         •  Microsoft SQL: jdbc:sqlserver://host.example.net:port;databaseName=SSPR

         •  Microsoft SQL using jTDS: jdbc:jtds:sqlserver://host.example.net:port/SSPR

         •  Oracle: jdbc:oracle:thin:@//host.example.net:1521/SSPR

   Database User Name

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

Specify a password for the database user.

Database Vendor

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

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

9 Click Save.

Integrating with Other NetIQ Products

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

- **NetIQ Access Manager**: For more information, see Chapter 10, “Integrating Self Service Password Reset with NetIQ Access Manager,” on page 115.
- **NetIQ Advanced Authentication**: For more information, see Chapter 11, “Integrating Self Service Password Reset with NetIQ Advanced Authentication,” on page 123.
- **NetIQ Identity Manager**: For more information, see Chapter 12, “Integrating Self Service Password Reset with NetIQ Identity Manager,” on page 125.
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.

- “Working with Configuration Editor” on page 49
- “Defining the Criteria for Administrators” on page 50
- “Configuring Macros for Messages and Actions” on page 50
- “Configuring Basic Settings” on page 51
- “Configuring LDAP Settings” on page 52
- “Configuring Security Settings” on page 57
- “Configuring External Web Services Extensions” on page 60

Working with Configuration Editor

Configuration Editor is a powerful tool that enables system administrators to configure all of the Self Service Password Reset settings.

To access the Configuration Editor:

1. Log in to the Self Service Password Reset administration console.
   
   https://localhost:port/sspr

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

In Configuration Editor, you can 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. To configure settings, Self Service Password Reset provides different tabs that include the list of related settings. The following chapters provide detailed information on each setting.

- **Search for configuration settings**: To quickly access a particular setting you can search for it by using the Search field in 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 Configuration Editor, select the Set configuration password in the top-right corner of Configuration Editor.

- **Save configuration settings**: To save the configuration that you update for all the settings, select the Save icon on the top-right corner of 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, you are prompted to confirm the changes. The confirmation dialog box includes a list of modified settings. After the administrators have saved the configuration setting, administrators that have access to 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.

### Defining the Criteria for Administrators

Self Service Password Reset allows you define criteria to determine if users are granted administration rights. By defining the criteria, Self Service Password Reset 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 > Modules > Authenticated > Administration.**
4. Specify the query for the users you want to be administrators. You can query by using **Add Filter** that includes the object class, and by using **Add Group** that includes the LDAP group.
5. Click **Save changes.**

### Configuring Macros for Messages and Actions

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

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 Open macro help and reference in the top right corner of the Configuration Editor.
4. 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.

Configuring Basic Settings

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

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

LocalDB Location
Specify the location of the local database directory. If the specified path is relative, the system considers the path relative to the servlet’s WEB-INF directory.

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://servername: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.

Localization > 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.

5 Select Save changes.

Configuring LDAP Settings
Self Service Password Reset enables you to configure settings to control interactions of Self Service Password Reset with LDAP. 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 values that are at their default. 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 12, "Integrating Self Service Password Reset with NetIQ Identity Manager," on page 125 and Chapter 10, "Integrating Self Service Password Reset with NetIQ Access Manager," on page 115.
Before configuring LDAP directory settings, you must import the corresponding LDAP server certificates. For more information, see “Exporting LDAP Certificates” on page 41.

- “Configuring the Global LDAP Settings” on page 53
- “Configuring NetIQ eDirectory Settings” on page 54
- “Configuring Microsoft Active Directory Settings” on page 56
- “Configure the Oracle Directory Settings” on page 56

### 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 95.

**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 > 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 54.

4. Select **LDAP > LDAP Settings > Global**.
5. 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, forgotten password, 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.

---

6 Select **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 54
- “Configuring the LDAP eDirectory Settings” on page 55

### 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 **LDAP > LDAP Settings > NetIQ eDirectory > eDirectory Challenge Sets**.
4. 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 NAMAS 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 NAMAS.

5 Select Save.

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 > Default Settings > LDAP Vendor Default Settings > NetIQ eDirectory.
4 Select LDAP > LDAP Settings > NetIQ eDirectory > eDirectory Settings.
5 Configure the following settings:
   Enable NMAS Extension
   Select this option to enable the NMAS extension.

   NOTE: If you have enabled NMAS Extension and Store NMAS Responses, ensure that you enable the universal password policy. Otherwise, the new user creation fails.

   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.
6 Select 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 > Default Settings > LDAP Vendor Default Settings > Microsoft Active Directory.
4 Select LDAP > LDAP Settings > Microsoft Active Directory.
5 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.
6 Select 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 > Default Settings > LDAP Vendor Default Settings > Oracle Directory Server.
4. Select LDAP > LDAP Settings > Oracle DS.
5. Configure the following settings:
   - **Allow Manipulation of Password**
     - 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).
6. Select Save changes.

### Configuring Security Settings

Self Service Password Reset provides different security settings for the security of the passwords and user information it manages.

- "Configuring Security for the Application" on page 57
- "Configuring Web Security" on page 58

#### Configuring Security for the Application

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

**To configure 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 > Settings > Security > Application.
4. 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.

5 Select 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 > Settings > Security > Web Security.
4 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.

   Force Basic Authentication
   Select this option to hide the form page from un-authenticated users.

   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.

5 Select 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 60
- "Configuring REST Services" on page 60

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 > Settings > Web Services > REST Clients
4. 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 rule 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 @Externalnumber: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.
   - **Web Service User Attributes**
     Specify the user attributes that various web services use as part of the user's data set.
5. Select 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 > Settings > Web Services > Rest Services.

4 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.

5 Select Save changes.
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 the User Interface” on page 63
- “Configuring Password Policy” on page 65
- “Configuring Challenge-Response Authentication” on page 67
- “Configuring Email Notification Settings” on page 69
- “Configuring SMS Notification Settings” on page 72
- “Configuring CAPTCHA” on page 75
- “Configuring Intruder Detection” on page 76
- “Configuring Token Settings” on page 78
- “Configuring One-Time Password” on page 80
- “Configuring OAuth SSO” on page 81

Customizing the Branding of the User Interface

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.

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 > Settings > User Interface > Look & Feel.
4. Configure the following settings:
   - **Interface Theme**
     - Select an appropriate theme from the list.
     - If you select Embedded, the system uses Embedded CSS style sheet and Embedded Mobile CSS style sheet to manage the custom CSS tags. If you select Custom, the system uses Custom CSS Location and Custom Mobile CSS Location.
Custom CSS Stylesheet Location

Specify the location and name of the custom style sheet. To implement this setting, you must set Embedded as theme under User Interface > Theme. If this is a relative URL, the system appends it to the context path.

Self Service Password Reset can enable multiple themes to be used. You can select the theme by adding the theme=themename parameter to the URL. For example, when linking to the Self Service Password Reset Forgotten Password module such as:

/sspr/public/ForgottenPassword?theme=myCustomTheme

Custom Mobile CSS Stylesheet Location

Specify the location and name of the mobile style sheet. To implement this setting, you must set Embedded as theme under User Interface > Theme. If this is a relative URL, the system appends it to the context path.

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 Upload File to upload the customized ZIP file that contains static HTTP resources that an application should retrieve from the HTTP path, /public/resources/ to be added to the configuration.

The maximum limit for the file size is 10 MB. The file must be HTML, text, images, and so on. No server side processing is performed when serving these files.

5 Click Settings > User Interface > UI Features.

6 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.

Select Save changes.

### Configuring Password Policy

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 of 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 sets 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 groups of users who are part of different profiles. For more information about the profile-specific password policy, see "Configuring a Profile for Password Policy" on page 98.

To configure a password policy you must configure two different sets of settings in Self Service Password Reset:

- "Configuring Password Settings" on page 66
- "Configuring the Word List Settings" on page 66
Configuring Password Settings

To configure a password policy:

1. Log in to Self Service Password Reset at \url{https://dns-name/sspr} as an administrator.
2. In the toolbar, click your name.
3. Click Configuration Editor > Settings > Policies > Password Settings.
4. 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)
5. Select 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 \url{https://dns-name/sspr} as an administrator.
2 In the toolbar, click your name.
3 Click Configuration Editor > Settings > Word Lists.
4 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.

5 Select Save changes.

### Configuring Challenge-Response Authentication

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 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 a Profile for a Challenge Response Policy” on page 108

Apart from configuring random and required questions, you can configure a number of other important settings such as force response setup, case of the responses, and so forth.
To configure the challenge 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 > Modules > Authenticated > Setup Security Questions.
4. 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**
     Select 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**
     Select 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**
     Do not select this option if you want users to enter unique value for each response.
   - **Save Challenge Permission**
     Define a filter to determine if the permission used is a user that is permitted to configure challenges. The user must be returned during this LDAP query or else the user is not permitted to configure challenges.
   - **Check Responses Match**
     Specify the LDAP response query.
     If the LDAP response 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.
5. Select 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 50.

- “Configuring Email Settings” on page 69
- “Configuring Email Templates” on page 70

**Configuring Email Settings**

You must have an SMPT server installed and configured for the email notifications in Self Service Password Reset to work. It is best to use a local SMPT server to your Self Service Password Reset system. The email settings allow you to configure Self Service Password Reset to communicate with your SMPT 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 > Settings > Email > Email Settings.
4. 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 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.
   - **User Email Attribute**
     Specify the user LDAP attribute containing the user's email address.
   - **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.

5 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 > Settings > Email > Email Templates.
4 Configure the appropriate templates to automatically send emails to users:

   **Change Password Email**
   Configure the email format that the 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 the 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, 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 $\text{TOKEN}$ 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 $\text{TOKEN}$ 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 $\text{TOKEN}$ 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.

5 Select 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 72
- “Configuring the SMS Messages” on page 74

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 > Settings > SMS > SMS Gateway.
4. Configure the following settings:
   - **SMS Destination Address LDAP Attribute**
     Specify the LDAP attribute that contains the mobile phone number for SMS messages for all of the users. It must be the same LDAP attribute for all users.
   - **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.

5 Select 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 > Settings > SMS > SMS Messages.

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.

4 Select 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 > Settings > CAPTCHA.
4 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.

For example, if the parameter is `okay`, Self Service Password Reset skips the CAPTCHA validation for this request: `/public/ForgottenPassword?skipCaptcha=okay`.

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.

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

5 Select Save changes.

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 > Settings > Intruder Detection > Intruder Settings.
4 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.

5 Click Settings > Intruder Detection > Intruder Timeouts.

6 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.

7 Select 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 > Settings > Tokens**.
4. 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.

   **DB**
   
   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 57.

   **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.

5. Select **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 a Profile for Forgotten Password Policy” on page 103.

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 > Settings > One Time Password.
4. 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 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 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.

5 Select Save changes.

**Configuring OAuth SSO**
This section discusses various settings that enable Self Service Password Reset to integrate with an OAuth Identity Server for a single sign-on.
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 > Settings > Single Sign On> OAuth SSO.
4. 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.
5. Select Save changes.
Configuring Modules

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 9, “Configuring LDAP and Policy Profiles,” on page 95.

To configure the modules, use the following information:

- “Configuring the Account Information Module” on page 83
- “Configuring the Change Password Module” on page 84
- “Configuring the Forgotten Password Settings” on page 86
- “Configuring Forgotten User Name” on page 88
- “Enabling User Activation” on page 89
- “Configuring the Update Profile Module” on page 90
- “Enabling Shortcut Menu” on page 91
- “Enabling the People Search Module” on page 92

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 > Modules > Account Information.
4. Configure the following settings:
   - Enable Account Information
     Displays the My Account tile on the web page for users.
   - Enable Account Information
     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.
5. 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. A new Account Information tile appears on the web page. The users see the following information about their own account:

- User information
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 from begging to the end for users. You can configure things users must do before changing their password and you can configure tasks the users must perform after they changed their passwords. For example, users must provide their current password before they can change their password.

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 Password Policy” on page 98.

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 > Modules > Change Password.
4. Configure the following settings:

**Change Password Permission**

Specify the query for the users who are allowed to change their password. You can query by using Add Filter that includes the object class, and by using Add Group that includes the LDAP group.

**Logout After Password Change**

Enables the system to log out the user after changing a password. For security reasons, enable this feature for all users especially if a user is using a single sign-on service.

**Change Password Required Values Form**

Specify the values required to be entered before changing the password.

**Require Current Password During Change**

Requires 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 being allowed to change the password. 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 50.

You can also configure this setting in a different language. Select the required language from the list, then click Add Locale.
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 50.

You can also configure this setting in a different language. Select the required language from the list, then click Add Locale.

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 50.

You can also configure this setting in a different language. Select the required language from the list, then click Add Locale.

Password Change Minimum Wait Time

Specify the time, in seconds, required for a password change to take effect. The system uses this time for background synchronization processes.

Password Sync Enable Replication Checking

Enables replica sync checking that polls all of the configured replicas on the users LDAP Profile to determine if the password change time has been updated. The particular method to determine the last password change time varies per LDAP vendor type.

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 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

Enables the system to 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 50.
When you add an action, following are the services available to set the actions:

**webservices**
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**
The user web page displays a link to users during the change password process to display a list of auto-generated sample passwords that are allowed by the configured password policies. The users have the option to select and use one of the values in the list. If you enable this option, the users are not forced to choose a password from the list.

**Show Strength Meter**
Displays the strength meter, for the password strength, on the Change Password page.

1. Click **Save changes**.

---

## Configuring the Forgotten Password Settings

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

You can also set up policies for Forgotten Password. This feature 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.

Forgotten Password requires users to enroll the challenge-response, or enroll the device with the OTP. You can configure the forgotten password settings by performing the following steps.

To enable the **Forgotten Password** option, ensure that you complete the following:

- Create a Forgotten Password policy. For more information, see “Configuring a Profile for Forgotten Password Policy” on page 103.

- Enable the Forgotten Password option.

- The user must complete the challenge-request setup before using the Forgotten Password option. For more information, see “Configuring Challenge-Response Authentication” on page 67.

You can also set up actions that Forgotten Password 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.

Apart from enabling the Forgotten Password feature, configuring the token setting, and configuring actions, you can configure various other settings for this feature. If you want to create different policies 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 a Profile for Forgotten Password Policy” on page 103.

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 > Modules > Forgotten Password > Forgotten Password Settings.
4. Configure the following settings:
   - **Enable Forgotten Password**
     Allows 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 must be executed after a user successfully completes the forgotten password process and the user's password gets modified.

You can also use macros. For more information, see “Configuring Macros for Messages and Actions” on page 50.

5 Click Save changes.

## Configuring Forgotten User Name

You can configure a search filter and attributes that enable users to search for a forgotten user name.

**To enable the Forgotten User Name:**

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 > Modules > Forgotten User Name.
4 Configure the following settings:
   - **Enable Forgotten User Name**
     Allows 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 user 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%)).
User Name LDAP Attribute

Specify an LDAP attribute to read as the user name of the user.

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.

5 Click Save changes.

Enabling User Activation

The User Activation module allows first-time users to activate their account and set a temporary password. When users create an account that does not have an established channel to send the passwords to the users, this feature helps the users activating their account. Configure the settings to allow only those users to activate the account who 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 > Modules > User Activation.
4 Configure the following settings:

Enable User Activation

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

Token Send Methods

Select a method for sending token code 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.

Activate User Form

Specify the attributes a user requires 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 would be 
 zosta (objectClass=person) (cn=%cn%) (sn=%sn%).

Activation Query Match

Specify a query.

The system allows only those users to activate the account who match this query, have never been authenticated, and are enabled to activate.

You can use any attribute to configure this option. The default attribute is 
obra (objectclass=person) (!userAccountControl:1.2.840.113556.1.4.803:=2) || (lastLogon=0) || (lastLogonTimestamp=*)).

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.

5 Select 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 required rights in the LDAP directory.

To enable users to update their profile, 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 In the Configuration Editor, click Modules > Update Profile > Update Profile Settings.
4 Enable Update Profile Attributes to enable the Update Profile module for users.
5 Click Modules > Update Profile > Update Profile Profiles > (default).
6 Configure the following settings:
   Update Profile Match
   Define a Profile Match that only allow users who match this query to update their profile. You add an LDAP profile to match as well as an LDAP search filter.
   Update Profile Actions
   Add actions to execute after a user's attributes are populated.
**Force Update Profile**

Enable this option to present the Update Profile module to the users upon login if the form configuration conditions are not satisfied. Specifically, the system checks the Required and Regular Expression conditions against the current LDAP form values. The user cannot perform other functions until the form values are updated 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.

**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**

Select 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**

If enabled, the system sends 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**

If enabled, 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.

7 Select *Save changes*.

---

**Enabling Shortcut Menu**

The *Shortcut* menu displays a list of links. To make it visible and available for users, you must enable the *Shortcut* menu. After enabling this feature, users can access it on the Main Menu. You can add a number of shortcuts for users by doing 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 In Configuration Editor, click *Modules* > *Shortcut Menu*.
4 Configure the following settings:

**Enable Shortcuts**

Select this option to enable it for users.
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.

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
If enabled, it launches the shortcuts in a new window (or tab).

5 Select Save changes.

Enabling 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 to be displayed in the search result.

If you enable the People Search module and configure it, anyone can use the People Search option to select the appropriate user and view the user details. You can see details such as, user name, email address, photo (if specified), and an organizational chart is displayed with 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 > Modules > People Search.
4 Configure the following settings:
   Enable People Search
   Select this option to enable the People Search module.
Permitted Users
Specifying an LDAP search filter to control the users who access People Search. The user must match this LDAP filter to use this feature.
You can either select the LDAP profile that you have already defined by using the settings for LDAP Directory Profiles, or specify the domain for LDAP search filter.
You can add multiple filters and add multiple groups for the query.

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 will show the Like search option.

Search Result Attributes
Add the LDAP attributes that Self Service Password Reset displays in the search result for a user.

Search Detail Attributes
Add the LDAP attributes that Self Service Password Reset should display during the detail view of an individual person’s record.

Search Result Limit
Specify the maximum number of records that should be displayed in the search result.

Use Proxy Account
This setting should not be enabled for security purpose, but if you require LDAP proxy account to perform searches then select Enabled.

UserDN Name Display
Specify the configuration value that Self Service Password Reset displays for the user’s name. Specify the value for this setting in the @LDAP:name@ format. This setting controls how the People Search details display the user names. For example, if you want Self Service Password Reset 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 must be displayed in the People Search details on the organization 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, the photos are uploaded from the LDAP directory.
This is an optional field. If an LDAP attribute is not specified, the People Search module does not display a photo of the user during the user search.

Photo URL Override
If user photos are not stored in LDAP, this setting can show photos from an external system.
For example: http://photos.example.com/employee/@LDAP:workforceID@.jpg

Search Maximum Cache Seconds
Set the interval in seconds to store the search information in cache.

Photo Display Permission
Specify the query for the users who are allowed to view the photo of other users in an organization chart.
People Search LDAP Filter

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=%USERNAME%\)||(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

If you want to allow all the users to search for other users through People Search by using ipaddress/sspr/public, select Enabled.

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.

Org 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.

Org Chart Child Attribute

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

5 Select Save changes.
This chapter describes how to configure Self Service Password Reset profiles for LDAP directory, and the Self Service Password Reset policies. You can create multiple LDAP profiles and select an appropriate template for the LDAP directory. Create user groups on which you can apply password policies, forgotten password policies, help desk policies, and challenge policies. The name you specify for the user group is the profile name for the respective password, forgotten password, help desk, or challenge policies. You must decide the profile name before you add the profile in the list because the profile name cannot be renamed. You can view and append the profile list by using the Edit List option. You can also change the precedence of profiles.

This chapter includes the following:
- “Configuring LDAP Directory Profile” on page 95
- “Configuring a Profile for Password Policy” on page 98
- “Configuring a Profile for Forgotten Password Policy” on page 103
- “Configuring a Profile for New User Registration” on page 106
- “Configuring a Profile for a Challenge Response Policy” on page 108
- “Configuring a Profile for a Help Desk Policy” on page 111

**IMPORTANT:** If you rename or remove a profile, the associated settings are also removed.

**Configuring LDAP Directory Profile**

Self Service Password Reset allows you to configure multiple LDAP directory profiles. If you are manually configuring Self Service Password Reset, you must create an LDAP directory profile. For more information, see “Creating an LDAP Profile for Your Environment” on page 46.

You can have more than one LDAP directory profile depending on your environment. 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.

**NOTE:** You can either use Active Directory or eDirectory for an instance of Self Service Password Reset configuration.

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 > LDAP > LDAP Directories > default.
4. (Conditional) If you want to create different profiles for a different set of users:
   - 4a Click Edit List, then add the profile names to the list by using Add Profile.
   - 4b In the Add Value field, enter the profile name.
The profile name must have the following format:

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

You can include multiple profiles. During authentication, Self Service Password Reset searches for the default profile first, and then the other profiles in the order mentioned. Self Service Password Reset does not allow changing the name of the profile but you can change the display name of the profile for the users.

4c Select the appropriate profile from the Selected Profile list.

5 Configure the following settings:

**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://servername: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.

**LDAP Certificates**

Displays details of LDAP server certificates. Click Import From Server to import the certificates from the server.

**LDAP Proxy User**

Configure an LDAP proxy user in 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 a 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 in which 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. Create a new test user account with the same privileges and policies as any other users in the system. You can change the password of this account and use it periodically to check the health of the LDAP server.

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 DN later also.

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.

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.

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.

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

User Selectable Login Contexts

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

- `ou=sf,ou=ca,o=example:::San Francisco`
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 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.

**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.

**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.

6 Click **Test LDAP Profile** to test if Self Service Password Reset is able to read the data of the users in a specific profile.

7 Click **Save changes**.

### Configuring a Profile for 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. 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 password policy for a specific profile, do 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 **Profiles > Password Policy Profiles > default**.
4 (Conditional) If you want to create different profiles for a different set of users:
   4a Click **Edit List**, then add the profile names to the list by using **Add Profile**.
   4b In the **Add Value** field, enter the profile name.

   The profile name must have the following format:
   - Start with a letter (a-Z)
• Contain only letters, numbers, and hyphens
• Length between 2 and 15 characters

You can include multiple profiles. During authentication, Self Service Password Reset searches for the default profile first, and then the other profiles in the order mentioned.

4c Select the appropriate profile name.
Self Service Password Reset does not allow changing the name of the profile.

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 exceed 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 exceed 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 Directory 2008 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 abcdefghijkl. 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 of patterns. 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.

6 Click **Save changes**.

**Configuring a Profile for Forgotten Password Policy**

You can configure a forgotten password policy for a particular profile and the users of that group can reset their passwords by using the method that you define in the settings for that profile. 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 80.

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 forgotten password.

- **LDAP Attributes**: This verification method requires the user to specify the values for all the LDAP attributes that are mentioned in the **Required LDAP Attributes** setting.

  If you have upgraded Self Service Password Reset from an earlier version where LDAP attributes were required for 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.

- **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 80.

• **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.

• **Advanced Authentication**: This verification method requires the users to use the authentication method that you configure in the Advanced Authentication setting. For more information about Advanced Authentication settings, see Chapter 11, “Integrating Self Service Password Reset with NetIQ Advanced Authentication,” on page 123.

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 users are prompted to enroll for OTP with an option to skip it. The Active Directory users are prompted to enroll for OTP before a password is reset and eDirectory users are prompted to enroll after a password is reset.

**To configure the Forgotten Password policy for 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 > Modules > Forgotten Password > Forgotten Password Profile > default**.
4. (Conditional) If you want to create different profiles for a different set of users:
   4a. Click **Edit List**, then add the profile names to the list by using **Add Profile**.
   4b. In the **Add Value** field, enter the profile name.
   The profile name must have the following format:
   - Start with a letter (a-Z)
   - Contain only letters, numbers, and hyphens
   - Length between 2 and 15 characters
   You can include multiple profiles. During authentication, Self Service Password Reset searches for the default profile first, and then the other profiles in the order mentioned.
   4c. Select the appropriate profile name.
   Self Service Password Reset does not allow changing the name of the profile.
5. Define the following setting for your environment:

   **Forgotten Password Profile Match**
   Specify the query for the users who are allowed to use Forgotten Password. You can query by using **Add Filter** that includes the object class, and by using **Add Group** that includes the LDAP group.

   **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.

   **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 69
- “Configuring SMS Notification Settings” on page 72

**Allow Unlock**

Allows unlock 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 users are given a chance 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 55.

**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 user can change the password without being required to provide the current password because the user has 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.

- **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 Click Save changes.
Configuring a Profile for New User Registration

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. You can also create multiple profiles for a different set of users.

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 desired 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 Registration 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**.

Configuring a profile for new user registration:

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 > Modules > New User Registration**.
4. Click **New User Settings** then on the right pane, then select **Enabled** to enable users to create a new user. After enabling, users can create a new user by clicking **New User Registration** on the login page.
5. Click **default**.
6. (Conditional) If you want to create a different profiles for a different set of users:
   6a. Click **Edit List**, then add the profile names to the list by using **Add Profile**.
   6b. In the **Add Value** field, enter the profile name. The profile name must have the following format:
      - Start with a letter (a-Z)
      - Contain only letters, numbers, and hyphens
      - Length between 2 and 15 characters
      You can include multiple profiles. During authentication, Self Service Password Reset searches for the default profile first, and then the other profiles in the order mentioned.
   6c. Select the appropriate profile name.
      Self Service Password Reset does not allow changing the name of the profile.
7. Configure the following settings:
   - **Creation Context**
     Specify an LDAP context in which the new users is be created.
   - **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.
   - **New User Form**
     Specify attributes that the users needs to enter while registering 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.

Delete On Creation Failure

Select this option to delete the partially created or invalid LDAP account. This setting is used when the new user account creation fails for some reason.

LDAP Entry ID Definition

Specify the display name, or entry ID that is included in the LDAP naming attribute for the new registered users. Some directories use an LDAP entry instead of a user name.

When you enable this setting, the system generates an entryID or an LDAP entry that includes random characters by default. You must specify macros for this setting. For more information about macros, see “Configuring Macros for Messages and Actions” on page 50.

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 for the new registered user as their email address.

Enable New User Email Verification

Enable this option to send an email to the new user's email address before the account is created. The new user must verify receipt of the email to complete the account creation.

**NOTE:** You must configure the Email settings to make this option work. For more information about how to configure email settings, see “Configuring Email Notification Settings” on page 69.

Enable New User SMS Verification

Enable this option to send an SMS to the new user's mobile phone number before the account is created. The new user must verify receipt of the SMS to complete the account creation.

**NOTE:** You must enable SMS to make this option work. For more information about how to configure email settings, see “Configuring SMS Notification Settings” on page 72.

Password Policy Template

Specify a user of whose password policy template you want to use for the user's password policy.

By default this value is set to TESTUSER, you can replace this with a distinguished name (dn) of a user whose password policy can be used for the specified profile.

New User Minimum Wait Time

Specify a time in seconds. During a new user creation process, the system waits for this specified time before sending the user to the next step.

Profile Display Name

Specify the publicly viewable display name for this profile.

8 Select 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.
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.

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 a profile for challenge response:

1. Log in to Self Service Password Reset at `https://dns-name/sspr` as an administrator.
2. In the toolbar, click your name.
3. Click `Policies > Challenge Policies > default`.
4. (Conditional) If you want to create different profiles for a different set of users:
   4a. Click `Edit List`, then add the profile names to the list by using `Add Profile`.
   4b. In the `Add Value` field, enter the profile name.

   The profile name must have the following format:
   - Start with a letter (a-Z)
   - Contain only letters, numbers, and hyphens
   - Length between 2 and 15 characters

   You can include multiple profiles. During authentication, Self Service Password Reset searches for the default profile first, and then the other profiles in the order mentioned.

4c. Select the appropriate profile name.

Self Service Password Reset does not allow changing the name of the profile.

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:
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. You specify your own questions for the users.

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.

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.

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**

Set up 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.

**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.

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 time of setup.

6 Click Save changes.

Configuring a Profile for a Help Desk Policy

Self Service Password Reset provides a help desk module. 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.

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 autocomplete (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.

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 challenge questions.
- When users have not set up challenge-responses.

To configure a profile for a help desk 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 > Modules > Help Desk > Help Desk Profiles > default.
4 (Conditional) If you want to create different profiles for a different set of users:
4a Click Edit List, then add the profile names to the list by using Add Profile.
4b In the Add Value field, enter the profile name.
The profile name must have the following format:
- Start with a letter (a-Z)
- Contain only letters, numbers, and hyphens
- Length between 2 and 15 characters
You can include multiple profiles. During authentication, Self Service Password Reset searches for the default profile first, and then the other profiles in the order mentioned.

4c Select the appropriate profile name.
Self Service Password Reset does not allow changing the name of the profile.

5 Configure the following settings:

**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 those set of users.
You can use LDAP Group or LDAP filters to query the 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%*)(sAMAccountName=*%USERNAME%*)(userPrincipalName=*%USERNAME%*)(givenName=*%USERNAME%*)(sn=*%USERNAME%*))
```

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

```
cn=admins,o=novell, 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 using **Add Form 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%*)(sAMAccountName=*%USERNAME%*)(userPrincipalName=*%USERNAME%*)(givenName=*%USERNAME%*)(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.

**Viewable Status Fields**
Select the fields that are available to help desk administrators to view the status of the users.
Help Desk Search Result Limit
Specify the limit of the search result for the help desk user.

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.

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.

Help Desk Actor Actions
Specify the actions that a help desk administrator can perform. You can use macros.

Idle Timeout Seconds for Help Desk Users
Specify the number of seconds after which an authenticated help desk administrator’s session requires re-authentication.

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

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.

**Enable Clear Responses Button**

Select 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**

Select 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**

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

**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**: Token verification is not performed
- **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
- **Operator choice**: If both mobile number and email address are available, the help desk operator can decide which method to use.

**Mask Password Value**

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

**Verification Methods**

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

**Help Desk Verification Form**

Define a verification form for the help desk.

6 Select **Save changes**.
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” on page 115
- “Integrating Self Service Password Reset with Access Manager” on page 118
- “Request Parameters” on page 120
- “Command Servlet” on page 120

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” on page 115
- “Configuring Protected Resources for Self Service Password Reset” on page 116
- “Configuring Single Sign-On to Self Service Password Reset” on page 117
- “Configuring Single Sign-On to Self Service Password Reset When Password Is Not Available” on page 117

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.
- Non-SSL: 8080
- SSL: 8443

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:

<table>
<thead>
<tr>
<th>URL</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>password.example.com/*</td>
<td>Public</td>
</tr>
<tr>
<td>password.example.com/sspr/private/*</td>
<td>Restricted</td>
</tr>
<tr>
<td>password.example.com/sspr/private/admin/*</td>
<td>Restricted</td>
</tr>
<tr>
<td>password.example.com/sspr/private/config/*</td>
<td>Restricted</td>
</tr>
</tbody>
</table>

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 116.

<table>
<thead>
<tr>
<th>Configuration</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Action for Identity Injection</td>
<td>Inject into Authentication Header</td>
</tr>
<tr>
<td>Auth Header – User Name</td>
<td>Credential Profile (LDAP Credentials: LDAP User DN)</td>
</tr>
<tr>
<td>Auth Header – Password</td>
<td>Credential Profile (LDAP Credentials: LDAP Password)</td>
</tr>
<tr>
<td>DN Format</td>
<td>LDAP format (default)</td>
</tr>
</tbody>
</table>

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. In Self Service Password Reset, go to Configuration Manager > Settings > Security.
2. In SSO Authentication Header Name, set the value to ssoAuthUsername.
3. In Access Manager, set the following policy for Self Service Password Reset protected resources:

<table>
<thead>
<tr>
<th>Configuration</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Action for Identity Injection</td>
<td>Inject into Custom Header</td>
</tr>
<tr>
<td>Custom Header Name</td>
<td>ssoAuthUsername</td>
</tr>
<tr>
<td>Value</td>
<td>Credential Profile (LDAP Credentials: LDAP User DN)</td>
</tr>
<tr>
<td>DN Format</td>
<td>LDAP format (default)</td>
</tr>
</tbody>
</table>
NOTE: If Self Service Password Reset is using the LDAP directory and Read User Password is enabled (Settings > NetIQ eDirectory > 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.

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 84. 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. Add a custom message to notify users about re-logging into their portal after a password change:
   - 3a Click Configuration Editor > Policies > Password Policy.
   - 3b Select the appropriate password policy. If you only have one password policy, click default.
   - 3c In the Password Change Message field, add the custom message.
   - 3d Click Save changes.
4 Add a URL where to forward users after completing any activity except password changes:
   4a Click Configuration Editor > Settings > Application > Forward URL.
   4b Click Add Value, then specify the URL where to forward users. For example:
      intranet.company.com
   4c Click Save changes.
5 Add an Access Manager logout URL.
   5a Click Configuration Editor > Settings > Application > Logout URL.
   5b Click Add Value, then specify the Access Manager logout URL. For example:
      intranet.company.com/AGLogout
   5c Click Save changes.
6 Enable Self Service Password Reset to log out users after a password change:
   6a Click Configuration Editor > Modules > Change Password.
   6b Enable the Logout After Password Change option.
   6c 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:

```html
<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`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>passwordExpired</td>
<td>Setting this parameter makes Self Service Password Reset override the state of the user's password expiration.</td>
<td>passwordExpired=true</td>
</tr>
<tr>
<td>forwardURL</td>
<td>Sets the forward URL. For example, <code>http://www.example.com/main.html</code>. The value must be URL encoded.</td>
<td>forwardURL=http%3A%2F%2Fwww.example.com%2Fmain.html</td>
</tr>
<tr>
<td>logoutURL</td>
<td>Sets the logout URL to Self Service Password Reset. The value must be URL Encoded.</td>
<td>logoutURL=%2Fsspr</td>
</tr>
<tr>
<td>locale</td>
<td>When a valid browser locale code is provided, Self Service Password Reset switches to the given locale to display all localized text.</td>
<td>locale=en</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>URL Example</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="http://portal.example.com">http://portal.example.com</a></td>
<td>Initial request from the browser.</td>
</tr>
<tr>
<td><a href="http://portal.example.com/Login">http://portal.example.com/Login</a></td>
<td>Access Gateway redirects the user to the login page.</td>
</tr>
<tr>
<td><a href="http://portal.example.com/">http://portal.example.com/</a></td>
<td>Access Gateway redirects the user to the portal root.</td>
</tr>
<tr>
<td><a href="http://portal.example.com/index.html">http://portal.example.com/index.html</a></td>
<td>Web server redirects the user to index.html.</td>
</tr>
</tbody>
</table>
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.html"/>
</head>
<body>
</body>
</html>
```

The following table lists various useful commands:

<table>
<thead>
<tr>
<th>Command</th>
<th>URL</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>checkExpire</td>
<td><a href="http://password.example.com/sspr/private/CommandServlet?processAction=checkExpire">http://password.example.com/sspr/private/CommandServlet?processAction=checkExpire</a></td>
<td>Checks the user's password expiration date. If the expiration date is within the configured threshold, the user requires to change password.</td>
</tr>
<tr>
<td>checkResponses</td>
<td><a href="http://password.example.com/sspr/private/CommandServlet?processAction=checkResponses">http://password.example.com/sspr/private/CommandServlet?processAction=checkResponses</a></td>
<td>Checks the user's challenge-responses. If no responses are configured, the user requires to set them up.</td>
</tr>
<tr>
<td>checkProfile</td>
<td><a href="http://password.example.com/sspr/private/CommandServlet?processAction=checkProfile">http://password.example.com/sspr/private/CommandServlet?processAction=checkProfile</a></td>
<td>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.</td>
</tr>
<tr>
<td>checkAll</td>
<td><a href="http://password.example.com/sspr/private/CommandServlet?processAction=checkAll">http://password.example.com/sspr/private/CommandServlet?processAction=checkAll</a></td>
<td>Calls checkExpire, checkResponses, and checkProfile consecutively.</td>
</tr>
</tbody>
</table>

Self Service Password Reset redirects the user to the actual portal URL.
Integrating Self Service Password Reset with NetIQ 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.

To integrate Self Service Password Reset with Advanced Authentication, you must configure few settings. The following sections describe the prerequisite and the required configuration:

**Prerequisite**

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

- Install the Advanced Authentication server version 5.0 or later.
- The administrator must configure the Advanced Authentication server.
  
  For more information about configuring the Advanced Authentication server, see the *Advanced Authentication Server Administration Guide*.
- In the Advanced Authentication administration web console, you must enable Endpoint41. For more information, see “Managing Endpoints” in the *Advance Authentication Server Administration Guide*.
- The repositories must be created and configured in the Advanced Authentication server.
- You must inform the users who are configured to use Advanced Authentication for forgotten password to enroll the devices depending on the authentication methods.
- A Self Service Password Reset administrator must know the Advanced Authentication identifier and the repository for the users.

**Configuring Advanced Authentication Settings for Forgotten Password**

You can configure the Advanced Authentication settings so that all the Advanced Authentication web service details are registered in the Self Service Password Reset system. This helps the Advanced Authentication users to use any authentication method for resetting their password. If users enroll the device for authentication in Advanced Authentication, they can choose the specified method to reset their password during a forgotten password process.

To enable Advanced Authentication users to reset their passwords during the forgotten password process:

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 > Settings > NAAF.

4 Configure the following settings:

   **NAAF Web Service URL**
   
   Specify the URL for Advanced Authentication appliance web service. For example, https://www.example.com/api/v1

   **NAAF Web Service Server Certificate**
   
   Click Import From Server to import the certificate for using the Advanced Authentication services.

   **NAAF User Identifier**
   
   Click Add Value to include the user identifier that is specified in the Advanced Authentication web service. The value must be specified in the format of repository\user name. You can also use macros instead of a user name.

   **NAAF Login Methods**
   
   Select the required methods for the users specified in Advanced Authentication User Identifier.

   The Advanced Authentication users must enroll their devices depending on the authentication method. Otherwise, they cannot use their devices to authenticate during the forgotten password process.

5 Click Save changes.
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 4.5 with the latest service pack 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 4.5 by using Integrated Installer, or if Self Service Password Reset is installed as a standalone product and configured with Identity Manager 4.5. 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.

IMPORTANT: To have Self Service Password Reset 4.0 work with Identity Manager 4.5 with the latest service pack, you must install Patch Update 1 or later for Self Service Password Reset 4.0. For more information, see "Adding a Patch Update" on page 138.

If you install Self Service Password Reset by using Identity Manager 4.5 Integrated Installer, the configuration settings are defined automatically in the Self Service Password Reset configuration file. For more information on installing Self Service Password Reset with Identity Manager, see "Installing Single Sign-on and Password Management for Identity Manager" in the NetIQ Identity Manager Setup Guide.

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.

Self Service Password Reset includes the NetIQ Identity Manager/OAuth Integration template that includes all the default settings that must be configured for the Identity Manager users. You can configure those settings by using the configuration details mentioned in the following sections.

- “Configuring Self Service Password Reset Settings for Identity Manager” on page 126
- “Enabling Self Service Password Reset Proxy Users to Read Passwords from eDirectory” on page 128
Configuring Self Service Password Reset Settings for Identity Manager

If you are using Self Service Password Reset as a standalone product, then you must perform the following to use Self Service Password Reset as the password management tool for Identity Manager 4.5:

- “Configure OAuth Settings for Self Service Password Reset” on page 126
- “Set the Self Service Password Reset Theme to Match the Identity Manager Theme” on page 127
- “Configure Syslog Audit server” on page 127

**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 4.5. 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 > Settings > Single Sign On > OAuth**.
4. 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 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.

5 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 > Settings > User Interface > Look & Feel.
4 Select IDM (Identity Manager) from the list of themes in the Interface Theme setting.
5 Click Save changes.

Configure Syslog Audit server

Self Service Password Reset provides logging and auditing functionality for sending 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. 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 136.
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 forgotten password, 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.

To allow a user to read password by using Self Service Password Reset proxy user, perform the following:

1. Login to iManager.
2. Select Roles and Tasks from the header icons.
4. Select the appropriate password policy.
5. 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.
Managing Self Service Password Reset

Self Service Password Reset provides tools to back up configuration information and to view the activity throughout the system. You can back up the configuration information if you are going to migrate to new hardware or you need to recover from a hardware failure.

- "Backing Up Configuration Information" on page 129
- "Importing Configuration Information" on page 129
- "Uninstalling Self Service Password Reset" on page 130
- "Viewing LDAP Permissions Recommendations" on page 131
- "Using the Dashboard" on page 131
- "Configuring Data Analysis" on page 133
- "Configuring Logging" on page 134
- "Auditing for Self Service Password Reset" on page 136
- "Adding a Patch Update" on page 138

### 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](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:
   1. Click the LocalDB tab.
   2. Click Download LocalDB and save the information somewhere safe.

If you need to restore the information, see “Importing Configuration Information” on page 129.

### 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.

Uninstalling Self Service Password Reset

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

- “Removing the Self Service Password Reset Appliance” on page 130
- “Uninstalling on Linux” on page 130
- “Uninstalling on Windows” on page 131

Removing the Self Service Password Reset Appliance

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

Uninstalling on Linux

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

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

3. (Optional) Back up the local database if you stored the challenge-response information in it.
   3a. In the Configuration Manager, click LocalDB.
   3b. Click Download LocalDB, then save the local database to a safe location.

4. Delete both the Tomcat_Home/webaps/sspr directory and the Tomcat_Home/webaps/sspr.war file.

5. Reboot the Linux server to complete the uninstall process.
Uninstalling on Windows

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

2 (Optional) Save the XML Configuration file to another location for future use.
   For more information, see “Backing Up Configuration Information” on page 119.

3 (Optional) Back up the local database if you stored the challenge-response information in it.
   3a In the Configuration Manager, click LocalDB.
   3b Click Download LocalDB, then save the local database to a safe location.

4 From the Windows Control Panel, uninstall Self Service Password Reset.

5 Reboot the Windows Server to complete the uninstall process.

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.

You can view a video demonstrating 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 > LDAP Permissions.
4 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.

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 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 136.

**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 133.

**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 153.

**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 Data Analysis
Self Service Password Reset helps analyzes the data passing through the system to create reports. You view the reports through the Administration module on the Dashboard, but you configure all of the settings in the Configuration Editor. If you do not enable Directory Reporting, the Data Analysis tab in the Dashboard does not display any information.

- “Configuring Reporting” on page 133
- “Viewing the Reports” on page 134

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 > Settings > Reporting.
4 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.

Select 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 134
- “Viewing Logs” on page 136

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 > Settings > Logging.
4 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 136.

   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 136.

      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.

Log4j Configuration File

Add the location and name of a log4j XML configuration file. If specified, the system uses this file to configure the log4j system. If unspecified, the system configures the application logging according to the settings here and the system ignores any configuration. The location specified by this setting is relative to the WEB-INF directory. For example, log4jconfig-sample.xml file is included in the WEB-INF directory.

5 Click Save changes.

6 (Conditional) To log all LDAP events to the Trace logging level:

6a In the Configuration Editor, click LDAP > LDAP Settings > Global.

6b Select Enable LDAP Wire Trace. For more information, see “Configuring LDAP Settings” on page 52.

6c 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 134 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 as well as actions users took. It also allows you to forward events to a Syslog server for further analysis of the information.

- “Configuring Auditing” on page 137
- “Forwarding Auditing Information” on page 137
- “Configuring Auditing for User History” on page 138
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 > Settings > Auditing > Audit Configuration.
4. 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.
5. Select 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 > Settings > Auditing > Audit Configuration.
4. 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.
5. Select 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 > Settings > Auditing > User History.
4. 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 LDAP Attribute**
     These are the attributes used to write a user event attribute in LDAP. The user event log attribute will hold an XML document with the users' event history. Leave blank to disable logging event history to LDAP.
   - **User History Maximum Events**
     Specify the maximum number of events to hold in the event history attribute for a user.

5. 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” on page 138
- ”Adding a Patch Update to Linux” on page 138
- “Adding a Patch Update to Windows” on page 139

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 150.

Ensure that you back up your configuration information before applying any updates. For more information, see “Backing Up Configuration Information” on page 129.

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” on page 27.

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 129.

   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 129.

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” on page 25.

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” on page 33.
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
- 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 143.

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**
- **Docker-SSPR (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
- Downloading Log Files for System Services

**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.

**Downloading Log Files for System Services**

If you experience an issue with the Web Interface, you might need to download the log files to send them to Technical Support.

1. Click System Services.
2. In the Log Files column, click the download link for the appropriate service to download the log files to your management workstation:
   - **SSH**: The SSH service that is running on the appliance has no relevant log files for download.
   - **Self Service Password Reset**: Collects, zips, and downloads the log files for Self Service Password Reset.
3. 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 145
- “Using an Existing Certificate and Key Pair” on page 146
- “Activating the Certificate” on page 146

Using the Digital Certificate Tool

- “Creating a New Self-Signed Certificate” on page 145
- “Getting Your Certificate Officially Signed” on page 146

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.
       - **Organizational Unit (OU):** (Optional) Small organization name, such as a department or division. For example, Purchasing.
       - **Organization (O):** (Optional) Large organization name. For example, My Company.
       - **City or Locality (L):** (Optional) City name. For example, Provo.
       - **State or Province (ST):** (Optional) State or province name. For example, Utah.
Two-letter Country Code (C): (Optional) Two-letter country code. For example, US.

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 146.

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 mails 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 146.

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 146.

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" on page 22.

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" on page 147
- “Viewing Ganglia Metrics Using the Appliance Management Console Port 9443 (Secure)” on page 148
- “Viewing Ganglia Metrics Directly Using Port 9080 (Not Secure)” on page 148

### 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.
Managing the Appliance

You might want to disable Ganglia monitoring by deselected 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, go to 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 (Go to Step 5.)
   - Customer Center (Go 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
   - Customer key obtained from the Customer Center
   - 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.
- **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.
Rebooting or Shutting Down the Appliance

You might need to initiate a graceful shut down 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.
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.

- “Troubleshooting Connections” on page 153
- “Troubleshooting Self Service Password Reset with the Provided Tools” on page 154
- “Troubleshooting User Issues with Self Service Password Reset” on page 155
- “Troubleshooting the Challenge Set Policy” on page 157

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.
   - 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.
4. Click Troubleshooting Bundle and download the file to obtain logs files and other information.
5. Click Home to exit the Configuration Manager.
Troubleshooting Self Service Password Reset with the Provided Tools

Use the following information to troubleshoot the tools provided with Self Service Password Reset.

- “Troubleshooting with the Dashboard” on page 154
- “An Unexpected LDAP Error for the Test User in the Configuration Manager” on page 154
- “One or More Responses is Not Correct Error for Users on Mobile Devices” on page 154
- “No Automated Emails from the SMTP Server” on page 155

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 131.

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 143.
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`.

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 155
- “Users Did Not Complete the Forgotten Password Process” on page 156
- “Helping Users Change the Default Language of Self Service Password Reset” on page 156
- “How to Enable Windows Desktop to Support Forgotten Password Reset” on page 156
- “How to Make Self Service Password Reset Honor the Active Directory Password History Policy” on page 157

Users in Active Directory See Delays in Accessing the User Website

**Issue**: When you LDAP identity source is Active Directory, sometimes users see a delay when accessing the user website for Self Service Password Reset.
**Troubleshooting 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 turn 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 users must 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.
The following section contain a list of the changes made to the documentation.

- “December 2016” on page 159
- “November 2016” on page 159

December 2016

<table>
<thead>
<tr>
<th>Location</th>
<th>Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>“Upgrading the Identity Manager Deployment of Self Service Password Reset” on page 34</td>
<td>Added this new section.</td>
</tr>
</tbody>
</table>

November 2016

<table>
<thead>
<tr>
<th>Location</th>
<th>Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>“Selecting an Appropriate Configuration” on page 19</td>
<td>Updated this section.</td>
</tr>
<tr>
<td>Chapter 3, “Installing Self Service Password Reset,” on page 21</td>
<td>Updated the installation information and rearrange content so that it is easier to access the information.</td>
</tr>
<tr>
<td>Chapter 4, “Upgrading Self Service Password Reset,” on page 31</td>
<td>Created a new chapter to move this information from the Installation Chapter so that it is easier to access. The upgrade procedures have been updates.</td>
</tr>
<tr>
<td>“Uninstalling Self Service Password Reset” on page 130</td>
<td>Moved this information from the Installation Chapter to the Managing Chapter so the information is easier to access.</td>
</tr>
</tbody>
</table>