Self Service Password Reset 3.2

Administration Guide

October 2014

www.netiq.com/documentation

Legal Notice

THIS DOCUMENT AND THE SOFTWARE DESCRIBED IN THIS DOCUMENT ARE FURNISHED UNDER AND ARE SUBJECT TO THE TERMS OF A LICENSE AGREEMENT OR A NON-DISCLOSURE AGREEMENT. EXCEPT AS EXPRESSLY SET FORTH IN SUCH LICENSE AGREEMENT OR NON-DISCLOSURE AGREEMENT, NETIQ CORPORATION PROVIDES THIS DOCUMENT AND THE SOFTWARE DESCRIBED IN THIS DOCUMENT "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. SOME STATES DO NOT ALLOW DISCLAIMERS OF EXPRESS OR IMPLIED WARRANTIES IN CERTAIN TRANSACTIONS; THEREFORE, THIS STATEMENT MAY NOT APPLY TO YOU.

For purposes of clarity, any module, adapter or other similar material ("Module") is licensed under the terms and conditions of the End User License Agreement for the applicable version of the NetIQ product or software to which it relates or interoperates with, and by accessing, copying or using a Module you agree to be bound by such terms. If you do not agree to the terms of the End User License Agreement you are not authorized to use, access or copy a Module and you must destroy all copies of the Module and contact NetIQ for further instructions.

This document and the software described in this document may not be lent, sold, or given away without the prior written permission of NetIQ Corporation, except as otherwise permitted by law. Except as expressly set forth in such license agreement or non-disclosure agreement, no part of this document or the software described in this document may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, or otherwise, without the prior written consent of NetIQ Corporation. Some companies, names, and data in this document are used for illustration purposes and may not represent real companies, individuals, or data.

This document could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein. These changes may be incorporated in new editions of this document. NetIQ Corporation may make improvements in or changes to the software described in this document at any time.

U.S. Government Restricted Rights: If the software and documentation are being acquired by or on behalf of the U.S. Government or by a U.S. Government prime contractor or subcontractor (at any tier), in accordance with 48 C.F.R. 227.7202-4 (for Department of Defense (DOD) acquisitions) and 48 C.F.R. 2.101 and 12.212 (for non-DOD acquisitions), the government's rights in the software and documentation, including its rights to use, modify, reproduce, release, perform, display or disclose the software or documentation, will be subject in all respects to the commercial license rights and restrictions provided in the license agreement.

© 2014 NetIQ Corporation. All Rights Reserved.

For information about NetIQ trademarks, see https://www.netiq.com/company/legal/.

Contents

About NetIQ Corporation 7
About this Book 9

1 Overview 11

1.1 Key Features . . . 12
1.2 Architecture . . . 12
1.3 Understanding Challenge-Response Storage Methods . . . 13
1.4 Security Considerations . . . 14
1.4.1 Over-The Wire Data Encryption . . . 14
1.4.2 At-Rest Data Encryption . . . 14
1.4.3 Best Practices for SSPR Security . . . 15
1.4.4 Best Practices for Password Policy . . . 15
1.5 Deployment Scenarios . . . 15
1.6 Working with Configuration Editor . . . 16

2 Installing Self Service Password Reset 17

2.1 Installation Requirements . . . 17
2.1.1 System Requirements . . . 17
2.1.2 Supported Platforms . . . 17
2.1.3 Supported Browsers . . . 17
2.1.4 Supported LDAP Directories . . . 18
2.1.5 Supported Databases . . . 18
2.1.6 Supported Application Servers . . . 18
2.2 Prerequisites . . . 18
2.3 Installing SSPR . . . 18
2.3.1 Installing Tomcat . . . 19
2.3.2 Setting Up a Secure Channel Between the Application Server and the LDAP Server . . . 19
2.3.3 Installing SSPR . . . 20
2.3.4 Setting Up a Secure Channel Between the Client and SSPR (Optional) . . . 22
2.4 Setting Up Your Environment . . . 25
2.4.1 Setting Up Directories . . . 25
2.4.2 Configuring Directories . . . 33
2.5 Upgrading SSPR . . . 35

3 Configuring Self Service Password Reset 37

3.1 Configuring LDAP Settings . . . 37
3.1.1 Importing LDAP Server Certificates . . . 38
3.1.2 Configuring Global Settings for LDAP Directory . . . 38
3.2 Configuring Macros for Messages and Actions . . . 39
3.3 Configuring General Settings . . . 40
3.4 Configuring User Interface Settings . . . 41
3.5 Configuring Password Policy . . . 44
3.6 Configuring Challenge-Response Authentication . . . 45
3.6.1 Configuring global Challenge-Response Settings . . . 45
3.7 Configuring Email Notification Settings . . . 46
3.8 Configuring SMS Notification Settings . . . 49
3.9 Configuring Security Settings . . . 52

3.10 Configuring CAPTCHA . . . 54
3.11 Configuring Intruder Detection . . . 54
3.12 Configuring Token Settings . . . 58
3.13 Configuring Logging and Auditing . . . 59
3.13.1 Setting Up SSL Auditing . . . 61
3.14 Configuring NetIQ eDirectory Settings . . . 61
3.15 Configuring Database . . . 62
3.15.1 Configuring Database Server . . . 63
3.15.2 Configuring Database Settings . . . 63
3.16 Configuring Reporting . . . 64
3.17 Configuring Extensions . . . 65
3.18 Configuring OAuth SSO . . . 67

4 Configuring Modules 69

4.1 Configuring Change Password . . . 69
4.2 Configuring Account Information . . . 71
4.3 Configuring Forgotten Password . . . 71
4.3.1 Enabling Forgotten Password Recovery . . . 72
4.3.2 Selecting a Forgotten Password Action . . . 72
4.3.3 Configuring Other Settings . . . 72
4.4 Configuring Forgotten Username . . . 75
4.5 Enabling New User Registration . . . 75
4.6 Enabling User Activation . . . 77
4.7 Enabling Profile Update . . . 78
4.8 Enabling Shortcut Menu . . . 79
4.9 Enabling People Search . . . 80
4.10 Configuring Helpdesk . . . 81

5 Configuring LDAP and Policy Profiles 85

5.1 Configuring LDAP Directory . . . 85
5.2 Configuring Password Policy for a Profile . . . 88
5.3 Configuring Challenge Response Policy for a Profile . . . 91

6 Integrating SSPR with NetIQ Access Manager 95

6.1 Configuring Access Gateway for SSPR . . . 95
6.1.1 Configuring Proxy Service for SSPR . . . 95
6.1.2 Configuring Protected Resource for SSPR . . . 96
6.1.3 Configuring Single Sign-On to SSPR . . . 96
6.1.4 Configuring Single Sign-On to SSPR When Password Is Not Available . . . 97
6.2 Integrating SSPR with Access Manager . . . 97
6.2.1 Configuring SSPR Parameters for Access Manager . . . 98
6.2.2 Configuring Password Expiration Servlet . . . 98
6.2.3 Integrating Forgotten Password URL . . . 99
6.3 Request Parameters . . . 99
6.4 Command Servlet . . . 99

7 Integrating SSPR with Identity Manager 103

7.1 Configuring SSPR Settings for Identity Manager . . . 103
7.1.1 Configure OAuth Settings for SSPR . . . 103
7.1.2 Set the SSPR Theme to Match the Identity Manager Theme . . . 104
7.1.3 Configure Syslog Audit server . . . 104
7.2 Setting Up the SSPR Configuration File with Identity Manager Settings . . . 105

7.2.1 NetIQ eDirectory Settings . . . 105
7.2.2 User Interface . . . 105
7.2.3 Application Settings . . . 106
7.2.4 Password Settings . . . 107
7.2.5 Challenge Settings . . . 107
7.2.6 Security Settings . . . 108
7.2.7 Integration/ Developer Settings . . . 108
7.2.8 LDAP Directory Profiles . . . 108
7.2.9 Password Policy Profiles . . . 109
7.2.10 Forgotten Password Modules . . . 109

A Frequently Asked Questions 111

A.1 Can I import data from LocalDB to RDBMS? . . . 112
A.2 When a new user is created, does SSPR send an email to the user with login credentials? . . . 112
A.3 Where can I see the account Information? . . . 112
A.4 Can I perform self-password reset if I forget answers to challenge questions? . . . 113
A.5 How do I resolve the No From Address error? . . . 113
A.6 Why Users cannot use their old password to login even when they did not complete the forgotten password process? . . . 113
A.7 Where can I see the password history? . . . 113
A.8 Can I reset password after utilizing my all eDirectory grace login without calling helpdesk? . . . 114
A.9 How to create a new user? . . . 114
A.10 Can SSPR use nspmComplexityRules? . . . 114
A.11 Does SSPR work with OpenLDAP? . . . 114
A.12 How to go to Main Menu from Configuration Editor? . . . 114
A.13 How to enable users to change password more than once a day? . . . 115
A.14 How to enable Windows desktop to support forgotten password reset? . . . 115
A.15 How to configure post password change actions? . . . 115
A.16 Where can I see version of installed SSPR? . . . 115
A.17 Does SSPR honor the Active Directory password history policy? . . . 115
A.18 How to set logging mechanism and where to see the logged result? . . . 116
A.19 How to enable SSPR to read custom http headers for authentication? . . . 116
A.20 How to import LDAP certificates? . . . 116
A.21 How to modify user interface strings? . . . 116
A.22 How do I change the default language of SSPR? . . . 116
A.23 Can audit events be forwarded to syslog and compatible servers? . . . 117
A.24 Where can I see SSPR audit logs? . . . 117
A.25 Can SSPR authenticate by using custom attributes? . . . 117
A.26 How to access reports and logs in SSPR? . . . 117

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
Web Site:	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
Web Site:	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 Web site 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

The *Administrator Guide* provides conceptual information about Self Service Password Reset. This guide intends to help you understand and configure all features of the product and includes the following chapters:

- Chapter 1, “Overview,” on page 11
- Chapter 2, “Installing Self Service Password Reset,” on page 17
- Chapter 3, “Configuring Self Service Password Reset,” on page 37
- Chapter 4, “Configuring Modules,” on page 69
- Chapter 5, “Configuring LDAP and Policy Profiles,” on page 85
- Chapter 6, “Integrating SSPR with NetIQ Access Manager,” on page 95
- Chapter 7, “Integrating SSPR with Identity Manager,” on page 103
- Appendix A, “Frequently Asked Questions,” on page 111

Intended Audience

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

1 Overview

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

It provides enhanced security. The user gets authenticated through a series of questions and answers known only to the user. During password reset, SSPR 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 internal database. Users can change their password and reset any forgotten password by using the configured challenge-response information.

User productivity is increased through automatic synchronization of changed passwords, which eliminates the need for users to wait for password resets and account unlocks. At the same time, helpdesk can perform more critical tasks rather than password resets.

SSPR provides the following functionalities:

- **Change password:** Users can change their password without an administrator's assistance.
- **Reset forgotten password:** Users can reset their password by answering challenge questions. You, as an administrator, can configure and store these questions by using SSPR. SSPR stores user responses in the standard RDBMS database, LDAP server, or Novell NMAS repositories based on the database configuration.
- **Recover forgotten username:** Users can search for a forgotten username by using a configurable search filter and attributes.
- **Configure challenge-response authentication:** You, as an administrator, can configure a set of questions for users. The questions include random and required questions. The system prompts users to specify answers for these questions at first login. Users reset their password by answering the same questions they saved earlier through SSPR.
- **New user self-registration:** Users have the ability to self-register.
- **Activate user accounts:** Users can activate an account if the account is deactivated and set a password for this account.
- **Activate Profile:** Users can view and update their profile attributes.
- **Search People:** Users can search for their colleagues' information.
- **Simplify helpdesk support response:** Helpdesk users can leverage the Helpdesk module to simplify the helpdesk tasks such as resetting passwords and unlocking user accounts.
- **Create password policies:** You, as an administrator, can enforce restrictions on the types of passwords users can create.
- **Report on usage and lockouts:** Self Service Password Reset can generate reports for intruder?lockout, daily usage statistics, and online log information for debugging.

This chapter includes the following topics:

- Section 1.1, "Key Features," on page 12
- Section 1.2, "Architecture," on page 12
- Section 1.3, "Understanding Challenge-Response Storage Methods," on page 13

- Section 1.4, “Security Considerations,” on page 14
- Section 1.5, “Deployment Scenarios,” on page 15
- Section 1.6, “Working with Configuration Editor,” on page 16

1.1 Key Features

The key features of SSPR include:

- Stand-alone, easy to deploy Java-based Web application
- Web-based configuration manager
- Support for LDAP server, standard RDBMS database, local database, and Novell NMAS repositories for storing responses
- Localization support for English, Chinese, Chinese Traditional, Czech, Dutch, Finnish, French, German, Hebrew, Italian, Japanese, Korean, Norwegian, Norwegian Nynorsk, Polish, Portuguese, Brazilian-Portuguese, Slovak, Spanish, Thai, and Turkish

  SSPR provides an easy way to add new languages by using Configuration Editor
- Helpdesk and administrator modules are provided for password reset, clearing intruder lockout, viewing online logs and daily statistics, and user information debugging
- Support for new user registration, account activation, and account management
- Easy customization
- Integration with external Web authentication methods
- People Search
- Interactive user search such as, wildcard search and searching while typing (ajax search)
- Support for extensive logging to help troubleshoot installation and configuration issues
- Icons for each button for a better visibility and understanding
- Database backup functionality
- Alerts and auditing support
- Workflow initialization and account claiming support
- Support for smartphone and tablet views

1.2 Architecture

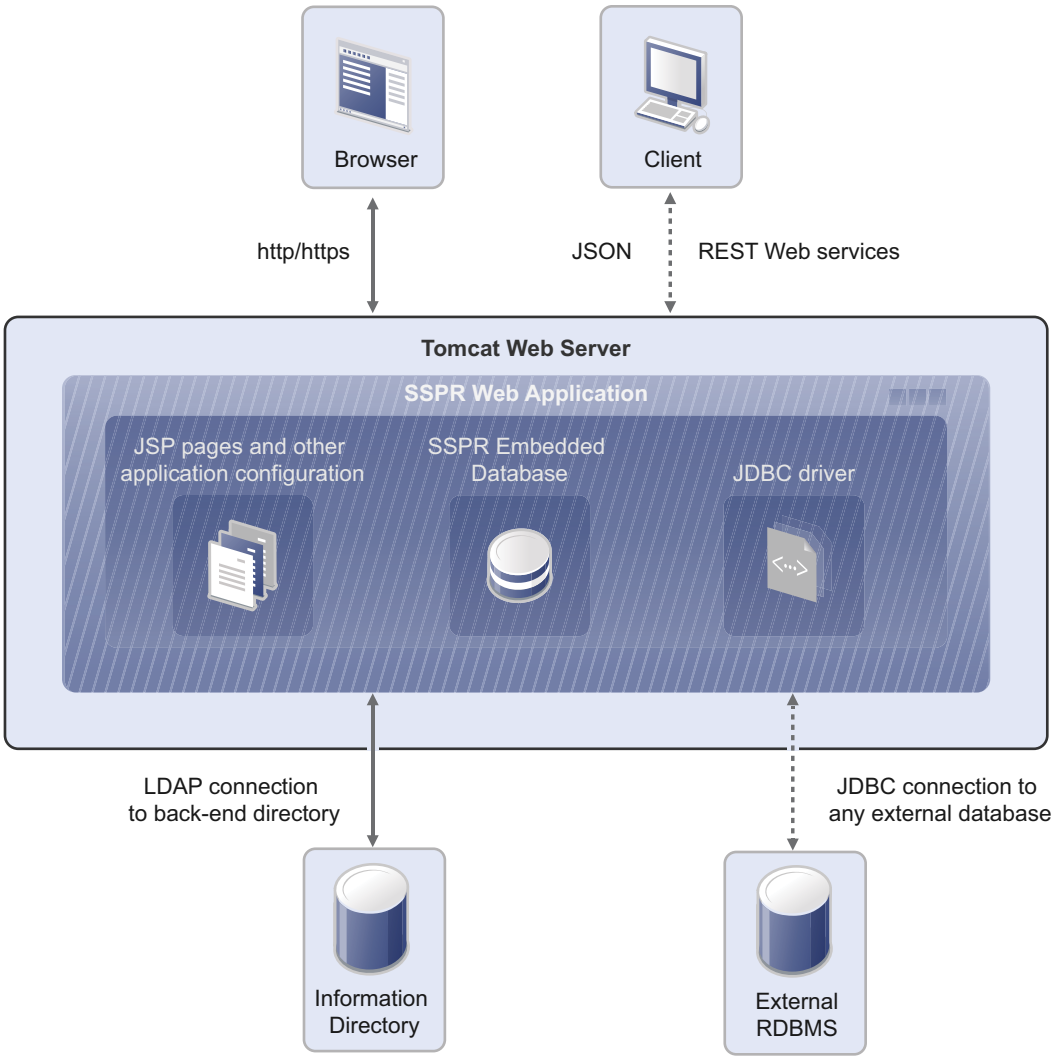
SSPR consists of the following components:

- **Web Server:** To deploy SSPR.
- **Back-end Information Directory:** To store information. For example, Active Directory, eDirectory, and Oracle Directory Server.
- **Database:** To store users’ information.

  Apache Derby is the default database.
- **User Interfaces:** Web interfaces that a user accesses.
- **Configuration Manager/ Configuration Editor:** Web interface that you, as an administrator, can use to configure SSPR.

The following diagram illustrates the architecture of SSPR:

Figure 1-1 *Architecture of SSPR*



1.3 Understanding Challenge-Response Storage Methods

SSPR supports the following directories to store users' challenge-responses:

- LDAP Directory
- LocalDB
- Database

You can configure SSPR to use any one or all three directories to save users' challenge-responses. When a user attempts to recover a forgotten password, SSPR reads the directories that you have configured. SSPR 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, SSPR uses answers in the same locale regardless of the current browser locale settings. SSPR stores answers by using a standardized XML format. Depending on the configuration, SSPR stores answers as plain text or one way hashed (encrypted) by using SHA1, Salted SHA1, or bcrypt.

NetIQ eDirectory Integration

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

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

1.4 Security Considerations

SSPR can be deployed along with applications that are available to the public Internet. As an administrator, you must protect SSPR so that unauthorized users cannot gain access to SSPR and make any change in the information. You need to check and control the installation, maintenance, and monitoring processes of SSPR to ensure that SSPR follows security practices.

This section includes:

- Section 1.4.1, "Over-The Wire Data Encryption," on page 14
- Section 1.4.2, "At-Rest Data Encryption," on page 14
- Section 1.4.3, "Best Practices for SSPR Security," on page 15
- Section 1.4.4, "Best Practices for Password Policy," on page 15

1.4.1 Over-The Wire Data Encryption

SSPR is an endpoint for several communication traffic channels. You must protect each channel.

Communication channels include the following:

- HTTP browser to SSPR traffic by using SSL/TLS over HTTP (HTTPS)
- SSPR to LDAP server traffic by using SSL/TLS over LDAP (LDAPS)
- SSPR to database server traffic, database specific (optional)

Each channel requires its own security configuration settings. But, you should encrypt all channels by using an end-to-end encryption protocol. Do not rely on private, secure networks. We recommend you to use the encryption protocols listed here.

1.4.2 At-Rest Data Encryption

SSPR can store sensitive security data in several locations.

Item	Location
Configuration File	SSPR Server: `webapps/SSPR/SSPRConfiguration.xml`
User Responses (Encrypted)	Configurable: LocalDB, Database, LDAP, or NMAS
Helpdesk Responses	Configurable: LocalDB, Database, or LDAP
Shared Password History	LocalDB

You must secure the operating system on which you have hosted SSPR, SSPR database, and LDAP directory by using the respective vendor's best practices.

1.4.3 Best Practices for SSPR Security

To enhance security of SSPR, 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 SSPR to see source network addresses for complete audit records to be maintained.

For more information about SSPR security configurations, see Section 3.9, "Configuring Security Settings," on page 52.

1.4.4 Best Practices for Password Policy

To enhance security of password policies:

- Use a Wordlist to prevent easily guessable passwords.
- Use a shared Wordlist 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 those are unlikely to have similar answers among different users.

For more information about how to configure policies, see Section 3.5, "Configuring Password Policy," on page 44.

1.5 Deployment Scenarios

The possible SSPR deployment scenarios include:

- When the back-end user store is NetIQ eDirectory.

  For more information about the configuration, see "Setting Up NetIQ eDirectory" on page 26 and Section 2.4.2, "Configuring Directories," on page 33.
- When the back-end user store is Active Directory.

For more information about the configuration, see "Setting Up Active Directory" on page 28 and Section 2.4.2, "Configuring Directories," on page 33.

- When the back-end user store is Oracle Directory Server.

  For more information about the configuration, see "Setting Up Oracle Directory Server" on page 32 and Section 2.4.2, "Configuring Directories," on page 33.

1.6 Working with Configuration Editor

Configuration Editor is a web interface that controls the settings for SSPR. You can launch Configuration Editor from the main menu or from Configuration Manager.

In Configuration Editor, you can do the following:

- **Configure settings for SSPR:** You can configure the default settings that define how a user can use SSPR. You can also define directory profiles, modules, and templates for the users.To configure settings, SSPR provides different tabs that include the list of related settings. Detailed information on each setting is provided in the proceeding chapters.
- **Search for configuration settings:** To quickly move to a particular setting you can search for it by using the search icon that is displayed on the top right corner of Configuration Editor. The search result is displayed 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, click the Set Configuration Password icon on the top-right corner of Configuration Editor. You can also click on **Actions > Set Configuration Password** to change the password for Configuration Editor.
- **Save configuration settings:** To save the configuration that you update for all the settings, click the Save icon on the top-right corner of Configuration Editor. You can also click on **Actions > Save** to save the settings.
- **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 the list of modified settings and these settings are listed in separate sections. Each section displays the details of the modified fields. After the configuration setting is saved, anyone who has access to Configuration Manager can view the last modified details of all the settings when they open Configuration Editor.
- **Change the precedence order of the setting fields:** To change the precedence of each field, you can use the arrow keys that are adjacent to the respective fields. You can change the precedence order for any setting that includes multiple fields.
- **Define custom texts:** To define the text that should be displayed to the users during a particular event, click the **Custom Text** tab and configure the required setting. You can define any error or caution messages.

2 Installing Self Service Password Reset

This chapter explains how to install Self Service Password Reset (SSPR).

Topics include:

- Section 2.1, “Installation Requirements,” on page 17
- Section 2.2, “Prerequisites,” on page 18
- Section 2.3, “Installing SSPR,” on page 18
- Section 2.4, “Setting Up Your Environment,” on page 25
- Section 2.5, “Upgrading SSPR,” on page 35

2.1 Installation Requirements

This section explains the requirements for installing SSPR.

- Section 2.1.1, “System Requirements,” on page 17
- Section 2.1.2, “Supported Platforms,” on page 17
- Section 2.1.3, “Supported Browsers,” on page 17
- Section 2.1.4, “Supported LDAP Directories,” on page 18
- Section 2.1.5, “Supported Databases,” on page 18
- Section 2.1.6, “Supported Application Servers,” on page 18

2.1.1 System Requirements

- 512 MB Java heap memory
- 1 GB hard disk

2.1.2 Supported Platforms

- Microsoft Windows Server 2008 (32-bit and 64-bit)
- Microsoft Windows Server 2003 R2 (32-bit and 64-bit)
- Microsoft Windows Server 2008 R2 (64-bit)
- Microsoft Windows Server 2012 (64-bit)
- SUSE Linux Enterprise Server 10 or later (32-bit and 64-bit)
- Red Hat Enterprise Linux (RHEL) 6.2 or later (64-bit)

2.1.3 Supported Browsers

- Mozilla Firefox 30 and later
- Microsoft Internet Explorer 8.0 or later (only for the main page)

NOTE: Configuration Editor does not work on Microsoft Internet Explorer 8.0. So, with Internet Explorer 8.0 you cannot modify the configuration settings but, you can access the SSPR main page.

- Google Chrome 36 and later
- Internet Explorer 10 or later (for configuring the directories)

2.1.4 Supported LDAP Directories

- NetIQ eDirectory
- Active Directory
- Oracle Directory Server

NOTE: SSPR does not support the AD 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 5, “Configuring LDAP and Policy Profiles,” on page 85.

2.1.5 Supported Databases

- Microsoft SQL Server
- Oracle

2.1.6 Supported Application Servers

- Java JDK 1.7 or later
- Apache Tomcat 6 or 7. Other Java Application Servers are not supported.

2.2 Prerequisites

Ensure that you have completed the following activities in your back-end directory:

- Install certificate services
- Export self-signed certificate for the directory
- Add self-signed certificate to GPO
- Create recommended users and groups for SSPR usage

For more information about how to perform these activities, see the related product documentation.

2.3 Installing SSPR

Before installing SSPR, determine which directory service you want to use for storing user details and responses to security questions. SSPR includes the following configuration templates:

- NetIQ eDirectory
- Active Directory
- Oracle Directory Server, OpenLDAP, DirectoryServer 389, Others

For more information about specific configurations steps, see Section 2.4, “Setting Up Your Environment,” on page 25.

SSPR installation consists of the following steps:

1. (Conditional) If you are installing SSPR by using the ZIP file, install Tomcat.

   See Section 2.3.1, “Installing Tomcat,” on page 19
2. Set up a secure channel between the application server and the LDAP server.

   See Section 2.3.2, “Setting Up a Secure Channel Between the Application Server and the LDAP Server,” on page 19
3. Install SSPR.

   See “Installing SSPR” on page 20
4. Set up a secure channel between the client and SSPR (optional).

   See Section 2.3.4, “Setting Up a Secure Channel Between the Client and SSPR (Optional),” on page 22

2.3.1 Installing Tomcat

For information about how to install Tomcat, see the Tomcat documentation.

You can verify the installation by accessing Tomcat at http://server:port/.

NOTE: Use -Xms1024m -Xmx1024m to control Java heap size. 1024m is only for example. The exact number depends on your system memory. The recommended value is 1 GB. Setting minimum and maximum heap size to the same is a best practice because JVM does not increase heap size at runtime. For more information about how to set Java heap size, see Tomcat documentation.

2.3.2 Setting Up a Secure Channel Between the Application Server and the LDAP Server

SSPR must trust the LDAP server’s certificate. To establish a secure channel between an application server and an LDAP server, perform the following steps:

1. Identify the certificate you want to use. You can use any one of the following certificates:
   - A certificate issued by a recognized commercial certificate authority. The certificate of this authority should be present in the certificate database. If the server name in the LDAP URL is identical to the common name of the certificate, the certification process is complete.
   - A certificate issued by a private certificate authority such as Novell iManager or Microsoft Active Directory. In this case, the certificates of that certificate authority need to be imported into the java certificate database.
   - A self-signed certificate. In this case, import the self-signed certificate in to the java certificate database.

   To export the eDirectory certificates by using iManager, see Exporting the SSL Certificate Using iManager.

   To export the Active Directory certificates, see Exporting the LDAPS Certificate and Importing for use with AD DS.

2 Import certificates in to the Java keystore by performing any one of the following ways:

2a **Using SSPR:** In Configuration Manager, click **Actions** > **Import LDAP Server Certificates**.

You can also import certificates during configuring the LDAP directory through the Configuration Guide.

2b **Manually**

On Windows: Use keytool to import the file.

```
cd <JAVA_HOME>\jre\bin
keytool -importcert -alias <alias>  -file <filepath> -keystore
..\lib\security\cacerts -storepass <password>
```

`keytool` prompts for a password. The default password is `changeit`.

The certificate database is located in the following location:

```
JAVA_HOME\lib\security\cacerts
```

`JAVA_HOME` is the directory where Java is installed.

On Linux: Do the following:

Use keytool to import the file.

```
cd <JAVA_HOME>/jre/bin
keytool -importcert -alias <alias>  -file <filepath> -keystore
../lib/security/cacerts -storepass <password>
```

`keytool` prompts for a password. The default password is `changeit`.

The certificate database is located in the following location:

```
JAVA_HOME/lib/security/cacerts
```

`JAVA_HOME` is the directory where Java is installed.

3 Continue with "Using SSPR_3.2.zip" on page 21.

2.3.3 Installing SSPR

SSPR is available for download in the following two formats:

- `SSPR.EXE` (recommended for a new installation)
- `SSPR_3.2.ZIP` (recommended for an upgrade)

Using SSPR_3.2_installer.exe

`SSPR.EXE` is an executable file that includes the installation of Tomcat, Java and SSPR service. You do not have to install Tomcat manually.

If you are installing SSPR for the first time and do not have Tomcat installed on the machine, then running the installer, with **SSPR Application Service** selected, installs Tomcat along with SSPR. The SSPR service is selected by default.

Incase you are using a previous version of SSPR then, deselect **SSPR Application Service** and run the installation wizard. The installer extracts the `sspr.war` file to the specified installation path, default path is `C:\Program Files (x86)\NetIQ Self Service Password Reset`. Copy the `sspr.war` file and place it in the existing `Tomcat/webapps` folder.

The installer file, `SSPR.EXE` launches an installation wizard. Follow the on-screen instructions to install the latest version of SSPR.

If you select the SSPR Service option, you need to provide the following information:

- Specify the display name of SSPR Service in the Windows Service Display Name for SSPR Service field.

  NOTE: Ensure that you provide the SSPR Service display name without any space. If you do not provide any display name then, the service is displayed as SSPR-Service.

- Specify the HTTP port number for SSPR Service.
- Select the Enable Secure HTTP check box if you require a secured port, and then provide the https port number.

Continue with "Deploying SSPR" on page 22.

Uninstalling SSPR: To uninstall SSPR, perform the following:

1. Shut down the tomcat Web service.
2. Download the XML configuration file for future use. (Optional)
3. Export the local database (if any challenge-response questions are saved there) by using the SSPR command utility. (Optional)
4. Run the following command to delete the SSPR service from the bin folder of Tomcat Service:

   ```
   ssprservice.bat remove <service>
   ```

   where, service is the name of the service.
5. Reboot the machine.
6. Delete the `NetIQ Self Service Password Reset` folder.

Using SSPR_3.2.zip

`SSPR_3.1.zip` is a compressed zip file that contains SSPR Web archive and tools. Unzip the SSPR package and save the sspr.war file to a preferred location.

To install SSPR by using the WAR file, perform the following:

1. Stop Tomcat.
   - **On Windows:**

     Tomcat as service: Right-click the Tomcat icon on the task bar to start or stop the Tomcat service.

     Standalone Tomcat: Go to the bin folder of Tomcat and run `shutdown.bat`.
   - **On Linux:** Run the `shutdown.sh` script that is available in the `<Tomcat_Home>/bin` folder.
2. Locate the `sspr.war` file from the folder where you saved it.
3. Copy the `sspr.war` file to the `Tomcat/webapps` folder.

Continue with "Deploying SSPR" on page 22.

Uninstalling SSPR: To uninstall SSPR, perform the following:

1. Shut down the tomcat Web service.
2. Download the XML configuration file for future use. (Optional)
3. Export the local database (if any challenge-response questions are saved there) by using the SSPR command utility. (Optional)

4 Delete the `sspr` folder and the `sspr.war` file from `<tomcat>/webapps`.

This path may vary on your system.

Deploying SSPR

To deploy SSPR, perform the following steps:

1 (Conditional) If SSPR is installed by using the EXE file, Start the SSPR Service that is displayed as the name you specified for the service when you installed SSPR.

2 (Conditional) If SSPR is installed by using the WAR file, Start Tomcat.

- **On Windows:**

  Tomcat as service: Go to **Start** > **All Programs** > **Apache Tomcat** and click **Monitor Tomcat** to start Tomcat as a service.

  You can also start the Tomcat service by right?clicking the Tomcat icon on the task bar.

  Standalone Tomcat: Go to the **bin** folder of Tomcat and run `start.bat`

- **On Linux:** Run the `startup.sh` script that is available in the `<Tomcat_Home>/bin` folder.

3 Go to http://localhost:<port>/sspr. This link takes you to the SSPR portal.

4 To confirm the successful installation, check the `tomcat\logs\catalina.out` file.

To check whether the Tomcat Web server is running, open the link http://localhost:<port>/. This will open an Apache Tomcat Web page.

5 Continue with one of the following:

- Section 2.3.4, “Setting Up a Secure Channel Between the Client and SSPR (Optional),” on page 22
- Section 2.4, “Setting Up Your Environment,” on page 25

2.3.4 Setting Up a Secure Channel Between the Client and SSPR (Optional)

SSPR is a Web-based application and you can access it with Internet browsers through http. You can also access SSPR through https. To access SSPR through https, perform the following actions:

1. Modify the operating system firewall settings for the SSPR server.
2. Configure SSL in Tomcat by using certificates from CA

Modifying the Firewall Settings

1 Go to **Control Panel** > **Security Center** > **Windows Firewall** > **Advanced** > **Windows Firewall Settings**.

2 Click **Inbound Rules** > **New Rule**.

3 Specify the port 8443 and other necessary ports.

4 In the **Profile** window, select the profiles this rule applies to, and then click **Next**.

5 Check if the profile has Inbound connections set to Block (default) and it allows these connections with rules specified.

Configuring SSL in Tomcat By Using Certificates from CA

You should configure SSL in Tomcat by using certificates from a trusted Certification Authority (CA) for more security.

For this configuration, you first require to generate a keystore and a Certificate Signing Request (CSR). CSRs include your public key and it must contain the same details that you have provided in the online request form. After your request is issued, download and install SSL in Tomcat.

- "Generating a Keystore and CSR in Tomcat" on page 23
- "Installing SSL in Tomcat" on page 24
- "Setting Up a Secure Channel (Optional)" on page 24

Generating a Keystore and CSR in Tomcat

Perform the following steps by using the keytool utility to generate a keystore and CSR on your server:

1. Run the following command in keytool to create a keystore:

   ```
   keytool -keysize 2048 -genkey -alias tomcat -keyalg RSA -keystore
   tomcat.keystore
   ```

2. Specify a password. The default password is `changeit`.
3. Specify the following distinguished information:

Field	Description
First and Last Name	The fully-qualified domain name, or URL that you want to secure. To request a wildcard certificate, add an asterisk (*) to the left of the common name where you want the wildcard, for example, *.ssprdomain.com.
Organizational Unit	Optional. If applicable, specify the DBA name.
Organization	The full legal name of your organization.
City/Locality	Name of the city in which your organization is registered or located. Do not abbreviate.
State/Province	Name of state or province where your organization is located. Do not abbreviate.
Country Code	The two-letter International Organization for Standardization (ISO) format country code for where your organization is legally registered.

4. The system prompts for a password for the private key within the keystore.

   If you press Enter, the key password is set to the same password that you specified in Step 2 on page 23. The key password must include at least six characters.

5. Run the following command in keytool to create a CSR:

   ```
   keytool -certreq -keyalg RSA -alias tomcat -file csr.csr -keystore
   tomcat.keystore
   ```

6. Specify the password you provided in Step 2 on page 23.

7 Open the CSR file, and copy all text (include ----BEGIN NEW CERTIFICATE REQUEST---- and -----END CERTIFICATE REQUEST----) into the online request form and complete your application.

For more information about how to complete the online request form, see respective certification authority documentation.

NOTE: This is a specific case. You can manage your certificates with Tomcat in other ways also. For more information about other configuration types, see the Tomcat documentation.

Installing SSL in Tomcat

Download the certificate and place it in the same folder where you have placed your keystore. Then, install the certificate by using the keytool utility.

To Install SSL in Tomcat, perform the following steps:

1 Run the following command in keytool to install the root certificate:

```
keytool -import -alias root -keystore tomcat.keystore -trustcacerts -file
<root.crt>
```

NOTE: Certificate names vary based on CA.

---

2 Install the intermediate certificate.

```
keytool -import -alias intermed -keystore tomcat.keystore -trustcacerts -file
<intermediate.crt>
```

3 Install the issued certificate into the keystore:

```
keytool -import -alias tomcat -keystore tomcat.keystore -trustcacerts -file
<name of your certificate>
```

4 Update the `server.xml` file with the correct keystore location in the Tomcat directory.

NOTE: The HTTPS connector is commented out by default. Remove the comment tags to enable HTTPS.

Update the following elements in `server.xml` for Tomcat 5.*x*, 6.*x* and 7.*x*:

```
<-- Define a SSL Coyote HTTP/1.1 Connector on port 8443 --> <!-- <Connector
port="8443" maxThreads="200"
scheme="https" secure="true" SSLEnabled="true"
keystoreFile="path to your keystore file" keystorePass="changeit"
clientAuth="false" sslProtocol="TLS"/>
```

5 Restart Tomcat.

Setting Up a Secure Channel (Optional)

For testing purpose, you can use self- signed certificates to setup a secure channel:

1 Create a self-signed certificate in the cacerts store. Change to the `%JAVA_HOME%\bin\` folder and run the following command:

Windows: `keytool -genkey -alias tomcat -keyalg RSA -keystore ..\<jre>\lib\security\cacerts`

Linux: `keytool -genkey -alias tomcat -keyalg RSA -keystore ../<jre>/lib/security/cacerts`

2 Enter `changeit` as the keystore password.

3 In the `<Tomcat_Home>/Conf` folder, modify the `server.xml` file to support https.

- Uncomment https connection and comment out http connection.
- When you uncomment https connection, add the following attribute:

  Linux: `keystoreFile="${java.home}\lib\security\cacerts" keystorePass="changeit"`

  Windows: `keystoreFile="${java.home}/lib/security/cacerts" keystorePass="changeit"`

4 Restart Tomcat.

2.4 Setting Up Your Environment

After installing SSPR, you must set up and configure the back-end directory for making SSPR functional. SSPR supports the following directories:

- NetIQ eDirectory

  For more information about how to set up and configure eDirectory, see "Setting Up NetIQ eDirectory" on page 26 and Section 2.4.2, "Configuring Directories," on page 33.

- Active Directory - schema mode

  For more information about how to set up and configure Active Directory in the schema mode, see "Setting Up Active Directory in the Schema Mode" on page 28 and Section 2.4.2, "Configuring Directories," on page 33.

- Active Directory - external RDBMS mode

  For more information about how to set up and configure Active Directory to store responses in an external database, see "Setting Up Active Directory in the RDBMS Mode" on page 30 and Section 2.4.2, "Configuring Directories," on page 33.

- Oracle Directory Server

  For more information about how to set up and configure Oracle Directory Server, see "Setting Up Oracle Directory Server" on page 32 and Section 2.4.2, "Configuring Directories," on page 33.

This section includes:

- Section 2.4.1, "Setting Up Directories," on page 25
- Section 2.4.2, "Configuring Directories," on page 33

2.4.1 Setting Up Directories

This section describes the following:

- "Setting Up NetIQ eDirectory" on page 26
- "Setting Up Active Directory" on page 28
- "Setting Up Oracle Directory Server" on page 32

Setting Up NetIQ eDirectory

The SSPR package includes the `edirectory-schema.ldif` file and the `edirectory-rights.ldif` in the `supplemental` directory. You must modify `edirectory-rights.ldif` manually to match it with your environment. Use `edirectory-schema.ldif` to extend the SSPR schema.

SSPR uses eDirectory attributes to store the following user data:

- The last time when a user changed the password
- The last time when SSPR sent an e-mail notification to the user about password expiry
- Secret questions and answers

This section discusses:

- "Using edirectory-schema.ldif to Extend the Schema" on page 26
- "eDirectory Rights" on page 26

Using edirectory-schema.ldif to Extend the Schema

You can import the `edirectory-schema.ldif` file through one of the following:

- iManager
- ICE command line
- Standard ldapmodify tool

For example, run the following command in eDirectory through the ldapmodify tool:

```
ldapmodify -x -h <host ip address> -p 389 -D cn=admin,o=context -w

password -f edirectory-schema.ldif
```

Running this command adds the following SSPR attributes to the directory schema:

- pwmEventLog
- pwmResponseSet
- pwmLastPwdUpdate
- pwmGUID

eDirectory Rights

SSPR requires permission to perform operations in eDirectory and uses the following two different eDirectory rights:

- "Proxy User Rights" on page 26
- "Authenticated User Rights" on page 27
- "Granting Rights to the pwmResponseSet Attribute" on page 27

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

---

NOTE: Create rights to `[Entry Rights]` will be needed if the New User Registration module is enabled. This right is not added by `edirectory-rights.ldif`. Add it manually by using 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 entry:

- Browse rights to `[Entry Rights]`
- Read, Compare, and Write rights to pwmResponseSet

After setting up eDirectory for SSPR, continue with Section 2.4.2, "Configuring Directories," on page 33.

Granting Rights to the pwmResponseSet Attribute

Users need access to write to the pwmResponseSet attribute. Perform the following steps in iManager:

1. Enable [this] support in iManager.
   - **1a** Log in to iManager.
   - **1b** Click **Configure**.
   - **1c** Select **iManager** > **Configure iManager**.
   - **1d** Select **Misc** > **Enable [this]**.
2. Assign rights to users.
   - **2a** Log in to iManager.
   - **2b** Select **View Objects**.
   - **2c** Select **Browse**.
   - **2d** Browse to the top level container of all users in the directory.
   - **2e** Click the container name and select **Modify Trustees**.
   - **2f** Click **Add Trustee**.
   - **2g** Select **[This]** and click **OK**.
   - **2h** Click **Assigned Rights** for the **[This]** trustee.
   - **2i** Click **Add Property**.
   - **2j** Select **Show all properties** > **pwmResponseSet**, and click **OK**.
   - **2k** Ensure that Write, Compare, Read, and Inherited options are selected.
   - **2l** Click **Done** > **OK**.

Other Rights

Depending on the SSPR configuration, users may need other rights assigned as well. In most cases, SSPR 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:** User must have all rights to read attributes that are part of the Update Profile module and write rights to any attributes they require to write to.
- **Helpdesk 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 Helpdesk module through configured actions or password setting and unlocking accounts.

NOTE: For eDirectory 8.8 SP7, apply the latest patch to eDirectory 8.8.7. to avoid any issue in changing passwords. For more information, see TID7010386.

Setting Up Active Directory

You can configure Active Directory in any one of the following modes:

- Database mode: Challenge-responses are stored in database. You do not need to extend schema if you are using this mode.
- Schema mode: Challenge-responses are stored in Active Directory. You must extend the schema and assign user rights to store data in Active Directory.
- RDBMS mode: Challenge-responses are stored in an external RDBMS.

Topics include:

- “Setting Up Active Directory in the Database Mode” on page 28
- “Setting Up Active Directory in the Schema Mode” on page 28
- “Setting Up Active Directory in the RDBMS Mode” on page 30

Setting Up Active Directory in the Database Mode

In this mode, Active Directory uses Derby as the default database. You do not need to do any other configuration.

Setting Up Active Directory in the Schema Mode

SSPR leverages the directory to store and manage the SSPR data. To accomplish this, SSPR extends the directory schema to add SSPR schema attributes where the SSPR data is stored.

After you extend the directory schema, you must give permissions to access objects, including the group policy, organizational units, and containers. Assigning user rights includes authorizing read or write rights to SSPR 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 SSPR 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 organizational unit below the root.

Extending the Active Directory Schema

Log in as the domain administrator and run the schema extension file on an Active Directory domain controller or machine that is connected to the Active Directory domain.

1. Log in to the server as an administrator.
2. Click **Schema Extension Tools** > **Active Directory Extension**.

   or

   If you are installing from the SSPR installer package, locate the `supplemental` folder, then double-click `ssprADSschema.exe`.
3. Select **Extend Active Directory Schema**.
4. Click **OK** to add the following SSPR attributes are added to the directory schema:
   - pwmEventLog
   - pwmResponseSet
   - pwmLastPwdUpdate
5. Click **OK.**

   After extending the directory schema, you must assign access rights to the relevant containers and organizational units. Continue with section Assigning User Rights.

Assigning User Rights

You must assign permission to objects in the directory to store the data against the new SSPR schema attributes. You assign rights to all the objects that access the SSPR data, including the user objects, containers, group policies, and organizational units.

When you assign rights to the containers and organizational units, rights filter all associated user objects. Do not assign rights at the user object level unless it is mandatory.

1. Run `ssprADSschema.exe` from `supplemental\Schema\AD`.

   NOTE: This tool is multi-functional. If you select to extend the schema again, a message listing the existing schema appears. Ignore this message.
2. Select **Assign User Rights**, then click **OK**.

   For example, if you assign rights to the Users container, the User container definition is:

   `cn=users,dc=www,dc=training,dc=com`

   To assign rights to an organizational unit, such as Marketing, in the `www.company.com` domain, the definition is:

   `ou=marketing,dc=www,dc=company,dc=com`
3. Specify your container or organizational unit definition in **Assign rights to this object**.
4. Click **OK**.
5. Repeat Step 2 through Step 4 to assign rights to all required user objects, containers, and organizational units.

   If you see an error message indicating `Error opening the specified object: -2147016661`, it means that the rights have already been assigned to the object.

   If you see an error message indicating `Error opening the specified object: -214716656`, it means that you have attempted to assign the rights to an object that does not exist in the directory.

Check your punctuation, syntax, and spelling, then repeat the procedure.

6 When all the required rights are successfully assigned, click **OK**.

7 Click **Cancel**.

NOTE: You can extend rights to objects any time after extending the schema. If you add organizational units, you need to rerun the `adschema.exe` tool and assign rights to the new object to permit the SSPR data to write to the directory.

Refreshing the Directory Schema

1 Run the Microsoft Management Console (MMC), then display the Active Directory Schema plug-in.

2 Right-click **Active Directory Schema**, then select **Reload the Schema**.

In a multi-server environment, schema updates occur after server replication.

After setting up Active Directory for SSPR, continue with Section 2.4.2, “Configuring Directories,” on page 33.

Setting Up Active Directory in the RDBMS Mode

If your back-end information directory is Active Directory, choose **Active Directory - Store responses in a database**, go to **Settings** > **Database** and configure the following:

- **Database Class:** Name of the database class. Specify the Java JDBC full driver class name.

  The classpath must include the corresponding JDBC driver JAR or ZIP file, typically, in the `WEB-INF/lib` directory or the application server's lib directory. For example, in Tomcat, it is `<TOMCAT_HOME>/webapps/<SSPR>/WEB-INF/lib` or `<TOMCAT_HOME>/lib`. The default folder name under which the application is deployed is `<SSPR>`. If you have changed this name, use the appropriate path name accordingly.
- **Database Connection String:** Specify the database connection string in the standard JDBC format.
- **Database Username:** Specify the name of the user who can connect to the database.
- **Database password:** Specify a password for the database user.

Sample Configuration

This example discusses steps for configuring SSPR with MicroSoft SQL Server 2008.

Download the Microsoft SQL Server jdbc driver `sqljdbc.jar` and add it to the server or application classpath and configure SSPR settings as follows:

Field	Description
Database Class	Specify com.microsoft.sqlserver.jdbc.SQLServerDriver
Database Connection String	The general form of the connection URL is: jdbc:sqlserver:// [serverName[\instanceName][:portNumber]][;property=value[;property=value]] **jdbc:sqlserver://:** (Required) Sub-protocol. It is constant. **serverName:** (Optional) Server address. Includes DNS, IP address, localhost, or 127.0.0.1 of the local computer. If not specified in the connection URL, the server name must be specified in the properties collection. **instanceName:** (Optional) Instance to connect to serverName. If not specified, a connection to the default instance is made. **portNumber:** (Optional) Port to connect to serverName. The default port number is 1433. If you are using the default, you do not require to specify the port in the URL. The following are few examples of connection string in different scenarios: In the examples below, Instance - LocalDB, server - DBHOST, port number- 1443 ◆ Connection string to connect `LocalDB` on `DBHOST` at port `1433` is jdbc:sqlserver:// DBHOST\LocalDB:1433; ◆ Connection string to connect `LocalDB` on `DBHOST` at port `1433` by using `USER1` and password `PWD` is jdbc:sqlserver:// DBHOST\LocalDB:1433;integratedSecurity=true;username=USER1;password=PWD ; Set the integratedSecurity property to true to enable the SQL server to use Windows credentials during user authentications. If this setting is set to false, users must provide the username and password. ◆ Connection string to connect `LocalDB` on `DBHOST` at port `1433` with Windows credentials is jdbc:sqlserver://DBHOST\LocalDB:1433;integratedSecurity=true; Copy the `sqljdbc_auth.dll` file to a directory on the Windows system path where the JDBC driver is installed. The `sqljdbc_auth.dll` files are installed in this location: `<installation directory>\sqljdbc_<version>\<language>\auth\` **NOTE:** For a 32-bit Java Virtual Machine (JVM), use `sqljdbc_auth.dll` from the `x86` folder, even if the operating system is x64 version. For a 64-bit JVM on a x64 processor, use `sqljdbc_auth.dll` from `x64`. For a 64-bit JVM on a IA-64 processor, use `sqljdbc_auth.dll` from `IA64`. You can set the `java.libary.path` system property to specify the directory of sqljdbc_auth.dll. For example, if the JDBC driver is installed in the default directory, you can specify the location of DLL by using this virtual machine argument when the Java application starts: Djava.library.path=C:\Microsoft SQL Server 2008 JDBC Driver\sqljdbc_<version>\enu\auth\x86" (This is environment specific)
Library Path	In Windows, set appropriate values for JAVA_OPTS in `catalina.bat` under the `<tomcat>/bin` folder. For more information, see the Tomcat documentation.
Database Username	You can leave this field blank when you mention the username in the connection string.

Field	Description
Database Password	You can leave this field blank if you mention the password in the connection string.

For information about other settings for SQL Server 2008 R2, see Microsoft SQL Server JDBC Driver 3.0.

NOTE: If you want to configure SSPR to connect to any LDAP server other than Active Directory and store the response in an external RDBMS database, navigate to **Modules** > **Forgotten Password** in SSPR Configuration Editor and do the following:

- Set **Response Read Location** to Database
- Set **Response Write Location** to Database

This setting is in addition to the database configuration steps above.

Setting Up Oracle Directory Server

The SSPR package includes the `ODS-schema.ldif` file in the `supplemental` directory. Use this file to extend the SSPR schema.

SSPR uses Oracle Directory Server attributes to store the following users' data:

- The last time when a user changed the password
- The last time when SSPR sent an e-mail notification to the user about password expiry
- Secret questions and answers

Using the ODS-schema.ldif File to Extend the Schema and Assign Rights

Import the ldif file by using the standard LDAP Modify tool.

For example, execute the following command in Oracle Directory Server by using the LDAP Modify tool:

```
ldapmodify -x -h <host ip address> -p 389 -D cn=admin,o=context -password -f ODS-schema.ldif
```

Running this command adds the following SSPR attributes to the Directory schema:

- pwmEventLog
- pwmResponseSet
- pwmLastPwdUpdate
- pwmGUID

Oracle Directory Server Rights

SSPR requires permission to perform operations in Oracle Directory Server and uses the following two rights:

- "Proxy User Rights" on page 26
- "Authenticated User Rights" on page 27

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

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 entry:

- Browse rights to [Entry Rights]
- Read, Compare, and Write rights to pwmResponseSet

After setting up Oracle Directory Server for SSPR, continue with Section 2.4.2, "Configuring Directories," on page 33.

2.4.2 Configuring Directories

You can configure directories either by using the Configuration Guide or manually. This section describes how to configure the directories using the Configuration Guide.

NOTE: To configure directories manually, click **Manual Configuration** on the Welcome page. For more information about configuration, see Section 3.1, "Configuring LDAP Settings," on page 37.

Before proceeding, ensure that you are using Internet Explorer 10 or later version.

To configure the directories using the configuration Guide, Perform the following:

1. Navigate to the Welcome page.
2. Click **Start Configuration Guide**.
3. Select a template from the list based on the back-end directory that you want to configure for your SSPR.
4. Click **Next**.
5. Specify the following details:

Field	Description
LDAP Hostname/Server Address	Specify the address or hostname of the LDAP server
LDAP Port	Specify the port number. For secure connection (HTTPS), use the ldaps://servername:636 format. For plain text servers, use the ldap://serverame:389 format (not recommended).

Field	Description
Secure (SSL Connection)	Select this check box to enable secure connection through HTTPS.
Proxy/Admin LDAP DN	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`
Password	Set a password for the LDAP proxy user.

6 Click **Check Settings** > **Next**.

If there is any error in the setting, you cannot proceed to the next configuration options. SSPR displays the error details to help you troubleshoot the issue.

7 Specify the following details:

Field	Description
Certificate(s) are trusted by default keystore	Select this check box to import and remove certificates manually into the Java keystore.
Use application configuration to manage certificate(s) and import certificates into configuration	Select this check box if you do not want to import the LDAP server's SSL certificate into the Java keystore. The system trusts all LDAP SSL certificate without any verification.

You can verify the LDAP server certificates available on the LDAP host server whether these match with your LDAP server certificates.

8 Click **Next**.

9 Specify the following details:

Field	Description
LDAP Contextless Login Root	Specify the top level LDAP context for your LDAP directory. This is the top level LDAP container under that your users exist. After completing the configuration, you can add multiple values through **Settings** > **LDAP Directory** > **LDAP Contextless Login Root**.

Field	Description
LDAP Test User DN	Specify the LDAP DN of a test user account. You need to 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 health of the LDAP server. Using a test user account increases the ability to detect and alert you about any configuration and health issues. You can test the following functionalities through a test user: ◆ Authentication ◆ Read password policy ◆ Set password ◆ Set challenge-responses ◆ Load challenge-responses This is a recommended setting. You can configure an LDAP Test User DN later also.
Administrator Search Filter	Specify the LDAP query to check whether a user can get the administrator's access to this system. Any user that authenticates and matches this filter can access the system as an administrator.

10 Click **Check Settings** > **Next**.

If there is any error in the setting, you cannot proceed to the next configuration options. SSPR displays the error details to help you troubleshoot the issue.

11 Specify a password to lock the configuration changes you have done.

To make any change in the existing configuring, you must provide the configured password.

12 Click **Next**> **Save Configuration**.

After setting up your environment, continue with Chapter 3, "Configuring Self Service Password Reset," on page 37.

2.5 Upgrading SSPR

Perform the following steps to upgrade the installed SSPR to the latest version:

1 Download the existing server configuration file by using the **Download Configuration File** option in the SSPR portal.

You can access the **Download Configuration File** option in Configuration Manager under **Actions**.

You can also access this file through the following URL:

When SSL is enabled: https://<IP address>:<port number>/sspr/config/ConfigManager#

When SSL is not enabled: http://<IP address>:<port number>/sspr/config/ConfigManager#

2 Stop the Tomcat service by running the following command:

Windows: Locate the Tomcat program folder, then run `bin\shutdown.bat`

Linux: `tomcat\bin\shutdown.sh`

NOTE: On Windows servers, you can start or stop the Tomcat service by right-clicking the Tomcat icon in the System tray and making the selection.

---

3 Copy the `LocalDB` directory in `webapps/sspr/WEB-INF/LocalDB` to a safe location.

You can copy LocalDB manually or by using the `SSPRCommand.bat ExportSSPRDB` command.

NOTE: LocalDB was previously known as SSPRDB in SSPR2.0.

---

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

5 Delete the existing installation from the tomcat Web application folder under `<tomcat>/webapps`. This path may vary on your system. Delete the `sspr` folder and the `sspr.war` file from the `webapps` folder under `tomcat`.

6 Copy `sspr.war` from the SSPR installation media to the `webapps` directory.

7 Go to `\apache-tomcat-7.0.50\work\` and delete the `catalina` folder

8 Restart the Tomcat service by running the following command:

Windows: Locate the Tomcat program folder, then run`tomcat\bin\startup.bat`

Linux: `tomcat\bin\startup.sh`

NOTE: On Windows servers, you can start or stop the Tomcat service by right-clicking the Tomcat icon in the System tray and making the selection.

---

9 Open the SSPR Web portal and configure it by using the Configuration Guide, manually, or by uploading an existing configuration file.

10 Copy `LocalDB` to its original location or import it by using the `SSPRCommand ExportSSPRDB` command.

11 Copy any customization as required.

12 Stop and restart the Tomcat service to apply the changes in steps 10 and 11.

NOTE: The directory extension is not required if you have provided it during the previous installation.

---

3 Configuring Self Service Password Reset

This section discusses about how to configure the default values for SSPR to make it functional and more effective.

Topics include:

- Section 3.1, “Configuring LDAP Settings,” on page 37
- Section 3.2, “Configuring Macros for Messages and Actions,” on page 39
- Section 3.3, “Configuring General Settings,” on page 40
- Section 3.4, “Configuring User Interface Settings,” on page 41
- Section 3.5, “Configuring Password Policy,” on page 44
- Section 3.6, “Configuring Challenge-Response Authentication,” on page 45
- Section 3.7, “Configuring Email Notification Settings,” on page 46
- Section 3.8, “Configuring SMS Notification Settings,” on page 49
- Section 3.9, “Configuring Security Settings,” on page 52
- Section 3.10, “Configuring CAPTCHA,” on page 54
- Section 3.11, “Configuring Intruder Detection,” on page 54
- Section 3.12, “Configuring Token Settings,” on page 58
- Section 3.13, “Configuring Logging and Auditing,” on page 59
- Section 3.14, “Configuring NetIQ eDirectory Settings,” on page 61
- Section 3.15, “Configuring Database,” on page 62
- Section 3.16, “Configuring Reporting,” on page 64
- Section 3.17, “Configuring Extensions,” on page 65
- Section 3.18, “Configuring OAuth SSO,” on page 67

3.1 Configuring LDAP Settings

SSPR allows you to configure settings to control interactions of SSPR with the back-end LDAP directory. You can select a template to configure the settings. SSPR provides templates to set default settings for your back-end directories. Changing the template will only affect values that are at their default. You can change the template at any time. Changing a template does not affect the modified settings.

SSPR provides the following templates:

- NetIQ eDirectory
- Active Directory
- Oracle Directory Server
- OpenLDAP, DirectoryServer 389, Others

Before configuring LDAP directory settings, you must import the corresponding LDAP server certificates.

3.1.1 Importing LDAP Server Certificates

In Configuration Manager, click **Actions** > **Import LDAP Server Certificates** to import LDAP server certificates.

3.1.2 Configuring Global Settings for LDAP Directory

The Global settings control the interaction with an LDAP directory. These settings are not applicable for the user's LDAP profile. To configure settings for the LDAP profile, see **Profiles** > **LDAP Directory Profiles**.

To configure LDAP settings, perform the following steps:

1. In Configuration Manager, click **Templates** and select a template.

   NOTE: If you select NetIQ eDirectory, you can configure NMAS settings. See, Section 3.14, "Configuring NetIQ eDirectory Settings," on page 61.

   If you have selected Active Directory - Store responses in a database, you must configure the database also. See Section 3.15, "Configuring Database," on page 62.

2. Click **Settings** > **LDAP Settings**.
3. Click **View** > **Always Show Advanced Settings**.
4. Configure the following settings:

Field	Description
LDAP Naming Attribute	Specify an attribute name that SSPR 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 a different attribute is used for the login search filter. Typically, the naming attribute is cn or uid.
LDAP Idle Timeout	Specify the time how long an LDAP session can remain inactive before the session times out and the user must authenticate again. If you specify zero, the LDAP connection does not time out in the http session unless you close it.
Administrator Query String	Specify the LDAP query string to check whether a user can get the administrator rights. During the user login process, the system runs this query and determines if this user is an administrator.
Last Password Update Attribute	Specify an attribute to record when a password is updated and when the password is used during replication checks and other processes.
User Object Class (Advanced)	Specify object classes of user entries in your LDAP directory.
Follow LDAP Referrals (Advanced)	Select this check box if you want SSPR to follow the referral LDAPs.

Field	Description
LDAP Duplicate Mode (Advanced)	Select the appropriate mode that provides 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 one 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 is discovered 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 is discovered in any context or profile. This option ignores any duplicate user in the search result.
User Selectable LDAP Context/ Profile (Advanced)	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 (Advanced)	Select this option if you want to ignore the profiles that are unreachable. This option is used when there are multiple LDAP profiles. A directory unavailable error message is displayed for the user when there is only a single configured LDAP Profile or all LDAP Profiles are unreachable.

5 Click **Actions** > **Save**.

3.2 Configuring Macros for Messages and Actions

SSPR allows you to configure macros to generate messages in a particular format and perform required actions. If you require a particular message to be displayed in an email or when a user performs a particular action, then you can add the required macro where the information is a variable value. If you require any particular action to be automated for a specific user action, then configure macros for that particular action. Following is an example that displays the usage of macros:

Dear, @LDAP:givenName@, Thank you for your activity today, @CurrentTime:EEE, MMM d, yyyy@. When the macros are activated the following message is displayed in the body of the email that is sent to specific user:

```
Dear, John, Thank you for your activity today, Wed, Jul 4, 2001.
```

The list of macros that can be used to define the configuration value are as following:

Macros	Result
@LDAP:<*name*>@	LDAP value of <name>
@LDAP:DN@	LDAP value of user's Distinguished Name

Macros	Result
@User:PwExpireTime@	Time when the user's password will expire and the time is represented in default format, which is PWM format.
@User:PwExpireTime:<*pattern*>@	Time when the user's password will expire and the time is represented in <*pattern*> format
@User:DaysUntilPwExpire@	Number of days that are remaining for the user's password expiry
@User:ID@	User ID of the authenticated user
@User:Email@	Email address of the authenticated user
@User:Password@	Current password of the authenticated user
@InstanceID@	Instance ID of the application that is used
@CurrentTime@	Current time in a default format
@CurrentTime:<*pattern*>@	Current time in <*pattern*> format.
@SiteURL@	URL of the site that is used. For example, `http://www.example.com/pwm`
@SiteHost@	Hostname of the site that is used. For example, `www.example.com`

3.3 Configuring General Settings

SSPR allows you to configure basic settings to control functionality and behavior of the system.

1. In Configuration Editor, click **Settings** > **Application**.
2. Configure the following general settings:

Field	Description
Site URL	Specify the URL to access SSPR. This URL is used in email 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 attempt to auto-detect the URL, however some network configuration prevent SSPR from accurately determining the URL.
Forward URL	After completing any activity, which does not require 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.

Field	Description
Logout URL	Specify a URL to which SSPR redirects users 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 SSPR session will have already been invalidated. You can override this URL for any user session by adding a `logoutURL` parameter to any HTTP request during the session.
Idle Timeout Seconds	Specify the duration of an authenticated session in seconds after which the session times out.
Instance Name (Advanced)	Specify the name of this application instance. If you leave this blank, the system uses a persistent and randomly generated value. Recommended value is blank.
Hide Configuration Health Warnings (Advanced)	Select this if you want to hide health warnings about configuration issues from the Health section of the Configuration Manager page.
Known Locales (advanced)	It 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 ISO code is used for the flag value.
LocalDB Location (Advanced)	Specify the location of the LocalDB directory. If you specify a relative path, it is considered relative to the servlet's WEB-INF directory.

3 Click **Actions** > **Save**.

3.4 Configuring User Interface Settings

SSPR includes a flexible theming mechanism that allows for maximum customization of look and branding of the SSPR application. You can customize SSPR by modifying CSS files. SSPR uses `style.css`, the default CSS file for standard browser displays, and `mobileStyle.css` for mobile devices. These files are included in the `SSPR/public/resources/` directory. It is recommended to not modify these files.

SSPR also includes another set of CSS files from a theme directory. By default, the location of this is `SSPR/public/resources/themes/default`. Because of their position in the page loading sequence, settings in these files override the settings in the default CSS files. This is the place to make your customization.

You can control SSPR themes through the **Interface Theme** setting (**Settings** > **User Interface** > **Interface Theme**). This setting controls the themes under `SSPR /public/resources/themes/`. SSPR includes different sample themes also.

The following are two important setting options:

- **Embedded**: When you select this option, the theme CSS files are stored as part of the SSPR configuration, not as part of the file system. There are two settings where the CSS file contents can be placed: **Settings** > **User Interface** > **Embedded CSS Stylesheet** and **Embedded Mobile CSS Stylesheet**. This allows an administrator to include customized CSS styles without modifying the file system.
- **Custom**: When you select this option, you can set a custom location storing CSS theme files. There are two settings where the CSS file contents can be placed: **Settings** > **User Interface** > **Custom CSS Stylesheet Location** and **Custom Mobile CSS Stylesheet Location**. These settings control the actual URLs of the custom theme. They can be relative URLs for files on the SSPR server or they can be absolute URLs to reference CSS files on any other accessible Web server.

SSPR can allow 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 SSPR Forgotten Password module such as:

```
/sspr/public/ForgottenPassword?theme=myCustomTheme
```

SSPR will use theme files from the `/public/resources/themes/myCustomTheme` directory for the current user's session. You can place any number of directories under `/public/resources/themes` and make them available to work in this way.

Along with themes, SSPR allows you to do the following configurations:

- Change the look and feel of the SSPR user interface.

  SSPR comes with a couple of 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 and determine the language of it.

To configure user interface settings

1. In Configuration Editor, click **Settings** > **User Interface**.
2. Click **View** > **Always Show Advanced Settings** to see and configure the advanced settings.
3. Configure the following settings:

Field	Description
Interface Theme	Select a theme from the list the SSPR interfaces 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.
Show Auto Generate Randoms	Select this check box if you want to display the auto-generate random password link on the change password screen.
Show Strength Meter	Select this check box if you want to display the password strength meter on the change password screen. Using this option, users can check the strength of the new password.

Field	Description
Show Show/Hide Password Button	Select this check box to allow the user to toggle between the **Show/ Hide Password** buttons wherever available.
Show Cancel Button	Select this check box to display the **Cancel** button to user 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 Reset Button	Select this check box to display the **Reset** button wherever appropriate.
Show Success Pages	Select this check box to enable SSPR to display a success messages when an activity completes successfully.
Show Password Event History	Select this to check box display the **Show Password History** menu in **Main Menu**.
Show User Account Information	Select this check box to display the **Show User Account Information** menu in **Main Menu**.
Show Login Page Options	Select this check to display the **Forgotten Password** and other options on the Login page.
Show Logout Button	Select this check box to display the **Log Out** button to an authenticated user.
Show Home Button	Select this check box to display the **Home** button to an authenticated user.
Show Idle Timeout Counter	Select this check box to display the user's remaining idle time. When that time reaches zero, the system redirects the user to the logout page.
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, system appends it to the context path.
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, 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.

Field	Description
Embedded JavaScript	Provide a java script to include a particular content in all pages inside an html tag near the bottom of the page.

4 Click **Actions** > **Save**.

3.5 Configuring Password Policy

SSPR lets you configure policies to increase security by setting rules for how users create their passwords. You can apply an SSPR password policy to all users in the following two ways:

- Apply only the SSPR policy
- Apply only the LDAP policy
- Merge the SSPR policy with the LDAP policy

When you merge the SSPR policy with the LDAP policy, SSPR reads both policies. If both policies conflict with each other, SSPR chooses the most restrictive policy.

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

SSPR allows storing the shared password history for all users, which provides more security. You can also configure profile specific password policy. For more information on profile specific password policy, refer Section 5.2, “Configuring Password Policy for a Profile,” on page 88

To configure a password policy, perform the following steps:

1 In Configuration Editor, click **Settings** > **Password Settings**.
2 Click **View** > **Always Show Advanced Settings** to see and configure the advanced settings.
3 Configure the following settings:

Field	Description
Password Policy Source	Select any one of the following: **LDAP:** SSPR reads the LDAP password policies. If you select this option, SSPR ignores some of the SSPR password policy settings. **Local:** SSPR reads the SSPR policies. If you select this option, SSPR ignores any policy settings of the LDAP directory **Merge Local and LDAP:** SSPR reads both policies. If any conflict between these policies, SSPR chooses the most restrictive value of the policy.
Wordlist File	Specify a Worldlist to prevent users from using commonly used words as passwords. This is an important part of the password security. The default Wordlist contains commonly used English words that an intruder may use to break the password. A new Wordlist setting takes some time to compile the Wordlist into a database. The Wordlist file format is one or more text files containing a single word per line, enclosed in a ZIP file.

Field	Description
Enable Shared History	Select this check box 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.
Wordlist Case Sensitivity	Select this check box if you want to use the Wordlist as case-sensitive for all matches. Changing this value causes wordlist re-compilation.
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)
Shared History Age	Specify the maximum age of the shared history storage in seconds. Default value is four weeks (2419200 seconds)
Wordlist Word Size Check	Specify the number of characters in a word that is checked against the configured Wordlist. For example, if the word to be checked is Wordlist 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 considered to match the Wordlist. If this value is set to zero or the word to check is smaller than the value specified here, then only the entire Wordlist checked.

4 Click **Actions** > **Save**.

3.6 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 a user forgets their password and tries to reset it, SSPR prompts the configured questions and asks user to specify the correct answer. When the answer matches with the response saved earlier by the user, SSPR will allow the user to reset the password. To configure the challenge-response policy for different profiles, refer Section 5.3, “Configuring Challenge Response Policy for a Profile,” on page 91

You must select **Enable Setup Responses** check box to enable SSPR to display the save responses page to users.

3.6.1 Configuring global Challenge-Response Settings

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, Wordlist, and so forth.

To configure the challenge settings, perform the following steps:

1 In Configuration Editor, click **Settings** > **Challenge Settings**.

2 Click **View** > **Always Show Advanced Settings** to see and configure the advanced settings.

The following table lists all configurable settings with their descriptions:

Field	Description
Enable Setup Responses	Select this check box to display the save responses page to users.
Force Response Setup	Select this check box to redirect users to configure challenge-response when they log in. This setting s users to save responses if they do not have stored responses yet.
Show Response Confirmation	Select this check box to show the responses to the user after they configure responses. This gives users an opportunity to read and review their responses before submitting.
Apply Wordlist	Select this check box to configure a Wordlist. The Wordlist prevents commonly used words to be used in responses. Users cannot use response values that are added in the Wordlist.
Case Insensitive Responses	Select this check box to make the responses case-insensitive. The setting will not affect or apply to users who have already configured their response prior to modifying this setting.
Maximum Characters of Challenge Allowed in Response	Specify the maximum number of a character to be allowed in the response. This prevents a user's response to be the same as the challenge.
Allow Duplicate Responses	Do not select this check box if you want users to enter unique value for each response.
Save Challenge Query Match (Advanced)	Specify the query string to detect whether a user can configure challenge-responses. If users do not match this query, then the user responses are not checked, and users are redirected to the forward URL. To view the list of users that match the query, click **View Matches**.
Check Responses Query Match	Specify the LDAP response query. If the command servlet is called with the checkResponses command (`/private/CommandServlet?processAction=checkResponses`), the users are first checked to see if they match the specified LDAP query before the user's password responses is checked. If users do not match this query, then the users responses are not checked, and users are redirected to the forward URL. To view the list of users that match the query, click **View Matches**.
Minimum Password Lifetime (Advanced)	When you select this check box, the user cannot change password until the minimum lifetime has completed.

3.7 Configuring Email Notification Settings

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

SSPR supports both plain text and HTML formats. For each configured setting and locale, you should configure both plain text and HTML email bodies. SSPR 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 Section 3.2, “Configuring Macros for Messages and Actions,” on page 39 or select **View** > **Macro Help** in the Configuration Editor page.

To configure email settings, perform the following steps:

1. In Configuration Editor, click **Settings** > **Email**.
2. Click **View** > **Always Show Advanced Settings** to see and configure the advanced settings.
3. Configure the following settings:

Field	Description
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.
Change Password Email	Users get email notifications after changing their passwords. Configure the email format and other details that a user receives after changing the password. For example, sender's address, subject, and format and text of the email body.
Helpdesk Change Password Email	Users get email notifications when helpdesk changes their passwords. Configure the email format and other details that a user receives when helpdesk changes the user's password. For example, sender's address, subject, and format and text of the email body.
Update Profile Email	Users get email notifications when they update their profiles. Configure the email format and other details that a user receives when they update their profiles. For example, sender's address, subject, and format and text of the email body.
New User Email	A new user gets a welcome email. Configure the email format and other details such a sender's address, subject, and format and text of the email body.
New User Verification Email	A new user gets a verification email with a link to verify the registration. Configure the email format and other details such a sender's address, subject, and format and text of the email body. Use `%TOKEN%` to insert the token value into the email.
Activation Email	A new user gets an email after the account activates. Configure the email format and other details such a sender's address, subject, and format and text of the email body.
Activation Verification Email	A new user gets an email during the account activation verification process. Configure the email format and other details such a sender's address, subject, text of the email body including the verification link. Use `%TOKEN%` to insert the token value into the email.
Forgotten Password Verification Email	When users request for the password reset, they get a verification email. Users need to click the link available in the email to authenticate the request. Configure the email format and other details such as sender's address, subject, text of the email body including the verification link. Use `%TOKEN%` to insert the token value into the email.
Intruder Notice Email	When a user or any intruder attempts to reset the password with incorrect responses that locks the user account, the user gets an email to notify that the account is disabled due to lockout. Configure the email format and other details such a sender's address, subject, and text of the email body.

Field	Description
SMTP Email Server Username (Advanced)	Specify the username 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.
SMTP Email Server Password (Advanced)	Set a password for the SMTP email server user. If you do not provide any value, the SMTP messages can be sent without authenticating the server user. Click **Store Password** and then specify an SMTP password or provide a random password on the Store Password page.
User Email Attribute (Advanced)	Specify the user LDAP attribute containing user's email address.
Maximum Email Queue Age (Advanced)	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 output error or network error to the SMTP server occurs while sending the email.
Send Password Email (Advanced)	An email is sent to the user with the new password during forgotten password reset process. This setting is valid if send password functionality is enabled. Configure the email format and other details such a sender’s address, subject, and text of the email body.
Send Username Email (Advanced)	An email is sent to the user with the new username during forgotten password reset process. Configure the email format and other details such a sender’s address, subject, and text of the email body.
SMTP Email Advanced Settings	Specify the name/value settings to control the behavior of the mail agent. Available settings are defined as part of the JavaMail API. The settings must be in "name=value" format, where name is the key value of a valid JavaMail API setting.

4 Click **Actions** > **Save**.

3.8 Configuring SMS Notification Settings

SSPR sends SMS notifications for the following actions:

- Password recovery
- New user account verification

You can configure settings of SMS messages. You should configure SMS text for each configured setting and locale. Messages will be delivered using the configured short message service gateway. For enabling SSPR to send SMS notifications, you need to have access to an HTTP or HTTPS based SMS gateway service.

To configure SMS notification, perform the following steps:

1 In Configuration Editor, click **Settings** > **SMS**.

2 Click **View** > **Always Show Advanced Settings** to see and configure the advanced settings.

3 Configure the following settings:

Field	Description
User SMS Number Attribute	Specify the user LDAP attribute containing the user's mobile phone number for SMS.
SMS Gateway	Specify the URL of the SMS service provider.
SMS Gateway User	Specify the user name of the SMS gateway.
SMS Gateway Password	Click **Set Password** to configure a password for the SMS gateway.
HTTP(S) Method	Specify the HTTP or HTTPS protocol method that you want to use for sending SMS messages.
SMS Gateway Authentication Method	Select a method from the list that the SMS gateway will use 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. For more information, see Apache Commons JavaDocs.
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 for the SMS text. Some services allow texts longer than one message (generally 140 bytes). If the text is longer than the configured maximum, multiple requests will be made.

Field	Description
Response Regular Expressions	Specify the regular expression. Using the regular expressions, you can determine whether the SMS has been sent successfully. ◆ Response matches any of the expressions: Transmission is successful ◆ No expressions are entered: All transmissions are successful. **NOTE:** The string must match an entire line. Use `.*` to match anything after the required texts.
SMS Sender ID	Specify the sender's identification. 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 SSPR will use 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**.
Challenge Token SMS Text	Customize the text that SSPR sends through SMS during forgotten password token process.
Challenge New Password SMS Text	Customize the text that SSPR sends through SMS with new password during the forgotten password process.
new User Verification SMS Text	Customize the text that SSPR sends through SMS during new user verification process.
Activation Token SMS Text	Customize the text of the token SMS that SSPR sends during the activation process.
Activation SMS Text	Customize the text of SMS that SSPR sends after a successful activation.
Maximum SMS Queue Age	Specify the maximum age, in seconds, an SMS can wait in the send queue. If an SMS is in the send queue longer than this time, system discards it. SMS messages persist in the send queue if there is an I/O or network error in the SMS gateway server while sending the message.
Use URL Shortner	Select this check box 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.

4 Click **Actions** > **Save**.

3.9 Configuring Security Settings

This section discusses various security settings available in SSPR.

To configure security settings, perform the following steps:

1. In Configuration Editor, click **Settings** > **Security**.
2. Click **View** > **Always Show Advanced Settings** to see and configure the advanced settings.
3. Configure the settings:

Field	Description
Security Key	A security key is used 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. Click **Set Password** to configure this. 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 Session Verification	Select this check box to allow sessions verification by using a session verification key and a redirect. This verification proves the following: ◆ The browser can correctly establish a session with the server. ◆ The browser either supports cookies or URL sessions (if enabled) ◆ The communication channel between browser and application server is sticky when there are multiple server instances It helps prevent some types of XSS attacks.
Require HTTPS	Select this check box to HTTPS (instead of cleartext HTTP) traffic to the application server. Non-secure connections are useful during testing. Production servers should always have this setting enabled.
Show Detailed Error Message	Select this check box to show detailed error messages. This setting is useful for administrators especially during configuration.
SSO Authentication Header Name	Select this check box to allow auto login providing only username, a password is not required. This setting controls the name of the HTTP header. For certain functionalities, user is prompted to enter the password.

Field	Description
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 webpage with the URL fragment that is defined in the whitelist. The URL forwarding will follow the following criteria: ◆ The forwarding URL from a webpage 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.
Enable Back Button Detection (Advanced)	Select this check box to detect the use of back button or other browser navigation irregularities. This option prevents duplicate HTTP form submissions.
Enable Form Nonce	Select this check box to ask for a form nonce for each form in SSPR to prevent certain types of cross-site scripting (XSS) attacks.
Disallowed HTTP Inputs	Specify the input value. If any input value (on any http parameter) matches these patterns, the matching portion will be stripped from the input.
Force Basic Authentication	Select this check box 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.
Enable Reverse DNS	Select this check box to use the system's reverse DNS system for recording the hostname of the client. In some cases, this can cause performance issues. Disabled it if it is not required.
Allow Roaming Source Network Address (Advanced)	Select this check box to allow a single HTTP session to be accessed from different source IP addresses. Some load balancing/proxy network infrastructures require this setting, but in most cases this option must be deselected.
Required HTTP Headers (Advanced)	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 (Advanced)	Specify the IP address ranges that permits only the connections that originated from those addresses. If no value is specified, any source address is permitted.
Maximum Session Duration (Advanced)	Specify the maximum duration of a session (in seconds).

Field	Description
Prevent HTML Framing (Advanced)	De-select this option to allow users to view SSPR in an inline frame for any application that includes the iframe html source code. If you select this option, SSPR is not included in the specified iFrame for the application.

4 Click **Actions** > **Save**.

3.10 Configuring CAPTCHA

SSPR has integrated support for the CAPTCHA protection. CAPTCHA prevents from automated attack. SSPR uses the online re CAPTCHA service for CAPTCHA generation and validation. You need to configure a reCAPTCHA account to use this service. Registration at the reCAPTCHA site provides a public and private key that you must configure in SSPR for the reCAPTCHA support.

To configure the CAPTCHA settings, perform the following steps:

1 In Configuration Editor, click **Settings** > **CAPTCHA**.

2 Click **View** > **Always Show Advanced Settings** to see and configure the advanced settings.

3 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: Click **Set Password** to create the private reCAPTCHA key. You can specify the key ly or generate a random one. Leave this field blank if you do not want to perform CAPTCHA verification.

Captcha Skip Parameter Value: Specify the parameters and include the `skipCaptcha` key for which you want to skip the CAPTCHA request. This setting is useful for internal clients and links where CAPTCHA is not required.

For example, if the parameter is `okay`, SSPR skips the CAPTCHA check for this request: /public/ForgottenPassword?skipCaptcha=okay.

Captcha Skip Cookie: Specify the browser cookies. for which you want SSPR to skip the CAPTCH request.

4 Click **Actions** > **Save**.

3.11 Configuring Intruder Detection

You can configure SSPR to prevent from intruder attacks. You can specify the number of consecutive login attempts a user can make. When a user attempts more than a specified number, SSPR locks that user’s account for a specified period. Users can re-attempt login after this period only. A user cannot recover the password by answering the challenge-response in this scenario. If users want to

unlock the account immediately, they need to call to helpdesk and provide the helpdesk challenge response. If the user's answers match the configured responses, the helpdesk user resets the account on behalf of the user.

To configure the intruder lockout settings, perform the following steps:

1. In Configuration Editor, click **Settings** > **Security**.
2. Click **View** > **Intruder Detection** to see and configure the advanced settings.
3. Configure the following settings:

Field	Description
Intruder Record Storage Location	Store the data for intruder records. This data can be saved either in the LDAP database or in the LocalDB. Select any one of the following from the list to store data for intruder records: **Auto Configure:** If the database is configured, this option lets you store data in the database otherwise, data is stored in LocalDB. **Database:** Lets you store the data in the database. If database is used, a common view for intruder status is shared on all application instances **LocalDB:** Stores data in the LocalDB. If LocalDB is used, an intruder status is determined with each instance of the application.
Intruder User Reset Time	Specify the time in seconds after that 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. Specify zero if you want to disable this functionality.
Intruder User Maximum Attempts	Specify the maximum number of attempts a user can make during the login process. When this value is exceeded, the user cannot perform any activities until the reset time interval has passed or helpdesk user has reset the password. Specify zero if you want to disable the user lockout functionality.
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.
Intruder Attribute Reset Time	Specify the time period, in seconds, after which a bad attempt will be cleared from the lockout table. Specify zero to disable the attribute lockout functionality.
Intruder Attribute Maximum Attempts	Specify the maximum number of attempts a user can make. This setting is used to limit the number of times a user can provide incorrect attribute value. When this value is exceeded, the user cannot perform any activities until the reset time interval has passed. Specify zero if you want to disable this functionality.
Intruder Attribute Check Time	Specify the maximum time period between each attempt a user can make for the attributes. When this time period is exceeded, the intruder attempt count is reset to zero.

Field	Description
Intruder Token Destination Reset Time	Specify the time period (in seconds) after which a bad attempt will be 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. Specify zero 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. Specify zero 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.
Intruder Address Reset Time	Specify the time in seconds after which SSPR removes an intruder attempt from the lockout table. Specify zero if you want to disable this functionality. The address lockout table contains logs for the source IP address of users 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 do any activities until the reset time interval has passed. Specify zero if you want to disable this 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. Specify zero if you want to disable this functionality.
Maximum Intruder Attempts Per Session	Specify the maximum amount of invalid password reset attemps 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. Specify zero to disable this functionality.
Enable Bad Password Simulation	Select this check box to enable bad password simulation process. This setting is used when user selects to use a forgotten password field.

4 Click **Actions** > **Save**.

3.12 Configuring Token Settings

SSPR sends tokens through email and SMS for secure user authorization. You can configure SSPR 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, SSPR 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 needs to enter this token into the Password Change form. When the token matches with the token sent by SSPR, the user's password is changed.

SSPR also sends tokens for new user registration confirmation.

You can configure the storage method used to save tokens. SSPR supports the following methods:

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

DB: Use this method to store tokens in a configured, remote 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 Section 3.9, “Configuring Security Settings,” on page 52.

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.

To configure token settings, perform the following steps:

1. In Configuration Editor, click **Settings** > **Tokens**.
2. Configure the following settings:

Field	Description
Token Storage Method	Select a method to store tokens.
Token Characters	Specify the characters you want to include in the 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. When using the LDAP token storage method, this attribute is used to store and search for tokens.

3. Click **Actions** > **Save**.

3.13 Configuring Logging and Auditing

SSPR uses Apache Log4j. Apache log4j is a Java-based logging utility. Log4j allows logging to a variety of outputs such as files, syslog, nt event log, databases, and so forth.

The following list includes available log levels in order of severity:

TRACE: Most detailed information. This level is recommended during initial configuration.

DEBUG: Detailed information on the flow through the system.

INFO: Informational messages that highlight the progress of the application at coarse-grained level. This level is recommended for normal operations. This is the default log level for StdOut. When used with tomcat, this logs to tomcat's `logs/catalina.out` file.

ERROR: Runtime errors or unexpected conditions.

WARN: Potentially harmful situations.

FATAL: Severe errors that cause premature termination.

You can configure SSPR to register a log4j xml configuration file.

SSPR also 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. In Configuration Editor, click **Settings** > **Logging & Auditing**.
2. Click **View** > **Always Show Advanced Settings** to see and configure the advanced settings.
3. Configure the following settings:

Field	Description
LocalDB Log Level	Select the log level to log events in LocalDB.
File Log Level	Select the log level to log events in local file log. Log files are written to the servlet's `WEB-INF/logs` directory.
Daily Summary Alerts	Select this check box to enable sending an email once a day (at 0:00 GMT) with summary of statistics and health for that day.
System Audit Event Email Alerts	Specify the email address on which 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.

Field	Description
Syslog Audit Servers	SSPR can send events to the Syslog service. Specify Syslog audit servers in the format `Protocol,Host,Port number`. Where, Protocol: TCP, UDP or TLS/ SSL Host: Host name or IP address of the machine running the Syslog service Port: Port number to which the Syslog service is listening to **NOTE:** To configure TLS/ SSL, you require to import the certificates from the JAVA keystore. For more information about importing the certificates, refer Section 3.13.1, "Setting Up SSL Auditing," on page 61
Health Check Frequency (Advanced)	Specify the time interval in seconds to perform a self-health check. Default value is two minute.
Java StdOut Log Level (Advanced)	Select a log level for StdOut. Default log level for StdOut is INFO.
Log4j Configuration File (Advanced)	Specify the location and name of a log4j xml configuration file. This file is used to configure the log4j system. If unspecified, a basic log4j configuration is used for logging only to StdOut. The location specified in this setting is relative to the **WEB-INF** directory. An example `log4jconfig.xml` file is included in the **WEB-INF** directory.
Maximum LocalDB Events	Specify the number of maximum log events that can be stored in LocalDB. LocalDB retains these events and display these in the Admin Event log screen. This setting does not affect the normal log files configured in `log4jconfig.xml` or tomcat's log file settings. 100,000 log events require approximately100 MB disk space to be stored.
Maximum Age LocalDB Events	Specify the maximum age of events stored in LocalDB in seconds. Default value is 2419200 seconds (four weeks). A value of zero disables this feature. This setting does not affect log files configured in `log4jconfig.xml` or tomcat's log file settings. SSPR periodically purges the events older than the configured value.
User History Storage Location (Advanced)	Select the data store location that is used for user-specific audit history.
User History Attribute (Advanced)	Specify the attribute to write a user event attribute in LDAP. The user event log attribute contains an XML document with the user's event history. Leave this field blank if you want to disable logging the event history to LDAP.
User History Maximum Events (Advanced)	Specify the maximum number of events to retain in the event history attribute for a user.
Enable LDAP Wire Trace (Advanced)	Select this check box to log all LDAP events to the TRACE logging level. **WARNING:** Enabling this option may allow user passwords and other sensitive data to be written to the log files.
Local Alerts Storage Max	Specify the maximum age in seconds of the local audit event log. The default value is 30 days.

4 Click **Actions** > **Save.**

3.13.1 Setting Up SSL Auditing

SSPR requires SSL certificate to audit the events. To send the audit events you require Syslog certificate that is imported to the JAVA TrustStore. Perform the following to import the certificate and audit the events:

1 Run the following command to view the certificate:

```
openssl s_client -host {ip} -port {port} -showcerts
```

Where, *ip* is the IP address of the machine that is running the syslog service and *port* is the listening port number for the syslog server.

2 Copy the certificate to any text file and save it with an extension `.pem`. For example, `<anyname>.pem`

3 Import the certificate to the JAVA keystore of SSPR by using the keytool.

4 Launch Configuration Editor and then click **Settings** > **Logging and Auditing**.

5 In the **Syslog Audit Servers** field, specify the value as `tls,<ipaddress>,1443`

Where, 1443 is the default port number.

3.14 Configuring NetIQ eDirectory Settings

When the back-end directory is NetIQ eDirectory, you can configure Modular Authentication Services (NMAS).

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

All NMAS operations require an SSL connection to the directory.

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

Perform the following steps:

1 In Configuration Manager, select **Template** > **NetIQ eDirectory**.

2 Click **Settings** > **NetIQ eDirectory**.

3 Click **View** > **Always Show Advanced Settings** to see and configure the advanced settings.

4 Configure the following settings:

Field	Description
Enable NMAS Extension	Select this check box 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 check box 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 check box to use NMAS stored responses during forgotten password recovery. SSPR tries all other configured storage methods before evaluating.
Read Challenge Sets	Select this check box if you want SSPR to read the challenge set configuration from the eDirectory universal password policy and apply it to users. If you want SSPR to use challenge sets configured in NAMAS only, do not configure the required and forgotten questions in SSPR, else SSPR will use these if no eDirectory policy exists.
Read User Passwords	Select this check box if you want SSPR 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 SSPR generates a temporary random password for the user.

5 Click **Actions** > **Save**.

3.15 Configuring Database

SSPR uses two types of databases:

- **LocalDB:** LocalDB is a local embedded database. SSPR uses it for storing local data. LocalDB requires no administration or maintenance, and the default values are sufficient.
- **RDBMS:** SSPR can use a traditional RDBMS database to store data for certain functions. Any standard RDBMS that supports a standard Java JDBC driver can work. SSPR connects to the database and create necessary tables. You can configure multiple SSPR server instances to the same database instance. SSPR officially supports MS SQL database.

Configure the following settings if you select RDBMS:

- **Database Class:** Name of the database class. Specify the Java JDBC full driver class name.

  The classpath must include the corresponding JDBC driver JAR or ZIP file, typically, in the `WEB-INF/lib` directory or the application server's lib directory. For example, in Tomcat, it is `<TOMCAT_HOME>/webapps/<SSPR>/WEB-INF/lib` or `<TOMCAT_HOME>/lib`. The default folder name under which the application is deployed is `<SSPR>`. If you have changed this name, use the appropriate path name accordingly.

- **Database Connection String:** Specify the database connection string in the standard JDBC format.
- **Database Username:** Specify the user name that can connect to the database.
- **Database password:** Specify a password for the database user.

NOTE: The RDBMS settings are applicable only if you have selected Active Directory - Store Responses in a Database.

This section discusses:

- Section 3.15.1, “Configuring Database Server,” on page 63
- Section 3.15.2, “Configuring Database Settings,” on page 63

3.15.1 Configuring Database Server

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 need to specify this administrator during SSPR configuration.
3. Create a user and associate it to the database you created in Step 1.
4. Ensure that the user has enabled the SQL server authentication mode and has suitable rights to open the database:
   - **4a** Go to the SQL Server **Object Explorer**.
   - **4b** Expand the server and instance and select **Security**.
   - **4c** Under **Security**, select **Logins**.
   - **4d** Under **Logins**, create a new user. While creating the user, select the authentication as `sqlserver authentication` instead of the default Windows authentication.
   - **4e** Select LocalDB as the default database for the user. Assign the user required administrator’s roles.

     After creating the user, map it to LocalDB.

3.15.2 Configuring Database Settings

If you want to store responses in the database, configure some specific settings. This section discusses about how to configure the database for your LDAP directory.

Perform the following steps:

1. Select a template in Configuration Manager under **Template**.
2. Click **Settings** > **Database**.
3. Configure the following settings:

Field	Description
Database Class	Specify the Java JDBC full driver class name. The corresponding JDBC driver JAR or ZIP file must be included in the classpath, typically in the `WEB-INF/lib` directory or the application server's `lib` directory.

Field	Description
Database Connection String	Specify the database connection string in the standard JDBC format.
Database Username	Specify a username.
Database Password	Set a password for the database user.
Database Key Column Type	Specify the database column type for key columns. The column type is used only during schema creation. All tables contain two columns, a key, and a value column. For most databases, the standard VARCHAR column format is appropriate for the key column. Generally, the data stored in the key column is US-ASCII key. For the Oracle database, set this to VARCHAR2.
Database Value Column Type	Specify the database column type for value columns. The column type is used only during schema creation. All tables contain two columns, a key, and a value column. For most databases, the standard TEXT column format is appropriate for the value column. Generally, the data stored in the value column is be UTF-8 formatted XML, JSON, or other text-based value data. For the Oracle database, set this to CLOB.
Database Trace Logging	Select this check box to log the data and the read/ write activity to the TRACE debug output. This option can send security-sensitive information to the debug output, including passwords.

4 Click **Actions** > **Save**.

3.16 Configuring Reporting

You can view the directory report that includes summary, detailed report on password change status, and other password self services field. The reports are maintained in the local cache till the time that is specified during the configuration. This section discusses various settings that enable SSPR to configure reporting.

To configure reporting, perform the following steps:

1 In Configuration Editor, click **Settings** > **Reporting**.

2 Click **View** > **Always Show Advanced Settings** to see and configure the advanced settings.

3 Configure the following settings:

Field	Description
Enable Directory Reporting	Select this check box to enable directory reporting. You, as an administrator, can maintain a local cache to store user data. To use this option you require additional disk space and Java heap memory.
Reporting Search Filter	Specify the LDAP search filter to generate the required report. If no value is provided, a filter based on the login query setting is automatically generated.

Field	Description
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 till 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 (Advanced)	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 (Advanced)	Specify the number of seconds to process records after midnight (GMT). Setting value to -1 will disable the nightly job processor.

3.17 Configuring Extensions

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

To configure integration of external authentication, perform the following steps:

1. In Configuration Editor, click **Settings** > **Integration/Developer**.
2. Click **View** > **Always Show Advanced Settings** to see and configure the advanced settings.
3. Configure the following settings:

Field	Description
External Judge Method	Specify the Java classes that SSPR calls to determine the strength of a given password. External judge methods must implement the interface password.pwm.ExternalJudgeMethod. During password checks, all listed classes are invoked. If multiple results are returned, the lowest returned value is used.
HTTP Proxy	Specify the URL of the HTTP proxy server. If the value is not provided then proxy server is not used. For an http proxy server, use the http://serverame:3128 format. For an authenticated proxy server, use the http://username:password@servername:3128 format.

Field	Description
Enable External Web Services	Select this check box 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 Read Answers	Select this check box 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 check box 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.
Web Services Third Party Query String	Specify the users that are permitted to execute REST web services and can specify a third party by using the 'username' parameter.
External Web Auth Methods	Specify the external Web authentication methods.
Enable URL Shortening Service Class (Advanced)	Specify the Java class name that implements a short URL service. You must include the corresponding JAR or ZIP file in the classpath, typically in the `WEB-INF/lib` directory or the application server's lib directory.
Regular Expression for Matching URLs (Advanced)	Specify a regular expression to match URLs that are shortened by the URL shortening service class.
Configuration Parameters for URL Shortening Service (Advanced)	Specify the Name/Value settings that are used in configuring the selected URL shortening service such as, API key, username, password and domain name. This setting must have the “name=value” format. Where, name is the key value of a valid service setting.
External Token Destination Server URLs (Advanced)	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 Macro REST Server URLs (Advanced)	Specify the URLs for the RESTful client API to provide additional macro functions. The format of this setting must be @External<*number*>:<*value*> where, number can be any number representing the order of the URL and value is the URL. For example, @External1:value@ corresponds to the first URL, @External2:value@ corresponds to the second URL and so on.
External Password Check REST Server URLs (Advanced)	Specify the URLs for the RESTful client API to allow additional password rule validation for an application.
Web Service User Attributes (Advanced)	Specify the user attributes that are used in various web services and are presented as part of the user's data set.
External Change Method	Specify Java classes that SSPR calls after a successful password change. These classes may take actions such as updating passwords in other systems or updating eDirectory. External password classes must implement the interface password.pwm.ExternalChangeMethod. Leave this field blank if you have not added custom Java code.

Field	Description
External Rule Method	Specify the Java classes that SSPR calls to determine any rule violations in a given password. External rule methods must implement the interface password.pwm.ExternalRuleMethod. Leave this field blank if you have not added custom Java code.
CAS ClearPass URL	Specify the ClearPass URL for Central Authentication Service (CAS) authentication integration. Edit the `WEB-INF/web.xml` file also to enable the CAS integration. Uncomment the section for the CAS servlet filters, and modify the CAS servlet parameters as appropriate for your configuration.
Configuration Parameters for Shortening Service	Specify the name and value settings used to configure the selected URL shortening service. For example, an API key, username, password, or domain name. The settings must be in the `name=value` format, where name is the key value of a service setting.

4 Click **Actions** > **Save**.

3.18 Configuring OAuth SSO

This section discusses various settings that enable SSPR to integrate with OAuth Identity Server for a single sign-on.

To configure OAuth SSO, perform the following:

1 In Configuration Editor, click **Settings** > **OAuth SSO**.

2 Click **View** > **Always Show Advanced Settings** to see and configure the advanced settings.

3 Configure the following settings:

Field	Description
OAuth Login URL	Specify the URL for OAuth server login. This is the URL to redirect the user for authentication.
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.
OAuth Get Attributes Service URL	Specify the URL for the Web service that the Identity Server provides to return attribute data about the user.
OAuth Client ID	Specify the client ID of the OAuth client. This value is provided by the OAuth Identity Service provider.
OAuth Shared Secret	Specify a password for the OAuth shared secret. This value is provided by the OAuth Identity Service provider.
OAuth Username/DN Login Attribute	Specify the attribute that you want the OAuth server to identify as username for local authentication. This value is then resolved as the same password the user had typed at the local authentication page.

4 Configuring Modules

This chapter describes how to configure Self Service Password Reset (SSPR) features. Topics include:

- Section 4.1, “Configuring Change Password,” on page 69
- Section 4.2, “Configuring Account Information,” on page 71
- Section 4.3, “Configuring Forgotten Password,” on page 71
- Section 4.4, “Configuring Forgotten Username,” on page 75
- Section 4.5, “Enabling New User Registration,” on page 75
- Section 4.6, “Enabling User Activation,” on page 77
- Section 4.7, “Enabling Profile Update,” on page 78
- Section 4.8, “Enabling Shortcut Menu,” on page 79
- Section 4.9, “Enabling People Search,” on page 80
- Section 4.10, “Configuring Helpdesk,” on page 81

4.1 Configuring Change Password

Users can change their passwords whenever they want by using SSPR. You, as an administrator, can configure various settings for the Change Password feature such as enforcing users to provide their current password while changing it, actions to take when a user changes password, and so forth.

To configure Change Password settings, perform the following steps:

1. In Configuration Editor, click **Modules** > **Change Password**.
2. Click **View** > **Always Show Advanced Settings**.
3. Configure the following settings:

Setting	Description
Logout After Password Change	Select this check box to enable the system to log out the user after changing a password. The recommendation is to 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.
Required Current Password During Change	Select this check box if you want users to provide their current passwords on the Change Password page while changing their passwords. This is required when a user is using single sign-on. In most cases, this is not required because the user gets authenticated prior to accessing the Change Password page.

Setting	Description
Password Change Agreement Message	Specify the message to display to user 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 about macros, see Configuring Macros for Messages and Actions or select **View** > **Macro Help** in Configuration Editor.
Password Change Minimum Wait	Specify the time in seconds required for a password change to take effect. System uses this time for background synchronization processes.
Password Change Maximum Wait Time	Specify the maximum time in seconds the system waits for the password to be synchronized to all configured LDAP servers during a password change action. This setting prevents the page from timing out when the synchronization takes longer time.
Password Pre-Expire Time	Specify the time in seconds. Users require to change their password earlier, based on the time specified here, than the actual password expiry date. If the user's password expires within this time frame, the system behaves as if the user's password has already expired. Setting this value prevents the users' passwords expiries while users are logged in. The recommend value for this setting is 86400 seconds (One day).
Password ExpireWarn Time	Specify the time in seconds. SSPR sends the password expiry notification before a user's password expires. If the user's password expires within this time frame, the system will warn the user during a CommandServlet, checkExpire, or checkAll operation. If this time is zero or less than expirePreTime, this feature is disabled. The recommended value for this setting is 432000 seconds (5 days).
Check Expire During Authentication	Select this check box to allow the system to verify whether a user’s password is expired or about to expire while authenticating the user. If the password is expired, system forwards the user to the Expired Password page.
Seedlist File	Specify the Seedlist file. SSPR uses words from the Seedlist file to generate random passwords. You require modifying Seedlist to ensure randomness and also to meet the configured policy for the user. SSPR generate user-friendly random passwords suggestions to users.
Post Password Change Actions	Specify actions to be taken when a user changes password. The system invokes the configured actions immediately after the password is changed. You can use Macros within the action.

4 Click **Actions** > **Save**.

4.2 Configuring Account Information

When this feature is enabled, the **My Account** button is displayed in the main menu. When you configure the settings for account information, SSPR allows user s to view the history of changed passwords, password policy and details of the user. As an administrator you can define what details should be displayed for the user.

To configure the settings for Account Information, perform the following:

1. In Configuration Editor, click **Modules > Account Information**.
2. Select **Enable Account Information**.
3. Configure the following settings:

Setting	Description
Show Password Event History	Select this setting to include the **Password History** tab in the **My Account** page. This setting allows the users to view the password event history when they log in to SSPR to view their account information.
Viewable Status Fields	Select from the available options the attributes that you want the users to view when they log in to **My Account.**

4.3 Configuring Forgotten Password

The Forgotten Password feature allows users to recover a forgotten password without contacting helpdesk. After enabling this feature, users get the **Forgotten Password** button on the login 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 and allowing a password change. Requiring a user to answer challenge questions before receiving forgotten password provides an additional level of security.

To make the **Forgotten Password** button work, ensure the following:

- You have enabled the Forgotten Password feature in SSPR.
- The user must do challenge-response setup before using the Forgotten Password feature.

  For more information about how to configure challenge-request, see Section 3.6, “Configuring Challenge-Response Authentication,” on page 45.

You can also set up actions that Forgotten Password performs during the password recovery process.

NOTE: (Only when the back-end directory is Active Directory) When users change their passwords, SSPR considers the password history only when the **Minimum Password Age** is set to `0` in Active Directory and proxy is disabled. If **Minimum Password Age** is non-zero, it is recommended that users change the password through the email token to the password history.

This section includes the following topics:

- Section 4.3.1, “Enabling Forgotten Password Recovery,” on page 72
- Section 4.3.2, “Selecting a Forgotten Password Action,” on page 72
- Section 4.3.3, “Configuring Other Settings,” on page 72

4.3.1 Enabling Forgotten Password Recovery

1. In Configuration Editor, click **Modules** > **Forgotten Password**.
2. Select the **Enable Forgotten Password** check box.
3. Click **Actions** > **Save**.

4.3.2 Selecting a Forgotten Password Action

You can configure SSPR to select an action to take when the user completes the forgotten password process.

SSPR provides the following options:

- **Allow user to reset password:** After answering challenge questions to prove their identity, users can change to a new password. Because the user has authenticated through answering the challenge questions, the user can change the password without being required to provide the current password. To use this option, you must require a challenge set and the user must have set up challenge-response by answering the challenge questions.
- **Email new password to user:** After answering challenge questions, the user receives the new password in an email. To enable this option, configure SMTP email server.

  For more information about how to configure email settings, see Section 3.7, “Configuring Email Notification Settings,” on page 46.
- **SMS new password to user:** After answering challenge questions, the user receives the new password through an SMS.

  For more information about how to configure email settings, see Section 3.8, “Configuring SMS Notification Settings,” on page 49.
- **Email and SMS new password to user:** After answering challenge questions, the user receives both an email and an SMS containing the new password.

Perform the following steps:

1. In Configuration Editor, click **Modules** > **Forgotten Password**.
2. Select an action from the **Forgotten Password Recovery Mode** list.
3. Click **Actions** > **Save**.

4.3.3 Configuring Other Settings

Apart from enabling the Forgotten Password feature, configuring token setting, and configuring actions, you can configure various other settings for this feature.

1. In Configuration Editor, click **Modules** > **Forgotten Password**.
2. Click **View** > **Always Show Advanced Settings** to see and configure the advanced settings.
3. Configure the settings:

Setting	Description
Forgotten Password User Search Form	Specify form attributes that a user specifies to be authenticated such as name, email ID, and so forth. These details are confidential. System uses these values internally to search for the users who request for the forgotten password recovery action.
Forgotten Password User Search Filter	Specify a filter to find username. Each attribute configured in the **Forgotten Password User Search Form** should be included in the search filter. Strings encoded with a percent sign (%) is replaced with values supplied by the user. For example, if **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 challenge-responses are stored. 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 to write the responses to. 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 to use 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.
Allow Unlock	Select this check box if you want to allow user to unlock their account during forgotten password. Users can unlock their account instead of resetting passwords if the account is locked due to invalid login attempts, and the user's password is not expired.
Required Attributes	Specify required LDAP attributes for challenge-response. Users provide these attributes as part of the forgotten password recovery process. The LDAP proxy user requires compare LDAP rights to these attributes.
Require Responses	Select this check box if you want users to provide previously saved responses to proceed with the forgotten password recovery process.
Token Send Method	You can configure a method for sending token code or new password to the user. The available methods include: ◆ None - SSPR does not perform token verification ◆ Email Only - SSPR sends token to email address ◆ SMS Only - SSPR sends token through SMS ◆ Both - SSPR sends token to both email address and SMS ◆ Email First - SSPR tries to send token through email; if no email address is available, sends through SMS ◆ SMS First - SSPR tries to send token through SMS; if no SMS number is available, sends through email

Setting	Description
Forgotten Password Recovery Mode	Select an option from the list. ◆ Allow user to set new password - Select this option to allow the user to reset their password by using the Forgotten Password option. ◆ Send new password - Select this option to send a random password to the user's email or SMS. This setting depends on which method is specified for the **New Password Send Method** setting. ◆ Send new password and mark as expired - Select this option to send a random password to the user for temporary login and user is prompted to change the random password during the login process.
Responses Storage Hashing Method	Select a hashing method used to store responses from the list. Storing the responses as plaintext facilitates synchronization or migration to other systems.
New Password Send Method (Advanced)	Select the appropriate option from the list to specify the method to send new password to the user after the user completes the forgotten password process. ◆ **Email Only:** Select this option to send the password through email ◆ **SMS Only:** Select this option to send the password through SMS ◆ **Both:** Select this option to send the password through both email and SMS ◆ **Email First:** Select this option if your first preference of sending the password is through email. Only if the email address is unavailable the password is sent through SMS. ◆ **SMS First:** Select this option if your first preference is sending the password through SMS. Only if SMS number is unavailable the password is sent to the email address.
Forgotten Password Post Actions (Advanced)	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. Macros can be used. ◆ webservice ◆ ldap

4 Click **Actions** > **Save**.

4.4 Configuring Forgotten Username

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

Perform the following steps:

1. In Configuration Editor, click **Modules** > **Forgotten Username**.
2. Configure the following settings:

Setting	Description
Enable Forgotten Username	Select this check box to allow users to recover their username based on the configured search filter and attributes.
Forgotten Username Form	Specify the fields to be used for searching the username.
Forgotten Username Search Filter	Specify the search filter query to find username. Include each attribute configured in **Forgotten Username Form**. Strings encoded with a percent sign (%) is replaced with values supplied by the user. For example, if **Forgotten Username Form** includes `mail` and `sn` attributes, the filter would be (&(objectClass=person)(cn=%mail%)(sn=%sn%)).
Username LDAP Attribute	Specify an LDAP attribute to read as the username of the user.
Username 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**.

3. Click **Actions** > **Save**.

4.5 Enabling New User Registration

You can enable users to create a new user account by clicking **New User Registration** on the login page of SSPR. You can specify the attributes that are required for registering a new user, also the actions that need to be performed when a new user is created.

When a new user registration is complete, SSPR generates a random name that is included as an LDAP name, or entry ID in the LDAP directory. You can specify the desired value that should be displayed 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.

Perform the following steps:

1. In Configuration Editor, click **Modules** > **New User Registration**.
2. Click **View** > **Always Show Advanced Settings** to see and configure the advanced settings.
3. Configure the following settings:

Setting	Description
Enable New User Registration	Select this check box 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.
Creation Context	Specify an LDAP context in which the new users will be created.
New User Agreement Message	Specify a message to display to user before allowing them to register a new user. You can include HTML tags in this message.
New User Form	Specify attributes that a user needs to fill while registering a new user.
New User Actions	Specify the actions the system takes when a user is created. Specify the value in the name=value pair format. You can specify multiple attributes by separating with a comma. You can also use macros.
LDAP Entry ID Definition	Specify the display name, or entry ID that should be included in the LDAP naming attribute for the new registered users. In some directories an LDAP entry is used instead of a username. When this setting is enabled, an entryID or an LDAP entry that includes random characters is generated by default.You must specify macros for this setting. For more information about macros, refer Section 3.2, “Configuring Macros for Messages and Actions,” on page 39. If you leave this field blank, SSPR does not generate a random username/ entry ID. For example, In the LDAP directory, if you require the display name/ entry ID for the new registered user to be displayed as their email address, specify the value as `@User:Email@`.
Enable New User Email Verification	Select this check box if you want 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 Section 3.7, “Configuring Email Notification Settings,” on page 46.
Enable New User SMS Verification	Select this check box if you want to send an SMS to the new user's 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 Section 3.8, “Configuring SMS Notification Settings,” on page 49.
New User Password Policy Template	Specify a user of whose password policy template you want to use for the user’s password policy. For example, if the value is `TESTUSER`, the configured test user's password policy is used. If the value is blank, then the configured local password policy is used.
Delete On Creation Failure (Advanced)	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.

Setting	Description
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 user to the next step.

4 Click **Actions** > **Save**.

NOTE: The proxy user requires additional rights to create new users through the New User Registration module. See, "Proxy User Rights" on page 26.

4.6 Enabling User Activation

The User Activation module allows first-time users to activate their account and set a temporary password. This feature helps user activating their account when the account is created by a person that does not have an established channel to send the password to the user. You should configure the settings to allow only those users to activate the account who have never been authenticated. This behavior may differ depending on the configuration and directory type.

Perform the following steps:

1 In Configuration Editor, click **Modules** > **User Activation**.

2 Click **View** > **Always Show Advanced Settings** to see and configure the advanced settings.

3 Configure the following settings:

Setting	Description
Enable User Activation	Select this check box. After enabling this, users can activate their account by clicking **Activate Account** on the login page.
Token Send Method(s)	Select a method for sending token code the user. The available methods include: ◆ None - Token verification will not be performed ◆ Email Only - Send to email address ◆ SMS Only - Send via SMS ◆ Both - Send token to both email and SMS ◆ Email First - Try to send token via email; if no email address is available, send via SMS ◆ SMS First - Try to send token via SMS; if no SMS number is available, send via 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.

Setting	Description
Activation 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 (&(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 `(&(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 will execute before the user configures a password post-activation. You can use macros.
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.

4 Click **Actions** > **Save**.

4.7 Enabling Profile Update

You can enable users to view and update their profile attributes. This is feature is available on 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 In Configuration Editor, click **Modules** > **Update Profile**.

2 Click **View** > **Always Show Advanced Settings** to see and configure the advanced settings.

3 Configure the following settings:

Setting	Description
Enable Update Profile	Select this check box.
Force Update Profile	Select this check box if you want to display the Update Profile module to users after login if **Update Check Query Match** evaluation returns true.
Update Profile Update 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 Query Match	Specify a query. Users who match this query can update their profile.
Update Write Actions	Specify the actions that system executes after a user's attributes are populated. You can use macros.

Setting	Description
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.
Update Check Query Match	Specify a query to determine whether a user wants to populate the param values when the checkProfile or checkAll parameter is used with the command servlet. If you leave this field blank, the system checks the user's values against the form requirements.
Show Update Profile Confirmation	Select this check box 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.

4 Click **Actions** > **Save**.

4.8 Enabling Shortcut Menu

The Shortcut menu displays a list of links to users. To make it available for users, you need to enable this feature. After enabling this feature, users can access it on the Main Menu. You can add a number of shortcuts for users.

Perform the following steps:

1 In Configuration Editor, click **Modules** > **Shortcut Menu**.

2 Configure the following settings:

Setting	Description
Enable Shortcuts	Select this check box to make it available for users.
Shortcut Items	Specify the shortcuts you want to make available to users in this format: label::url::ldapQuery::description Here, label: Label of the shortcut that user will see. dapQuery: LDAP syntax style query. Users must match this query to access the shortcut. urlhttp: URL of the Web page for which you are adding the shortcut. description: Description of the shortcut. For example, if you want to add a shortcut for the NetIQ home page, the value would be `NetIQ::http://www.netiq.com::(objectClass=person)::NetIQ Home Page`.

Setting	Description
Shortcut Headers	Specify HTTP headers to control the list of visible shortcuts. 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.

3 Click **Actions** > **Save**.

4.9 Enabling People Search

You can configure SSPR to allow users to search for their colleagues' information and also configure the attributes to be displayed in the search result.

If you enable People Search and configure it, anyone can use the Peoplesearch option to select the appropriate user and view the user details such as, user name, email address, photo (if specified), and names of other users who report to the selected user (in a hierarchy). You can also use wildcards or ajax (searching and displaying results while typing) search for searching specific names.

Perform the following steps to configure user's search:

1 In Configuration Editor, click **Modules** > **People Search**.
2 Click **View** > **Always Show Advanced Settings** to see and configure the advanced settings.
3 Configure the following settings:

Setting	Description
Enable People Search	Select this check box. After enabling this, users can search for people by clicking **People Search**.
Permitted Users	Specify 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.
Search Filter	Specify an LDAP search filter to query the directory. Replace `%USERNAME` with user supplied username.
LDAP Search Base	Specify the LDAP search base. If you leave this field blank, the system uses the default LDAP search bases.
PeopleSearch Result Form	Specify the attributes that you want to display for individuals in the search result.
PeopleSearch Detail Form	Specify the attributes that you want to display for an individual in the detail view.

Setting	Description
PeopleSearch Result Limit	Specify the maximum number of results that the system can display in the result window. For example, if you specify 10, the search result includes first ten people. Configuring this limit improves search speed.
User Name Display	Specify the configuration value that SSPR should display for the user's name. The value for this setting is specified in the @LDAP:<name>@ format. This setting controls how user names should be displayed in the PeopleSearch details. For example, if you want SSPR to display the user's first and last names then you can provide the following configuration value: `@LDAP:givenName@ @LDAP:sn@`
Use Proxy Account	Select this check box to use LDAP proxy account to perform searches. This is not a recommended setting.
LDAP Photo Attribute (Advanced)	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, photo of the user is not displayed during the user search.
Photo URL Override (Advanced)	Specify the URL where the photo of the user is stored. The user detail will load the same photo for PeopleSearch. For example, use the @LDAP:x@ macros. If this setting is specified, the photo is fetched from the specified URL and not from the LDAP directory.
LDAP Photo HTML Style Attribute (Advanced)	Specify the height and width of the photo in pixels. SSPR displays the photo with these dimensions during the user detail search. For example, height: *100*px; width: *100*px
PeopleSearch Maximum Cache Seconds (Advanced)	Set the interval in seconds to store the search information in cache.

4 Click **Actions** > **Save**.

4.10 Configuring Helpdesk

SSPR provides a Helpdesk module. Helpdesk administrators can view user account data except password, such as password modification, login details, last password change, account status, and so forth.

SSPR allows Helpdesk administrators to search user details by using the wildcard search. For example, If the helpdesk user types *a*b* in the search field, the search result displays the list of users with name that includes the letter *a* followed by any letter and then include the letter *b* as the last letter of the name. SSPR also allows ajax search that searches the user details while they type.

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

To perform Helpdesk administrators activities, a user must be a member of an LDAP directory' group that has required rights.

In the following scenarios, a user cannot reset their password through the configured challenge-responses and call Helpdesk to reset passwords for them:

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

Perform the following steps:

1. In Configuration Editor, click **Modules** > **Helpdesk**.
2. Click **View** > **Always Show Advanced Settings** to see and configure the advanced settings.
3. Configure the following settings:

Setting	Description
Enable Helpdesk Module	Select the check box. When enabled, Helpdesk administrators can perform their tasks by clicking **Helpdesk** on Main Menu.
Helpdesk Search Filter	Specify an LDAP search filter to query the directory for users. For example, (&(objectClass=Person)(|((cn=*%USERNAME%*)(uid=*%USERNAME%*)(sAMAccountName=*%USERNAME%*)(userprincipalname=*%USERNAME%*)(givenName=*%USERNAME%*)(sn=*%USERNAME%*)))) Replace `%USERNAME` with the username supplied by a user.
Helpdesk Search Form	Specify the user attributes that you want to display to Helpdesk administrators in the search result.
Helpdesk Detail Form	Specify the user attributes that you want to display to Helpdesk administrators for an individual user.
LDAP Search Base	Specify the LDAP search base. If you leave this field blank, the system uses the default LDAP search bases.
Set Password UI Mode	Select a mode from the list to allow Helpdesk administrators to set passwords. The options include: None: Helpdesk administrators cannot change a user's password. Type: Helpdesk administrators require to type a password ly. Auto Generate: Helpdesk administrators can select a password from the auto generated passwords list and assign it to the user. Both: Helpdesk administrators can set a password by selecting an auto generated password or by typing it.
Send Password to User	Select this check box to send the reset password to users. The method of sending the password is selected under **Forgotten Password** > **New Password Send Method**.
Enable Unlock	Select this check box to enable Helpdesk administrators to unlock an intruder locked account.
Enforce User Password Policy	Select this check box if you want the Helpdesk administrators to follow the same password policies that a user does while setting their passwords.
Viewable Status Fields	Select the fields that should be available to helpdesk operators to view the status of the required user.

Setting	Description
Idle Timeout Seconds for Helpdesk Users	Specify the number of seconds after which an authenticated Helpdesk administrator's session requires re-authentication.
Clear Responses on Password Set	Select a mode to allow Helpdesk administrators to clear responses after setting passwords, which a user provides during password change request. The available options include: True: Automatically removes the user's secret questions and answers. 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.
Enable Clear Responses Button	Select this check box to allow the helpdesk operator to use a button for clearing the stored responses of the user.
Enable Delete User Button	Select this option to allow helpdesk operator to delete the user account from the LDAP directory.
Helpdesk Profile Match	Set the required LDAP profile from the drop down list. It sets the search criteria depending on the settings that were configured during the creation of LDAP Directory Profiles. You can also filter the search by specifying the LDAP domain name such as, *(memberOf=cn=Domain Admins,cn=Users,DC=site,DC=example,DC=net)*.
Helpdesk search result limit (Advanced)	Specify the limit of search result for the helpdesk user.
Post Set Password Actions (Advanced)	Specify the actions that the system executes after a Helpdesk administrator modifies a user's password. You can use macros.
Helpdesk Actor Actions (Advanced)	Specify the actions that a Helpdesk administrator can perform. You can use macros.
Use Proxy Connection (Advanced)	Select this check box to use the application proxy connection for all the actions that are initiated in the helpdesk module. If deselected, the actions are initiated using the LDAP connection of the logged in user. The user must have appropriate privileges in the LDAP directory.

4 Click **Actions** > **Save**.

5 Configuring LDAP and Policy Profiles

This chapter describes how to configure Self Service Password Reset (SSPR) profiles for LDAP directory, password policy, and challenge policy. You can create multiple LDAP profiles and select an appropriate template for the LDAP directory. You can create user groups on which you can apply password policy and challenge policies. The name you specify for the user group is the profile name for the respective password or challenge policies.

This chapter includes the following:

- Section 5.1, “Configuring LDAP Directory,” on page 85
- Section 5.2, “Configuring Password Policy for a Profile,” on page 88
- Section 5.3, “Configuring Challenge Response Policy for a Profile,” on page 91

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

5.1 Configuring LDAP Directory

SSPR allows to configure multiple LDAP directory profiles. Before configuring the LDAP directory, you must configure the LDAP settings. For more information on configuring LDAP settings, refer to Section 3.1, “Configuring LDAP Settings,” on page 37. 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 SSPR configuration.

To configure LDAP profiles, perform the following steps:

1. In Configuration Manager, click **Profiles** > **LDAP Directory Profiles**.
2. In the Selected Profile field, select **Edit Profile List**, to specify name of the profile.
3. 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, SSPR searches for the default profile first, and then the other profiles in the order mentioned.
4. Click **Return to configuration editor**.
5. Select the appropriate profile from the **Selected Profile** list.
6. Click **View** > **Always Show Advanced Settings**.
7. Configure the following settings:

Field	Description
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 next available server in the list is used. SSPR checks unavailable servers periodically to check their availability. For secure SSL, use the ldaps://servername:636 format. For plain text servers, use the ldap://serverame:389 format (not recommended). When using secure connections, the Java virtual machine 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** ◆ Avoid using non-secure connections because many LDAP servers reject password operations on non-secure connections. ◆ Avoid using a virtual IP address or a load balancer device. ◆ Instead of using a load-balancing device for LDAP high availability, use the built-in LDAP server fail-over functionality. ◆ Avoid using a DNS round-robin address.
LDAP Certificates	Displays details of LDAP server certificates.
LDAP Proxy Users	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 usernames during authentication and other operations. This is the top level LDAP container in which your users exist. You can add multiple contexts. SSPR searches each context until it finds a single match. To improve search performance, do not add large numbers of contexts because SSPR searches each context serially.

Field	Description
LDAP Test User	Specify an LDAP test user account. You must 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 about any configuration or health issues. You can test the following functionalities through a test user: ◆ Authentication ◆ Read password policy ◆ Set password ◆ Set challenge-responses ◆ Load challenge-responses This is a recommended setting. You can configure an LDAP Test User DN later also.
Username Search Filter	Specify the username search query in the following format: `(&(objectClass=person)(cn=%USERNAME%))` Replace the value `%USERNAME%` with the actual username value. SSPR uses this filter for the contextless login and for finding users in the LDAP directories.
LDAP GUID Attribute	Specify an attribute to identity 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.
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. It is required only if schema is extended to store challenge response information. This is not required for Active Directory even with schema extension
LDAP Chai Settings	Specify a Name/Value setting to control behavior of the LDAP Chai API. The settings must be in the `name=value` format, where name is the key value of a valid ChaiSetting.
Attribute to use for Username	Specify an attribute to allow pages to display other details such as, the username of a user instead of the **LDAP Naming Attribute** value.
Auto-Add GUID Value	Select this check box 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.
User Selectable Login Contexts	Specify the values in this format: display value:::context. For example, ou=sf,ou=ca,o=example:::San Francisco ou=lon,ou=uk,o=example:::London ou=nyc,ou=ny,o=example:::New York This is an optional setting. If you configure this, system adds a field to the form-based login screen and other user search screens. This field allows users to select a specific context.

Field	Description
LDAP Profile Display Name	Specify the name of the LDAP profile that you have configured.

8 Click **Actions** > **Save**.

5.2 Configuring Password Policy for a Profile

You can configure password policy for specific group of users by using the password policy profile. You can create different profiles for different group of users so that, specified password policy is applied for each profile.

To configure password policy for a specific profile, perform the following steps:

1 Click **Profiles** > **Password Policy Profiles**.
2 Click **View** > **Always Show Advanced Settings**.
3 Select the appropriate LDAP profile name.
4 Configure the following settings:

Field	Description
Password Policy Profile Query Match	Specify the query that matches specific users for the specified profile.
Minimum Length	Specify the minimum length of password. Specify zero to disable this feature.
Maximum Length	Specify the maximum length of password. Specify zero 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 zero 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 zero to disable this feature
Allow Numeric Characters	Select this check box to allow numeric characters in the password.
Allow First Character Numeric	Select this check box 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 check box 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 zero to disable this feature.

Field	Description
Minimum Numeric	Specify the minimum number of numeric characters you want to allow in the password. This setting is applicable when you allow numeric character in the password. Specify zero to disable this feature.
Allow Special Characters	Select this check box to allow non-alphanumeric characters in the password.
Allow First Character Special	Select this check box 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 check box 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 zero 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 zero to disable this feature.
Maximum Alphabetic	Specify the maximum number of alphabetic characters allowed in the password. Specify zero to disable this feature.
Minimum Alphabetic	Specify the minimum number of alphabetic characters required in the password. Specify zero to disable this feature.
Maximum Non-Alphabetic	Specify the maximum number of non-alphabetic characters allowed in the password. Specify zero to disable this feature.
Minimum Non-Alphabetic	Specify the minimum number of non-alphabetic characters required in the password. Specify zero to disable this feature.
Maximum Uppercase	Specify the maximum number of uppercase characters allowed in the password. Specify zero to disable this feature.
Minimum Uppercase	Specify the minimum number of uppercase characters required in the password. Specify zero to disable this feature.
Maximum Lowercase	Specify the maximum number of lowercase characters allowed in the password. Specify zero to disable this feature.
Minimum Lowercase	Specify the minimum number of lowercase characters required in the password. Specify zero to disable this feature.

Field	Description
Minimum Unique Characters	Specify the minimum number of unique characters required in the password. Specify zero 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 zero to disable this feature.
Enable Wordlist	Select this check box to enable users to check the password against the configured Wordlist.
Enforce Microsoft-AD 2003 Password Complexity	Select this check box to the following Microsoft Active Directory style password complexity rules: ◆ 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, !, $, #, %) **NOTE:** This option is allowed on Windows server 2008 R2 SP1 or later.
Disallowed Values	Specify the list of case insensitive values that you do not want to allow in the password. For example, password, username, and name of the organization.
Minimum Password Strength	Specify the minimum password strength level required. 45 to 69 are good and above 69 are strong. A value of zero disables this check.
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 may overwrite this setting.
Required Regular Expression Matches (Advanced)	Specify a regular expression pattern that a valid password must match. You can list multiple patterns. Patterns must follow the rules listed for the pattern. A pattern must match the entire password to be applied. A partial match is not accepted.
Disallowed Regular Expression Matches (Advanced)	Specify a regular expression pattern that a password must not match to be allowed. You can list multiple patterns. A partial match is ignored.
Disallowed Attributes (Advanced)	Specify the list of case-insensitive attributes that you do not want to allow in the password. For example, cn and sn.

Field	Description
Password Rule Text (Advanced)	Specify the password rules that you want to display to users. If you do not specify the full path, SSPR uses the `WEB-INF` directory by default. By default, this field is blank and an appropriate rule text is automatically generated. When you configure this setting, the text in this setting replaces the automatically generated rule text. You can use HTML tags.
Disallow Current Password (Advanced)	Select this check box if you want to prevent users from repeating the current password as new password. You can this setting if the login method permits the user's password to be known.

5.3 Configuring Challenge Response Policy for a Profile

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.

An SSPR 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 helpdesk person can use for authenticating the users to reset their password.

To configure challenge response, perform the following:

1. Click Profiles > Challenge Profiles
2. Click **View** > **Always Show Advanced Settings**.
3. Configure the following settings:

Field	Description
Challenge Profile Query Match	Specify the query that matches users for the specified profile.
Random Questions	Set up random questions for challenge-response in this field. Users need to answer all or some of these questions while setting up their responses. Use `%<text>%` to indicate a user supplied question. **Format of the question:** question::minimumLength::maximumLength For example: ◆ %user%::5::200 ◆ What is favorite food?::5::200 ◆ What is your fathers middle name?::5::200

Field	Description
Required Questions	Set up the required questions for challenge-response. The user must answer all these questions while setting up their responses. Users must provide answers to these questions during resetting process of forgotten password. Use `%<text>%` to indicate a user supplied question. **Format of the question:** question::minimumLength::maximumLength For example: ◆ %user%::5::200 ◆ What is favorite food?::5::200 ◆ What is your fathers middle name?::5::200
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, users are prompted to answer the same number of challenge questions during Forgotten Password process instead of answering the modified number of challenge responses. But if the users clear the responses and answer the challenge response again then user is 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 in two different scenarios: during initial setup and during forgotten password recovery. Specify zero to force all available random questions to be configured at the time of setup.

Field	Description
Helpdesk Random Questions	Set up helpdesk 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 Helpdesk Random Challenges Required During Setup** setting. The helpdesk users can access the questions and its responses. These questions are not used for forgotten password recovery. Use `%user%` to indicate a user supplied question. **Format of the question:** question::minimumLength::maximumLength Where, question is the text of the challenge question, minimumLength is minimum field length and maximum length is maximum field length. For example, ◆ What is your maiden name?::5::200 ◆ %user%::5::200
Helpdesk Required Questions	Set up helpdesk required questions for challenge-response. Users must supply answers for all of these questions when setting up their responses. Use %user% to indicate a user-supplied question The helpdesk users can access the questions and its responses. These questions are not used for forgotten password recovery. **Format of the question:** question::minimumLength::maximumLength Where, question is the text of the challenge question, minimumLength is minimum field length and maximum length is maximum field length. For example, ◆ What is your maiden name?::5::200 ◆ %user%::5::200
Minimum Helpdesk Random Challenges Required During Setup	Specify the minimum number of helpdesk random questions the user is required to answer while setting up the response. If this number is higher than the available helpdesk random questions, or lower than the required questions, the setting is adjusted accordingly. Specify zero to force all available helpdesk random questions to be configured at time of setup

6 Integrating SSPR with NetIQ Access Manager

NetIQ 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 SSPR with Access Manager provides a comprehensive and secure access management solution. For this integration, you require to configure few settings in the Access Gateway, a component of Access Manager.

To enable SSPR to integrate with Access manager, you must configure the extension settings. For more information, see Section 3.17, “Configuring Extensions,” on page 65.

Topics include:

- Section 6.1, “Configuring Access Gateway for SSPR,” on page 95
- Section 6.2, “Integrating SSPR with Access Manager,” on page 97
- Section 6.3, “Request Parameters,” on page 99
- Section 6.4, “Command Servlet,” on page 99

6.1 Configuring Access Gateway for SSPR

This section discusses the configuration required for the Access Gateway to integrate it with SSPR.

- Section 6.1.1, “Configuring Proxy Service for SSPR,” on page 95
- Section 6.1.2, “Configuring Protected Resource for SSPR,” on page 96
- Section 6.1.3, “Configuring Single Sign-On to SSPR,” on page 96
- Section 6.1.4, “Configuring Single Sign-On to SSPR When Password Is Not Available,” on page 97

6.1.1 Configuring Proxy Service for SSPR

You can configure SSPR as path based multi-homing or domain based multi-homing proxy service on Access Manager. For more information about these proxy services, see Domain-Based Multi-Homing and Path-Based Multi-Homing in the NetIQ Access Manager Access Gateway Guide.

The following table lists the sample configuration for path-based multi-homing setup:

Configuration	Setup
Proxy service type	Path based multi-home
	For example, Published DNS Name = intranet.company.com
Ports	SSL port of Web server: 8443
	Non-SSL port of Web server: 8080

Configuration	Setup
Configured multi-homing path	/sspr
Remove path on fill	Disabled
Host header	SPR Web server hostname
Rewriter configuration	Default

6.1.2 Configuring Protected Resource for SSPR

Some modules of SSPR, 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 SSPR is set up so that the user enters the following URL to access:

```
http://password.example.com/sspr
```

You can configure the URL to be public or restricted as follows:

URL	Mode
password.example.com/*	Public
password.example.com/sspr/private/*	Restricted
password.example.com/sspr/private/admin/*	Restricted
password.example.com/sspr/private/config/*	Restricted

Though SSPR 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 SSPR application.

6.1.3 Configuring Single Sign-On to SSPR

SSPR, by default, performs an HTML form-based authentication when an un-authenticated 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 SSPR for the authenticated user in the Access Manager Identity Server.

Configure the Identity Injection policy for SSPR as follows and enable this policy for restricted URL paths discussed in "Configuring Protected Resource for SSPR" on page 96:

Configuration	Value
Action for Identity Injection	Inject into Authentication Header
Auth Header – User Name	Credential Profile (LDAP Credentials: LDAP User DN)
Auth Header – Password	Credential Profile (LDAP Credentials: LDAP Password)
DN Format	LDAP format (default)

For more information about Identity Injection policies, see Creating Identity Injection Policies in the NetIQ Access Manager Policy Guide.

6.1.4 Configuring Single Sign-On to SSPR 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 SSPR to accept only the username during SSO. In this partially authenticated state, users can perform some functions without providing their password. For example, the CommandServlet actions can be invoked without any user interaction.However, if users need to interact with SSPR, such as to change password or setup responses, they must provide their password before proceeding.

To use this functionality, configure SSPR and Access Manager as follows:

1. In SSPR, go to **Configuration Manager** > **Settings** > **Security**.
2. In **SSO Authentication Header Name**, set the value `ssoAuthUsername`.
3. In Access Manager, set the following policy for SSPR protected resources:

Configuration	Value
Action for Identity Injection	Inject into Custom Header
Custom Header Name	ssoAuthUsername
Value	Credential Profile (LDAP Credentials: LDAP User DN)
DN Format	LDAP format (default)

NOTE: If SSPR 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 will not be prompted for their passwords when authenticated to SSPR by using this method.

6.2 Integrating SSPR with Access Manager

SSPR provides various options for integration with Access Gateways including configurable redirection URLs, servlet command options, support for HTTP basic authentication, and so forth.

Among these configurations, the following two are the most important settings:

- **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 SSPR 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.

For more information about other setting options, see Section 3.3, “Configuring General Settings,” on page 40.

You must force the user to log out from SSPR and Access Manager after a password change operation is completed. Otherwise, users may experience authentication failures and intruder lockout if they continue to use the same Access Manager session. For more information about how to configure this, see Section 4.1, “Configuring Change Password,” on page 69.

There are two instances when a user is 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 SSPR 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.

6.2.1 Configuring SSPR Parameters for Access Manager

Configure the following SSPR settings through Configuration Editor:

Configuration	Value
Settings > User Interface > Password Change Message	Custom message to notify users about re-login to their portal after password change.
Settings > Application > Forward URL	After completing any activity except password change, which does not require a logout, users are forwarded to this URL. For example, `intranet.company.com`.
Settings > Application > Logout URL	Access Manager logout URL. For example, intranet.company.com/AGLogout
Modules > Change Password > Logout After Password Change	Select the check box.

6.2.2 Configuring Password Expiration Servlet

You must configure the Access Gateway to redirect users to SSPR when their password expires. You can configure this in Access Manager here: **Identity Server** > **Edit** > **Local** > **Contracts** > **[Contract Name]** > **Password Expiration Servlet**. The administrator may configure this URL option to SSPR Change Password URL.

For example, `http://password.example.com/sspr/private/ChangePassword?passwordExpired=true`

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 SSPR change password portal.

6.2.3 Integrating Forgotten Password URL

Administrators can configure the Access Manager Identity Server login page to include the forgotten password URL for SSPR. On the Identity Server, add the following HTML code in the `login.jsp` file (`/opt/novell/nids/lib/webapp/jsp/login.jsp`) above the last two </body></html> tags:

```
<CENTER>
   <a href="https://intranet.company.com/sspr/public/ForgottenPassword?
   forceAuth=TRUE&logoutURL=https://intranet.company.com/AGLogout" target="_top">
   Forgot Password - Self Service Password Reset</a>
</CENTER>
```

6.3 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 SSPR.

For example, `http://password.example.com/sspr/private/ChangePassword?passwordExpired=true&forwardURL=http://www.example.com`

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

6.4 Command Servlet

Command Servlet allows you to redirect a user to SSPR and have it perform some specific command. You can use Command Servlet functions during a user's login sequence to a portal or other landing point.

Use Command Servlet functions with a proxy service, Access Gateway, or devices that auto-authenticate users. Otherwise, the user requires to authenticate to SSPR during each login.

You can combine Command Servlet calls with request parameters such as forwardURL.

The following table lists an example of the user login redirect sequence:

URL Example	Description
http://portal.example.com	Initial request from browser.
http://portal.example.com/Login	Access Gateway redirects the user to the login page.
http://portal.example.com/	Access Gateway redirects the user to the portal root.
http://portal.example.com/index.html	Web server redirects the user to `index.html`.
http://password.example.com/sspr/private/CommandServlet?processAction=checkAll&forwardURL=http%3A%2F%2Fportal.example.com%2Fportalpage.html	`index.html` has meta redirect to the SSPR checkAll CommandServlet with an URLEncoded forwardURL value.
http://portal.example.com/portal/main.html	SSPR redirects the user to the actual portal URL.

The `index.html` file contains the following content:

```
<html>
 <head>
  <meta http-equiv="REFRESH" content="0; URL=http://password.example.com/sspr/
private/CommandServlet?
processAction=checkAll&forwardURL=http%3A%2F%2Fportal.example.com%2Fportalpage.htm
l"/>
 </head>
 <body>
 <p>If your browser doesn't automatically load, click
 <a href="http://password.example.com/sspr/private/CommandServlet?
processAction=checkAll&forwardURL=http%3A%2F%2Fportal.example.com%2Fportalpage.htm
l">here</a>.
 </p>
 </body>
</html>
```

The following table lists various useful commands:

Command	URL	Description
checkExpire	http://password.example.com/sspr/private/CommandServlet?processAction=checkExpire	Checks the user's password expiration date. If the expiration date is within the configured threshold, the user requires to change password.
checkResponses	http://password.example.com/sspr/private/CommandServlet?processAction=checkResponses	Checks the user's challenge-responses. If no responses are configured, the user requires to set them up.
checkProfile	http://password.example.com/sspr/private/CommandServlet?processAction=checkProfile	Checks the user's profile. If the user's attributes do not meet the configured requirements, the user requires to set profile attributes.
checkAll	http://password.example.com/sspr/private/CommandServlet?processAction=checkAll	Calls checkExpire, checkResponses, and checkProfile consecutively.

7 Integrating SSPR with Identity Manager

NetIQ Identity Manager (IDM) 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.

SSPR integrates with Identity Manager 4.5 to manage passwords for all the users who access the identity applications. This integration is possible if SSPR is installed with Identity Manager 4.5 by using Integrated Installer, or if SSPR 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 SSPR and the user is allowed to access the webpages depending on the password policy that is defined for the user.

If you install SSPR by using Identity Manager 4.5 Integrated Installer, the configuration settings are defined automatically in the SSPR configuration file. For more information on installing SSPR with Identity Manager, see Installing Single Sign-on and Password Management for Identity Manager in the *NetIQ Identity Manager Setup Guide.* But, if you have installed SSPR as a standalone product and want to utilize the SSPR password management functionality for Identity applications then, you can provide the configurable values for the required settings by using the SSPR Configuration Editor page. The default location for the `SSPRConfiguration` file is `<drive name>:\Program Files (x86)\NetIQ Self Service Password Reset\apache-tomcat-7.0.50\webapps\sspr\WEB-INF`. If you make any changes in the settings by using the Configuration Editor, the configuration file gets updated with those changes.

To enable SSPR to integrate with Identity manager, you must update the SSPR configuration file by defining the default values for the SSPR settings that are applicable for Identity applications.

7.1 Configuring SSPR Settings for Identity Manager

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

- Section 7.1.1, “Configure OAuth Settings for SSPR,” on page 103
- Section 7.1.2, “Set the SSPR Theme to Match the Identity Manager Theme,” on page 104
- Section 7.1.3, “Configure Syslog Audit server,” on page 104

NOTE: Ensure that you have selected **Password Management Provider** as **Self Service password Reset (SSPR)** in the Roles Based Provisioning Module (RBPM) Configuration utility of Identity Manager 4.5. For more information about configuring settings in RBPM Configuration utility, refer Configuring the Settings for the Identity Applications in the *NetIQ Identity Manager Setup Guide*.

7.1.1 Configure OAuth Settings for SSPR

This section discusses various settings that enable SSPR to integrate with OAuth Identity Server for a single sign-on. The Identity Manager RBPM configuration utility includes OAuth settings under **Self Service Password Reset** in the **SSO clients** tab. The OAuth settings that are defined in the RBPM

configuration utility must be included in the SSPR OAuth settings. For more information about configuring or viewing the settings in the RBPM configuration utility, refer Configuring Identity Manager to Use Self Service Password Reset in the NetIQ Identity Manager Setup Guide.

To specify the Identity Manager 4.5 OAuth settings in SSPR, perform the following in the SSPR Configuration Editor page:

1. In Configuration Editor, click **Settings** > **OAuth SSO**.
2. Specify the following values for the respective fields:

Field	Value	Description
OAuth Login URL	http://<IP address of the server>:8180/osp/a/idm/auth/oauth2/grant	Specify the URL for OAuth server login. This is the URL to redirect the user for authentication.
OAuth Code Resolve Service URL	http://<IP address of the server>:8180/osp/a/idm/auth/oauth2/authcoderesolve	Specify the URL for OAuth Code Resolve Service. This Web service URL is used for resolving the artifact that the OAuth identity server returns.
OAuth Profile Service URL	http://<IP address of the server>/osp/a/idm/auth/oauth2/getattributes	Specify the URL for the Web service that the Identity Server provides to return attribute data about the user.
OAuth Client ID	sspr	Specify SSPR as the client ID of the OAuth client. This value is provided by the OAuth Identity Service provider.
OAuth Username/DN Login Attribute	name	SSPR identifies this value as the username for local authentication. This value is then resolved as the same password the user had typed at the local authentication page.

3. Click **Actions** > **Save**.

7.1.2 Set the SSPR Theme to Match the Identity Manager Theme

SSPR includes an option to use the Identity Manager theme for the SSPR password management page. To set the theme of the SSPR webpage to match the Identity manager theme, perform the following in the SSPR Configuration Editor page:

1. Click **Settings** > **User Interface**.
2. Select **IDM** from the list of themes in the **Interface Theme** setting.

7.1.3 Configure Syslog Audit server

SSPR provides logging and auditing functionality for sending event alerts. To configure SSPR audit server with the IDM 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, refer Section 3.13, “Configuring Logging and Auditing,” on page 59.

7.2 Setting Up the SSPR Configuration File with Identity Manager Settings

The SSPR configuration file must include the details on all the Identity Manager settings. So, apart from the values that you set for SSPR settings, you must configure the following settings from the Configuration Editor page:

- Section 7.2.1, “NetIQ eDirectory Settings,” on page 105
- Section 7.2.2, “User Interface,” on page 105
- Section 7.2.3, “Application Settings,” on page 106
- Section 7.2.4, “Password Settings,” on page 107
- Section 7.2.5, “Challenge Settings,” on page 107
- Section 7.2.6, “Security Settings,” on page 108
- Section 7.2.7, “Integration/ Developer Settings,” on page 108
- Section 7.2.8, “LDAP Directory Profiles,” on page 108
- Section 7.2.9, “Password Policy Profiles,” on page 109
- Section 7.2.10, “Forgotten Password Modules,” on page 109

7.2.1 NetIQ eDirectory Settings

SSPR provides a template to set default settings for eDirectory. To set default LDAP settings for eDirectory, click **Template** and then select the **NetIQ eDirectory** template.

To configure the LDAP settings, perform the following steps:

1. In Configuration Editor, select **Template** > **NetIQ eDirectory**.
2. Click **Settings** > **NetIQ eDirectory**.
3. Specify the following values for the respective fields:

Field	Description
Enable NMAS Responses for Forgotten Password	Select this check box to use NMAS stored responses during forgotten password recovery. SSPR tries all other configured storage methods before evaluating.

4. Click **Actions** > **Save**.

7.2.2 User Interface

SSPR includes the IDM theme to provide the users the same look and feel as they get when working on an IDM interface.

To specify the IDM user interface, perform the following:

1. In Configuration Editor, click **Settings** > **User Interface**.
2. Click **View** > **Always Show Advanced Settings** to see and configure the advanced settings.
3. Specify the following values for the respective fields:

Field	Value	Description
Interface Theme	IDM	Select this theme from the list the SSPR interfaces list.
Show Home Button	Deselect the Enabled checkbox	Deselecting this check box does not display the **Home** button.

4 Click **Actions** > **Save**.

7.2.3 Application Settings

SSPR allows you to configure basic settings for the identity applications to control functionality and behavior of the system.

1 In Configuration Editor, click **Settings** > **Application**.

2 Specify the following Values for the respective fields:

Field	Value	Description
Site URL	http://<ip address>:<port number>/sspr Where, ip address is the IP address of the server where SSPR is installed and port number is 8180 by default.	This is the default URL to access SSPR. This URL is used in email and other user communications.
Forward URL	http://<ipaddress>:<port number>/landing	After completing any activity, which does not require a logout, users are forwarded to this URL.
Logout URL	http://<ipaddress>:<port number>/osp/a/idm/auth/app/logout	This is the default URL to which SSPR redirects users after logout.

3 Click **Actions** > **Save**.

7.2.4 Password Settings

These settings are applicable for all the users and are not dependant on the password policy or any profile. For more information on profile specific password policy, refer Section 5.2, “Configuring Password Policy for a Profile,” on page 88.

To configure the password setting, perform the following:

1. In Configuration Editor, click **Settings** > **Password Settings**.
2. Specify the following value for the respective field:

Field	Value	Description
Password Policy Source	Select **LDAP** form the drop down list.	SSPR reads the LDAP password policies.

3. Click **Actions** > **Save**.

7.2.5 Challenge Settings

These settings control the challenge/ response feature. These settings are not dependant on the challenge policy.

To configure the challenge settings, perform the following steps:

1. In Configuration Editor, click **Settings** > **Challenge Settings**.
2. Specify the following values for the respective fields:

Field	Value	Description
Maximum Characters of Challenge Allowed in Response	0	This setting allows you to use for the response the same characters that you use for the challenge questions. This allows a user's response to be the same as the challenge.

7.2.6 Security Settings

These settings control the security of the applications.

To configure the security settings, perform the following:

1. In Configuration Editor, click **Settings** > **Security**.
2. Specify the following values for the respective fields:

Field	Value	Description
Redirect Whitelist	http://<ipaddress>:<port number>	This value is the URL fragment that can be used for URL forwarding.
Prevent HTML Framing (Advanced)	De-select **Enabled**	De-selecting this option allows users to view SSPR in an inline frame for any identity application that includes the iframe html source code.

3. Click **Actions** > **Save**.

7.2.7 Integration/ Developer Settings

These settings are intended for the developers and the component integrators to integrate SSPR with other external source.

To configure these settings, perform the following:

1. In Configuration Editor, click **Settings** > **Integration/Developer**.
2. Specify the following value for the respective field:

Field	Value	Description
Enable External Web Services	Select **Enabled (True)**	Selecting this check box allows public use of Web services.

3. Click **Actions** > **Save**.

7.2.8 LDAP Directory Profiles

These settings control the SSPR interaction with the LDAP directory.

To configure the settings for LDAP directory profiles, perform the following:

1. In Configuration Editor, click **Profiles** > **LDAP Directory Profiles**.
2. Specify the following values for the respective fields:

Field	Value	Description
LDAP URLs	`ldaps://<IP address of the LDAP server>:<LDAP port>`	Specify the LDAP URLs.
LDAP Proxy User	cn=admin,ou=sa,o=system	You can gain access to the LDAP directory through the LDAP proxy user.
LDAP Contextless Login Roots	ou=sa,o=data	This is the top level LDAP container in which the eDirectory users exist.

3 Click **Actions** > **Save**.

7.2.9 Password Policy Profiles

These settings control configuration of password policy for specific group of users by using the password policy profile.

1 In Configuration Editor, click **Profiles** > **Password Policy Profiles**.

2 Specify the following values for the respective fields:

Field	Value	Description
Enable Wordlist	De-select **Enabled (True)**	De-selecting this option specifies that SSPR is not required to verify the password from the wordlist.
Disallowed Values		This option specifies the list of case insensitive values that you do not want to allow in the password. For IDM, you do not require to add any value for this option.

3 Click **Actions** > **Save**.

7.2.10 Forgotten Password Modules

The Forgotten Password feature allows users to recover a forgotten password without contacting helpdesk.

To configure settings for forgotten password, perform the following:

1 In Configuration Editor click **Modules** > **Forgotten Password**.

2 Specify the following values for the respective fields:

Field	Value	Description
Forgotten Password User Search Form	Name: cn, Label: *Username*, and select **text** from the drop down list.	These are form attributes and are required to authenticate the users. These details are confidential.
Forgotten Password User Search Filter	`(&(objectClass=person)(cn=%cn%))`	

A Frequently Asked Questions

This section provides the frequently asked questions about SSPR.

- Section A.1, “Can I import data from LocalDB to RDBMS?,” on page 112
- Section A.2, “When a new user is created, does SSPR send an email to the user with login credentials?,” on page 112
- Section A.3, “Where can I see the account Information?,” on page 112
- Section A.4, “Can I perform self-password reset if I forget answers to challenge questions?,” on page 113
- Section A.5, “How do I resolve the No From Address error?,” on page 113
- Section A.6, “Why Users cannot use their old password to login even when they did not complete the forgotten password process?,” on page 113
- Section A.7, “Where can I see the password history?,” on page 113
- Section A.8, “Can I reset password after utilizing my all eDirectory grace login without calling helpdesk?,” on page 114
- Section A.9, “How to create a new user?,” on page 114
- Section A.10, “Can SSPR use nspmComplexityRules?,” on page 114
- Section A.11, “Does SSPR work with OpenLDAP?,” on page 114
- Section A.12, “How to go to Main Menu from Configuration Editor?,” on page 114
- Section A.13, “How to enable users to change password more than once a day?,” on page 115
- Section A.14, “How to enable Windows desktop to support forgotten password reset?,” on page 115
- Section A.15, “How to configure post password change actions?,” on page 115
- Section A.16, “Where can I see version of installed SSPR?,” on page 115
- Section A.17, “Does SSPR honor the Active Directory password history policy?,” on page 115
- Section A.18, “How to set logging mechanism and where to see the logged result?,” on page 116
- Section A.19, “How to enable SSPR to read custom http headers for authentication?,” on page 116
- Section A.20, “How to import LDAP certificates?,” on page 116
- Section A.21, “How to modify user interface strings?,” on page 116
- Section A.22, “How do I change the default language of SSPR?,” on page 116
- Section A.23, “Can audit events be forwarded to syslog and compatible servers?,” on page 117
- Section A.24, “Where can I see SSPR audit logs?,” on page 117
- Section A.25, “Can SSPR authenticate by using custom attributes?,” on page 117
- Section A.26, “How to access reports and logs in SSPR?,” on page 117

A.1 Can I import data from LocalDB to RDBMS?

Yes. However, importing data from LocalDB to RDBMS consists of two steps. First step includes exporting the data from the currently configured response read and write locations to a file. Second step includes importing the responses to RDBMS to achieve migration.

1. Run the following:

   Windows: `/webapps/sspr/WEB-INF/Command.bat`

   Linux:`/webapps/sspr/WEB-INF/Command.sh`

   You should see an option to export response data from LocalDB.

2. Re-run `Command.bat` or `Command.sh`with appropriate options.

   For example, `Command.bat exportresponses c:\dump\<filename>`

   NOTE: The file provided in the command should exist.

3. After exporting the data, you can import all response data in to an

   external RDBMS database by using the `ImportResponsesToDB` command.

   For example, `Command.bat ImportResponsesToDB c:\dump\<filename>`

   NOTE: The file provided in the command should be the same that you used for exporting data from LocalDB.

   The `Command` utility uses the SSPRConfiguration.xml file to read appropriate configuration information. You should configure SSPR to connect to an RDBMS database and restart. This ensures that all required database tables are created in the RDBMS database.

A.2 When a new user is created, does SSPR send an email to the user with login credentials?

Yes, but not by default. You should configure the email settings. For more information, see Section 3.7, “Configuring Email Notification Settings,” on page 46

A.3 Where can I see the account Information?

To view the account information, you must select **Show User Account Information** in Configuration Editor. See, Section 3.4, “Configuring User Interface Settings,” on page 41.

1. Log in to SSPR.
2. Click **Account Information**.

   You can see the following:

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

A.4 Can I perform self-password reset if I forget answers to challenge questions?

It depends on how the administrator has configured the Forgotten Password module. Administrators can configure the module requiring users to provide any one or more of the following information for resetting password:

- Challenge-response questions
- User's attributes
- Email or SMS token

A.5 How do I resolve the No From Address error?

Users do not receive any automated emails from the SMTP server even when SSPR is configured to send emails. You receive the error `Unable to send Email: No From Address`. This message is displayed only when SSPR is installed on a SLES machine and the machine name is not defined in the host file.

To resolve this issue, perform the following:

On the SLES server where SSPR is installed, include the machine name in the host file of the etc folder. You require to replace `127.0.0.1 localhost` with `127.0.0.1 <name of the machine> localhost`.

A.6 Why Users cannot use their old password to login even when they did not complete the forgotten password process?

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 then, user cannot use the old password. This happens because SSPR recognizes the random password that was created when the user clicked on **Forgotten password**.

To resolve this issue perform the following:

- For Oracle Directory Server, the user needs to complete the forgotten password process and then use the new password to login.
- For Active Directory, you can enable the "**Use Proxy When Password Forgotten**" setting from the Configuration Editor.
- For eDirectory, you require to enable the **Allow admin to retrieve passwords** option from the eDirectory settings page.

A.7 Where can I see the password history?

You can see the password history on Main Menu. To see this, you must select **Show Password Event History** in Configuration Editor. See, Section 3.4, "Configuring User Interface Settings," on page 41.

NOTE: Password history is available only when the schema has been extended. SSPR stores the password history on the LDAP attribute configured in the setting under **Settings** > **Logging & Alerts** > **User History Attribute**. If this attribute is not available to SSPR, the password history is not stored and available for viewing.

1. Log in to SSPR.
2. Click **Account Information** > **Password History**.
3. Click **Continue** to go back to **Main Menu**.

A.8 Can I reset password after utilizing my all eDirectory grace login without calling helpdesk?

Yes, you can if you have enrolled into SSPR.

A.9 How to create a new user?

1. Ensure that you have selected the **Enable New User Registration** check box under **Modules** > **New User Registration**.

   For more information, see Section 4.5, “Enabling New User Registration,” on page 75.
2. On the login page, click **New User Registration**.

   NOTE: You can also access the New User Registration page through http://<ip/hostname>:<port number>/<sspr webhost name>/public/NewUser.
3. Specify the appropriate details as prompted.
4. Click **Create**.

   The user may require to validate the account by providing the token sent through email or SMS. This depends on the configuration.
5. Click **Continue** to complete the registration process.

A.10 Can SSPR use nspmComplexityRules?

Yes. SSPR can use nspmComplexityRules (XML RuleSet), but it does not display rules to users.

A.11 Does SSPR work with OpenLDAP?

Yes. You can configure SSPR to work with OpenLDAP, although this has not been tested officially.

A.12 How to go to Main Menu from Configuration Editor?

Click **Actions** > **Cancel**. SSPR redirects you to **Main Menu**.

A.13 How to enable users to change password more than once a day?

Go to **Configuration Manager** > **Settings** > **Password Policy** and set an appropriate value in **Minimum Lifetime**.

A.14 How to enable Windows desktop to support forgotten password reset?

Integration of SSPR 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 Novell 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 information about how to integrate CLE with SSPR, see Client Login Extension User Guide.

A.15 How to configure post password change actions?

1. In Configuration Editor, click **Modules** > **Change Password**.
2. In **Post Password Change Actions**, specify actions to be taken when a user changes password. The system invokes the configured actions immediately after the password is changed. You can use Macros within the action.
3. Click **Actions** > **Save**.

A.16 Where can I see version of installed SSPR?

1. Log in to SSPR.
2. Click **Main Menu** > **Administration** > **System** > **About**.

   You can see the SSPR version along with other details such as version of Chai API and Dojo API.

A.17 Does SSPR honor the Active Directory password history policy?

Forgotten Password recovery or reset is generally performed by using a proxy or administrator's account in SSPR. However, you can configure to use the user's account while setting the forgotten password by disabling **Use Proxy When Password Forgotten** under **Settings**> **Active Directory**. In this scenario, the Active Directory policy is d 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.

A.18 How to set logging mechanism and where to see the logged result?

SSPR provides extensive logging to help troubleshoot installation and configuration issues. For best results during installation, set the log levels to **trace** in the `log4jconfig.xml`. You can monitor the output in `SSPR.log`. For more information about logging, see Section 3.13, “Configuring Logging and Auditing,” on page 59.

You can also configure audit records to be sent to a syslog server.

A.19 How to enable SSPR to read custom http headers for authentication?

To enable SSPR to read custom http headers for authentication, you need to set **SSO Authentication Header Name** under **Settings** > **Security**.

This allows authentication to SSPR without the user's password. However, before being able to interact with the directory such as setting a new password, the users are prompted for their existing passwords.

A.20 How to import LDAP certificates?

In Configuration Manager, click **Actions** > **Import LDAP Server Certificates**.

A.21 How to modify user interface strings?

SSPR allows you to modify user interface text such as button labels, error messages, and event logs. When you modify a text in one language, the modified text overrides all default locale-specific values for that particular text.

To modify the user interface strings:

1. In Configuration Manager, click **Custom Text** and select any one of the following options:
   - **Display**: To modify the display text.
   - **Error**: To modify the error message.
   - **Message**: To modify messages except error messages.
2. Click **Actions** > **Save**.

A.22 How do I change the default language of SSPR?

You can override the default language through the locale parameter by using a link to SSPR. For example, http://sspr.example.com/sspr/?locale=it.

This sets the locale to Italian, regardless of the browser locale settings.

A.23 Can audit events be forwarded to syslog and compatible servers?

Yes. To enable forwarding audit events to syslog and compatible servers, configure the Syslog Audit Servers property. For more information about how to configure it, see Section 3.13, “Configuring Logging and Auditing,” on page 59.

A.24 Where can I see SSPR audit logs?

You can view the system audit logs under **Main Menu** > **Administration** > **System** and audit logs for user activities under **Main Menu** > **Administration** > **Current Status**.

A.25 Can SSPR authenticate by using custom attributes?

Yes, you can configure SSPR to use custom attributes for authentication. You need to configure **Username Search Filter** under **Settings** > **LDAP Directory** in Configuration Manager. For more information about how to configure, see Section 3.1, “Configuring LDAP Settings,” on page 37.

Example configurations:

- `(&(objectClass=inetOrgPerson)(myCurrentName=%USERNAME%)`

  In this example, the username value entered in the login page should match the attribute myCurrentName and the matched object should be of type InetOrgPerson.

- `(&(objectClass=person)(|(myCurrentName=%USERNAME%)(samAccountName=%USERNAME%)(cn=%USERNAME%)))`

  In this example, the matched object should be of type person and the username value on the login page should match with myCurrentName, samAccountName, or CN attributes.

A.26 How to access reports and logs in SSPR?

1. Log in to SSPR as an administrator.

   An SSPR administrator is one whose LDAP object matches the **Administrator Query String** (**Settings** > **LDAP Directory** > **Administrator Query String**).

2. In **Main Menu**, click **Administration**.
3. Under **System**, click any one of the following based on your requirement:
   - **System Details**: To see the status and health of LocalDB, Services, Java, and Java Threads.
   - **Event Log**: To see the event logs.
   - **Audit Log**: To see the audit log. Audit logs can also be forwarded to Syslog and compatible servers.

     For more information about how to configure SSPR to forward logs to the Syslog service, see Section 3.13, “Configuring Logging and Auditing,” on page 59.
   - **User Report**: To generate user reports. You can export reports in the CSV format.

NOTE: You can configure the log level in SSPR. For more information, see Section 3.13, “Configuring Logging and Auditing,” on page 59.