

User Guide

Novell[®] Self Service Password Reset

1.0.0

April, 2011

www.novell.com



Legal Notices

Novell, Inc. makes no representations or warranties with respect to the contents or use of this documentation, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc. reserves the right to revise this publication and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes.

Further, Novell, Inc. makes no representations or warranties with respect to any software, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc. reserves the right to make changes to any and all parts of Novell software, at any time, without any obligation to notify any person or entity of such changes.

Any products or technical information provided under this Agreement may be subject to U.S. export controls and the trade laws of other countries. You agree to comply with all export control regulations and to obtain any required licenses or classification to export, re-export or import deliverables. You agree not to export or re-export to entities on the current U.S. export exclusion lists or to any embargoed or terrorist countries as specified in the U.S. export laws. You agree to not use deliverables for prohibited nuclear, missile, or chemical biological weaponry end uses. See the [Novell International Trade Services Web page \(http://www.novell.com/info/exports/\)](http://www.novell.com/info/exports/) for more information on exporting Novell software. Novell assumes no responsibility for your failure to obtain any necessary export approvals.

Copyright © 2006-2011 Novell, Inc. All rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the express written consent of the publisher.

Novell, Inc.
404 Wyman Street, Suite 500
Waltham, MA 02451
U.S.A.
www.novell.com

Online Documentation: To access the online documentation for this and other Novell products, and to get updates, see www.novell.com/documentation.

Novell Trademarks

For Novell trademarks, see the [Novell Trademark and Service Mark list \(http://www.novell.com/company/legal/trademarks/tmlist.html\)](http://www.novell.com/company/legal/trademarks/tmlist.html)

Third-Party Materials

All third-party trademarks are the property of their respective owners.

Contents

About This Guide	7
1 Overview	9
2 System Requirements	11
2.1 Software Prerequisites	11
2.2 Supported Platforms	11
2.3 Supported Browsers	11
3 Installing Self Service Password Reset	13
3.1 Prerequisites	13
3.2 Installation Overview	13
3.3 Configuring the SSPR Database	14
3.3.1 Creating an SSPR Database	14
3.3.2 Configuring the JDBC Data Source	14
3.3.3 Completing the SSPR Installation	15
3.4 Configuring Novell eDirectory	15
3.4.1 eDirectory Schema	15
3.4.2 eDirectory Rights	15
3.4.3 Using the Idif file to Extend the Schema and Assign Rights	16
3.4.4 Completing the SSPR Installation	17
3.5 Configuring Active Directory	17
3.5.1 Extending the Active Directory Schema and Assigning Rights	17
3.5.2 Refreshing the Directory Schema	19
3.5.3 Completing the SSPR Installation	19
3.6 Deploying the PWM.war File	19
3.7 Integrating SSPR with the Client Login Extension	19
3.8 Enabling NMAS	20
4 Web Integration	21
4.1 Access Gateways	21
4.2 Request Parameters	22
5 Challenge Response Store Configuration	23
5.1 Installing and Configuring the SSPR Database	23
5.2 Configuring the Database Backup	23
5.3 Restoring Data from Backup	23
6 Policies	25
6.1 Password Policy	25
6.2 Challenge Policy	25

7	Localization	27
8	Sample Files	29

About This Guide

This guide provides an overview of Novell Self Service Password 1.0.0. The guide includes instructions on how to install, configure, and manage Novell SecretStore.

Audience

This guide is written primarily for network administrators.

Feedback

We want to hear your comments and suggestions about this manual and other documentation included with this product. Please use the User Comment feature at the bottom of each page of the online documentation, or go to www.novell.com/documentation/feedback.html, then enter your comments there.

Documentation Updates

For the most recent version of the *Novell Self Service Password Reset User Guide*, see (<http://www.novell.com/documentation/sspr10/index.html>).

Overview

1

You can reduce help desk costs by setting up self-service so users can recover from forgotten passwords or reset their passwords while viewing the rules you have specified in the password policy.

Self Service Password Reset enables end user to do the following:

- ◆ **Reset Password:** Users change their passwords while viewing the rules that you have specified in the password policy.
- ◆ **Change current password:** Users can change their current password.
- ◆ **Reporting:** Users can get report about different users details like intruder detection and daily statistics report.

System Requirements

2

Make sure the following requirements are met by the system where you will install the Self-Service Password Reset (SSPR).

- ♦ [Section 2.1, “Software Prerequisites,” on page 11](#)
- ♦ [Section 2.2, “Supported Platforms,” on page 11](#)
- ♦ [Section 2.3, “Supported Browsers,” on page 11](#)

2.1 Software Prerequisites

- ♦ Tomcat V6 and later
- ♦ JDK 1.5 and later
- ♦ Novell SSPR package

2.2 Supported Platforms

The SSPR application has been tested on the following platforms:

- ♦ Sun Java versions 1.5 and 1.6
- ♦ Tomcat versions 5.0.28 and 6.0.20
- ♦ iPhone Mobile

2.3 Supported Browsers

The following are the supported browsers:

- ♦ Microsoft Internet Explorer 6.0, 7.0, and 8.0
- ♦ Mozilla Firefox 3.6
- ♦ Google Chrome latest version

Installing Self Service Password Reset

3

The installation procedure varies depending on the type of datasource that you intend to configure to store the challenge response information. SSPR supports the SSPR database, eDirectory, and Active Directory as datasources.

NOTE: In all of these datasources, the information related to wordlists, eventlogs, user logins, and resets is stored in an embedded database. Many types of database are available, but the default is the Berkeley DB embedded database.

- ◆ [Section 3.1, “Prerequisites,” on page 13](#)
- ◆ [Section 3.2, “Installation Overview,” on page 13](#)
- ◆ [Section 3.3, “Configuring the SSPR Database,” on page 14](#)
- ◆ [Section 3.4, “Configuring Novell eDirectory,” on page 15](#)
- ◆ [Section 3.5, “Configuring Active Directory,” on page 17](#)
- ◆ [Section 3.6, “Deploying the PWM.war File,” on page 19](#)
- ◆ [Section 3.7, “Integrating SSPR with the Client Login Extension,” on page 19](#)
- ◆ [Section 3.8, “Enabling NMAS,” on page 20](#)

3.1 Prerequisites

Before installing Self Service Password Reset (SSPR), you must have installed the following:

- ◆ JDK 1.5 or later.

You can download and install the JDK software from [the Apache Tomcat Downloads Web site \(http://tomcat.apache.org/download-60.cgi\)](http://tomcat.apache.org/download-60.cgi).

- ◆ Apache Tomcat V6 or later.

You can download and install the Apache Tomcat software from [the Apache Tomcat Setup Web site \(http://tomcat.apache.org/tomcat-6.0-doc/setup.html\)](http://tomcat.apache.org/tomcat-6.0-doc/setup.html).

3.2 Installation Overview

The following steps are required to install SSPR:

- 1 Ensure that the prerequisites mentioned in [Section 3.1, “Prerequisites,” on page 13](#) are met.
- 2 Configure a datasource of your choice to store the challenge response information.
 - ◆ To configure the SSPR database as a datasource, see [Section 3.3, “Configuring the SSPR Database,” on page 14](#).

- ♦ To configure eDirectory as a datasource, see [Section 3.4, “Configuring Novell eDirectory,”](#) on page 15.
 - ♦ To configure Active Directory as a datasource, see [Section 3.5, “Configuring Active Directory,”](#) on page 17.
- 3 Deploy the `PWM.war` file to complete the installation. See [Section 3.6, “Deploying the PWM.war File,”](#) on page 19.

3.3 Configuring the SSPR Database

- ♦ [Section 3.3.1, “Creating an SSPR Database,”](#) on page 14
- ♦ [Section 3.3.2, “Configuring the JDBC Data Source,”](#) on page 14
- ♦ [Section 3.3.3, “Completing the SSPR Installation,”](#) on page 15

3.3.1 Creating an SSPR Database

- 1 Unzip the `<*.zip>` file to a location of your choice.

The files are extracted to the `<novell-sspr>` folder. This folder contains the `PWM.war` file and a supplemental folder.

- 2 Run the `<novell-sspr>\supplemental\database\InstallDB.bat` file to set up the SSPR database.
- 3 When you are prompted, enter the following details:
 - ♦ Boot password with a minimum of eight characters.
 - ♦ Password for the SSPR database administrator.
 - ♦ The absolute path of the directory where the database will be created.

After you specify the details, the SSPR database is created under the specified folder.

IMPORTANT: Take note of all the details. You need them when you configure a JDBC data source on the Tomcat server to enable the application to connect to the SSPR database.

3.3.2 Configuring the JDBC Data Source

You need to define a data source that is specific to your application and that is not visible to other Tomcat applications.

- 1 Copy `derby.jar` from `<novell-sspr>\supplemental\database\derby\lib` to the `<tomcat>\apachetomcat-6.0.29\lib` folder.
- 2 Edit the `Server.xml` file at `Tomcat/conf/` to create a resource definition for the `Context` element.

The `Context` element should look something like the following:

```
<Context ...>
...
  <Resource name="jdbc/EmployeeDB"
            auth="Container"
            type="javax.sql.DataSource"/>
```

```

        username="dbusername"
        password="dbpassword"
        driverClassName="org.hsql.jdbcDriver"
        url="jdbc:derby:<Path of the Database>/
ssprdb;dataEncryption=true;bootPassword=<BootPassword>;user=ssprdbadmin;p
assword=<Password of SSPR database administrator>"
        maxActive="8"
        maxIdle="4"/>
    ...
</Context>

```

3.3.3 Completing the SSPR Installation

After configuring the SSPR database, you must deploy the `PWM.war` file to complete the installation. For detailed information, see [Section 3.6, “Deploying the PWM.war File,”](#) on page 19.

3.4 Configuring Novell eDirectory

- ♦ [Section 3.4.1, “eDirectory Schema,”](#) on page 15
- ♦ [Section 3.4.2, “eDirectory Rights,”](#) on page 15
- ♦ [Section 3.4.3, “Using the ldif file to Extend the Schema and Assign Rights,”](#) on page 16
- ♦ [Section 3.4.4, “Completing the SSPR Installation,”](#) on page 17

3.4.1 eDirectory Schema

SSPR uses eDirectory attributes to store the following data about the users:

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

The SSPR package includes the `edirectory-schema.ldif` file in the `supplemental` directory. You use the file to extend the SSPR schema. The schema uses an auxiliary class that is added to the users to enable the removal of the auxiliary class and attributes from eDirectory in the future.

For detailed information about extending the schema, see, [“Using the ldif file to Extend the Schema and Assign Rights”](#) on page 16.

3.4.2 eDirectory Rights

SSPR requires permission to perform operations in eDirectory and uses two different eDirectory logins:

- ♦ A generic proxy user that is used for certain operations such as pre-authentication.
- ♦ After the user is authenticated, most of the operations are performed with the user's connection and permissions.

Proxy User Rights

By default, the following rights are required for the proxy user to the 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

By default, the following rights are required by each user for their own user entry:

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

To allow a password reset by any user in the container, you must set the rights of the parent level container to modify pwmResponseSet. This right allows any user in the container to modify this attribute for any other user in the container.

It is optional for SSPR to have rights to read the password. This is configured as part of the eDirectory password policies. SSPR randomly generates a password during the recovery process when a user uses the SSPR Forgotten Password recovery feature. When a user enters a new password, then SSPR can authenticate the user by using the random password and reset the password by using the user's credential.

For detailed information on assigning rights, see [“Using the ldif file to Extend the Schema and Assign Rights” on page 16](#).

3.4.3 Using the ldif file to Extend the Schema and Assign Rights

You can import the ldif file by using any one of the following tools:

- ◆ ConsoleOne Wizard
- ◆ iManager
- ◆ ICE command line
- ◆ Standard ldapmodify tools

Example: To import the schema file by using the ICE command line:

```
ice -SLDIF -f edirectory-schema.ldif -DLDAP -s 192.168.75.132 -d
cn=admin,ou=ou,o=o -w password
```

NOTE: If you don't want to use the standard SSPR schema, all of the attributes used by SSPR can be changed by using the configuration editor.

3.4.4 Completing the SSPR Installation

After configuring eDirectory, extending the schema, and assigning rights, you must do the following:

1. Deploy the `PWM.war` file to complete the installation. For detailed information, see [Section 3.6, “Deploying the PWM.war File,”](#) on page 19.
2. (Optional) Enable NMAS. For detailed information, see [Section 3.8, “Enabling NMAS,”](#) on page 20

3.5 Configuring Active Directory

Before you install SSPR, you must first extend the Active Directory schema and assign user rights.

- ♦ [Section 3.5.1, “Extending the Active Directory Schema and Assigning Rights,”](#) on page 17
- ♦ [Section 3.5.2, “Refreshing the Directory Schema,”](#) on page 19
- ♦ [Section 3.5.3, “Completing the SSPR Installation,”](#) on page 19

3.5.1 Extending the Active Directory Schema and Assigning Rights

SSPR leverages the directory to store and manage the SSPR data. To accomplish this, SSPR extends the directory schema to add three 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. Authorizing read or write rights to the SSPR directory schema attributes is referred to as assigning user rights.

The SSPR Microsoft Active Directory schema extension executable extends the schema on the server and enables you to assign user rights. You must determine which containers and organizational units need SSPR access, and 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 Microsoft Active Directory schema to the root of the domain and assign rights to each container and organizational unit below the root.

IMPORTANT: If the Microsoft Active Directory instance is deployed by copying and running the `ssprAdSchema.exe` file from another location, you must copy the entire folder containing the Microsoft Active Directory schema and configuration files to the new preferred location. The Microsoft Active Directory schema and configuration files must be located in the same folder for the Active Directory instance to be deployed successfully.

Extending the Schema

The following instructions apply to the configuration of the Microsoft Active Directory instance stored and administered on a separate server from the Active Directory server domain controller.

- 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 `ssprADSchema.exe`.

The SSPR Active Directory Schema dialog box is displayed.

- 3 Select *Extend Active Directory Schema*.
- 4 Click *OK*.

The following SSPR attributes are added to the Directory schema:

- ♦ `pwmEventLog`
- ♦ `pwmResponseSet`
- ♦ `pwmLastPwdUpdate`

A confirmation message is displayed.

IMPORTANT: If the Microsoft Active Directory instance is deployed by copying and running the `ssprADSchema.exe` file from another location, you must copy the entire folder containing the Microsoft Active Directory Schema and configuration files to the new preferred location. The Microsoft Active Directory Schema and configuration files must be located in the same folder for the Active Directory instance to deploy successfully.

- 5 Click *OK* to return to the Active Directory Schema dialog box.

Because the directory schema is now extended, you must assign access rights to the relevant containers and organizational units.

If you have previously extended the schema, a message listing the existing schema appears. Ignore this message.
- 6 Continue with [“Assigning User Rights” on page 18](#) to assign user access rights to the relevant containers and organizational units.

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, the rights filter down to all associated user objects. Unless you are required to do so, it is not necessary to assign rights at the individual user object level.

- 1 Run `ssprADSchema.exe`, which is found in `supplemental\Schema\AD`.
- 2 Select *Assign User Rights*, then click *OK*.

The Assign Rights to This Object dialog box is displayed.

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 the Assign rights to this object field. The confirmation dialog box appears.
- 4 Click *OK* to return to the Active Directory Schema dialog box.

- 5 Repeat [Step 2](#) to [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 After all the required rights are successfully assigned, click *OK* to return to the Active Directory Schema dialog box.
- 7 Click *Cancel*.

NOTE: You can extend the rights to the objects any time after the schema is extended. 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.

3.5.2 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*.
- 3 On the *Console* menu, click *Exit* to close the MMC.

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

3.5.3 Completing the SSPR Installation

After configuring eDirectory, you must run the `PWM.war` file to complete the SSPR installation. For detailed information, see [Section 3.6, “Deploying the PWM.war File,”](#) on page 19.

3.6 Deploying the PWM.war File

After configuring any datasource of your choice, use the following procedure to complete the installation:

- 1 Copy `PWM.war` from the `<novell-sspr>` folder to the `Tomcat\webapps` folder to complete the SSPR installation .

3.7 Integrating SSPR with the Client Login Extension

You should use the Client Login Extension (CLE) to enable the reset password functionality. The Client Login Extension facilitates password self-service by adding a link to the Novell Credential Provider (MSCP) and Microsoft GINA login clients.

To integrate SSPR with the Client Login Extension:

- ◆ Specify the URL that the Client Login Extension restricted browser uses to connect to the Forgotten Password page of the User Application. You can use either a DNS name or an IP address. An example URL using a DNS name that links to the Forgotten Password page is as follows:

```
https://<IP :PORT>/pwm/public/ForgottenPassword.jsf
```

NOTE: CLE supports only the HTTPS protocol, and the URL varies, depending on your application server.

If you are using Tomcat as the host application server, see “[SSL Configuration How-To](http://tomcat.apache.org/tomcat-6.0-doc/ssl-howto.html)” on the [Apache Tomcat Web site](http://tomcat.apache.org/tomcat-6.0-doc/ssl-howto.html) (<http://tomcat.apache.org/tomcat-6.0-doc/ssl-howto.html>).

For detailed information on Client Login Extension, see the [Client Login Extension Administration Guide](http://www.novell.com/documentation/cle37/ns1_cle/data/front.html) (http://www.novell.com/documentation/cle37/ns1_cle/data/front.html).

3.8 Enabling NMAS

When you use eDirectory as your SSPR datasource, you can enable NMAS for better error reporting and integration with eDirectory.

SSPR performs all operations against eDirectory by using generic LDAP calls unless the NMAS support is enabled.

To enable NMAS:

- 1 Select *Configuration Editor > eDirectory* .
- 2 Set the value of *Always Use Proxy* as *True*.

If the option to store NMAS responses is enabled, then whenever a user saves responses by using SSPR, these responses are stored in NMAS. This allows Novell forgotten password clients to use the same responses. However, SSPR itself cannot directly use these responses for forgotten passwords.

Web Integration

Self Service Password Reset (SSPR) has been designed and tested to work with portals and Web access gateways. After a user completes a function on the SSPR page, the user is redirected to the `forwardURL` site.

SSPR uses the following two configurable URLs:

- ♦ **forwardURL:** By default, the user is redirected to the `forwardURL` site.
- ♦ **logoutURL:** If the password has been modified and the *Logout After Password Change* setting is set to *True*, then the user is redirected to the `logoutURL` site instead of the `forwardURL` site.

NOTE: These URLs are configured as part of the PWM 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.

There are two instances when a user is not immediately redirected to the `forwardURL`:

- ♦ When *Check Expiration During Authentication* is set to *True* and the user's password is about to expire, then the user is redirected to the change password screen instead of the `forwardURL` site. After changing the password, the user is redirected to `forwardURL` or `logoutURL`.
- ♦ When *Force Setup of Challenge Responses* is set to *True*, 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 module, the user is then redirected to the `forwardURL` or `logoutURL`.
- ♦ [Section 4.1, "Access Gateways," on page 21](#)
- ♦ [Section 4.2, "Request Parameters," on page 22](#)

4.1 Access Gateways

SSPR supports basic authentication. If an `http Authorization` header is present, SSPR uses the credentials in the header to authenticate the user.

Some parts of SSPR, such as the forgotten password modules and new user registration, must be publicly accessible. To support this, configure the URLs as public or restricted by your proxy or gateway configuration.

For example, assume that SSPR is set up so that the user enters the following URL for access:

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

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

Table 4-1 Adding Protected URLs to SSPR

URL	Mode
password.example.com/*	Public

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

If your access gateway supports it, you should configure the gateway to redirect to SSPR if the password expires.

`http://password.example.com/pwm/private/ChangePassword?passwordExpired=true`

4.2 Request Parameters

On the locations where you specify URLs, you can specify different commands as parameters to SSPR. The parameters are case sensitive.

Example: `http://password.example.com/pwm/private/ChangePassword?passwordExpired=true&forwardURL=http://www.example.com`

Challenge Response Store Configuration

5

- ♦ [Section 5.1, “Installing and Configuring the SSPR Database,” on page 23](#)
- ♦ [Section 5.2, “Configuring the Database Backup,” on page 23](#)
- ♦ [Section 5.3, “Restoring Data from Backup,” on page 23](#)

5.1 Installing and Configuring the SSPR Database

For detailed information on installing and configuring an SSPR database, see [Section 3.3, “Configuring the SSPR Database,” on page 14](#).

5.2 Configuring the Database Backup

SSPR allows you to configure the way your backup files are created and stored. You can configure automatic backups by defining the interval and path to store the backups.

- 1 Select *Configuration Editor > Advanced* .
- 2 Set the value of *PwmDB Backup* as *True*.
- 3 In the *PwmDB Backup Directory* text box, type the location where you want the backup to be stored.

The backup directory should be an absolute value. The backup is created in a folder that carries the date and time of the backup as its name. This folder is contained within the *PwmDB Backup* directory.

- 4 Enter the interval duration in *PwmDB Backup Frequency* to configure the frequency at which the database backup should be performed. By default, it is 24 hours.

5.3 Restoring Data from Backup

- 1 Unzip the `<*.zip>` file to a location of your choice.
The files are extracted to the `<novell-sspr>` folder. This folder contains a `PWM.war` file and a supplemental folder.
- 2 Run the `<novell-sspr>\supplemental\database\RestoreDB.bat` file to restore the database.
- 3 The batch file prompts you to enter the following details:
 - ♦ The name of the current database that needs to be restored.
 - ♦ The boot password with minimum of eight characters.
 - ♦ The password for the SSPR database administrator.
 - ♦ The absolute path of the directory where the database was created.

NOTE: Use the same location that you specified when you configured the database backup.

You can use password policies to increase security by setting rules on how users create their passwords. You can also decrease the help desk costs by providing users with self-service options for forgotten passwords and for resetting passwords.

- ◆ [Section 6.1, “Password Policy,” on page 25](#)
- ◆ [Section 6.2, “Challenge Policy,” on page 25](#)

6.1 Password Policy

Each password policy setting is available in the Self Service Password Reset configuration. These password policies represent the *minimum* policies applicable to the user.

For example, If you set the directory setting as Novell eDirectory and configured *Read eDirectory Password Policy* as *True*, then SSPR tries to locate a Universal Password policy configured for that user. If such a policy is found, the policy is merged with the settings in the policies set in the PWM configuration. The most restrictive setting is used.

Example: If the SSPR configuration sets the minimum password length as *five* and the Universal Password policy sets it as *four*, the minimum password length for the user is *four*.

6.2 Challenge Policy

Challenge questions are used to verify the user identity identity during the login when a user has forgotten his or her the password. At setup time, SSPR can be configured to allow the users to:

- ◆ Enter all random password questions.
- ◆ Enter only a minimum number of required random questions.

Localization

7

Self Service Password Reset (SSPR) is localized in the following languages:

- ◆ Czech
- ◆ Dutch
- ◆ French
- ◆ German
- ◆ Italian
- ◆ Polish
- ◆ Portugese
- ◆ Spanish

NOTE: Only pages and configuration options that affect the end users are localized. Most administrator screens are not localized.

Sample Files

8

The following sample files are available at `\supplemental\conf`:

- ◆ `PwmConfiguration-Edir(pure).xml`
- ◆ `PwmConfiguration-AD(pure).xml`
- ◆ `PwmConfiguration-Edir.xml`
- ◆ `PwmConfiguration-AD.xml`

Example: After authenticating the user rights, you can modify `edirectory-rights.ldifs`. In this sample file, the proxy user name is `cn=PwmProxy` and user container is `ou=USERS,o=O`.

