User Guide

Self Service Password Reset 2.0.0

April 2012

Novell

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/) for more information on exporting Novell software. Novell assumes no responsibility for your failure to obtain any necessary export approvals.

Novell, Inc.
1800 South Novell Place
Provo, UT 84606
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)

Third-Party Materials

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

Source Code: SSPR is developed using PWM, which is governed the by GNU-GPL 2.0 license. For more information, see GNU General Public Licence.

To download the source code of SSPR, see Novell Downloads.

Contents

About This Guide

This guide provides an overview of Novell Self Service Password 2.0.0. The guide includes instructions on how to install, configure, and manage Novell Self Service Password Reset.

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/sspr20/index.html).

1 Overview

There are chances when a user might forget the password and has to rely on the help desk for support. Self Service Password Reset (SSPR) helps reduce help desk costs by enabling users to reset the password based on the rules specified in the password policy.

SSPR enables end user to do the following:

- **Change current password:** Users can change their current password.
- **Challenge response setup:** SSPR allows an Administrator to configure a set of questions which can be a combination of random and required questions. The users can save the responses for these set of questions and store them using SSPR. The responses are used to validate the authenticity of the user when the user tries to change or reset their directory password.
- **Reset forgotten password:** Users can reset their directory password by answering challenge questions that are configured and stored using SSPR. SSPR stores the responses in the standard RDBMS database, LDAP server, or Novell NMAS repositories as configured.
- **New user registration:** Using SSPR you can create new user profiles.
- **Simplify help desk support response:** SSPR has a helpdesk module which can be leveraged by the help desk users to change a users password.

In addition to the above features administrators of SSPR can generate reports from the administration modules such as; intruder-lockout manager, online log viewer, daily statistics viewer and user information debugging.

2 Prerequisites

The following sections describe the hardware, operating system, browser, and software requirements for SSPR.

2.1 System Requirements

- 512 MB of Java heap memory. Heavily utilized sites may require larger heap sizes.
- 1 GB of disk space for the ssprDB for default configurations

2.2 Software Prerequisites

- Apache Tomcat V6 or later. To download Apache Tomcat, goto Apache Tomcat Downloads (http://tomcat.apache.org/download-60.cgi).
- JDK 1.5 or later.

2.3 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 (32-bit and 64-bit)
- SUSE Linux Enterprise Server 10 or later

2.4 Supported Browsers

- Mozilla Firefox 6.0 and later
- Microsoft Internet Explorer 8.0

NOTE: You might encounter minor compatibility issues when using Internet Explorer to edit the SSPR configurations.

3 Installation

3.1 Setting up a Secure Channel Between the Application Server and LDAP Server

In a production environment, SSPR should trust the LDAP server’s certificate. The three scenarios based on which a secure channel can be established are:

- Use a certificate issued by a generally 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.
- Use a certificate issued by a private certificate authority, like Novell iManager or Microsoft Active Directory. In this case the certificate(s) of that certificate authority need(s) to be imported into the java certificate database.
- Use a self signed certificate. In this case, the self signed certificate should be imported into the java certificate database

To export the certificate from eDirectory using iManager, see (http://www.novell.com/communities/node/8757/exporting-ssl-certificate-using-imanager).

To export certificate from Active Directory, see (http://technet.microsoft.com/en-us/library/cc772393).

3.1.1 Importing Certificate into Java Keystore

The certificate database is located in the following location:

`JAVA_HOME\lib\security\cacerts`

where `JAVA_HOME` is the directory where java is installed.

Use the `keytool` to import the file

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

The `keytool` prompts for a password, which is `changeit` by default.

3.2 Installing the sspr.war File

Ensure that the prerequisites are met as mentioned in Chapter 2, “Prerequisites,” on page 9.

- Shutdown Tomcat.
- Unzip the Novell SSPR package and locate the `sspr.war` file from `<novell-sspr>\SSPR.war`
- Copy the `sspr.war` file from the `<novell-sspr>` folder to the `Tomcat/webapps` folder to complete the SSPR installation.
- Start Tomcat

  To Start or Stop Tomcat on Windows Platform:

  - **Tomcat as service:**
    - Go to *Start -> All Programs-> Apache Tomcat 5.0 -> Monitor Tomcat* to start Tomcat as a service.
    - Right-click on the Tomcat icon on the taskbar to start or stop the Tomcat service.
  - Tomcat as standalone:
    - To shutdown Tomcat, go to the bin folder of Tomcat and execute `shutdown.bat` in the command line.
    - To start Tomcat, go to the bin folder of Tomcat and execute `start.bat` in the command line

    To start Tomcat execute `start.bat` in the command line

  To start or stop Tomcat on Linux Platforms:

  - To stop Tomcat, run the `shutdown.sh` script which is available in the `<Tomcat_Home>/bin` folder.
  - To start Tomcat, run the `startup.sh` scripts which is available in the `<Tomcat_Home>/bin` folder.

3.3 Setting up a Secure Channel Between the Client and the SSPR portal (Optional)

Since SSPR is a web based application, it can be accessed with Internet Explorer or Firefox using http. However, you can also access SSPR using https. To set up a secure channel between the browser and application (https):

1. Create a self signed certificate in the cacerts store. In the command line goto `%JAVA_HOME%\bin\` folder and execute the following command:

   ```
   keytool -genkey -alias tomcat -keyalg RSA -keystore ../<jre6>/lib/security/
   cacerts
   ```

2. Enter keystore paasword as `changeit`.
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 one more attribute value called keystoreFile="${java.home}/lib/security/cacerts" keystorePass="changeit"
4. Restart Tomcat.

4 Configuration

4.1 Configuring Novell eDirectory for SSPR

Configure eDirectory if you want the backend directory as eDirectory. If the backend directory to be configured is Active Directory, goto Section 4.2, “Configuring Active Directory for SSPR,” on page 14.

4.1.1 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.

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

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

- iManager
- ICE command line
- Standard `ldapmodify` tool

Example: Execute the following command in eDirectory using LDAP Modify tool:

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

password -f `edirectory-schema.ldif`

The following SSPR attributes are added to the Directory schema:

- pwmEventLog
- pwmResponseSet
- pwmLastPwdUpdate
- pwmGUID

4.1.3 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-authenticaton.
- 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.

After configuring eDirectory for SSPR, goto Section 4.3, “Configuring SSPR,” on page 16.

4.2 Configuring Active Directory for SSPR

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

4.2.1 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.

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 `ssprADSschema.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.
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.

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 `ssprADSschema.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.

4.2.2 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.

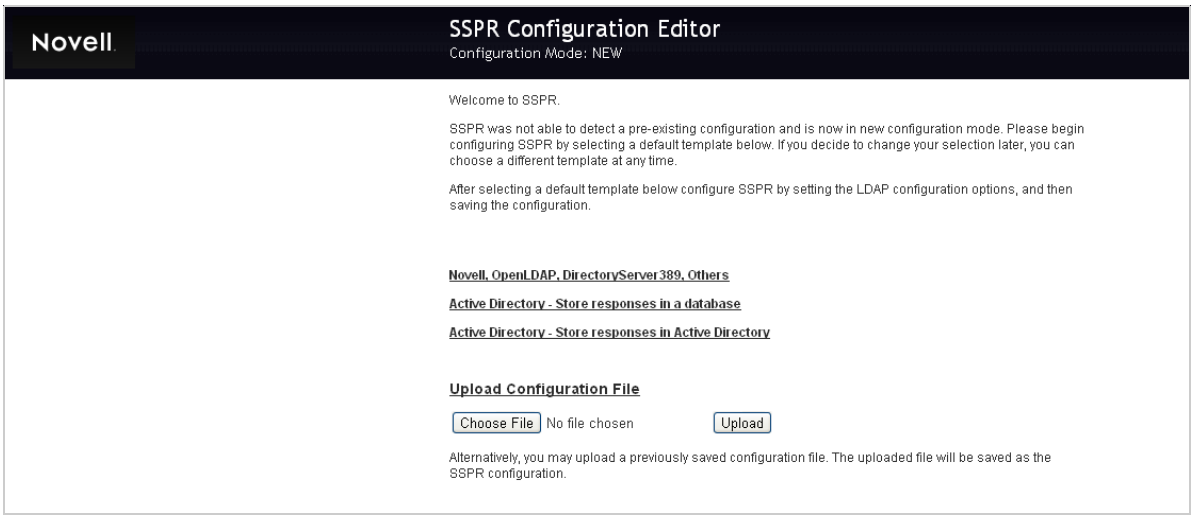
After configuring Active Directory for SSPR, goto Section 4.3, “Configuring SSPR,” on page 16

4.3 Configuring SSPR

To access SSPR application, open a web browser and navigate to http:// <host_name>:<port_number> / sspr.

- `<host_name>`: ip address or host name of the server on which SSPR is deployed.
- `<port_number>`: http port number of Tomcat server. Default http port number is 8080.

NOTE: SSPR will run on http, however to set up a secure channel between the browser and application, enable https. To enable https, see Section 3.3, “Setting up a Secure Channel Between the Client and the SSPR portal (Optional),” on page 12



- Novell, OpenLDAP, DirectoryService389, Others: Select this option if the backend directory server is eDirectory and you would want to store the challenge responses in eDirectory.
- Active Directory - Store responses in a database: Select this option if the back end directory server is active directory and you would like to store the challenge response information in a database of your choice. SSPR provides support for most of the commercially available RDBMS database(s).

  Ensure that the *Forgotten Password* Module is configured properly. To configure Forgotten Password module, goto *Configuration Editor* > *Modules* > *Forgotten password*.
- Active Directory - Store responses in Active Directory: Select this option if the back end directory server is Active directory you would want to store the challenge responses in Active Directory.

After selecting an option, configure the following options appropriately. This sections explains only the basic settings which are just enough to start using SSPR. Refer the Configuration editor for more options:

- Section 4.3.1, “LDAP Directories,” on page 17
- Section 4.3.2, “Challenge Policy,” on page 18
- Section 4.3.3, “Database,” on page 18
- Section 4.3.4, “Password Policy,” on page 19

4.3.1 LDAP Directories

Configure the following basic settings:

- **LDAP URLs:** List the LDAP servers in URL format. SSPR will use these servers in a fail-over configuration. The servers are used in order of appearance in this list. If the first server is unavailable SSPR will use the next available server in the list. SSPR will then periodically fall-back to the first server to see if it is available.
  - For secure SSL, use the *ldaps://servername:636* format
  - For plain-text servers, use *ldap://serverame:389* format (not recommended)
- **LDAP Proxy User:** LDAP Proxy User used by SSPR to access the ldap directory. This user must have rights to browse users, and manage password attributes on the user object.

This value should be in LDAP distinguished name format, even if your ldap directory accepts other types of values for the bind DN. For example, `cn=admin,o=example` or `cn=administrator,cn=users,dc=subdomain,dc=domain,dc=net`.

- **LDAP Proxy Password:** The corresponding password of *LDAP Proxy User* user.
- **LDAP Contextless Login Root:** Base context to search for usernames during login.
- **SSPR Admin Query String:** This query string is used to detect if a user is a SSPR Administrator. An LDAP query is performed during SSPR login against the logged in user to determine if the user is a SSPR Administrator. If the user matches the query, then the user is considered a SSPR administrator.

4.3.2 Challenge Policy

Configure the following basic settings:

- **Force Response Setup:** If true, the user will be directed to configure challenge/response before logging out of SSPR. This accounts for new user creation and activation, and other scenarios. The user is forced check to see if eligible for allowSetup, and also if they do not have valid responses already configured.

  NOTE: When *Force Response Setup* is set to *True* and you click *Cancel*, ensure that you enter the responses before exiting the page.

- **Random Questions for Challenge/Response:** Some of these questions will be presented to the user during forgotten password.

  Format: question::minimumLength::maximumLength

- **Required Questions for Challenge/Response:** The user must supply answers for all of these questions when setting up their responses.

  Format: question::minimumLength::maximumLength

- **Minimum Random Required:** Minimum number of random questions required at time of forgotten password recovery.
- **Minimum Random Challenges Required During Setup** The minimum number of random questions the user is required to complete during Response Setup

4.3.3 Database

The RDBMS settings will be applicable only if you have selected *Active Directory - Store responses in a database* in the *SSPR Configuration Editor*.

SSPR uses two types of databases:

- **SSPRDB:** The SSPRDB is a local, embedded database that is used by SSPR for storage of local data. In most cases, the SSPRDB requires no administration or maintenance, and the defaults are sufficient.
- **RDBMS Database:** If configured, 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. Upon startup, SSPR will connect to the database and create any necessary tables. Multiple SSPR server instances can be configured for the same database instance.

  Configure the following options if RDBMS is selected:

  - Database Class
  - Database Connection String

- Database Username
- Database Password

4.3.4 Password Policy

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.

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 SSPR configuration. The most restrictive setting is used.

5 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 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.

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.

5.1 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/sspr
```

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

Table 5-1 Adding Protected URLs to SSPR

URL	Mode
password.example.com/*	Public
password.example.com/sspr/private/*	Restricted
password.example.com/sspr/admin/*	Restricted
password.example.com/sspr/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/sspr/private/ChangePassword?passwordExpired=true`

5.2 Request Parameters

Various commands to SSPR can be specified as parameters on URLs. Parameters are case sensitive. These request parameters can be placed on any link that will access SSPR.

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

Parameter	Description	Example
passwordExpired	Setting this parameter will make SSPR override the state of the user's password expiration.	`passwordExpired=true`
forwardURL	Set the forward URL to (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`
pwmLocale	When a valid browser locale code is provided, SSPR will switch to the given locale to display all localized text	`pwmLocale=en`

5.3 Command Servlet

The `CommandServlet` allows you to redirect a user to SSPR and have it perform some specific command. The `CommandServlet` functions are used during a user's login sequence to a portal or other landing point.

The `CommandServlet` functions work best when used with a proxy, access gateway, or some other device that will auto-authenticate the user. Otherwise, the user will have to authenticate to SSPR during every login.

The `CommandServlet` calls can be combined with any of the request parameters described earlier, such as the `forwardURL parameter`.

For Example, the user login redirect sequence will be as mentioned in the following table:

URL Example	Description
`http://portal.example.com`	Initial request from browser.
`http://portal.example.com/Login`	Access gateway redirects to login page.
`http://portal.example.com/`	Access gateway redirects back to portal root.
`http://portal.example.com/index.html`	Web server redirects 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 a URLEncoded `forwardURL` value.
`http://portal.example.com/portal/main.html`	SSPR redirects back to the actual portal URL.

The `index.html` described above would have 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>
```

5.3.1 Command

- **Command:** `checkExpire`

  URL: http://password.example.com/sspr/private/CommandServlet?processAction=checkExpire

  Description: Checks the user's password expiration. If the expiration date is within the configured threshold, the user will be required to change password.

- **Command:** `checkResponses`

  URL: http://password.example.com/sspr/private/CommandServlet?processAction=checkResponses

  Description: Checks the user's challenge responses. If no responses are configured, the user will be required to set them up.

- **Command:** `checkProfile`

  URL: http://password.example.com/sspr/private/CommandServlet?processAction=checkProfile

  Description: Checks the user's profile. If the user's attributes do not meet the configured requirements, the user will be required to set their profile attributes..

- **Command:** `checkAll`

URL: http://password.example.com/sspr/private/CommandServlet?processAction=checkAll

Description: Calls checkExpire, checkResponses and checkProfile consecutively.