IceWall SSO

Version 10.0

Installation Guide for Dynamic Menu Portal

August 2010

Printed in Japan

HP Part No. B1544-97004

Rev.111031A

Notice

The information contained in this document is subject to change without notice.

Meticulous care has been taken in the preparation of this document, however, if a questionable or erroneous item, or an omission of content is found, please contact us.

Hewlett-Packard shall not be liable for errors contained herein or for incidental or consequential damage in connection with the furnishing, performance or use of this document.

This manual and media, such as the CD-ROM supplied as a part of the product's package, are only to be used with this product.

– Table of Contents –

1 Introduction

Dynamic Menu Portal is an expanded version of the earlier Dynamic Menu with the added functions of a simple portal. This manual describes an overview of Dynamic Menu Portal, installation and sample setup methods, a guide to customizing the standard HTML, and other reference materials.

For more information on the earlier Dynamic Menu, see the “IceWall SSO Sample Setup Guide” and “IceWall SSO Reference Manual.”

1.1 Version designations in the text

The table below gives the meanings of the version designations added to the text.

Designation	Meaning
10.0	An item added with the version enclosed in the square. In this case, the designation indicates the item was added with 10.0.
10.0	An item where the specification was changed or function added with the version enclosed in the oval. In this case, the designation indicates a specification change or added function with 10.0.

2 Overview

This chapter describes an overview of Dynamic Menu Portal.

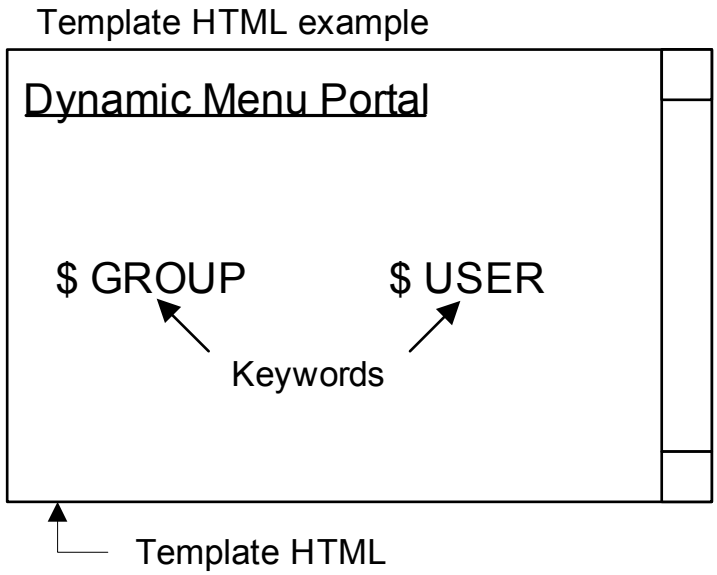
2.1 Dynamic Menu Portal functions

Dynamic Menu Portal provides simple portal functions. For example, it can display content for the group a user belongs to and it can also display content for the individual user. It provides dynamic content display functions to implement a portal.

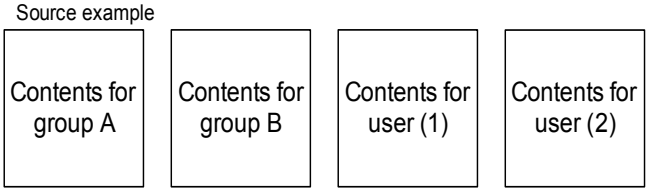
2.2 Dynamic Menu Portal specifications

Dynamic Menu Portal implements the display of dynamic content with the following structure.

The administrator provides an HTML file called “Template HTML (Template)” which uses keywords to describe the parts that display dynamic content.



The administrator also prepares in advance the “Source” that corresponds to the dynamically displayed content in HTML format.



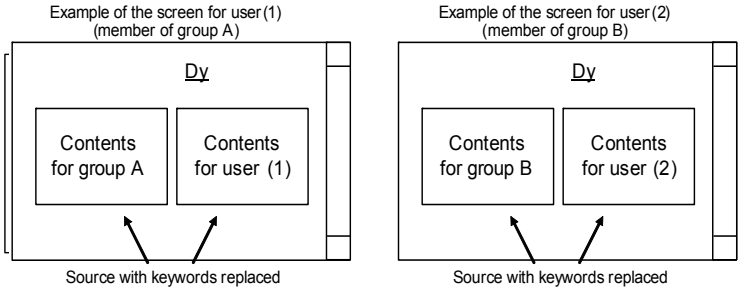
When the user accesses Dynamic Menu Portal, the keywords are replaced (“Replace”) with the “Source,” and the page is displayed.

Specific “Condition” can be specified when replacing (“Replace”) the keyword. The administrator can specify these conditions within the configuration file.

Configuration file example

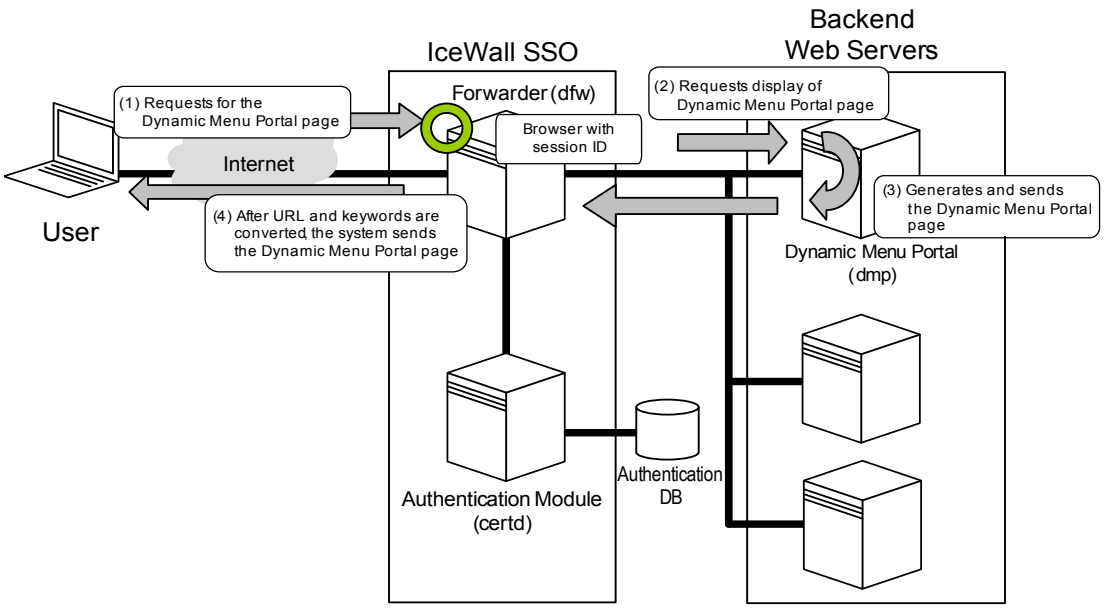
```
Condition (1): If the user is a member of group A
Condition (2): If the user is a member of group B
Condition (3): If the user it user (1)
Condition (4): If the user it user (2)

Source (1): Contents for group A
Source (2): Contents for group B
Source (3): Contents for user (1)
Source (4): Contents for user (2)

Replace (1): If condition (1) is true,
             $GROUP is replaced with source (1).
             $USER is replaced with source (3).
Replace (2): If condition (2) is true,
             $GROUP is replaced with source (2).
             $USER is replaced with source (4).
```

With the structure like this, a page can be displayed according to the conditions.



2.3 Dynamic Menu Portal processing flow

The following diagram shows the processing flow for displaying dynamic content by Dynamic Menu Portal.



(1) The user enters the URL for the Dynamic Menu Portal page in the browser.
(2) Once the login transaction has been completed, Forwarder sends a request to Dynamic Menu Portal to display the page.
(3) Dynamic Menu Portal, which receives the request from Forwarder, performs the following processes to create and send the page:
   a) Reads the configuration file
   b) Checks the login status
   c) Searches for keywords inside the template HTML file
   d) Evaluates the conditions
   e) Acquires the source and replaces the keywords if the conditions are satisfied
   f) Steps c, d, and e are repeated in the order described in the configuration file.
(4) Dynamic Menu Portal sends the created page (template HTML with all replacements completed) to Forwarder. Forwarder performs URL conversion and keyword conversion on the received page and sends it to the user.

3 System Requirements

This chapter describes the system requirements of Dynamic Menu Portal.

- Server
  [HP-UX]
  HP server series

  [Linux]
  HP ProLiant or equivalent compatible server (recommended by HP)

- OS
  [HP-UX]
  HP-UX 11i v3 (Itanium) 10.0

  [Linux]
  Red Hat Enterprise Linux Ver5.4 (x86_64) or later 10.0*1

- Web application server (servlet container)
  [HP-UX]
  HP-UX Tomcat-based Servlet Engine 5.5.x (x is 27 or higher) 10.0*2*3

  [Linux]
  Apache Tomcat 5.5.23 *4

- Java SDK (Java Development Kit)
  [HP-UX]
  HP J2SE JDK 6.0.x (x is 06 or higher) 10.0*3

  [Linux]
  OpenJDK 6.0 (build 1.6.0-b09) *4

- IceWall SSO
  IceWall SSO 10.0 or higher (It must operate as the backend of IceWall SSO Forwarder and be able to communicate with the IceWall SSO Authentication Module.)

*1 Operation is not guaranteed in environments where NSA Security-Enhanced Linux (SELinux) is enabled.
*2 Only OS vendor supplied packages of Tomcat are supported. Customer compiled packages are not supported.
*3 Only HP supplied modules of HP-UX JDK are supported. HP-UX JDK can be downloaded from http://www.hp.com/go/java.
*4 Use the package bundled with Red Hat Enterprise Linux 5.4.

4 Installation

This chapter describes how to install Dynamic Menu Portal.

4.1 Installation

This section describes how to install Dynamic Menu Portal.

Before installing Dynamic Menu Portal, ensure that it is not already installed. (The installation cannot be overwritten. If it is already installed, it must first be uninstalled.)

(1) Log in as root to the server where Dynamic Menu Portal will be installed.

(2) Insert the IceWall SSO CD-ROM into the CD-ROM drive.

(3) Mount the CD-ROM.

■ HP-UX ■
Check the CD-ROM drive's devicefile name.
(Devicefile name example: /dev/dsk/c1t2d0)

```
# ioscan -fn | more
```

Mount the CD-ROM.

```
# mount [devicefile name] [mount point]
```

Example: When the devicefile name is ": /dev/dsk/c1t2d0" and the mount point is "SD_CDROM"
mount /dev/dsk/c1t2d0 /SD_CDROM

■ Linux ■
Mount the CD-ROM.

```
# mount -t iso9660 /dev/cdrom /mnt/cdrom
```

* This is an example when the mount point is /mnt/cdrom. If the mount point does not exist, create one with the mkdir command.

(4) Install Dynamic Menu Portal.

■ HP-UX ■
For HP-UX, the installation package is different respectively depending on the server and OS type.

HP-UX 11i v3 (Itanium)

```
# swinstall -s /SD_CDROM/SSO/hpux/IceWall-SSO-ia64_e.sw dmp
```

■ Linux ■

```
# rpm -ivh --nodeps /mnt/cdrom/SSO/linux/IceWall-SSO-dmp_e-
10.0.
0-1.x86_64.rpm
```

(5) Check the installation files.
Dynamic Menu Portal is installed to a directory under /opt/icewall-sso. The directory and file names after installation are provided below:

Directory and file names (permission)		
/dmp(775)	/bin(775)	dp.war(644) sample.war(644)
	/config(775)	dmp.xml(644) log4j.properties(644)
	/html(755)	dmp_nologin.html(644) dmp_reqaclerr.html(644) 10.0 dmp_syserr.html(644) menu.html(644)
	/chtml(755)	dmp_nologin.html(644) dmp_reqaclerr.html(644) 10.0 dmp_syserr.html(644) icewall_logo_s.gif(444) menu.html(644)
	/sample(755)	user01.html(644) user02.html(644) user03.html(644) hp.html(644) scc.html(644) morning.html(644) afternoon.html(644)
/logs(777)		

* When using an Authentication Module failover, grant write permission for the Dynamic Menu Portal configuration file to the user executing the web application server.

4.2 Extracting the dp.war file

The following procedure shows how to extract the dp.war file.

(1) Log in as root to the server where Dynamic Menu Portal was installed.

(2) Move to this directory.

```
# cd /opt/icewall-sso/dmp/bin
```

(3) Create a directory for extracting the files, and move to this directory.

```
# mkdir dp
# cd ./dp
```

(4) Extract the dp.war file using the jar command.

```
# jar xfv ../dp.war
```

(5) Change the owner of the extracted files to one of the users below.
Tomcat server: root or user who starts the Tomcat server
Example: changing the owner to www:other

```
# chown -R www:other /opt/icewall-sso/dmp
```

4.3 Deploying to the server

The following procedure shows how to deploy Dynamic Menu Portal to a Tomcat server.
The example below shows the case when the Tomcat server is installed to the [Tomcat installation directory].

(1) Log in as the user who runs the Tomcat server to the server where Dynamic Menu Portal was installed.

(2) If the Tomcat server is running, execute the following command to stop the Tomcat server.

```
$ [Tomcat installation directory]/bin/shutdown.sh
```

(3) Open server.xml with an editor.

```
$ vi [Tomcat installation directory]/conf/server.xml
```

(4) Add the settings below inside the <Host> tag that defines the information for the virtual host where Dynamic Menu Portal runs.

```
<Context path="/dp" docBase="/opt/icewall-sso/dmp/bin/dp"
debug="0" reloadable="true"/>
```

(5) Save server.xml and close the editor.

(6) Execute the following command to start the Tomcat server.

```
$ [Tomcat installation directory]/bin/startup.sh
```

4.4 Verifying installation with the sample page

To verify the operation of Dynamic Menu Portal, it is recommended that you check the sample page according to “6 Sample Setup.”

4.5 Obtaining version information

When you need to obtain the version information of binary modules, such as when making inquiries, take the following steps:

(1) Log in as root to the server where Dynamic Menu Portal was installed.

(2) Move to the directory where the Dynamic Menu Portal class is stored.

```
# cd /opt/icewall-sso/dmp/bin/dp/WEB-INF/classes
```

(3) Enter the following command to view the version information.

```
# java com.hp.icewall.dmp.Version
```

(4) An example is shown below.

```
@(#)IceWall SSO Dynamic Menu Portal
@(#)Version: 10.00.00.xxxxxxX
@(#)(c) Copyright 2003-2010 Hewlett-Packard Development Compan
y, L.P.
```

4.6 Remarks when upgrading from previous versions 10.0

You must take note of these items when upgrading from previous versions.

(1) Starting from this version, the request execution error page has been added to the deployment descriptor (web.xml), and configuration elements (RequestACLErrorFilePath, RequestACLErrorFileEncoding) have also been added, so the previous web.xml cannot be used without any changes. Use web.xml included with this version.

(2) Starting from this version, a portion of the configuration method for the log configuration file (log4j.properties) has been changed. Dynamic Menu Portal will operate with the previous configuration, but we recommend the configuration in this version.

5 Uninstallation

This chapter describes how to uninstall Dynamic Menu Portal.

5.1 Undeploying from the server

The following procedure shows how to undeploy Dynamic Menu Portal from a Tomcat server.

(1) Log in as the user who runs the Tomcat server to the server where Dynamic Menu Portal was installed.

(2) If the Tomcat server is running, execute the following command to stop it.

```
$ [Tomcat installation directory]/bin/shutdown.sh
```

(3) Open server.xml with an editor.

```
$ vi [Tomcat installation directory]/conf/server.xml
```

(4) Delete the settings below from the definition of the virtual host where Dynamic Menu Portal runs.

```
<Context path="/dp" docBase="/opt/icewall-sso/dmp/bin/dp" debug="0" reloadabl
e="true"/>
```

(5) Save server.xml and close the editor.

(6) Execute the following command to start the Tomcat server.

```
$ [Tomcat installation directory]/bin/startup.sh
```

5.2 Uninstallation

The following procedure shows how to uninstall Dynamic Menu Portal.

(1) Log in as root to the server where Dynamic Menu Portal was installed.

(2) Uninstall Dynamic Menu Portal.

■ HP-UX ■

```
# swremove dmp
```

■ Linux ■

```
# rpm -e IceWall-SSO-dmp_e
```

6 Sample Setup

This chapter describes how to run the Dynamic Menu Portal sample.

6.1 Sample overview

You can check the procedures up to displaying the Dynamic Menu Portal page for each user by setting this configuration. The actual server configuration may be more complicated than the sample in this document. However, completing this sample setup can help to gain an understanding of configuring Dynamic Menu Portal.

6.2 Prerequisite conditions

- IceWall SSO must be configured according to the “IceWall SSO Sample Setup Guide.”
- Dynamic Menu Portal must be installed according to “4. Installation.”

6.3 IceWall backend configuration

The following procedure shows how to configure Dynamic Menu Portal to run as IceWall backend.

(1) Open the Forwarder configuration file (dfw.conf) with an editor.

```
# vi /opt/icewall-sso/dfw/cgi-bin/dfw.conf
```

(2) Add the following line:

```
HOST=DMP=[host name]:[port]
```

For [host name] and [port], specify the host name and port of the web application server running Dynamic Menu Portal.

(3) Add the following line:

```
SVRFILE=DMP,./sample.conf
```

(4) Save the configuration file and close the editor.

6.4 IceWall access control configuration

The following procedure shows how to configure the IceWall access control settings.

(1) Open the Authentication Server access control file (cert.acl) with an editor.

```
# vi /opt/icewall-sso/certd/config/cert.acl
```

(2) Add the following line:

```
http://[host name]:[port]/=ALL|SccOnly|HpOnly
```

For [host name] and [port], specify the host name and port of the web application server running Dynamic Menu Portal.

(3) Save the access control file and close the editor.

(4) Restart the Authentication Module.

6.5 IceWall information inheritance configuration

The following procedure shows how to configure the IceWall information inheritance configuration.

(1) Open the Forwarder host configuration file (sample.conf) with an editor.

```
# vi /opt/icewall-sso/dfw/cgi-bin/sample.conf
```

(2) Add the following line based on the configuration in the Authentication DB column information file.

```
HTTPDATA=LLOGINDATE column (attribute) name,LLOGINDATE
```

Example:
If ORACLE is used as the Authentication DB

```
HTTPDATA=LASTDATE,LLOGINDATE
```

If LDAP is used as the Authentication DB

```
HTTPDATA=displayName,LLOGINDATE
```

(3) Save the configuration file and close the editor.

6.6 Extracting the sample.war file

The following procedure shows how to extract the deployment file.

(1) Log in as root to the server where Dynamic Menu Portal was installed.

(2) Move to this directory.

```
# cd /opt/icewall-sso/dmp/bin
```

(3) Create a directory for the sample program.

```
# mkdir sample
```

(4) Move to the created directory.

```
# cd sample
```

(5) Extract the sample program using the jar command.

```
# jar xfv ../sample.war
```

(6) Change the owner of the extracted directory to one of the users below.
Tomcat server: root or user who runs the Tomcat server

Example: changing the owner to www:other

```
# chown -R www:other /opt/icewall-sso/dmp/bin/sample
```

6.7 Deploying a web application to acquire the HTTP source

This section describes how to deploy a web application to acquire the HTTP source used in the sample.

The following procedure shows how to deploy to a Tomcat server.
The example below shows the case when the Tomcat server is installed to the [Tomcat installation directory].

(1) Log in as root to the server where Dynamic Menu Portal was installed.

(2) If the Tomcat server is running, execute the following command to stop it.

```
# [Tomcat installation directory]/bin/shutdown.sh
```

(3) Open server.xml with an editor.

```
# vi [Tomcat installation directory]/conf/server.xml
```

(4) Add the settings below inside the <Host> tag that defines the information for the virtual host where the sample program runs.

```
<Context path="/sample" docBase="/opt/icewall-sso/dmp/bin/sample" debug="0"
reloadable="true"/>
```

(5) Save the server.xml and close the editor.

(6) Execute the following command to start the Tomcat server.

```
# [Tomcat installation directory]/bin/startup.sh
```

6.8 Editing the Dynamic Menu Portal configuration file

The following procedure shows how to edit the Dynamic Menu Portal configuration file.

(1) Open the Dynamic Menu Portal configuration file (dmp.xml) with an editor.

```
# vi /opt/icewall-sso/dmp/config/dmp.xml
```

(2) If the actual host name and port number of the Authentication Server differ from the ones used in the configuration file, edit the double-underlined area.

```
:
  <dmp:Active>localhost:14142</dmp:Active>
:
```

(3) If the actual host name and port of the web application for acquiring the HTTP source is different, edit the double-underlined area.

```
:
  <dmp:URL>http://localhost:[port]/sample/uid.jsp</dmp:URL>
:
  <dmp:URL>http://localhost:[port]/sample/llogindate.jsp</dmp:URL>
:
```

For [port], specify the port number of the web application server running the web application for acquiring the HTTP source.

6.9 Using the sample

By executing the operating procedure below, you can display the Dynamic Menu Portal sample page and experience displaying pages for different users.

Before logging in again as a different user, either log out from the Dynamic Menu Portal sample page or close the browser once.

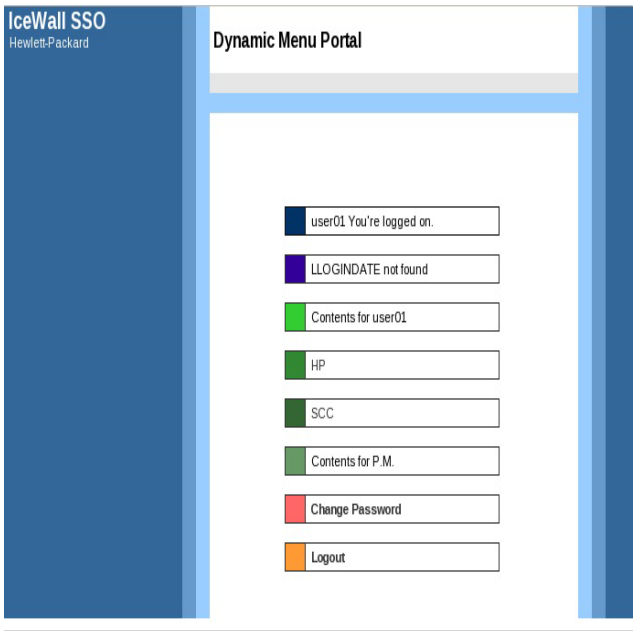
(1) After opening the browser and entering the following URL, the sample login page is displayed.

```
http://[hostname]/fw/dfw/DMP/dp/dmp
```

For [hostname], specify the IceWall server name or IP address.

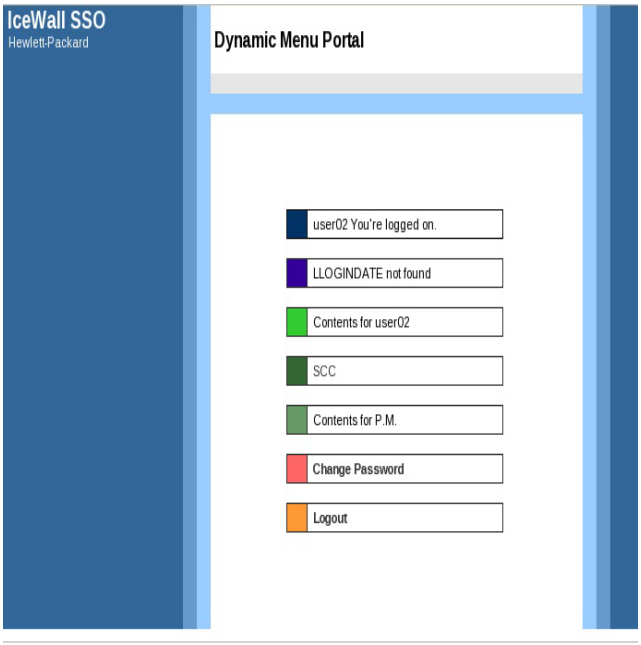
Sample login page

(2) Log in with the user name (user01) and password (user01) on the sample login page and the following page is displayed.



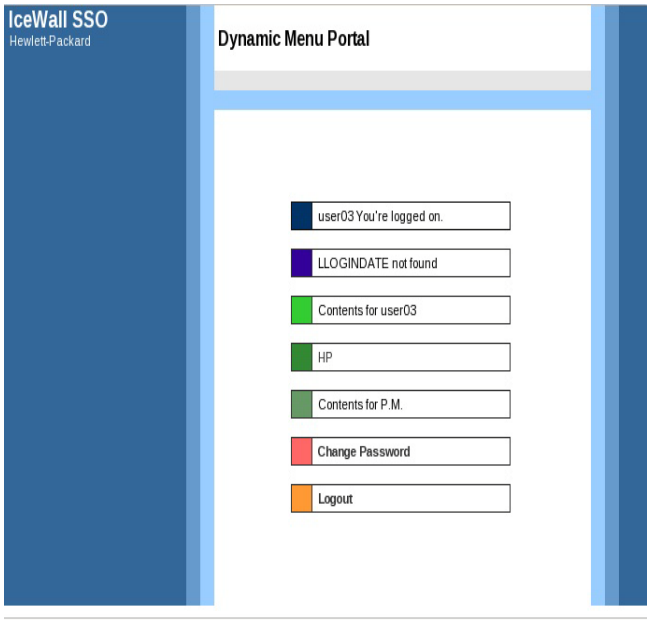
Dynamic Menu Portal page (for user01)

(3) Log in with the user name (user02) and password (user02) on the sample login page and the following page is displayed.



Dynamic Menu Portal page (for user02)

(4) Log in with the user name (user03) and password (user03) on the sample login page and the following page is displayed.



Dynamic Menu Portal page (for user03)

7 Notice

Please be aware of the important point below when using Dynamic Menu Portal.

7.1 When using a client certificate

If using a client certificate to log in, the Authentication Module must be configured as shown below.

Authentication Module configuration file (cert.conf)

```
ACCCTRLFLG=2
```

8 Reference

This chapter contains the reference for each of the Dynamic Menu Portal configuration files. There are three types of configuration files for Dynamic Menu Portal.

- Deployment descriptor (web.xml)
- Log configuration file (log4j.properties)
- Dynamic Menu Portal configuration file (dmp.xml)

8.1 Deployment descriptor (web.xml)

Overview

This file configures the initial settings of Dynamic Menu Portal. It configures the character encoding of output content and paths for the log configuration file and the Dynamic Menu Portal configuration file.

Storage location

/opt/icewall-sso/dmp/bin/dp/WEB-INF/web.xml

Note

1) Restart the web application server after making changes to the file configuration.

Initial value

```
<!DOCTYPE web-app PUBLIC "-//Sun Microsystems, Inc.//DTD Web Application 2.2//EN" "http://java.sun.com/j2ee/dtds/web-app_2_2.dtd">
<web-app>
 <context-param>
  <param-name>ContentEncoding</param-name>
  <param-value>Shift_JIS</param-value>
 </context-param>
 <context-param>
  <param-name>Log4jPropertiesFilePath</param-name>
  <param-value>/opt/icewall-sso/dmp/config/log4j.properties</param-value>
 </context-param>
 <context-param>
  <param-name>ConfigurationFilePath</param-name>
  <param-value>/opt/icewall-sso/dmp/config/dmp.xml</param-value>
 </context-param>
 <context-param>
  <param-name>SystemErrorFilePath</param-name>
  <param-value>/opt/icewall-sso/dmp/html/dmp_syserr.html</param-value>
 </context-param>
 <context-param>
  <param-name>SystemErrorFileEncoding</param-name>
  <param-value>Shift_JIS</param-value>
 </context-param>
 <context-param>
  <param-name>NoLoginErrorFilePath</param-name>
  <param-value>/opt/icewall-sso/dmp/html/dmp_nologin.html</param-value>
 </context-param>
 <context-param>
  <param-name>NoLoginErrorFileEncoding</param-name>
  <param-value>Shift_JIS</param-value>
 </context-param>
 <context-param>
  <param-name>RequestACLErrorFilePath</param-name>
```

```
    <param-value>/opt/icewall-sso/dmp/html/dmp_reqaclerr.html</param-value>
  </context-param>
  <context-param>
    <param-name>RequestACLErrorFileEncoding</param-name>
    <param-value>Shift_JIS</param-value>
  </context-param>
  <servlet>
    <servlet-name>DynamicMenuPortalServlet</servlet-name>
    <servlet-class>com.hp.icewall.dmp.DynamicMenuPortalServlet</servlet-class>
    <load-on-startup>1</load-on-startup>
  </servlet>
  <servlet-mapping>
    <servlet-name>DynamicMenuPortalServlet</servlet-name>
    <url-pattern>/dmp</url-pattern>
  </servlet-mapping>
</web-app>
```

The parameters are described in the following pages.

ContentEncoding (<context-param><param-name>)

Overview

Sets the character encoding of the output page.

Format

```
<context-param>
  <param-name>ContentEncoding</param-name>
  <param-value>encoding_format</param-value>
</context-param>
```

- The value of <param-name> is fixed.
- The value of <param-value> is defined with a character encoding format supported by JAVA (IANA).

Configuration example

1) To set the character encoding of the page output by Dynamic Menu Portal as Shift_JIS:
   <param-value>Shift_JIS</param-value>

Remark

None

Log4jPropertiesFilePath (<context-param><param-name>)

Overview

Sets the path of the log configuration file.

Format

```
<context-param>
  <param-name>Log4jPropertiesFilePath</param-name>
  <param-value>log_configuration_file_name</param-value>
</context-param>
```

- The value of <param-name> is fixed.
- The value of <param-value> is defined as an absolute path.

Configuration example

1) To set the standard configuration file as the log configuration file name:
   <param-value>/opt/icewall-sso/dmp/config/log4j.properties </param-value>

Remark

- If changes are made to the log configuration file, the web application server must be restarted.

ConfigurationFilePath (<context-param><param-name>)

Overview

Sets the path of the Dynamic Menu Portal configuration file.

Format

```
<context-param>
  <param-name>ConfigurationFilePath</param-name>
  <param-value>configuration_file_name</param-value>
</context-param>
```

- The value of <param-name> is fixed.
- The value of <param-value> is defined as an absolute path.

Configuration example

1) To set the standard Dynamic Menu Portal configuration file as the configuration file name:
   <param-value>/opt/icewall-sso/dmp/config/dmp.xml</param-value>

Remark

- The web application server does not need to be restarted after adding changes to the Dynamic Menu Portal configuration file. If there is a change to the date that the file was last modified, the file is reloaded automatically.

SystemErrorFilePath (<context-param><param-name>)

Overview

Sets the path of the system error page file.

Format

```
<context-param>
  <param-name>SystemErrorFilePath</param-name>
  <param-value>file_name_of_the_system_error_page</param-value>
</context-param>
```

- The value of <param-name> is fixed.
- The value of <param-value> is defined as an absolute path.

Configuration example

1) To set the standard file name as the file name of the system error page:
   <param-value>/opt/icewall-sso/dmp/html/dmp_syserr.html</param-value>

Remark

- If changes are made to the system error page file, the web application server must be restarted.

SystemErrorFileEncoding (<context-param><param-name>)

Overview

Sets the character encoding when loading the system error page file.

Format

```
<context-param>
  <param-name>SystemErrorFileEncoding</param-name>
  <param-value>encoding_format</param-value>
</context-param>
```

- The value of <param-name> is fixed.
- The value of <param-value> is defined with a character encoding format supported by JAVA (IANA).

Configuration example

1) To set the input character encoding of the system error page file as Shift_JIS:
   <param-value>Shift_JIS</param-value>

Remark

- The character encoding set with ContentEncoding is used to output the file.

NoLoginErrorFilePath (<context-param><param-name>)

Overview

Sets the file path of the no login error page.

Format

```
<context-param>
  <param-name>NoLoginErrorFilePath</param-name>
  <param-value>file_name_of_the_no_login_error_page</param-
  value>
</context-param>
```

- The value of <param-name> is fixed.
- The value of <param-value> is defined as an absolute path.

Configuration example

1) To set the standard file name as the file name of the no login error page:
   <param-value>/opt/icewall-sso/dmp/html/dmp_nologin.html</param-value>

Remark

- If changes are made to the no login error page file, the web application server must be restarted.

NoLoginErrorFileEncoding (<context-param><param-name>)

Overview

Sets the character encoding when loading the no login error page file.

Format

```
<context-param>
  <param-name>NoLoginErrorFileEncoding</param-name>
  <param-value>encoding_format</param-value>
</context-param>
```

- The value of <param-name> is fixed.
- The value of <param-value> is defined with a character encoding format supported by JAVA (IANA).

Configuration example

1) To set the input character encoding of the file of the no login error page as Shift_JIS:
   <param-value>Shift_JIS</param-value>

Remark

- The character encoding set with ContentEncoding is used to output the file.

RequestACLErrorFilePath (<context-param><param-name>)

10.0

Overview

Sets the file path of the request execution error page.

Format

```
<context-param>
  <param-name>RequestACLErrorFilePath</param-name>
  <param-value>file_name_of_the_request_execution_error_page</
param-value>
</context-param>
```

- The value of <param-name> is fixed.
- The value of <param-value> is defined as an absolute path.

Configuration example

1) To set the standard file name as the file name of the request execution error page:
   <param-value>/opt/icewall-sso/dmp/html/dmp_nologin.html</param-value>

Remark

- If changes are made to the request execution error page file, the web application server must be restarted.

RequestACLErrorFileEncoding (<context-param><param-name>) 10.0

Overview

Sets the character encoding when loading the request execution error page file.

Format

```
<context-param>
  <param-name>RequestACLErrorFileEncoding</param-name>
  <param-value>encoding_format</param-value>
</context-param>
```

- The value of <param-name> is fixed.
- The value of <param-value> is defined with a character encoding format supported by JAVA (IANA).

Configuration example

1) To set the input character encoding of the file of the no login error page as Shift_JIS:
   <param-value>Shift_JIS</param-value>

Remark

- The character encoding set with ContentEncoding is used to output the file.

<servlet>

Overview

Configures the servlet.

Format

```
<servlet>
  <servlet-name>DynamicMenuPortalServlet</servlet-name>
  <servlet-class>com.hp.icewall.dmp.DynamicMenuPortalServlet</
  servlet-class>
  <load-on-startup>1</load-on-startup>
</servlet>
```

- The value of <servlet-name> is fixed.
- The value of <servlet-class> is fixed.
- The value of <load-on-startup> is fixed.

Configuration example

None

Remarks

- Use the initial values.
- The servlet is configured to be initialized at web application server startup; therefore, after starting the web application server, verify that no errors are output to the web application server log or the Dynamic Menu Portal log.

<servlet-mapping>

Overview

Configures the servlet mapping.

Format

```
<servlet-mapping>
  <servlet-name>DynamicMenuPortalServlet</servlet-name>
  <url-pattern>/dmp</url-pattern>
</servlet-mapping>
```

- The value of <servlet-name> is fixed.

Configuration example

1) To map the servlet to /dmp:
   <url-pattern>/dmp</url-pattern>

Remark

None

8.2 Log configuration file (log4j.properties) 10.0

Overview

This file configures settings related to the Dynamic Menu Portal log output. It configures the log output destination, output format, output level, and other properties.

Storage location

/opt/icewall-sso/dmp/config/log4j.properties

Notes

1) Restart the web application server after making changes to the file configuration.
2) Shut down the web application server before making changes to the output log file names or deleting log files. Failure to do so may result in the logs not being output correctly.

Initial value

```
log4j.rootLogger=ERROR,DMPLOG
log4j.category.com.hp.icewall.dmp=ERROR
log4j.category.ICEWALL_LOG=ERROR

# log
log4j.appender.DMPLOG = org.apache.log4j.FileAppender
log4j.appender.DMPLOG.File = /opt/icewall-sso/logs/dmp.log
log4j.appender.DMPLOG.layout = org.apache.log4j.PatternLayout
log4j.appender.DMPLOG.layout.ConversionPattern = %-5p [%d{yyyy/MM/dd HH:mm
:ss}] %C %M %m%n
```

Configuration examples

1) To set the level for messages output to the log to INFO or higher:

```
log4j.rootLogger=ERROR,DMPLOG
log4j.category.com.hp.icewall.dmp=INFO
log4j.category.ICEWALL_LOG=INFO

# log
log4j.appender.DMPLOG = org.apache.log4j.FileAppender
log4j.appender.DMPLOG.File = /opt/icewall-sso/logs/dmp.log
log4j.appender.DMPLOG.layout = org.apache.log4j.PatternLayout
log4j.appender.DMPLOG.layout.ConversionPattern = %-5p [%d{yyyy/MM/dd
HH:
mm:ss}] %C %M %m%n
```

2) To set the level for messages output to the log to DEBUG or higher:

```
log4j.rootLogger=ERROR,DMPLOG
log4j.category.com.hp.icewall.dmp=DEBUG
log4j.category.ICEWALL_LOG=DEBUG

# log
log4j.appender.DMPLOG = org.apache.log4j.FileAppender
log4j.appender.DMPLOG.File = /opt/icewall-sso/logs/dmp.log
```

```
log4j.appender.DMPLOG.layout = org.apache.log4j.PatternLayout
log4j.appender.DMPLOG.layout.ConversionPattern = %-5p [%d{yyyy/MM/dd
HH:
mm:ss}] %C %M %m%n
```

Remarks

Dynamic Menu Portal uses log4j for log output. For details on how to configure log4j, see the log4j document.

8.3 Dynamic Menu Portal configuration file (dmp.xml)

Overview

This file configures Dynamic Menu Portal. It configures Authentication Module information, the sources, conditions, replacements, and other parameters.

Storage location

/opt/icewall-sso/dmp/config/dmp.xml

Notes

1) The web application server does not need to be restarted even if changes are made to this configuration file. If there is a change to the date that the file was last modified, the file is reloaded automatically.
2) When using an Authentication Module failover or failback, grant write permission for this file to the user executing the web application server.
3) After an Authentication Module failover or failback, the character encoding of the file is set to Shift_JIS.
4) The host names and IP address in the elements can be written in the IPv6 format. For details, see “IPv6 Support” in the “IceWall SSO User’s Manual.”

Initial value

```
<?xml version="1.0" encoding="Shift_JIS"?>

<dmp:DynamicMenuPortal xmlns:dmp="http://icewall.hp.com/dmp">

 <dmp:CertInformation>
  <dmp:Active>localhost:14142</dmp:Active>
  <dmp:Timeout>10</dmp:Timeout>
  <dmp:RetryInterval>5</dmp:RetryInterval>
  <dmp:RetryCount>3</dmp:RetryCount>
  <dmp:SessionHeaderName>Session</dmp:SessionHeaderName>
  <dmp:TransactionHeaderName>X-iw-transid</dmp:TransactionHeaderName>
  <dmp:ICPVersion>2.0</dmp:ICPVersion>
 </dmp:CertInformation>

 <dmp:Template>
  <dmp:Path>/opt/icewall-sso/dmp/html/menu.html</dmp:Path>
  <dmp:Encoding>Shift_JIS</dmp:Encoding>
 </dmp:Template>

 <dmp:Source>
  <dmp:Alias>S_FILE_USER01</dmp:Alias>
  <dmp:Type>file</dmp:Type>
  <dmp:Params>
   <dmp:Path>/opt/icewall-sso/dmp/sample/user01.html</dmp:Path>
   <dmp:Encoding>Shift_JIS</dmp:Encoding>
  </dmp:Params>
 </dmp:Source>

 <dmp:Source>
  <dmp:Alias>S_FILE_USER02</dmp:Alias>
  <dmp:Type>file</dmp:Type>
  <dmp:Params>
```

```
    <dmp:Path>/opt/icewall-sso/dmp/sample/user02.html</dmp:Path>
    <dmp:Encoding>Shift_JIS</dmp:Encoding>
  </dmp:Params>
</dmp:Source>

<dmp:Source>
  <dmp:Alias>S_FILE_USER03</dmp:Alias>
  <dmp:Type>file</dmp:Type>
  <dmp:Params>
    <dmp:Path>/opt/icewall-sso/dmp/sample/user03.html</dmp:Path>
    <dmp:Encoding>Shift_JIS</dmp:Encoding>
  </dmp:Params>
</dmp:Source>

<dmp:Source>
  <dmp:Alias>S_FILE_HP</dmp:Alias>
  <dmp:Type>file</dmp:Type>
  <dmp:Params>
    <dmp:Path>/opt/icewall-sso/dmp/sample/hp.html</dmp:Path>
    <dmp:Encoding>Shift_JIS</dmp:Encoding>
  </dmp:Params>
</dmp:Source>

<dmp:Source>
  <dmp:Alias>S_FILE_SCC</dmp:Alias>
  <dmp:Type>file</dmp:Type>
  <dmp:Params>
    <dmp:Path>/opt/icewall-sso/dmp/sample/scc.html</dmp:Path>
    <dmp:Encoding>Shift_JIS</dmp:Encoding>
  </dmp:Params>
</dmp:Source>

<dmp:Source>
  <dmp:Alias>S_FILE_MORNING</dmp:Alias>
  <dmp:Type>file</dmp:Type>
  <dmp:Params>
    <dmp:Path>/opt/icewall-sso/dmp/sample/morning.html</dmp:Path>
    <dmp:Encoding>Shift_JIS</dmp:Encoding>
  </dmp:Params>
</dmp:Source>

<dmp:Source>
  <dmp:Alias>S_FILE_AFTERNOON</dmp:Alias>
  <dmp:Type>file</dmp:Type>
  <dmp:Params>
    <dmp:Path>/opt/icewall-sso/dmp/sample/afternoon.html</dmp:Path>
    <dmp:Encoding>Shift_JIS</dmp:Encoding>
  </dmp:Params>
</dmp:Source>

<dmp:Source>
  <dmp:Alias>S_HTTP_UID</dmp:Alias>
  <dmp:Type>http</dmp:Type>
  <dmp:Params>
    <dmp:URL>http://localhost/sample/uid.jsp</dmp:URL>
```

```
    <dmp:Text>FAILED TO GET.&lt;br&gt;</dmp:Text>
    <dmp:HeaderName>uid</dmp:HeaderName>
   </dmp:Params>
</dmp:Source>

<dmp:Source>
  <dmp:Alias>S_HTTP_LLOGINDATE</dmp:Alias>
  <dmp:Type>http</dmp:Type>
  <dmp:Params>
    <dmp:URL>http://localhost/sample/llogindate.jsp</dmp:URL>
    <dmp:Text>FAILED TO GET.&lt;br&gt;</dmp:Text>
    <dmp:HeaderName>LLOGINDATE</dmp:HeaderName>
  </dmp:Params>
</dmp:Source>

<dmp:Source>
  <dmp:Alias>S_TEXT_NONE</dmp:Alias>
  <dmp:Type>text</dmp:Type>
  <dmp:Params>
    <dmp:Text></dmp:Text>
  </dmp:Params>
</dmp:Source>

<dmp:Condition>
  <dmp:Alias>C_HEADER_IS_USER01</dmp:Alias>
  <dmp:Type>header</dmp:Type>
  <dmp:Params>
    <dmp:HeaderName>uid</dmp:HeaderName>
    <dmp:HeaderValue>user01</dmp:HeaderValue>
  </dmp:Params>
</dmp:Condition>

<dmp:Condition>
  <dmp:Alias>C_HEADER_IS_USER02</dmp:Alias>
  <dmp:Type>header</dmp:Type>
  <dmp:Params>
    <dmp:HeaderName>uid</dmp:HeaderName>
    <dmp:HeaderValue>user02</dmp:HeaderValue>
  </dmp:Params>
</dmp:Condition>

<dmp:Condition>
  <dmp:Alias>C_HEADER_IS_USER03</dmp:Alias>
  <dmp:Type>header</dmp:Type>
  <dmp:Params>
    <dmp:HeaderName>uid</dmp:HeaderName>
    <dmp:HeaderValue>user03</dmp:HeaderValue>
  </dmp:Params>
</dmp:Condition>

<dmp:Condition>
  <dmp:Alias>C_ACL_HP</dmp:Alias>
  <dmp:Type>ACL</dmp:Type>
  <dmp:Params>
    <dmp:URL>http://welcome.hp.com/country/jp/jpn/welcome.htm</dmp:URL>
```

```
  </dmp:Params>
</dmp:Condition>

<dmp:Condition>
  <dmp:Alias>C_ACL_SCC</dmp:Alias>
  <dmp:Type>ACL</dmp:Type>
  <dmp:Params>
    <dmp:URL>http://www.scc-kk.co.jp/</dmp:URL>
  </dmp:Params>
</dmp:Condition>

<dmp:Condition>
  <dmp:Alias>C_TIME_IS_MORNING</dmp:Alias>
  <dmp:Type>time</dmp:Type>
  <dmp:Params>
    <dmp:Time>...../AM/...</dmp:Time>
  </dmp:Params>
</dmp:Condition>

<dmp:Condition>
  <dmp:Alias>C_TIME_IS_AFTERNOON</dmp:Alias>
  <dmp:Type>time</dmp:Type>
  <dmp:Params>
    <dmp:Time>...../PM/...</dmp:Time>
  </dmp:Params>
</dmp:Condition>

<dmp:Condition>
  <dmp:Alias>C_UNCONDITIONAL</dmp:Alias>
  <dmp:Type>unconditional</dmp:Type>
  <dmp:Params/>
</dmp:Condition>

<dmp:Replace>
  <dmp:Alias>$DMP_01</dmp:Alias>
  <dmp:SourceAlias>S_HTTP_UID</dmp:SourceAlias>
  <dmp:ConditionAlias>C_UNCONDITIONAL</dmp:ConditionAlias>
</dmp:Replace>

<dmp:Replace>
  <dmp:Alias>$DMP_02</dmp:Alias>
  <dmp:SourceAlias>S_HTTP_LLOGINDATE</dmp:SourceAlias>
  <dmp:ConditionAlias>C_UNCONDITIONAL</dmp:ConditionAlias>
</dmp:Replace>

<dmp:Replace>
  <dmp:Alias>$DMP_03</dmp:Alias>
  <dmp:SourceAlias>S_FILE_USER01</dmp:SourceAlias>
  <dmp:ConditionAlias>C_HEADER_IS_USER01</dmp:ConditionAlias>
</dmp:Replace>

<dmp:Replace>
  <dmp:Alias>$DMP_03</dmp:Alias>
  <dmp:SourceAlias>S_FILE_USER02</dmp:SourceAlias>
  <dmp:ConditionAlias>C_HEADER_IS_USER02</dmp:ConditionAlias>
```

```
</dmp:Replace>

<dmp:Replace>
 <dmp:Alias>$DMP_03</dmp:Alias>
 <dmp:SourceAlias>S_FILE_USER03</dmp:SourceAlias>
 <dmp:ConditionAlias>C_HEADER_IS_USER03</dmp:ConditionAlias>
</dmp:Replace>

<dmp:Replace>
 <dmp:Alias>$DMP_03</dmp:Alias>
 <dmp:SourceAlias>S_TEXT_NONE</dmp:SourceAlias>
 <dmp:ConditionAlias>C_UNCONDITIONAL</dmp:ConditionAlias>
</dmp:Replace>

<dmp:Replace>
 <dmp:Alias>$DMP_04</dmp:Alias>
 <dmp:SourceAlias>S_FILE_HP</dmp:SourceAlias>
 <dmp:ConditionAlias>C_ACL_HP</dmp:ConditionAlias>
</dmp:Replace>

<dmp:Replace>
 <dmp:Alias>$DMP_04</dmp:Alias>
 <dmp:SourceAlias>S_TEXT_NONE</dmp:SourceAlias>
 <dmp:ConditionAlias>C_UNCONDITIONAL</dmp:ConditionAlias>
</dmp:Replace>

<dmp:Replace>
 <dmp:Alias>$DMP_05</dmp:Alias>
 <dmp:SourceAlias>S_FILE_SCC</dmp:SourceAlias>
 <dmp:ConditionAlias>C_ACL_SCC</dmp:ConditionAlias>
</dmp:Replace>

<dmp:Replace>
 <dmp:Alias>$DMP_05</dmp:Alias>
 <dmp:SourceAlias>S_TEXT_NONE</dmp:SourceAlias>
 <dmp:ConditionAlias>C_UNCONDITIONAL</dmp:ConditionAlias>
</dmp:Replace>

<dmp:Replace>
 <dmp:Alias>$DMP_06</dmp:Alias>
 <dmp:SourceAlias>S_FILE_MORNING</dmp:SourceAlias>
 <dmp:ConditionAlias>C_TIME_IS_MORNING</dmp:ConditionAlias>
</dmp:Replace>

<dmp:Replace>
 <dmp:Alias>$DMP_06</dmp:Alias>
 <dmp:SourceAlias>S_FILE_AFTERNOON</dmp:SourceAlias>
 <dmp:ConditionAlias>C_TIME_IS_AFTERNOON</dmp:ConditionAlias>
</dmp:Replace>

<dmp:Replace>
 <dmp:Alias>$DMP_06</dmp:Alias>
 <dmp:SourceAlias>S_TEXT_NONE</dmp:SourceAlias>
 <dmp:ConditionAlias>C_UNCONDITIONAL</dmp:ConditionAlias>
</dmp:Replace>
```

```
</dmp:DynamicMenuPortal>
```

The parameters are described in the following pages.

<CertInformation> 10.0

Overview Configures information related to the Authentication Module.

Format

```
<dmp:CertInformation>
  <dmp:Active>primary_authentication_module_information</
  dmp:Active>
  <dmp:Standby>secondary_authentication_module_information</
  dmp:Standby>
  <dmp:Master>primary_authentication_module_information</
  dmp:Master>
  <dmp:Replica>secondary_authentication_module_information</
  dmp:Replica>
  <dmp:CertLB>
    <dmp:Active>primary_authentication_module_information</
    dmp:Active>
    <dmp:Standby>ssecondary_authentication_module_information</
    dmp:Standby>
    <dmp:Master>primary_authentication_module</dmp:Master>
    <dmp:Replica>secondary_authentication_module_information</
dmp:Replica>
    <dmp:CertUniqueKey>authentication_module_identification_key</
dmp:CertUniqueKey>
  </dmp:CertLB>
  <dmp:Timeout>receive_timeout_value</dmp:Timeout>
  <dmp:RetryInterval>connection_retry_interval</dmp:RetryInterval>
  <dmp:RetryCount>connection_retry_count</dmp:RetryCount>
  <dmp:SessionHeaderName>session_ID_name</
  dmp:SessionHeaderName>
  <dmp:TransactionHeaderName>retrieved_header_name_of_
  transaction_ID_information</dmp:TransactionHeaderName>
  <dmp:ICPVersion>ICP_version</dmp:ICPVersion>
  <dmp:ICPAgentStr>user-defined_character_string</
  dmp:ICPAgentStr>
  <dmp:ICPRemoteAddressHeader-
Name>retrieved_header_name_of_client_IP_address_information</
dmp:ICPRemoteAddressHeaderName>
  <dmp:ICPMethodHeader-
Name>retrieved_header_name_of_method_information_requested_by
_client</dmp:ICPMethodHeaderName>
```

```
  <dmp:ICPUserAgentHeader-
Name>retrieved_header_name_of_browser_User-Agent_information</
dmp:ICPUserAgentHeaderName>
</dmp:CertInformation>
```

The parameters are described in the following pages.

<Active> (<CertInformation>) 10.0

Overview

Sets the host name (or IP address) and port number of the Authentication Module.

Format

<dmp:Template>host_name(or IP_address):port_number</dmp:Active>

- There is no default value in the executable binary.
- The initial value set in the standard configuration file is localhost:14142.

Configuration examples

1) To set cert1.com:14142 as the Primary Authentication Module:
<dmp:Active>cert1.com:14142</dmp:Active>

Remarks

- Failover is enabled by configuring this element and <dmp:Standby>. The "IceWall SSO FailOver Option" is required to implement a failover configuration with this element.
- When an Authentication Module failover occurs, the values of <dmp:Active> and <dmp:Standby> are rewritten alternately.
- This element is ineffective when the <dmp:CertLB> element is configured.

<Standby> (<CertInformation>) 10.0

Overview

Sets the host name (or IP address) and port number of the Secondary Authentication Module.

Format

<dmp:Standby>host_name(or IP_address):port_number</dmp:Standby>

- There is no default value in the executable binary.
- The initial value is not set in the standard configuration file.

Configuration examples

1) To set the Secondary Authentication Module to connect to when the Primary Authentication Module is down to cert2.com:14142:
<dmp:Standby>cert2.com:14142</dmp:Standby>

Remarks

- Failover is enabled by configuring this element. The “ICEWALL SSO FailOver Option” is required to implement a failover configuration with this element.
- When an Authentication Module failover occurs, the values of <dmp:Active> and <dmp:Standby> are rewritten alternately.
- This element is ineffective when the <dmp:CertLB> element is configured.

<Master> (<CertInformation>) 10.0

Overview

Sets the Primary Authentication Module in the event of failback, for the Authentication Module connection settings with failover enabled.

This parameter is available since version 10.0.

Format

<dmp:Master>host_name(or IP_address):port_number</dmp:Master>

- There is no default value in the executable binary.
- The initial value is not set in the standard configuration file.

Configuration examples

1) To perform failback operations with the <dmp:Active> element configured for failovers:
<dmp:Active>cert1.com:14142</dmp:Active>
<dmp:Standby>cert2.com:14142</dmp:Standby>
<dmp:Master>cert1.com:14142</dmp:Master>
<dmp:Replica>cert2.com:14142</dmp:Replica>

Remarks

- By configuring this element, failback operations can be performed with the <dmp:Active> element configured for failovers.
- This element is only effective when 2.0 is configured in the <dmp:ICPVersion> element (when using ICP 2.0).
- Always use this element in a set with the <dmp:Active>, <dmp:Standby>, and <dmp:Replica> elements.
- The Authentication Module connection settings configured by this element are overwritten with the Authentication Module connection settings in the <dmp:Active> element when performing a failback operation.
- Configure this element with the same values as the initial state of the Authentication Module connection settings in the <dmp:Active> element. If the host name specification is defined with different formats, this element is overwritten with Authentication Module connection settings that differ from the initial state when a failback occurs.
- This element is only effective when configured to announce the primary Authentication Module is live with the FAILBACK parameter in the secondary Authentication Module configuration file.

<Replica> (<CertInformation>) 10.0

Overview

Sets the Secondary Authentication Module in the event of failback, for the Authentication Module connection settings with failover enabled.

This parameter is available since version 10.0.

Format

<dmp:Replica>host_name(or IP_address):port_number</dmp:Replica>

- There is no default value in the executable binary.
- The initial value is not set in the standard configuration file.

Configuration examples

1) To perform failback operations with the <dmp:Standby> element configured for failovers:
<dmp:Active>cert1.com:14142</dmp:Active>
<dmp:Standby>cert2.com:14142</dmp:Standby>
<dmp:Master>cert1.com:14142</dmp:Master>
<dmp:Replica>cert2.com:14142</dmp:Replica>

Remarks

- By configuring this element, failback operations can be performed with the <dmp:Standby> element configured for failovers.
- This element is only effective when 2.0 is configured in the <dmp:ICPVersion> element (when using ICP 2.0).
- Always use this Element in a set with the <dmp:Active>, <dmp:Standby>, and <dmp:Master> elements.
- The Authentication Module connection settings configured by this element are overwritten with the Authentication Module connection settings in the <dmp:Standby> element when performing a failback operation.
- Configure this element with the same values as the initial state of the Authentication Module connection settings in the <dmp:Standby> element. If the host name specification is defined with different formats, this element is overwritten with Authentication Module connection settings that differ from the initial state when a failback occurs.
- This element is only effective when configured to announce the Primary Authentication Module is live with the FAILBACK parameter in the Secondary Authentication Module configuration file.

<CertLB> (<CertInformation>) 10.0

Overview

Sets the connection information for the Authentication Modules performing load balancing.

This parameter is available since version 10.0.

Format

```
<dmp:CertLB>
  <dmp:Active>host_name(or IP_address):port_number</dmp:Active>
  <dmp:Standby>host_name(or IP_address):port_number</
  dmp:Standby>
  <dmp:Master>host_name(or IP_address):port_number</
  dmp:Master>
  <dmp:Replica>host_name(or IP_address):port_number</
  dmp:Replica>
  <dmp:CertUniqueKey>authentication_module_identification_key</
  dmp:CertUniqueKey>
</dmp:CertLB>
```

- Configure the <dmp:Active> element with the Primary Authentication Module connection information. Configure the <dmp:Standby> element with the Secondary Authentication Module connection information.
- Failback operations can be performed by configuring the <dmp:Master> and <dmp:Replica> elements.
- Define the Authentication Module identifier key as 1 character.
- Set the Authentication Module identifier key to the CERTUNIQUEKEY parameter value of the Authentication Module configured by the <dmp:Active> element.
- This element can configure multiple items.
- There is no default value in the executable binary.
- The initial value is not set in the standard configuration file.

Configuration examples

1) To connect to two Authentication Module groups with the load balancing function:

```
<dmp:CertLB>
  <dmp:Active>cert1a.com:14142</dmp:Active>
  <dmp:CertUniqueKey>a</dmp:CertUniqueKey>
</dmp:CertLB>
<dmp:CertLB>
  <dmp:Active>cert1b.com:14142</dmp:Active>
  <dmp:CertUniqueKey>b</dmp:CertUniqueKey>
</dmp:CertLB>
```

2) To connect to two Authentication Module groups with the load balancing function, and failover and failback functionalities are enabled:

```
<dmp:CertLB>
  <dmp:Active>cert1a.com:14142</dmp:Active>
  <dmp:Standby>cert2a.com:14142</dmp:Standby>
  <dmp:Master>cert1a.com:14142</dmp:Master>
  <dmp:Replica>cert2a.com:14142</dmp:Replica>
  <dmp:CertUniqueKey>a</dmp:CertUniqueKey>
</dmp:CertLB>
<dmp:CertLB>
  <dmp:Active>cert1b.com:14142</dmp:Active>
  <dmp:Standby>cert2b.com:14142</dmp:Standby>
  <dmp:Master>cert1b.com:14142</dmp:Master>
  <dmp:Replica>cert2b.com:14142</dmp:Replica>
  <dmp:CertUniqueKey>b</dmp:CertUniqueKey>
</dmp:CertLB>
```

Remarks

- If this element is configured multiple times, the load balancing function is enabled. The Authentication Module group that the user connects to during login is automatically determined and the destination Authentication Module group is assigned.

- If this element is configured multiple times, always set different Authentication Module identifier keys.

- when this element is configured, the <dmp:Active>, <dmp:Standby>, <dmp:Master, and <dmp:Replica> elements under <CertInformation> are ineffective.

<Timeout> (<CertInformation>)

Overview

Sets the receive timeout counter for Authentication Module communication.

Format

<dmp:Timeout>timeout_value (seconds)</dmp:Timeout>

- The unit for setting the timeout value is seconds.
- There is no default value in the executable binary.
- The initial value set in the standard configuration file is 10 seconds.

Configuration examples

1) To set the receive timeout value for communications from the Authentication Module to 10 seconds:
<dmp:Timeout>10</dmp:Timeout>

Remarks

- Once connectivity to the Authentication Module has been established, the value set by this element specifies the timeout counter for receiving a response message after a request has been sent. It is not the timeout counter when connecting to the Authentication Module.

<RetryInterval> (<CertInformation>)

Overview

Sets the retry interval when connecting to the Authentication Module fails.

Format

<dmp:RetryInterval>retry_interval</dmp:RetryInterval>

- The unit for setting the timeout value is seconds.
- There is no default value in the executable binary.
- The initial value set in the standard configuration file is 5 seconds.

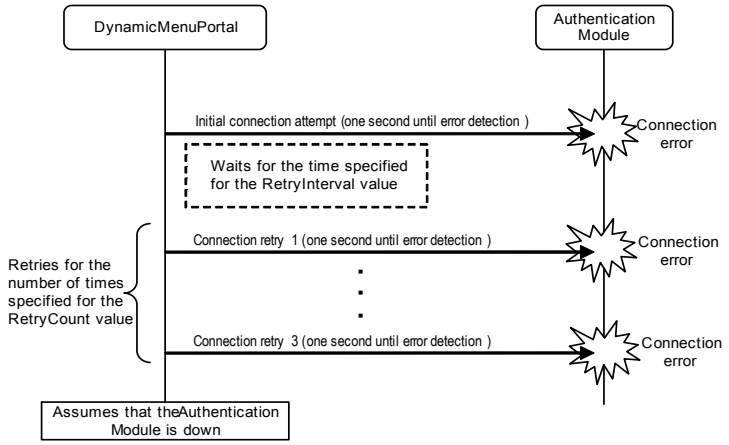
Configuration examples

1) To set the connection retry interval when a connection attempt to the Authentication Module fails to 5 seconds:
<dmp:RetryInterval>5</dmp:RetryInterval>
In this case, the system waits 5 seconds from the connection failure and then retries the connection.

Remarks

- The value set with this element is the wait time until the next attempt to reconnect to the Authentication Module.

- The time period for determining whether the Authentication Module is down is the result of the following expression;
"((the setting value for RetryCount + 1) × Connection error detection time) + (the setting value for RetryInterval × the setting value for RetryCount)."



Example: RetryCount=3, RetryInterval=2
Connection error detection time=1 second
In this case, the time until the Authentication Module is recognized as down is

((3 + 1) × 1) + (3 × 2) = 10 seconds.

- The connection error detection time differs for when the server is stopped and when the Authentication Module is stopped. Virtually no waiting time occurs when the Authentication Module is stopped, but a long waiting time occurs when the server is stopped.

<RetryCount> (<CertInformation>)

Overview

Sets the connection retry count when a connection error occurs when connecting to the Authentication Module.

Format

<dmp:RetryCount>number_of_retries</dmp:RetryCount>

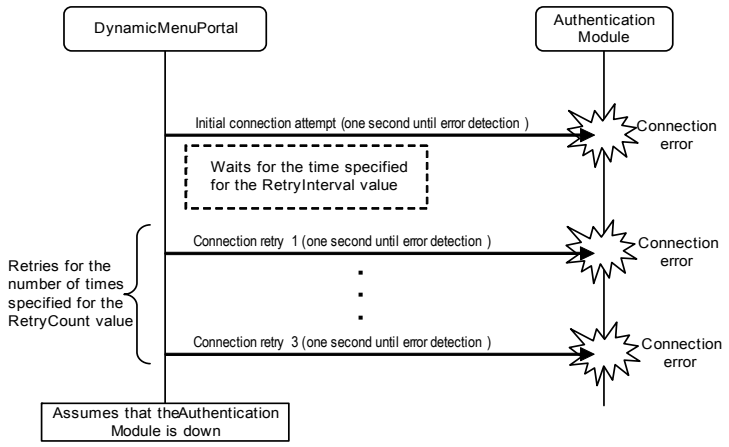
- If the number of retries is set to zero or less, no retries will be attempted.
- There is no default value in the executable binary.
- The initial value set in the standard configuration file is 3.

Configuration examples

1) To set the retry count after a failed connection attempt to the Authentication Module to 3 times:
<dmp:RetryCount>3</dmp:RetryCount>

Remarks

- The initial connection attempt is not included in the retry count.
- The value set with this element is the number of retries allowed to connect to the Authentication Module. It is not the number of retries allowed for requesting a response after connecting to the module.



Example: RetryCount=3, RetryInterval=2
Connection error detection time=1 second
In this case, the time until the Authentication Module is recognized as down is
((3 + 1) × 1) + (3 × 2) = 10 seconds.

- The time period for determining whether the Authentication Module is down is the result of the following expression;

"((the setting value for RetryCount + 1) × Connection error detection time) + (the setting value for RetryInterval × the setting value for RetryCount)."

- The connection error detection time differs for when the server is stopped and when the Authentication Module is stopped. Virtually no waiting time occurs when the Authentication Module is stopped, but a long waiting time occurs when the server is stopped.

<SessionHeaderName> (<CertInformation>)

Overview

Sets the send header name for the session ID information sent from Forwarder.

Format

<dmp:SessionHeaderName>header_name</dmp:SessionHeaderName>

- For header_name, set the header name to be used when sending session ID information to the Backend Web Server.
- The characters used in the header name are based on general HTTP header specifications.
- There is no default value in the executable binary.
- The initial value set in the standard configuration file is Session.

Configuration examples

1) To change the header name for the session ID information sent to the Backend Web Server to Iw-Session:
<dmp:SessionHeaderName>Iw-Session</dmp:SessionHeaderName>

Remarks

- Operation is not guaranteed when using characters in the header name that cannot be used as an HTTP header.

<TransactionHeaderName> (<CertInformation>) 10.0

Overview

Sets the send header name for the transaction ID information sent from Forwarder.

Format

<dmp:TransactionHeaderName>header_name<dmp:TransactionHeaderName>

- For header_name, set the HTTP header name for the transaction ID information to be used sent from Forwarder.
- When this parameter is set and a transaction ID is sent from Forwarder, the transaction ID is output as additional log information.
- Transaction ID information is not retrieved when this parameter is not set.
- The characters used in the header name are based on general HTTP header specifications.
- There is no default value in the executable binary.
- The initial value set in the standard configuration file is X-iw-transid.

Configuration examples

1) To change the transaction ID information header name to Icewall-transactionid:
<dmp:TransactionHeaderName>Icewall-transactionid</dmp:TransactionHeaderName>

Remarks

- Operation is not guaranteed when using characters in the header name that cannot be used as an HTTP header.
- When this element is configured and the <dmp:ICPVersion> element is set to 2.0, the remote address information is announced when communicating with the Authentication Module.

<ICPVersion> (<CertInformation>) 10.0

Overview

Sets the communication protocol between Dynamic Menu Portal and the Authentication Module.

This parameter is available since version 10.0.

Format

<dmp:ICPVersion>version</dmp:ICPVersion>

- One of the following values can be specified for the version:
  1.1: Communication by ICP 1.0 expansion
  2.0: Communication by ICP 2.0
- The default value set in the executable binary is 1.1.
- The initial value set in the standard configuration file is 2.0.
- The default value from the executable binary is used if the line for the value is not present in the configuration file.
- If the value for this parameter is out of range, the default value is used.

Configuration examples

1) To use ICP 2.0 for communication with the Authentication Module:
   <dmp:ICPVersion>2.0</dmp:ICPVersion>

Remarks

- This element must be set to 2.0 when the <dmp:Master> and <dmp:Replica> elements are configured to perform failback operations.
- This element must be set to 2.0 when the TransactionHeaderName element is configured and the transaction ID retrieved from Forwarder is announced when communicating with the Authentication Module.
- This element must be set to 2.0 when configuring the ICPAgentStr element to set a user-specified character string as the request AGENT_ID when communicating with the Authentication Module.
- This element must be set to 2.0 when configuring the ICPRemoteAddressHeaderName element to set the send header name for remote address information sent from Forwarder when communicating with the Authentication Module.
- This element must be set to 2.0 when configuring the ICPMethodHeaderName element to set the send header name for HTTP method information sent from Forwarder when communicating with the Authentication Module.

- This element must be set to 2.0 when configuring the ICPUserAgentHeaderName element to set the send header name for browser's User-Agent information sent from Forwarder when communicating with the Authentication Module.

<ICPAgentStr> (<CertInformation>) 10.0

Overview

Sets a user-defined character string that is added to the AGENT_ID in ICP 2.0 requests. Setting this parameter gives a unique ID to the sender of the request.

Format

<dmp:ICPAgentStr>user-defined_character_string</dmp:ICPAgentStr>

- The user-defined character string may contain uppercase and lowercase alphanumeric characters.
- The system may not run properly if characters other than uppercase and lowercase alphanumeric characters are used for the user-defined text string.
- This parameter is ineffective when the <dmp:ICPVersion> element is not 2.0.
- There is no default value in the executable binary.
- The initial value is not set in the standard configuration file.

Configuration examples

1) To add dmp1 to AGENT_ID when communicating with the Authentication Module:
<dmp:ICPAgentStr>dmp1</dmp:ICPAgentStr>

Remarks

- This element is only effective when 2.0 is configured in the <dmp:ICPVersion> element (when using ICP 2.0).
- When the LOGINFO parameter in the Authentication Module configuration file is set to 2, AGENT_ID is output to the Authentication Module error log and access log. In this case, the log output from the Authentication Module may be cut off if the user-defined character string is over 35 characters.
- The standard setting for the AGENT_ID is shown below.
[ICP communication library information];[Module version information];[<dmp:ICPAgentStr> element value]
example: When <dmp:ICPAgentStr> is set to dmp1
JALIB;08.00.00.2007.xxxxxxX;dmp;10.00.00.xxxxxxX;dmp1

<ICPRemoteAddressHeaderName> (<CertInformation>) 10.0

Overview

Sets the send header name for the remote address information sent from Forwarder.

Format

<dmp:ICPRemoteAddressHeaderName>header_name</dmp:ICPRemoteAddressHeaderName>

- For header_name, set the HTTP header name of the remote address information to be sent from Forwarder.
- Remote address information is not retrieved when this element is not configured.
- The characters used in the header name are based on general HTTP header specifications.
- There is no default value in the executable binary.
- The initial value is not set in the standard configuration file.

Configuration examples

1) To set the remote address information header name to RemoteAddr:
<dmp:ICPRemoteAddressHeaderName>RemoteAddr</dmp:ICPRemoteAddressHeaderName>

Remarks

- Operation is not guaranteed when using characters in the header name that cannot be used as an HTTP header.
- When this element is configured and the <dmp:ICPVersion> element is set to 2.0, the remote address information is announced when communicating with the Authentication Module.

<ICPMethodHeaderName> (<CertInformation>) 10.0

Overview

Sets the send header name for the HTTP method information sent from Forwarder.

Format

<dmp:ICPMethodHeaderName>header_name</dmp:ICPMethodHeaderName>

- For header_name, set the HTTP header name of the HTTP method information to be sent from Forwarder.
- Method information is not retrieved when this element is not configured.
- The characters used in the header name are based on general HTTP header specifications.
- There is no default value in the executable binary.
- The initial value is not set in the standard configuration file.

Configuration examples

1) To set the method information header name to Method:
<dmp:ICPMethodHeaderName>Method</dmp:ICPMethodHeaderName>

Remarks

- Operation is not guaranteed when using characters in the header name that cannot be used as an HTTP header.
- When this element is configured and the <dmp:ICPVersion> element is set to 2.0, the HTTP method information is announced when communicating with the Authentication Module.

<ICPUserAgentHeaderName> (<CertInformation>) 10.0

Overview

Sets the send header name of the browser User-Agent information to be sent from Forwarder.

Format

<dmp:ICPUserAgentHeaderName>header_name</dmp:ICPUserAgentHeaderName>

- For header_name, set the HTTP header name of the browser User-Agent information to be sent from Forwarder.
- Browser User-Agent information is not retrieved when this element is not configured.
- The characters used in the header name are based on general HTTP header specifications.
- There is no default value in the executable binary.
- The initial value is not set in the standard configuration file.

Configuration examples

1) To set the User-Agent information header name to User-Agent:
<dmp:ICPUserAgentHeaderName>User-Agent</dmp:ICPUserAgentHeaderName>

Remarks

- Operation is not guaranteed when using characters in the header name that cannot be used as an HTTP header.
- When this element is configured and the <dmp:ICPVersion> element is set to 2.0, the browser User-Agent information is announced when communicating with the Authentication Module.

<Template>

Overview

Configures information related to the template HTML.

Format

```
<dmp:Template>
  <dmp:Path>template_HTML_file_name</dmp:Path>
  <dmp:Encoding>encoding_format</dmp:Encoding>
</dmp:Template>
```

- Only one <dmp:Template> element can be defined.
- The value of <dmp:Path> is defined as an absolute path.
- The value of <dmp:Encoding> is defined with a character encoding format supported by JAVA (IANA).

Configuration examples

1) To set the standard file name as the template HTML file name:
<dmp:Path>/opt/icewall-sso/dmp/html/menu.html</dmp:Path>

2) To set the input character encoding of the template HTML file as Shift_JIS:
<dmp:Encoding>Shift_JIS</dmp:Encoding>

Remarks

- The template HTML file is an HTML file that corresponds to the static area of the user page.
- The dynamic area of the user page is defined by keywords in the template HTML file.
- The template HTML must be a standard HTML file with <HTML> and </HTML> tags.
- The web application server does not need to be restarted after adding changes to the template HTML file. If there is a change to the date that the file was last modified, the file is reloaded automatically.
- The character encoding specified by ContentEncoding in web.xml is used when output.

<Source> (FILE format)

Overview

Configures information related to a source in the FILE format.

Format

```
<dmp:Source>
  <dmp:Alias>source_alias_name</dmp:Alias>
  <dmp:Type>file</dmp:Type>
  <dmp:Params>
    <dmp:Path>source_file_name</dmp:Path>
    <dmp:Encoding>encoding_format</dmp:Encoding>
  </dmp:Params>
</dmp:Source>
```

- n <dmp:Source> elements can be defined.
- The value of <dmp:Alias> is defined uniquely among <dmp:Source> elements.
- The value of <dmp:Type> is “file” (fixed).
- The value of <dmp:Path> is defined as an absolute path.
- The value of <dmp:Encoding> is defined with a character encoding format supported by JAVA (IANA).

Configuration examples

1) To set S_FILE_USER01 as the source alias name:
   <dmp:Alias>S_FILE_USER01</dmp:Alias>

2) To set /opt/icewall-sso/dmp/sample/user01.html as the source file name:
   <dmp:Path>/opt/icewall-sso/dmp/sample/user01.html</dmp:Path>

3) To set Shift_JIS as the input character encoding of the source file:
   <dmp:Encoding>Shift_JIS</dmp:Encoding>

Remarks

- The source is HTML text that corresponds to the dynamic area of the user page.
- The keywords that indicate the dynamic area of the template HTML are replaced with the source during execution. For this reason, the source must provide partial HTML text without the <HTML> and </HTML> tags.
- A source in the FILE format is partial HTML text saved as a file.
- The web application server does not need to be restarted after adding changes to the file. If there is a change to the date the file was last modified, the file is

reloaded automatically.

- The administrator can manage content by replacing the files.
- The character encoding specified by ContentEncoding in web.xml is used when output.

<Source> (TEXT format)

Overview

Configures information related to a source in the text format.

Format

```
<dmp:Source>
  <dmp:Alias>source_alias_name</dmp:Alias>
  <dmp:Type>text</dmp:Type>
  <dmp:Params>
    <dmp:Text>text_string</dmp:Text>
  </dmp:Params>
</dmp:Source>
```

- n <dmp:Source> elements can be defined.
- The value of <dmp:Alias> is defined uniquely among <dmp:Source> elements.
- The value of <dmp:Type> is “text” (fixed).
- The value of <dmp:Text> must be escaped properly according to XML specifications.

Configuration examples

1) To set S_TEXT_TEST as the source alias name:
   <dmp:Alias>S_TEXT_TEST</dmp:Alias>

2) To set TEST as the source HTML text:
   <dmp:Text>TEST</dmp:Text>

   In this case, “<” and “>” must be escaped as shown in the above example.

Remarks

- The source is HTML text that corresponds to the dynamic area of the user page.
- The keywords that indicate the dynamic area in the template HTML are replaced with the source during execution. For this reason, the source must provide partial HTML text without <HTML> and </HTML> tags.
- A source in the text format directly defines the partial HTML text in the Dynamic Menu Portal configuration file.

<Source> (HTTP format) 10.0

Overview

Configures information related to a source in the HTTP format.

Format

```
<dmp:Source>
  <dmp:Alias>source_alias_name</dmp:Alias>
  <dmp:Type>http</dmp:Type>
  <dmp:Params>
    <dmp:URL>source_URL</dmp:URL>
    <dmp:Text>text_string_when_acquisition_fails</dmp:Text>
    <dmp:HeaderName>forward_header_name</dmp:HeaderName>
  </dmp:Params>
</dmp:Source>
```

- n <dmp:Source> elements can be defined.
- The value of <dmp:Alias> is defined uniquely among <dmp:Source> elements.
- The value of <dmp:Type> is “http” (fixed).
- The value of <dmp:URL> is defined as an absolute path.
- If an IPv6 address is specified in the value of <dmp:URL>, the IPv6 address portion must be enclosed in [ ]. 10.0
- The value of <dmp:Text> must be escaped properly.

Configuration examples

1) To set S_HTTP_UID as the source alias name:
   <dmp:Alias>S_HTTP_UID</dmp:Alias>

2) To set http://localhost/sample/uid.jsp as the source URL:
   <dmp:URL>http://localhost/sample/uid.jsp</dmp:URL>

3) To set http://[::1]/sample/uid.jsp as the source URL: 10.0
   <dmp:URL>http://[::1]/sample/uid.jsp</dmp:URL>

4) To set FAILED TO GET.
 as the text displayed when failing to acquire content from the URL set with <dmp:URL>:
   **<dmp:Text> FAILED TO GET.
</dmp:Text>**

   In this case, “<” and “>” must be escaped as shown in the above example.

5) To set uid as the HTTP header forwarded to the source URL:
   <dmp:HeaderName>uid</dmp:HeaderName>

If there is no header to be forwarded, do not include this element.

Remarks

- The source is the HTML text that corresponds to the dynamic area of the user page.
- The keywords that indicate the dynamic area of the template HTML are replaced with the source during execution. For this reason, the source must provide partial HTML text without <HTML> and </HTML> tags.
- A source in the HTTP format is configured to acquire the partial HTML text via HTTP. Access to the set URL is conducted every time without using the cache. Care is required due to an increase in performance overhead.
- The administrator can use dynamic content with JSP.
- When Japanese or other text that does not use 7-bit ASCII is set as a value in the HTTP header sent from Forwarder, garbled characters may be generated during acquisition of the value. In addition, garbled characters may be sent as is when sending the value.
- The header to be resent is encoded in Shift_JIS and then sent.

<Condition> (Header format)

Overview

Configures information related to the header format judgment conditions.

Format

```
<dmp:Condition>
  <dmp:Alias>condition_alias_name</dmp:Alias>
  <dmp:Type>header</dmp:Type>
  <dmp:Params>
    <dmp:HeaderName>condition_header_name</dmp:HeaderName>
    <dmp:HeaderValue>evaluation_conditions</dmp:HeaderValue>
  </dmp:Params>
</dmp:Condition>
```

- n <dmp:Condition> elements can be defined.
- The value of <dmp:Alias> is defined uniquely among <dmp:Condition> elements.
- The value of <dmp:Type> is “header” (fixed).
- The value of <dmp:HeaderValue> is defined with the regular expressions supported by JAVA.

Configuration examples

1) To set the condition alias name to C_HEADER_IS_USER01:
   <dmp:Alias>C_HEADER_IS_USER01</dmp:Alias>

2) To set uid as the condition header name for comparing conditions:
   <dmp:HeaderName>uid</dmp:HeaderName>

3) To set user01 as the evaluation condition:
   <dmp:HeaderValue>user01</dmp:HeaderValue>

   In this case, when the value of the set header is “user01,” the condition evaluation is true.

Remarks

- The condition is evaluated when keywords indicating the dynamic areas in the template HTML are replaced with the source during execution. Replacement occurs only when the evaluation result is true.
- The header format condition is the condition that acquires the HTTP header sent from Forwarder and returns true or false after matching the value with regular expressions.

- When Japanese or other text that does not use 7-bit ASCII is set as the value in the HTTP header sent from Forwarder, garbled characters may be generated during acquisition of the value. In addition, matching with regular expressions may be performed with these garbled characters.

<Condition> (ACL format)

Overview

Configures information related to the ACL format judgment conditions.

Format

```
<dmp:Condition>
  <dmp:Alias>condition_alias_name</dmp:Alias>
  <dmp:Type>ACL</dmp:Type>
  <dmp:Params>
    <dmp:URL>target_URL_for_access_privilege_check</dmp:URL>
  </dmp:Params>
</dmp:Condition>
```

- n <dmp:Condition> elements can be defined.
- The value of <dmp:Alias> is defined uniquely among <dmp:Condition> elements.
- The value of <dmp:Type> is "ACL" (fixed).
- The value of <dmp:URL> is defined in URL format.

Configuration examples

1) To set C_ACL_HP as the condition alias name:
   <dmp:Alias>C_ACL_HP</dmp:Alias>

2) To set http://localhost/sample/uid.jsp as the target URL for access privilege check:
   <dmp:URL>http://localhost/sample/uid.jsp</dmp:URL>

   In this case, when access privilege to the set URL is granted, the condition evaluation is true.

Remarks

- The condition is evaluated when keywords indicating the dynamic areas in the template HTML are replaced with the source during execution. Replacement occurs only when the evaluation result is true.

- The ACL format condition is the condition that inquires with the Authentication Module about user access privileges to the set URL and returns true or false as a result.

<Condition> (Time format)

Overview

Configures information related to the time format judgment conditions.

Format

```
<dmp:Condition>
  <dmp:Alias>condition_alias_name</dmp:Alias>
  <dmp:Type>time</dmp:Type>
  <dmp:Params>
    <dmp:Time>time_evaluation_conditions</dmp:Time>
  </dmp:Params>
</dmp:Condition>
```

- n <dmp:Condition> elements can be defined.
- The value of <dmp:Alias> is defined uniquely among <dmp:Condition> elements.
- The value of <dmp:Type> is “time” (fixed).
- The value of <dmp:Time> is defined with the regular expressions supported by JAVA.

Configuration examples

1) To set C_TIME_IS_MORNING as the condition alias name:
   <dmp:Alias>C_TIME_IS_MORNING</dmp:Alias>

2) To set “AM” as the time comparison condition:
   <dmp:Time>...../AM/...</dmp:Time>

   In this case, when the present time is morning, the condition evaluation is true.

Remarks

- The current time for matching uses the following format:
  yyyyMMddHHmmss'/'a'/'EEE (English locale)
  Example: 20030821235959/PM/Tue

- The condition is evaluated when keywords indicating the dynamic areas in the template HTML are replaced with the source during execution. Replacement occurs only when the evaluation result is true.

- The time format condition is the condition that performs matching between the date, time, and day of the week at the time of evaluation that is converted to the specific format and the set regular expressions, and returns true or false as a result.

- The time used in the evaluation is the current time of the evaluation day. Therefore, when the same conditions are evaluated multiple times during a single run of Dynamic Menu Portal, different results may be returned for the same conditions depending on the timing of the evaluation.

<Condition> (Unconditional format)

Overview

Configures information related to the unconditional format judgment conditions.

Format

```
<dmp:Condition>
  <dmp:Alias>condition_alias_name</dmp:Alias>
  <dmp:Type>unconditional</dmp:Type>
  <dmp:Params/>
</dmp:Condition>
```

- n <dmp:Condition> elements can be defined.
- The value of <dmp:Alias> is defined uniquely among <dmp:Condition> elements.
- The value of <dmp:Type> is “unconditional” (fixed).
- The value of <dmp:Params> is fixed.

Configuration examples

1) To set C_UNCONDITIONAL as the condition alias name:
   <dmp:Alias>C_UNCONDITIONAL</dmp:Alias>

2) Because detailed parameters do not exist for the unconditional format, only the element name is defined.
   <dmp:Params/>

Remarks

- The condition is evaluated when keywords indicating the dynamic areas in the template HTML are replaced with the source during execution. Replacement occurs only when the evaluation result is true.

- The unconditional format condition is the condition that returns a true value unconditionally.

<Replace>

Overview

Configures information related to keyword replacement.

Format

```
<dmp:Replace>
  <dmp:Alias>keyword</dmp:Alias>
  <dmp:SourceAlias>source_alias_name</dmp:SourceAlias>
  <dmp:ConditionAlias>condition_alias_name
  </dmp:ConditionAlias>
</dmp:Replace>
```

- n <dmp:Replace> elements can be defined.
- The value of <dmp:Alias> sets the keywords defined in the template HTML.
- The value of <dmp:SourceAlias> sets the alias set with <dmp:Source>.
- The value of <dmp:ConditionAlias> sets the alias set with <dmp:Condition>.

Configuration examples

1) To set $DMP_01 as the replacement keyword:
   <dmp:Alias>$DMP_01</dmp:Alias>

2) To set S_HTTP_UID as the alias of the source replaced with the keyword:
   <dmp:SourceAlias>S_HTTP_UID</dmp:SourceAlias>

3) To set C_UNCONDITIONAL as the alias of the condition evaluated during replacement of the keyword:
   <dmp:ConditionAlias>C_UNCONDITIONAL</dmp:ConditionAlias>

Remarks

- The keywords that indicate the dynamic area of the template HTML are replaced with the source during execution when specific conditions are satisfied. “Replace” (this parameter) ties together this “Keyword,” “Source,” and “Condition.”

- Replace (this parameter) is processed in the order defined in the Dynamic Menu Portal configuration file. To avoid unnecessary condition evaluations, it is recommended that you consider the order of definitions so that the replacement items with conditions that are most likely to be true are placed first.
- If the same keyword is set multiple times, once the condition is true, the condition evaluation is not performed for that keyword thereafter.

- To avoid the occurrence of keywords that are not replaced, it is recommended that you prepare an unconditional replacement for each keyword.

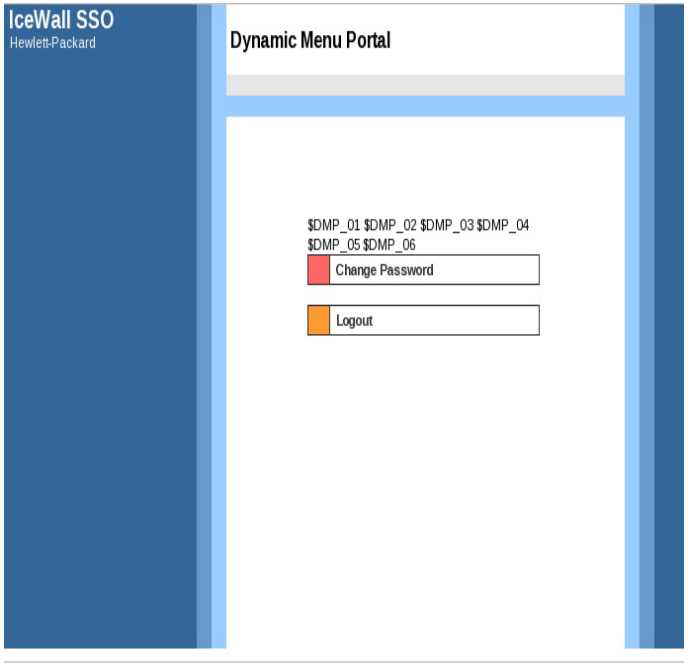
9 Customizing Standard HTML Codes

This chapter describes the HTML files provided as standard with Dynamic Menu Portal.

9.1 Template (menu.html)

This is the template of the Dynamic Menu Portal page. When this page is executed, the keywords defined in this file ($DMP_01 through 06) are replaced with the source and displayed.

Screen image	Source

	<!-- $Workfile: menu.html $ $Revision: 1 $ $Date: 10/03/19 17:00 $ -->
	<html>
	<head>
	<title>IceWall SSO - Dynamic Menu Portal</title>
	<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
	
	<style type="text/css">
	<!--
	BODY, TD {
	font-family: Verdana, Geneva, Arial, Helvetica, Sans-serif;
	font-size: 12px;
	}
	a:link {
	color: #333333;
	text-decoration: none;
	}
	a:visited {
	color: #666666;
	text-decoration: none;
	}
	a:hover {
	color: #ff3300;
	text-decoration: underline;
	}

Screen image	Source

	.title {
	font-size: 18px;
	font-family: Verdana, Geneva, Arial, Helvetica, Sans-serif;
	}
	.sub-title {
	font-size: 16px;
	font-family: Verdana, Geneva, Arial, Helvetica, Sans-serif;
	line-height: 18px;
	}
	.sub-title2 {
	font-size: 14px;
	font-family: Verdana, Geneva, Arial, Helvetica, Sans-serif;
	}
	.footer {
	font-size: 11px;
	font-family: Verdana, Geneva, Arial, Helvetica, Sans-serif;
	}
	-->
	</style>
	
	</head>
	
	<body bgcolor="#ffffff" text="#000000" link="#333333" vlink="#666666" alink="#ff3300" leftmargin="0" topmargin="0" marginwidth="0" marginheight="0">
	
	<table border="0" width="100%" height="98%" cellpadding="0" cellspacing="0">
	<tr>
	<td width="195" height="80" bgcolor="#336699" valign="top" class="title" nowrap> IceWall SSO
	
	   Hewlett-Packard
	</td>

Screen image	Source
	<td width="15" bgcolor="#6699cc" rowspan="2" nowrap> <table border="0" width="15" height="5" cellpadding="0" cellspacing="0"> <tr> <td width="15" height="5" bgcolor="#6699cc" nowrap> </td> </tr> </table> </td> <td width="15" bgcolor="#99ccff" rowspan="2" nowrap> <table border="0" width="15" height="5" cellpadding="0" cellspacing="0"> <tr> <td width="15" height="5" bgcolor="#99ccff" nowrap> </td> </tr> </table> </td> <td width="100%" height="100%" valign="top" rowspan="2"> <table border="0" width="100%" cellspacing="0" cellpadding="0"> <tr> <td width="100%" height="50" align="left" class="sub-title"> Dynamic Menu Portal </td> </tr> <tr> <td height="15" bgcolor="#e6e6e6" nowrap> </td> </tr> <tr> <td height="15" bgcolor="#99ccff" nowrap> </td> </tr> <tr> <td height="70" nowrap> </td> </tr> <tr> <td align="center" nowrap> <table border="0" height="100%" cellspacing="0" cellpadding="0">

Screen image	Source
	<tr> <td width="240" height="100%" nowrap> $DMP_01 $DMP_02 $DMP_03 $DMP_04 $DMP_05 $DMP_06 <table border="0" width="220" height="22" cellpadding="0" cellspacing="0"> <tr> <td bgcolor="#333333" nowrap> <table border="0" width="220" height="22" cellpadding="3" cellspacing="1"> <tr> <td width="15" bgcolor="#ff6666" align="center" nowrap> <table border="0" width="15" height="5" cellpadding="0" cellspacing="0"> <tr> <td width="15" height="5" bgcolor="#ff6666" nowrap> </td> </tr> </table> </td> <td width="205" bgcolor="#ffffff" nowrap> Change Password</td> </tr> </table> </td> </tr> </table> <table border="0" width="220" height="22" cellpadding="0" cellspacing="0"> <tr>

Screen image	Source
	<td bgcolor="#333333" nowrap> <table border="0" width="220" height="22" cellpadding="3" cellspacing="1"> <tr> <td width="15" bgcolor="#ff9933" align="center" nowrap> <table border="0" width="15" height="5" cellpadding="0" cellspacing="0"> <tr> <td width="15" height="5" bgcolor="#ff9933" nowrap> </td> </tr> </table> </td> <td width="205" bgcolor="#ffffff" nowrap> Logout</td> </tr> </table> </td> </tr> </table> </td> </tr> </table> </td> <td width="15" height="100%" bgcolor="#99ccff" rowspan="2" nowrap> <table border="0" width="15" height="5" cellpadding="0" cellspacing="0"> <tr> <td width="15" height="5" bgcolor="#99ccff" nowrap> </td> </tr> </table> </td>

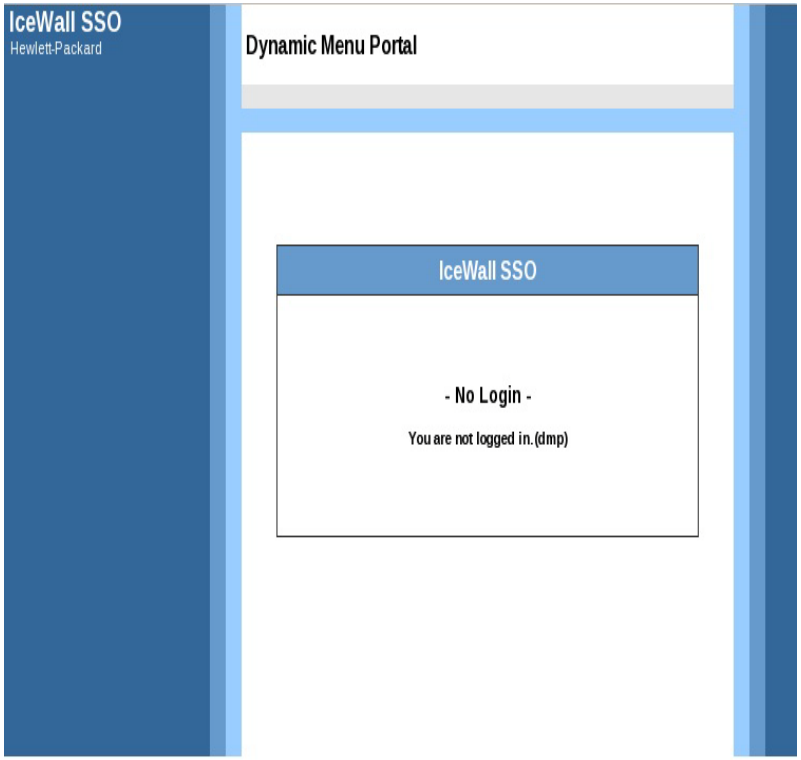
Screen image	Source
	<td width="15" nowrap bgcolor="#6699cc" rowspan="2"> <table border="0" width="15" height="5" cellpadding="0" cellspacing="0"> <tr> <td width="15" height="5" bgcolor="#6699cc" nowrap> </td> </tr> </table> </td> <td width="30" bgcolor="#336699" rowspan="2" nowrap> <table border="0" width="30" height="5" cellpadding="0" cellspacing="0"> <tr> <td width="30" height="5" bgcolor="#336699" nowrap> </td> </tr> </table> </td> </tr> <tr> <td width="195" height="100%" bgcolor="#336699" align="left" valign="top" nowrap> </td> </tr> </table> </body> </html>

* These keywords must be configured uniquely in the template HTML file.
* The same keyword cannot be used multiple times.

9.2 No login page (dmp_nologin.html)

This page is displayed when directly accessing Dynamic Menu Portal without going through Forwarder (dfw) (without logging into IceWall SSO).

Screen image	Source

	<!-- $Workfile: dmp_nologin.html $ $Revision: 1 $ $Date: 10/03/19 16:58 $ -->
	<html>
	<head>
	<title>IceWall SSO - No Login -</title>
	<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
	
	<style type="text/css">
	<!--
	BODY, TD {
	font-family: Verdana, Geneva, Arial, Helvetica, Sans-serif;
	font-size: 12px;
	}
	a:link {
	color: #333333;
	text-decoration: none;
	}
	a:visited {
	color: #666666;
	text-decoration: none;
	}
	a:hover {
	color: #ff3300;
	text-decoration: underline;
	}
	.title {
	font-size: 18px;
	font-family: Verdana, Geneva, Arial, Helvetica, Sans-serif;
	}

Screen image	Source

	.sub-title {
	font-size: 16px;
	font-family: Verdana, Geneva, Arial, Helvetica, Sans-serif;
	line-height: 18px;
	}
	.sub-title2 {
	font-size: 14px;
	font-family: Verdana, Geneva, Arial, Helvetica, Sans-serif;
	}
	.footer {
	font-size: 11px;
	font-family: Verdana, Geneva, Arial, Helvetica, Sans-serif;
	}
	-->
	</style>
	
	</head>
	
	<body bgcolor="#ffffff" text="#000000" link="#333333" vlink="#666666" alink="#ff3300" leftmargin="0" topmargin="0" marginwidth="0" marginheight="0">
	
	<table border="0" width="100%" height="98%" cellpadding="0" cellspacing="0">
	<tr>
	<td width="195" height="80" bgcolor="#336699" valign="top" class="title" nowrap> IceWall SSO
	
	   Hewlett-Packard
	</td>
	<td width="15" bgcolor="#6699cc" rowspan="2" nowrap>
	<table border="0" width="15" height="5" cellpadding="0" cellspacing="0">
	<tr>

Screen image	Source
	<td width="15" height="5" bgcolor="#6699cc" nowrap> </td> </tr> </table> </td> <td width="15" bgcolor="#99ccff" rowspan="2" nowrap> <table border="0" width="15" height="5" cellpadding="0" cellspacing="0"> <tr> <td width="15" height="5" bgcolor="#99ccff" nowrap> </td> </tr> </table> </td> <td width="100%" height="100%" valign="top" rowspan="2"> <table border="0" width="100%" cellspacing="0" cellpadding="0"> <tr> <td width="100%" height="50" class="sub-title" align="left"> Dynamic Menu Portal </td> </tr> <tr> <td height="15" bgcolor="#e6e6e6" nowrap> </td> </tr> <tr> <td height="15" bgcolor="#99ccff" nowrap> </td> </tr> <tr> <td height="70" nowrap> </td> </tr> <tr> <td align="center" nowrap> <table border="0" width="400" cellpadding="0" cellspacing="0"> <tr> <td bgcolor="#333333" nowrap> <table border="0" width="400" cellpadding="3" cellspacing="1"> <tr>

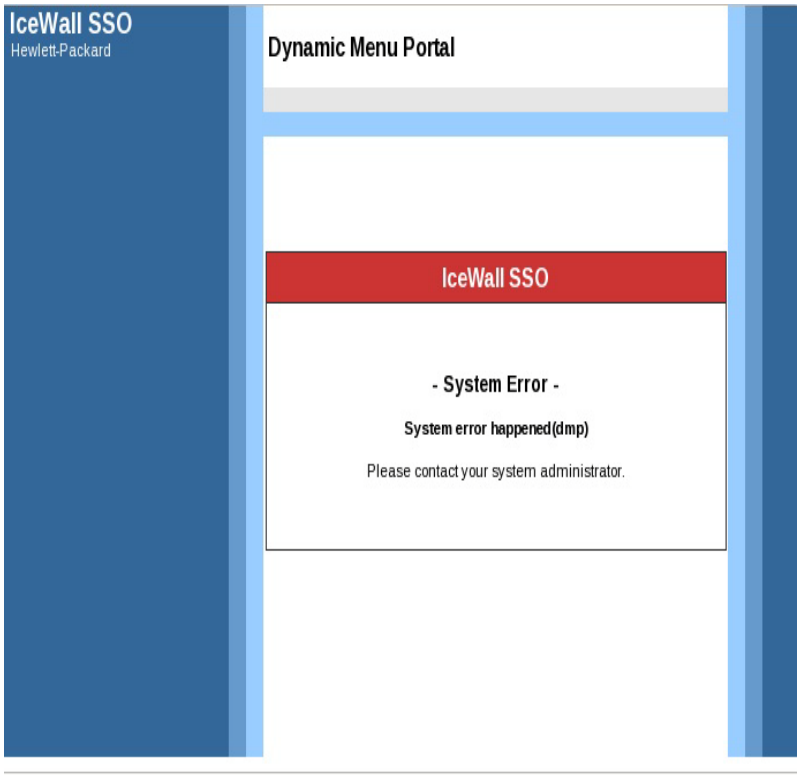
Screen image	Source
	<td height="30" bgcolor="#6699cc" align="center" class="sub-title" nowrap>IceWall SSO</td> </tr> <tr> <td height="150" bgcolor="#ffffff" align="center" nowrap> - No Login - <p>You are not logged in.(dmp) </td> </tr> </table> </td> </tr> </table> </td> </tr> </table> </td> <td width="15" height="100%" bgcolor="#99ccff" rowspan="2" nowrap> <table border="0" width="15" height="5" cellpadding="0" cellspacing="0"> <tr> <td width="15" height="5" bgcolor="#99ccff" nowrap> </td> </tr> </table> </td> <td width="15" bgcolor="#6699cc" rowspan="2" nowrap> <table border="0" width="15" height="5" cellpadding="0" cellspacing="0"> <tr> <td width="15" height="5" bgcolor="#6699cc" nowrap> </td> </tr> </table> </td> <td width="30" bgcolor="#336699" rowspan="2" nowrap> <table border="0" width="30" height="5" cellpadding="0"

Screen image	Source
	cellspacing="0"> <tr> <td width="30" height="5" bgcolor="#336699" nowrap> </td> </tr> </table> </td> </tr> <tr> <td width="195" height="100%" bgcolor="#336699" align="left" valign="top" nowrap> </td> </tr> </table> </body> </html>

9.3 System error page (dmp_syserr.html)

This page is displayed when an error occurs in the Dynamic Menu Portal for some reason and the menu cannot be displayed.

Screen image	Source

	<!-- $Workfile: dmp_syserr.html $ $Revision: 1 $ $Date: 10/03/19 16:58 $ -->
	<html>
	<head>
	<title>IceWall SSO - System Error -</title>
	<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
	
	<style type="text/css">
	<!--
	BODY, TD {
	font-family: Verdana, Geneva, Arial, Helvetica, Sans-serif;
	font-size: 12px;
	}
	a:link {
	color: #333333;
	text-decoration: none;
	}
	a:visited {
	color: #666666;
	text-decoration: none;
	}
	a:hover {
	color: #ff3300;
	text-decoration: underline;
	}
	.title {
	font-size: 18px;
	font-family: Verdana, Geneva, Arial, Helvetica, Sans-serif;
	}
	.sub-title {
	font-size: 16px;
	font-family: Verdana, Geneva, Arial, Helvetica, Sans-serif;

Screen image	Source

	line-height: 18px;
	}
	.sub-title2 {
	font-size: 14px;
	font-family: Verdana, Geneva, Arial, Helvetica, Sans-serif;
	}
	.footer {
	font-size: 11px;
	font-family: Verdana, Geneva, Arial, Helvetica, Sans-serif;
	}
	-->
	</style>
	
	</head>
	
	<body bgcolor="#ffffff" text="#000000" link="#333333" vlink="#666666" alink="#ff3300" leftmargin="0" topmargin="0" marginwidth="0" marginheight="0">
	
	<table border="0" width="100%" height="98%" cellpadding="0" cellspacing="0">
	<tr>
	<td bgcolor="#336699" width="195" height="80" valign="top" class="title" nowrap> IceWall SSO
	
	   Hewlett-Packard
	</td>
	<td width="15" bgcolor="#6699cc" rowspan="2" nowrap>
	<table border="0" width="15" height="5" cellpadding="0" cellspacing="0">
	<tr>
	<td width="15" height="5" bgcolor="#6699cc" nowrap> </td>
	</tr>
	</table>
	</td>

Screen image	Source
	<td width="15" bgcolor="#99ccff" rowspan="2" nowrap> <table border="0" width="15" height="5" cellpadding="0" cellspacing="0"> <tr> <td width="15" height="5" bgcolor="#99ccff" nowrap> </td> </tr> </table> </td> <td width="100%" height="100%" valign="top" rowspan="2"> <table border="0" width="100%" cellspacing="0" cellpadding="0"> <tr> <td width="100%" height="50" align="left" class="sub-title"> Dynamic Menu Portal</td> </tr> <tr> <td height="15" bgcolor="#e6e6e6" nowrap> </td> </tr> <tr> <td height="15" bgcolor="#99ccff" nowrap> </td> </tr> <tr> <td height="70" nowrap> </td> </tr> <tr> <td align="center" nowrap> <table border="0" width="400" cellpadding="0" cellspacing="0"> <tr> <td bgcolor="#333333" nowrap> <table border="0" width="400" cellpadding="3" cellspacing="1"> <tr> <td height="30" bgcolor="#cc3333" align="center" class="sub-title" nowrap>IceWall SSO</td> </tr> <tr>

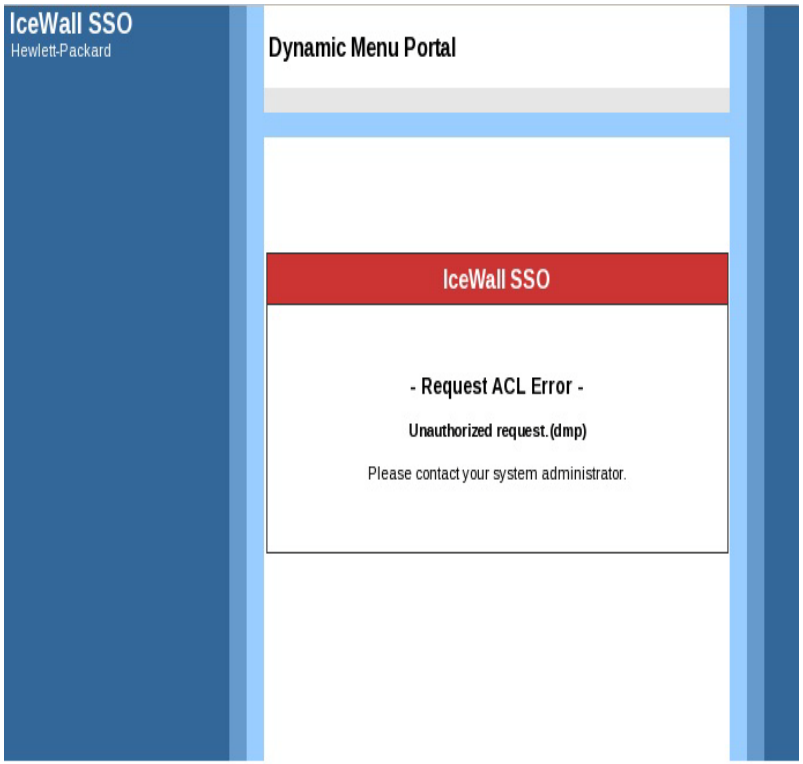
Screen image	Source
	<td height="150" bgcolor="#ffffff" align="center" nowrap> - System Error - <p>System error happened(dmp) <p>Please contact your system administrator. </td> </tr> </table> </td> </tr> </table> </td> </tr> </table> </td> <td width="15" height="100%" bgcolor="#99ccff" rowspan="2" nowrap> <table border="0" width="15" height="5" cellpadding="0" cellspacing="0"> <tr> <td width="15" height="5" bgcolor="#99ccff" nowrap> </td> </tr> </table> </td> <td width="15" bgcolor="#6699cc" rowspan="2" nowrap> <table border="0" width="15" height="5" cellpadding="0" cellspacing="0"> <tr> <td width="15" height="5" bgcolor="#6699cc" nowrap> </td> </tr> </table> </td> <td width="30" bgcolor="#336699" rowspan="2" nowrap> <table border="0" width="30" height="5" cellpadding="0" cellspacing="0"> <tr> <td width="30" height="5" bgcolor="#336699" nowrap> </td>

Screen image	Source
	</tr> </table> </td> </tr> <tr> <td width="195" height="100%" bgcolor="#336699" align="left" valign="top" nowrap> </td> </tr> </table> </body> </html>

9.4 Request privileges error page (dmp_reqaclerr.html)

This page is displayed when a request privileges error is returned from the Authentication Module when judging a condition.

Screen image	Source

	<!-- $Workfile: dmp_reqaclerr.html $ $Revision: 1 $ $Date: 10/03/19 16:58 $ -->
	<html>
	<head>
	<title>IceWall SSO - Request ACL Error -</title>
	<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
	
	<style type="text/css">
	<!--
	BODY, TD {
	font-family: Verdana, Geneva, Arial, Helvetica, Sans-serif;
	font-size: 12px;
	}
	a:link {
	color: #333333;
	text-decoration: none;
	}
	a:visited {
	color: #666666;
	text-decoration: none;
	}
	a:hover {
	color: #ff3300;
	text-decoration: underline;
	}
	.title {
	font-size: 18px;
	font-family: Verdana, Geneva, Arial, Helvetica, Sans-serif;
	}

Screen image	Source

	.sub-title {
	font-size: 16px;
	font-family: Verdana, Geneva, Arial, Helvetica, Sans-serif;
	line-height: 18px;
	}
	.sub-title2 {
	font-size: 14px;
	font-family: Verdana, Geneva, Arial, Helvetica, Sans-serif;
	}
	.footer {
	font-size: 11px;
	font-family: Verdana, Geneva, Arial, Helvetica, Sans-serif;
	}
	-->
	</style>
	
	</head>
	
	<body bgcolor="#ffffff" text="#000000" link="#333333" vlink="#666666" alink="#ff3300" leftmargin="0" topmargin="0" marginwidth="0" marginheight="0">
	
	<table border="0" width="100%" height="98%" cellpadding="0" cellspacing="0">
	<tr>
	<td bgcolor="#336699" width="195" height="80" valign="top" class="title" nowrap> IceWall SSO
	
	   Hewlett-Packard
	</td>
	<td width="15" bgcolor="#6699cc" rowspan="2" nowrap>
	<table border="0" width="15" height="5" cellpadding="0" cellspacing="0">
	<tr>

Screen image	Source
	<td width="15" height="5" bgcolor="#6699cc" nowrap> </td> </tr> </table> </td> <td width="15" bgcolor="#99ccff" rowspan="2" nowrap> <table border="0" width="15" height="5" cellpadding="0" cellspacing="0"> <tr> <td width="15" height="5" bgcolor="#99ccff" nowrap> </td> </tr> </table> </td> <td width="100%" height="100%" valign="top" rowspan="2"> <table border="0" width="100%" cellspacing="0" cellpadding="0"> <tr> <td width="100%" height="50" align="left" class="sub-title"> Dynamic Menu Portal</td> </tr> <tr> <td height="15" bgcolor="#e6e6e6" nowrap> </td> </tr> <tr> <td height="15" bgcolor="#99ccff" nowrap> </td> </tr> <tr> <td height="70" nowrap> </td> </tr> <tr> <td align="center" nowrap> <table border="0" width="400" cellpadding="0" cellspacing="0"> <tr> <td bgcolor="#333333" nowrap> <table border="0" width="400" cellpadding="3" cellspacing="1"> <tr>

Screen image	Source
	<td height="30" bgcolor="#cc3333" align="center" class="sub-title" nowrap>IceWall SSO</td> </tr> <tr> <td height="150" bgcolor="#ffffff" align="center" nowrap> - Request ACL Error - <p>Unauthorized request.(dmp) <p>Please contact your system administrator. </td> </tr> </table> </td> </tr> </table> </td> </tr> </table> </td> <td width="15" height="100%" bgcolor="#99ccff" rowspan="2" nowrap> <table border="0" width="15" height="5" cellpadding="0" cellspacing="0"> <tr> <td width="15" height="5" bgcolor="#99ccff" nowrap> </td> </tr> </table> </td> <td width="15" bgcolor="#6699cc" rowspan="2" nowrap> <table border="0" width="15" height="5" cellpadding="0" cellspacing="0"> <tr> <td width="15" height="5" bgcolor="#6699cc" nowrap> </td> </tr> </table> </td> <td width="30" bgcolor="#336699" rowspan="2" nowrap>

Screen image	Source
	<table border="0" width="30" height="5" cellpadding="0" cellspacing="0"> <tr> <td width="30" height="5" bgcolor="#336699" nowrap> </td> </tr> </table> </td> </tr> <tr> <td width="195" height="100%" bgcolor="#336699" align="left" valign="top" nowrap> </td> </tr> </table> </body> </html>