

OTP SERVER
INTEGRATION MODULE

NOVELL® GROUPWISE™
V7 WEBACCESS

Copyright, NordicEdge®, 2005

1 Introduction

OTP Server Overview

Nordic Edge OTP Server adds an extra security layer to protect your applications. When the user id and password is successfully verified, a “One Time Password” is sent to the user’s mailbox or mobile phone through SMS (Short Message Services). This “One Time Password” will be verified and only then will the user be authenticated to the application.

Novell® GroupWise™ v7 Webaccess integration Overview

NordicEdge® integration for Novell® GroupWise™ v7 WebAccess enables strong authentication for access to mail and documents through web.

Pre-requisites & System requirements

GroupWise

Novell® GroupWise Webaccess v 7, configured to use a servlet engine with support for JAVA 2 Servlet 2.3 (IE Tomcat 4 and above, Orion, etc)

OTP Server

OTP Server 14c or higher.

OTP Server must be configured before the filter can be used. See OTP Server Administration Manual for more information on how to configure this.

Other

Access to the LDAP v3 directory used by GroupWise

2 Installation

Installing the integration module

Files needed

Unzip the file otp4gw7.zip:

otpwebaccess.jar – The NordicEdge® OTP login servlet
otpclient.jar – The NordicEdge® OTP Client API
login.jsp – Login page
login2.jsp – Response page
login.htt – Modified Webaccess template file

web.xml – Sample web.xml
otpwebaccess.properties – Sample properties file
server.xml – Sample tomcat server.xml file

Install

Follow these steps for a successful installation of the integrations module:

1. Unzip the file otp4gw7.zip:
 - a. Copy the content of the directory gw to the application server (normally sys:\tomcat\4\webapps\gw)
 - b. Copy the otpwebaccess.properties from the sample directory to a directory on the server running the servlet engine (sample sys:\tomcat\4\Novell)
2. Environment change:

- a. Edit the web.xml file on the servlet engine (normally sys:\tomcat\4\webapps\gw\WEB-INF\web.xml), and add the following at the start of the <web-app> section:

```
<filter>
  <filter-name>AuthenticationFilter</filter-name>
  <filter-class>se.nordicedge.otp.AuthenticationFilter</filter-class>
  <init-param>
    <param-name>LOGIN_PAGE</param-name>
    <param-value>/otp/login.jsp</param-value>
  </init-param>
  <init-param>
    <param-name>DEBUG</param-name>
    <param-value>ON</param-value>
  </init-param>
</filter>
<filter-mapping>
  <filter-name>AuthenticationFilter</filter-name>
  <url-pattern>/webacc</url-pattern>
</filter-mapping>
<servlet>
  <servlet-name>OTPWebaccess</servlet-name>
  <servlet-class>se.nordicedge.otp.OTPWebaccess</servlet-class>
  <init-param>
    <param-name>PROFFILE_PATH</param-name>
    <param-value>/tomcat/4/Novell/otpwebaccess.properties</param-
value>
  </init-param>
  <init-param>
    <param-name>DEBUG</param-name>
    <param-value>>true</param-value>
  </init-param>
</servlet>
```

Also make sure the web.xml have the correct tag:

```
<!DOCTYPE web-app
PUBLIC "-//Sun Microsystems, Inc.//DTD Web Application 2.3//EN"
"http://java.sun.com/dtd/web-app_2_3.dtd">
```

And add the following at the end of the <web-app> section:

```
<servlet-mapping>  
  <servlet-name>OTPWebaccess</servlet-name>  
  <url-pattern>/OTPWebaccess</url-pattern>  
</servlet-mapping>
```

Note! Make sure that the environment specific params match the current environment. A sample web.xml is provided under the sample directory. In some Tomcat versions the url-pattern have to end with /*, like:

```
/OTPWebaccess/*
```

- b. Edit the webacc.cfg used by GroupWise Webaccess or use Console One to change the parameters, and change:
Logout.url=/gw/otp/login.jsp?OTPSTATUS=3
- c. Edit the Tomcat server config (normally sys:\tomcat\4\conf\server.xml) and open the HTTP connector on port 8080. The section for the connector is not enabled by default. There is a sample server.xml in the sample directory.

3 Configuration

Configuration

Parameters otpwebaccess.properties

Parameters	Description
hostname	OTP Serverhost , all OTP server names and port, syntax "hostname:portnr;hostname2:portnr" etc.
loginpage	Login page URL , the URL to the login.jsp. Sample: /gw/otp/login.jsp
encryption	OTP Encryption , if the login servlet should use encrypted communication to NordicEdge® OTP-Server OTP server. If set to NO, encryption will be turned off.
responsepage	Response Page URL , the URL to the response page. Sample: /otp/login2.jsp
localscheme	The protocol used to access the webaccess servlet, no default. Valid values http and https.
localhost	The hostname to access the the webaccess servlet, default is localhost
localport	The portnumber to access the the webaccess servlet, no default
userattribute	The allowed attributes to be used to read data from user object. If this is not set, the OTP server configuration will be used. The attributes should be comma separated. A mapped named can be used to hide the actual LDAP attribute name. Like "sms mobile". The form should post the value in the parameter "userattribute".
debug	If the servlet should send out debug information.

Parameters	Description
	Value YES.
AllowNoneOTPAuthentication	Set to true to allow for none OTP authentication. WARNING! This will effect the overall security of the webaccess solution.
accept.x	This setting can be used to allow other units, accept normal browser, to get the correct html setup. For example to use a WAP browser, the value should be: accept.1=text/vnd.wap.wml home The x need to be replaced with a number, starting with 1.

Sample otpwebaccess.properties

A sample otpwebaccess.properties can be found in the sample directory.

Configuring the NordicEdge® OTP-Server for Novell® GroupWise

Information needed to proceed with the configuration:

- * The IP address of the server where the Tomcat instance running the integration servlet.
- * The IP address/host name and port number of a eDirectory server with LDAP enabled.
- * A user name and password for the OTP server to search for users in the directory. This user need only read rights to the user object and the attribute where the mobile phone number/mail address is stored. in the case when using the disable attribute to prevent to many login retries, the user also need read and write access to the disable attribute to be used.
- * The base DN where to search for users.
- * The attribute to search for users when the authenticate. Normally this is the cn attribute.

Configuration:

1. Install NordicEdge® OTP-Server as described in the Installation documentation.

2. To set up the NordicEdge® OTP-Server to support the Novell® GroupWise integration, start the OTP configuration, go to the “Radius & Clients” tab and press “Add Client”. Deselect the “Is RADIUS” checkbox. Enter the IP address of the server where the Tomcat instance running the integration servlet. Select the “Accept User Lookup Only” checkbox.
3. Under User Database, press “New”, and configure the eDirectory:
4. **Database Display Name** – Enter a display name of the configured directory
Database Type – Make sure it's LDAP
Host Address – The IP address/host name of the eDirectory server where the GroupWise users exists
Portnumber – The port number LDAP is running on the eDirectory server
Admin DN – The full DN of the user that the OTP server will authenticate as. Note! This is LDAP DN syntax using comma, sample `cn=gwuser,o=nordicedge`.
Admin Password – The admin password
Search Base DN – The DN where to search for the user
Search Scope – What type of scope (SUB, ONE, BASE), normally this is set to SUB
Search Filter Start – The start of the search filter to be used when searching for users, use the “Sample button” to get a sample of how the filter could look like for Novell eDirectory
Search Filter End - The end of the search filter to be used when searching for users
OTP Attribute – The attribute that holds the users mobile phone number or mail address
5. Press OK twice, and then Save.

4 Appendix A: Misc

Troubleshooting

For troubleshooting and support, please go to <http://www.nordicedge.se>.