

OTP SERVER
INTEGRATION MODULE

NETEGRITY®
SITEMINDER™ 6

Copyright, NordicEdge®, 2005

1 Introduction

1.1 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.

1.2 Netegrity® SiteMinder™ 6 integration Overview

NordicEdge® Secure Custom Authentication scheme for Netegrity® SiteMinder™ 6 enables strong authentication for applications using the Netegrity SiteMinder SSO framework.

1.3 Pre-requisites & System requirements

1.3.1 SiteMinder

SiteMinder 6 and above

1.3.2 OTP Server

OTP Server 14C or higher.

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

2 Installation

2.1 Installing custom authentication scheme

2.1.1 Files needed

Unzip the file otp4siteminder.zip:

nordicedgeotp.jar – NordicEdge® OTP Authentication Scheme

otp1.fcc – Sample Login Page

otp2.fcc – Sample Response Page

pwchange.jsp – Sample jsp file to support password services

pwchange.asp – Sample asp file to support password services

PWSelfChangeLogin.template – Sample password services CGI template file

2.1.2 Other

<SM installation> = the path where SiteMinder policy server was installed.

<SM agent installation> = the path where SiteMinder agent was installed.

2.1.3 Install

Follow these steps for a successful installation of the custom authentication scheme:

1. Copy nordicedgeotp.jar to all policy servers to the directory. Sample:
`<SM installation>\bin`

2. Copy otp1.fcc and otp2.fcc to the web server where the agent is installed to the directory <SM agent installation>\samples\forms
3. Add the jar file to the classpath in <siteminder>\Config\JVMOptions.txt, like:
*-Djava.class.path=C:/Program
Files/Netegrity/SiteMinder/bin/nordicedgeotp.jar;C:/Program
Files/Netegrity/SiteMinder/config/properties;C:/Program
Files/Netegrity/SiteMinder/bin/jars/SmJavaApi.jar;.....*

3 Configuration

3.1 Scheme Configuration

All settings for the authentication scheme are defined in SiteMinder custom authentication scheme. If a value is to be left blank a comma still has to be entered to maintain the enumeration of the parameters.

3.1.1 Parameters

Nr	Default value	Description
1	/siteminderagent/forms/otp1.fcc	Login URL , the URL to redirect to for initial login.
2	/siteminderagent/forms/otp2.fcc	Redirect URL , the URL to redirect to for challenge input.
3	localhost:3100	OTP Serverhost , all OTP server names and port, syntax "hostname:portnr;hostname2:portnr" etc.
4	YES	OTP Encryption , if the client should use encrypted communication to OTP server. Value YES/NO.
5	mail	Identity Attribute , the attribute to fetch the user value (mobile number, mail, etc.). Multiple values (max 3) separated by \$, like "idattr1\$idattr2\$idattr3".
6	/siteminderagent/pwccgi/smpwsewicescgi.exe/	Password services URL , the URL where SiteMinder Password Services resides.
7	N/A	Password Change URL , the URL where the password changes jsp/asp resides. Only use this if PWS is enabled.
8	N/A	OTS Attribute , used for integration with OTS (One Time signing). OTS is an additional product. Contact NordicEdge authorized reseller for more info. Leave blank if you don't have that product.

OTP SERVER - INTEGRATION MODULE

Nr	Default value	Description
9	N/A	Additional attribute in redirect. Sample: graceLogins LOGINRET OTP scheme will add the value of the users graceLogins to the URL as parameter LOGINRET when redirecting to otp2.fcc.
10	NO	Debug , enable/disable debug, set YES to enable.

3.2 SiteMinder Configuration

3.2.1 Administration

1. In the SiteMinder Admin GUI, create a new auth scheme.
2. Select a name and description.
3. Choose “Custom Template” in the “Authentication Scheme Type” drop down list.
4. Change the protection level to apply to your company security policy.
5. Enter “smjavaapi” as “Library”.
6. Enter your parameters starting with “se.nordicedge.NordicEdgeOTP” followed by a space and the parameters with a “,” as separator, see Parameters section above.
NOTE! There must be no CR or new line since that will cause the scheme to not load. Make sure there is only a space, “ ”, leading the parameter list.
Sample:
se.nordicedge.NordicEdgeOTP
/siteminderagent/forms/otp1.fcc,/siteminderagent/forms/otp2.fcc,192.168.10.1:3100,no,mobile,,,,,yes
7. Save the auth scheme.
8. Choose the newly created scheme as “Authentication Scheme” in your realms.

The screenshot shows a 'SiteMinder Authentication Scheme Dialog' window. The title bar reads 'SiteMinder Authentication Scheme Dialog'. The main title is 'Authentication Scheme Properties' with a 'HELP' button. The dialog is divided into two main sections: 'Scheme Common Setup' and 'Scheme Setup' (Advanced).

Scheme Common Setup:

- *Name: NordicEdge OTP
- Description: NordicEdge OTP
- Authentication Scheme Type: Custom Template
- Protection Level: 1000 [0 - 1,000, higher is more secure]
- Password Policies Enabled for this Authentication Scheme

Scheme Setup (Advanced):

- Library: %smjavaapi
- Secret: [Redacted]
- Confirm Secret: [Redacted]
- Parameter: %se.nordicedge.NordicEdgeOTP /siteminderagent/forms/otp1.fcc,/siteminderagent/forms/otp2.fcc,192.168.10.1:3100,,mobile,,,,yes
- Enable this scheme for SiteMinder Administrators

Buttons at the bottom: OK, Cancel, Apply.

Footer text: Authentication Scheme jotp2

3.2.2 SiteMinder® Password Services

Due to limitations in the SiteMinder® API, a work-around has to be done to enable password services support. This includes a jsp/asp page and a modified password services template.

To configure this:

1. Copy PWSelfChangeLogin.template to the agent where the redirect is configured (parameter 8).
2. Copy pwchange.jsp or pwchange.asp to a directory on the web server.
3. Create a basic auth scheme with a lower “Protection Level” than the OTP auth scheme.
4. Create a realm that protect the pwchange.* and protect it with the basic auth scheme.
5. Under the realm, create a rule with action “get”.
6. Create a policy, add the rule and make sure to give the users access.

4 Appendix A: Misc

4.1 Troubleshooting

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