

OTP SERVER
INTEGRATION MODULE

MICROSOFT® ISA
SERVER 2006™

Copyright, NordicEdge®, 2010

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 Microsoft® ISA Server 2006™ integration Overview

NordicEdge® integration for Microsoft® ISA Server 2006™ enables strong authentication for web publishing using the applications using the Microsoft® ISA Server 2006™ framework.

1.3 Pre-requisites & System requirements

1.3.1 Microsoft ISA Server

Microsoft ISA Server 2006

1.3.2 OTP Server

OTP Server 1.6 (Build 2471) 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.

1.3.3 Other

Access to a AD using LDAP/LDAPS (port 389 or 636).

LDAP/LDAPS port must be opened from OTP server to the AD server.

RADIUS port, 1812, must be opened from ISA server to OTP server.

OTP port, 3100, must be opened from ISA server to OTP server.

2 Installation

2.1 Installing the integration module

2.1.1 Files needed

Unzip the file sin NE_OTP_ISA2006_ver2.0.zip:

otpwebfilter.dll – The NordicEdge ISA web filter

usr_pwd_pcode.htm – OTP login template

nordicedge.js – OTP login javascript

dojo.js – AJAX javascript

otp.reg – Registry file to set OTP server address

2.1.2 Installing

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

1. Backup file:
Backup the login page
<isa_home>\CookieAuthTemplates\ISA\HTML\usr_pwd_pcode.htm
sample:
*C:\Program Files\Microsoft ISA
Server\CookieAuthTemplates\ISA\HTML\usr_pwd_pcode.htm*
2. Copy files:
Copy the content in isa directory of the otp4isa2006.zip to the ISA server
installation directory, sample:
C:\Program Files\Microsoft ISA Server
3. Register otp webfilter
Register otpwebfilter.dll with the command:

regsvr32 otpwebfilter.dll

3 Configuration

3.1 Configuration

3.1.1 Parameters used by the OTP filter

| Parameters | Description |
|-------------|---|
| OTPSERVERIP | OTP Serverhost , all OTP server names and ports, syntax "hostname:portnr;hostname2:portnr2" Note: This values must match the order in the |

Edit the otp.reg, and replace the IP address with the current address of the OTP server. Run the reg file on the ISA server.

3.2 Microsoft ISA Server 2006 Configuration

3.2.1 Administration

1. Start the Microsoft ISA Server Management tool
2. Open the web listener that you wish to protect
3. Go to the tab "Authentication"
4. Enable "HTML Form Authentication"
5. Enable "Collect additional delegation credentials in the form"
6. Press the button "Configure Validation Server"
7. Press "Add"
8. Enter the DNS name or IP address of the OTP server
9. Enter a description for the server
10. Enter "Shared secret" (Must match shared secret in OTP server)
11. If using multiple OTP servers for fail over, set down the timeout to decrease the wait time during a fail over, sample value set to 3 will have the ISA server try 3 times and wait 3 second each time, result in a wait of 9 seconds for the user.
12. Press "OK" to save
13. If using multiple OTP servers, complete step 7-12 for each server, and make sure that the order of the server match the orde configured in step 3.1.1 (in otp.reg)
14. Press "Advanced" button
15. Make sure that "Require all users to authenticate" is enabled
16. Press "OK" twice to save
17. Go to the "Configuration" and "Add-ins"
18. Click on "Web Filters"

19. Make sure that "OTP authentication filter" is in the list, and that it is higher in order than any other authentication filter.
20. Press "Apply" to save the configuration to ISA
21. Restart the "Microsoft Firewall" service

3.2.2 Configuring the NordicEdge® OTP-Server for Microsoft® ISA Server 2006

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

1. To set up the NordicEdge® OTP-Server, go to the "RADIUS & Clients" tab
2. Make sure that RADIUS Portnr is set to 1812
3. Press "Add Client", and enter:
 - a client display name, e.g. "ISAServer"
 - the ip adress of the ISA Server
 - enter the "Shared Secret" (this must match shared secret set up in the ISA server RADIUS configuration)
 - deselect the "Uses Challenge/Response" check box
 - enter the ip address of the ISA server in "Auth. Server IP Address"

1. Press "New" to configure a new database:

Host Settings

Database Display Name – Enter a display name, e.g. "AD"
Host Address – The IP address of the Active directory server
Port number – The port number of the Active directory server
Admin DN – The admin DN or username@domain
Admin Password – The password for the Admin DN user.
Test LDAP Connection – Use this button to verify your settings.

Search Settings

Search Base DN – The DN where to start searching for users.
Search Scope – What level of search, SUB, ONE or BASE. Use SUB unless you understand the implications of the other settings.
Nr of Connections – The number of LDAP connections the OTP server should use.
Search Filter start – The start of the search filter to be used to authenticate

users.

Search Filter end – The end of the search filter to be used to authenticate users.

Account Settings

OTP Attribute – The attribute on the user where to get the mobile number/mail address.

4. Press OK twice, and then Save.
5. If not already started, start the NordicEdge® OTP-Server

4 Appendix A: Misc

4.1 Troubleshooting

When using multiple OTP servers for fail over, the ISA filter will keep track of the OTP server being used, by adding the server address in the registry value OTPSERVERACTIVE. This value is cleared at startup of the ISA server, so when a OTP server is brought back up (after failure), the value of the registry value OTPSERVERACTIVE must be deleted, or the ISA server needs to be restarted.

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