

OTP SERVER
INTEGRATION MODULE

OUTLOOK WEB ACCESS

Copyright, NordicEdge[®], 2008

1 Introduction

1.1 Overview

NordicEdge One Time Password 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 Integration Module Overview

Outlook Web Access integration module for NordicEdge One Time Password Server™ enables strong authentication for Microsoft OWA. An ISAPI filter, IIS Secure Access Filter, protects the OWA web application and communicates with the OTP Server.

Product Features:

- Supports Basic and Forms authentication
- Installed as an ISAPI filter to protect all incoming requests
- Customizable login and error templates
- Logging
- Secure logoff
- Set default domain name

1.3 Pre-requisites & System requirements

1.3.1 OS

IIS Secure Access Filter runs on the following Windows platforms:

Windows 2003 SP2 64 bit (X64)

Itanium IA64 not supported.

1.3.2 IIS & Exchange

IIS Secure Access Filter runs on the following IIS and Exchange versions:

IIS 6

Exchange 2007

1.3.3 Active Directory

Active Directory must be setup and configured for NordicEdge® OTP Server to authenticate and retrieve mobile numbers for users.

OTP can use any LDAP v3 compatible Directory Service and also an ODBC compliant database server to perform authentication and mobile lookup. AD is the recommended Directory Service for OWA.

1.3.4 OTP Server

NordicEdge One Time Password Server™ 1.6 or higher.

2 Installation

2.1 Installing Outlook Web Access integration module

2.1.1 Install OWA Integration module

Before installing the OWA Integration Module make sure that Exchange is installed and working and also that there is an installed NordicEdge One Time Password Server™ available (does not have to be on the same machine as OWA 2003).

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

1. Download the latest package and the latest revision of this document from the NordicEdge One Time Password Server™ product site.
2. Unzip and copy to [C:/Program Files/NordicEdge/](#) or other location of choice. Be sure to change any references to the new location if changed.
3. Change the “install dir”/OtpFilter/OtpFilter13.ini to OtpFilter13.ini.org
4. Change the “install dir”/OtpFilter/OtpFilter13.ini.outlook2007 to OtpFilter13.ini
5. In the ini file make sure that OtpServerList is set to the correct address and also check any path references like logfiles etc, that they are correct.
6. Open IIS manager and navigate to the default web site (or the website that contains the exchange application).
7. Select properties and click the ISAPI-Filter tab.
8. Select add.
9. Enter OtpFilter13 as the name of the filter and browse for the OtpFilter13.dll found in the “install dir”/filter folder. Note that the dll can be placed in any folder as long as the ini file is placed in the same folder.
10. Click Apply.

11. Create a new virtual folder named OtpWeb (change if you specified another name during install). Browse for "install dir"/OtpWeb/Outlook2007. Set Basic authentication only and change the Application pool to MExchangeOWAAppPool.
12. Open IIS Manager and navigate to /exchange, /owa and /exchweb virtual folders.
13. Uncheck Integrated Windows Authentication under Directory Security.
14. Restart IIS to load the filter. Open the ISAPI-Filter tab again and check that the filter is running. Note that IIS 6.0 does not load the filter until the first request.

3 Configuration

3.1 Filter Configuration

All settings for the filter are defined in the OtpFilter13.ini file. This file must exist in the same folder as the filter dll (OtpFilter13.dll). If any parameters are missing default data will be used by the filter. Several parameters specify URL or file paths which obviously must be valid for the filter to run properly. All file paths used by the filter must have the necessary access rights.

3.1.1 Parameters used by OWA integration module

Value	Meaning
FilterActive	FilterActive specifies if the filter is active or not. If set to 1 the filter is activated and if set to 0 the filter is deactivated and does not perform any actions. Default value is 0.
LogonTemplateURL	LogonTemplateURL specifies the URL for the page which collects credentials from the user. The default value is '/otpweb/OtpLogonExchange2007_en.aspx'. Note that if any images or other resources is used on the logon template those resources must be excluded using the ExcludeUrl directive.
LogoffURL	LogoffURL specifies the URL for the page that should be used to reset OTP authentication for the logged on user. This could be any page. The default value is '/otpweb/otplogoff.gif'. Note that if any images or other resources is used on the logon template those resources must be excluded using the ExcludeUrl directive.
ErrorTemplateURL	ErrorTemplateUrl specifies the URL for the template that the filter redirects any errors to. The default value is '/otpweb/ErrorExchange2007_en.aspx'. Note that if any images or other resources is used on the logon template those resources must be excluded using the ExcludeUrl

OTP SERVER – INTEGRATION MODULE

Value	Meaning
ErrorTemplateURL	ErrorTemplateUrl specifies the URL for the template that the filter redirects any errors to. The default value is '/otpweb/ErrorExchange2007_en.aspx'. Note that if any images or other resources is used on the logon template those resources must be excluded using the ExcludeUrl directive.
IncludeUrl	IncludeUrl specifies the URL's that the filter should include in a comma separated list. If an empty value is used the filter will protect root. The default value is '/exchange, /otpweb,/owa,/exchweb,/public'.
ExcludeUrl	ExcludeUrl specifies the URL that the filter should exclude in a comma separated list. The filter will only trigger on URL's with its base from IncludeUrl. This must be used for pages specified in LogonTemplateUrl, LogoffUrl or ErrorTemplateUrl if they include any resources like images, css etc. Use empty value to not exclude any URL's. The default value is '/otpweb/open'.
MaxCacheUsers	MaxCacheUsers specifies the maximum amount of users that simultaneously can exist in the filters user cache. Note that this setting may affect server memory usage and performance. A higher setting will use more RAM memory. The default value is '1000'.
CacheReorderThreshold	CacheReorderThreshold specifies the point when a user should be moved to the top of the cache. Note that this setting may affect performance. The default value is '50'.
OtpServerList	OtpServerList specifies the OTP fail-over servers in a comma separated list. Each server contains dns:port where dns is the server dns name, like 123.123.123.123 or otp.company.com and port is the portnumber that the OTP server listens to. The default value is '127.0.0.1:3100'. The filter will always try the first server in the list.
EnableLogging	EnableLogging specifies if logging is enabled or not. If set to 1 logging is enabled and if set to 0 logging is disabled and does not perform any logging. Default value is 0.
LogPath	LogPath specifies the URL for the log file. The default value is 'install dir\OtpFilter\Log\OtpFilter12.log'. If the log file is not found or cannot be read or created, the filter will not be started.

OTP SERVER – INTEGRATION MODULE

Value	Meaning
LogLevel	LogLevel specifies the level of log information written to the log file. The default value is 0. LogLevel can be set to 0, 1, 2 and 99. Higher values means that more information is written to the log file. Note that extensive logging affects performance. Only use LogLevel 99 for debug or test purposes.
SecurityLevel	SecurityLevel specifies the level of security for the filter. The highest security value is 1. Set security value to 2 to allow OTP in mixed mode that makes it possible to configure OTP to disable the need for an OTP challenge for certain users. Only use security levels of 2 and higher for debugging and test purposes. Production environments should always use security level 1. The default value is 1.
CacheExpireTime	CacheExpireTime specifies the amount of time in seconds that users are allowed to be inactive. If a user has been inactive for the specified time the user will need to login again with a new OTP. The default value is 3600 (1 hour). Set the value to 0 to never expire users.
AuthMode	AuthMode specifies which authentication mode to use. Valid authentication modes are Basic and OtpForm. On IIS only basic authentication must be used for all protected paths (both included and excluded URL's). Default is OtpForm.
OtpFormLogonTemplateUrl	OtpFormLogonTemplateURL specifies the template to use for collecting user credentials, when using OtpForm authentication mode. Default is /otpweb/OwaLogonExchange2007_en.aspx.
OtpFormUserParam	OtpFormUserParam specifies the parameter that is used to send the username in the GET response from the logon page. Default is username. If changed make sure to also change the OTP form logon template.
OtpFormPasswordParam	OtpFormPasswordParam specifies the parameter that is used to send the password in the GET response from the logon page. Default is password. If changed make sure to also change the OTP form logon template.
DefaultDomainName	DefaultDomainName specifies what windows domain name to use if no domain name is supplied by the user. Default is empty.

Value	Meaning
Excludelp	Excludelp specifies a comma separated list of ip-addresses that the filter should ignore. This could be used if internal applications need to communicate with the server without using OTP. Default is empty.

3.1.2 Defining logoff URL

In the filter it is possible to define a logoff URL that will reset the users IIS Secure Access Filter status, so that the user must logon again with a One Time Password.

This is very important because Exchange does not completely logoff a user using the built in logoff page. The user must close the browser to do this (except when using Exchange 2003 and IE 6 sp1). Some Exchange versions does not even have a logoff function.

It would then be possible to create a logoff link, button etc that can be mapped to the filters logoff URL. Make sure that any resources in the page used as the logoff page are excluded in the filter configuration (ExcludeUrl).

One problem with for example Exchange 2007 is that several different logoff pages can be used for different languages, but only one logoff page can be defined in the filter. One solution for this would be to include an image in all logoff pages that is mapped to the filters logoff parameter. Make sure that this image is only used for these logoff pages or users might be logged of unexpectedly.

3.2 Exchange Configuration

3.2.1 OWA Basic Authentication

Follow these steps to configure the OWA module to use forms based authentication.

1. For the filter to function properly, only basic authentication must be set on the “/exchange”, “/owa” and “/exchweb” folders in IIS.

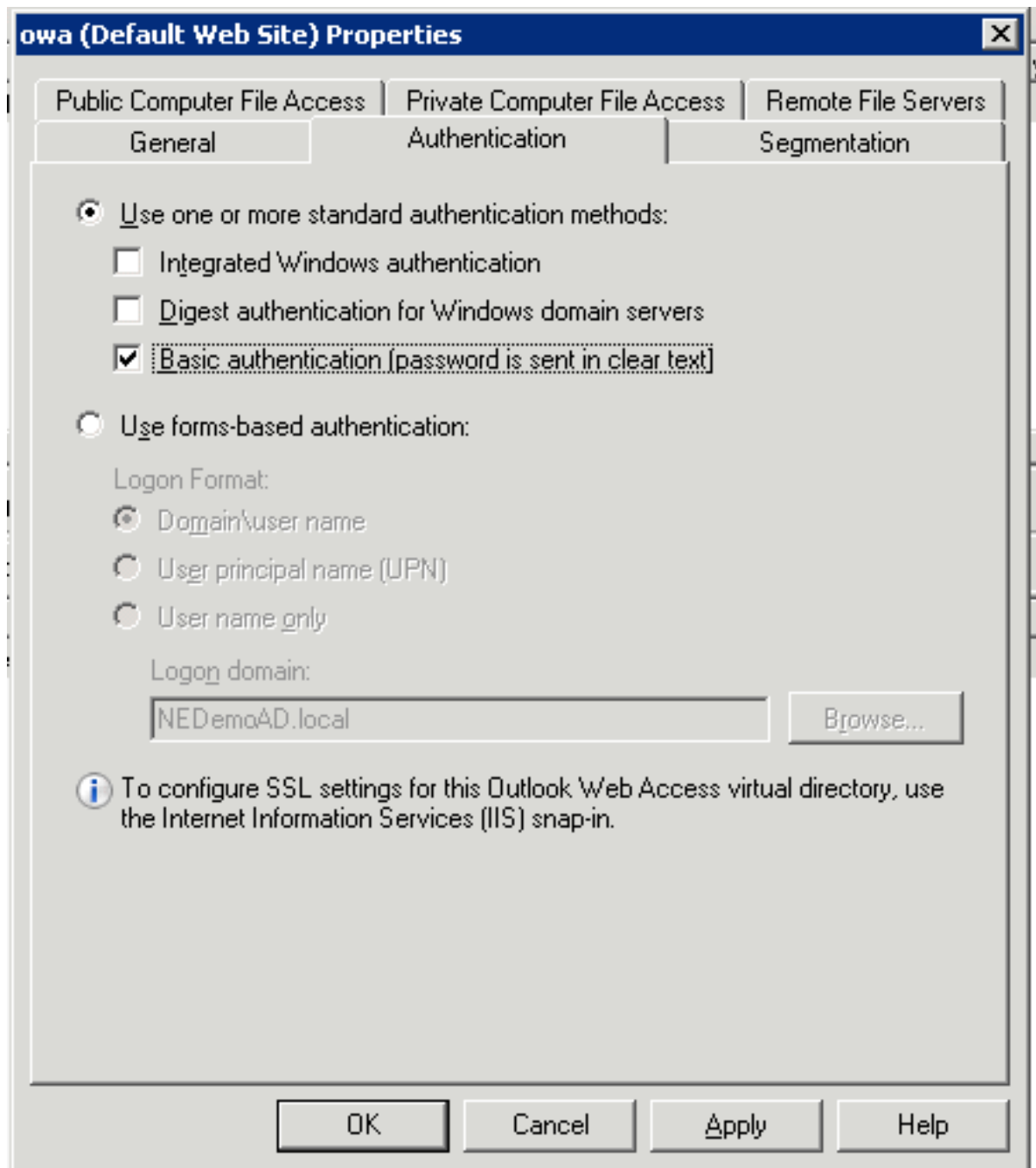
2. In Exchange system manager, forms based authentication must be turned **OFF** (The NordicEdge ISAPI filter is used instead of the one shipped with OWA).

Also note that experimenting with permissions and settings for Exchange can seriously damage your Exchange installation. If the filter does not work as expected, always test exchange without the filter to see that exchange is ok.

3.2.2 OWA Forms Authentication

Follow these steps to configure the OWA module to use forms based authentication.

1. For the filter to function properly, only basic authentication must be set on the “/exchange”, “/owa” and “/exchweb” folders in IIS.
2. Under /otplib make sure that the directory /open and the files OwaLogonExchange2007_en.aspx and ErrorExchange2007_en.aspx is set to anonymous authentication.
3. In Exchange system manager, forms based authentication must be turned **OFF** (The NordicEdge ISAPI filter is used instead of the one shipped with OWA).

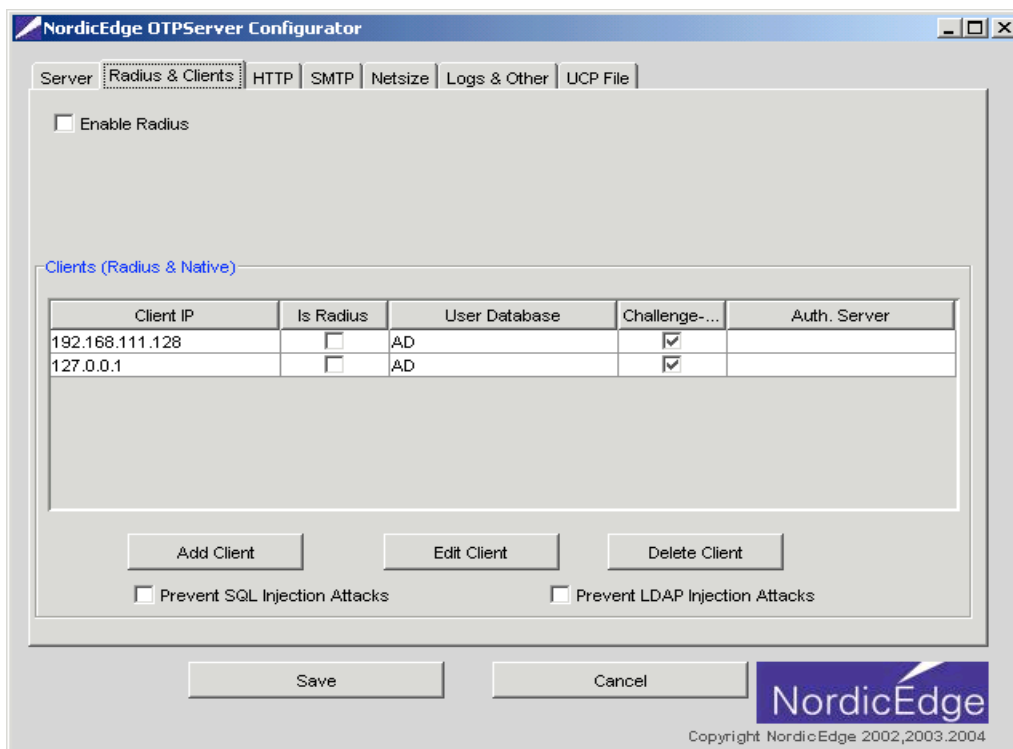


Also note that experimenting with permissions and settings for Exchange can seriously damage your Exchange installation. If the filter does not work as expected, always test exchange without the filter to see that exchange is ok.

3.3 OTP Configuration

For the filter to communicate with the NordicEdge One Time Password Server™ correctly certain configuration parameters must be set on the NordicEdge One Time Password Server™.

First OTP must be able to lookup the user name sent to the NordicEdge One Time Password Server™ by the filter. This means that the IIS server must be set up as a radius client and that an LDAP or SQL must be configured to lookup the user's mobile number.



3.3.1 Radius client sample

Make sure that the IIS server is added as a client in NordicEdge OTP Server™. For detailed information about NordicEdge OTP Server™ parameters, please consult the NordicEdge One Time Password Server™ administration guide.

The screenshot shows a dialog box titled "Native or Radius Client" with a close button (X) in the top right corner. The main heading is "Modify Client '192.168.111.128'". Below this, there are several fields and checkboxes:

- Client IPAddress:** A text box containing "192.168.111.128" and a checkbox labeled "Is RADIUS" which is currently unchecked.
- Shared Secret:** An empty text box.
- Uses Challenge/Response:** An unchecked checkbox.
- Accept User Lookup only:** An unchecked checkbox.
- User Database:** A dropdown menu with "AD" selected. Above the dropdown is the text "User Database" in blue.

At the bottom of the dialog, there are three buttons: "New", "Edit", and "Delete". Below these are three more buttons: "OK", "Options", and "Cancel".

3.3.2 Modify Radius client sample:

Make sure that the Accept User Lookup Only is checked. If not set, the filter will not work properly. For detailed information about NordicEdge OTP server parameters, please consult the NordicEdge One Time Password Server™ administration guide.

Editing AD UserDatabase

Database Display Name:

Database Type:

LDAP | JDBC | Database Group

Host Settings

Host Address:

Portnumber: SSL TLS

Admin DN:

Admin Password:

LDAP Settings

OTP Attribute: ...

Login Retries:

Inactive Attribute: ...

Inactive Value:

Disable OTP Attribute: ...

Disable OTP Value: Not

OneTime Password Prefetch

Enable OTP Prefetching

Search Settings

Search Base DN: ...

Search Scope: Nr of Connections:

Search Filter Start:

Search Filter End:

3.3.3 Edit LDAP database sample

Make sure that the search filter can retrieve the user names that should be used by the filter to authenticate through the NordicEdge OTP Server. For detailed information about NordicEdge OTP server parameters, please consult the NordicEdge One Time Password Server™ administration guide.

4 Appendix A: Misc

4.1 Memory planning

The filter stores all user information in an in-memory cache for fast lookups and a minimal performance overhead. To calculate how much RAM memory the server needs for the expected amount of users, use the formula below. Note that the operating system, IIS server and other services also need memory to run properly.

RAM needed by filter (Kb) = 1.2Kb * max amount of users

4.2 Troubleshooting

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