

**OTP SERVER**  
INTEGRATION MODULE

**IIS SECURE ACCESS**  
**FILTER 1.3**

Copyright, NordicEdge<sup>®</sup>, 2006

# 1 Introduction

## 1.1 Overview

Nordic Edge 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 IIS Secure Access Filter Overview

Nordic Edge® Secure Access Filter for IIS enables strong authentication for applications running on Microsoft IIS Server, like Outlook Web Access (OWA). Use existing authentication technologies like Basic authentication in combination with our One Time Password protection to secure your web applications for use on the internet, intranet or extranet environments. It is also possible to us form based authentication using the OtpForm method.

Product Features:

- Supports Basic, Forms authentication
- Installed as an ISAPI filter to protect all incoming requests
- Inactivity expire time
- Customizable login and error templates
- Logging
- Secure logoff
- Supports proxy servers

## 1.3 Prerequisites & system requirements

---

### 1.3.1 OS

---

IIS Secure Access Filter runs on the following Windows platforms:

- Windows NT 4 Server SP 6
- Windows 2000 Server SP 4
- Windows 2003 Server

---

### 1.3.2 IIS

---

IIS Secure Access Filter runs on the following IIS versions:

IIS 4, IIS 5, IIS 6

---

### 1.3.3 Active Directory & LDAP

---

Active Directory must be setup and configured for Nordic Edge One Time Password Server™ to authenticate and retrieve mobile numbers for users.

Nordic Edge® OTP Server 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 IIS Secure Access Filter.

---

### 1.3.4 OTP Server

---

Nordic Edge One Time Password Server™ 14C or higher.

Nordic Edge OTP Server must be configured before the filter can be used. See Nordic Edge One Time Password Server™ Administration Manual for more information on how to configure this.

## 2 Installation

### 2.1 Installing IIS Secure Access Filter

---

#### 2.1.1 Install IIS Secure Access Filter

---

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

1. Download the latest package and the latest revision of this document from the Nordic Edge One Time Password Server™ product site.
2. Unzip and copy to C:\Program Files\Nordic Edge\ or other location of choice. Be sure to change any references to the new location if changed.
3. Open IIS management console and select the web that should be protected.
4. Select properties and click the ISAPI-Filter tab.
5. Select add.
6. 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.
7. Click Apply.
8. Restart IIS to load the filter. Open the ISAPI-Filter tab again and check that the filter is running. Note that if you are running IIS 6.0, the filter will not be loaded until the first request has been made.
9. Continue to configure the filter described in Chapter 3 to change the default settings. Note that the installer will configure a number of attributes.
10. After all configuration parameters have been set, IIS must be restarted to load the new settings. Remember to set FilterActive=1 in the configuration file.

## 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

---

Value	Meaning
<b>FilterActive</b>	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.
<b>OtpTemplateURL</b>	OtpTemplateURL specifies the URL for the page which collects the OTP challenge from the user. The default value is '/otpweb/logon.asp'. Note that if any images or other resources is used on the logon template those resources must be excluded using the ExcludeUrl directive.
<b>LogoffURL</b>	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/logoff.asp'. Note that if any images or other resources is used on the logon template those resources must be excluded using the ExcludeUrl directive.

## OTP SERVER – INTEGRATION MODULE

Value	Meaning
<b>ErrorTemplateURL</b>	ErrorTemplateUrl specifies the URL for the template that the filter redirects any errors to. The default value is '/otpweb/error.asp'. Note that if any images or other resources is used on the logon template those resources must be excluded using the ExcludeUrl directive.
<b>IncludeUrl</b>	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 '/otpweb'.
<b>ExcludeUrl</b>	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'.
<b>MaxCacheUsers</b>	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'.
<b>CacheReorderThreshold</b>	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'.
<b>OtpQueryString</b>	OtpQueryString specifies which query string parameter should be used by the filter to read the OTP challenge from the logon page. The default value is 'otppwd'.
<b>OtpServerList</b>	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.

## OTP SERVER – INTEGRATION MODULE

Value	Meaning
<b>EnableLogging</b>	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.
<b>LogPath</b>	LogPath specifies the URL for the log file. The default value is 'C:\inetpub\Filter\OtpFilter.log'. If the log file is not found or cannot be read or created, the filter will not be started.
<b>LogLevel</b>	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.
<b>SecurityLevel</b>	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.
<b>CacheExpireTime</b>	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.
<b>AuthMode</b>	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 value is Basic.
<b>OtpFormLogonTemplateUrl</b>	OtpFormLogonTemplateURL specifies the template to use for collecting user credentials, when using OtpForm authentication mode.  Default value is /otpweb/otpform.asp.

## OTP SERVER – INTEGRATION MODULE

Value	Meaning
<b>OtpFormUserParam</b>	OtpFormUserParam specifies the parameter that is used to send the username in the GET response from the logon page. Default value is username. If changed make sure to also change the OTP form logon template.
<b>OtpFormPasswordParam</b>	OtpFormPasswordParam specifies the parameter that is used to send the password in the GET response from the logon page. Default value is password. If changed make sure to also change the OTP form logon template.
<b>DefaultDomainName</b>	DefaultDomainName specifies what windows domain name to use if no domain name is supplied by the user. Default value is empty.

## 3.2 IIS configuration

---

### 3.2.1 Filter templates

---

The filter uses three templates to display the OTP logon page (if using OtpForm authentication mode), OTP challenge page and OTP error page. These templates can be custom made to fit any corporate standards. If the default templates are changed, they must still perform certain functions for the filter to work properly. Do not remove any code that is marked as necessary by the filter.

The templates can be placed in any folder as long as it can be added as a directory in IIS.

Create template directories in IIS:

1. Open IIS manager.
2. Browse to the web site where the filter is installed.
3. Right-click on the web site and select to create a new virtual directory.
4. Add “otpweb” as the alias for the directory. Browse for the folder that contains the templates, “install dir/OtpWeb/Generic”. The alias does not need to be named “otpweb”, just make sure that the configuration file is updated accordingly.
5. Set authentication type to Basic. If using OtpForm the folder /open and the files specified by **ErrorTemplateURL** and **OtpFormLogonTemplateUrl** must be set to anonymous authentication.
6. Update the configuration file to point to the logon, challenge and error templates.

If there are any images or other resources in any templates or logoff URL, those resources must be placed in a directory that is excluded from the filter. This is done using the ExcludeUrl parameter in the configuration file.

**Note:** All linked resources under a protected URL must be included in the IncludeURL or in the ExcludeURL configuration parameter. If not, unexpected results could occur.

---

## 3.2.2 Authentication Type

---

The filter supports Basic and form based authentication types, but IIS must only be set to Basic authentication. Make sure that all resources that should be protected by the filter use the chosen authentication type (exceptions are pages used before the user is authenticated by the filter).

Set authentication type in IIS:

1. Open IIS manager.
2. Browse to the web site where the filter is installed.
3. Browse to the directory that should be protected.
4. Right-click and select properties.
5. Select the Directory Security tab and then edit.
6. Select Basic authentication. These settings must also match the setting of the filter configuration file.
7. Continue with step 3 for all resources that should be protected.

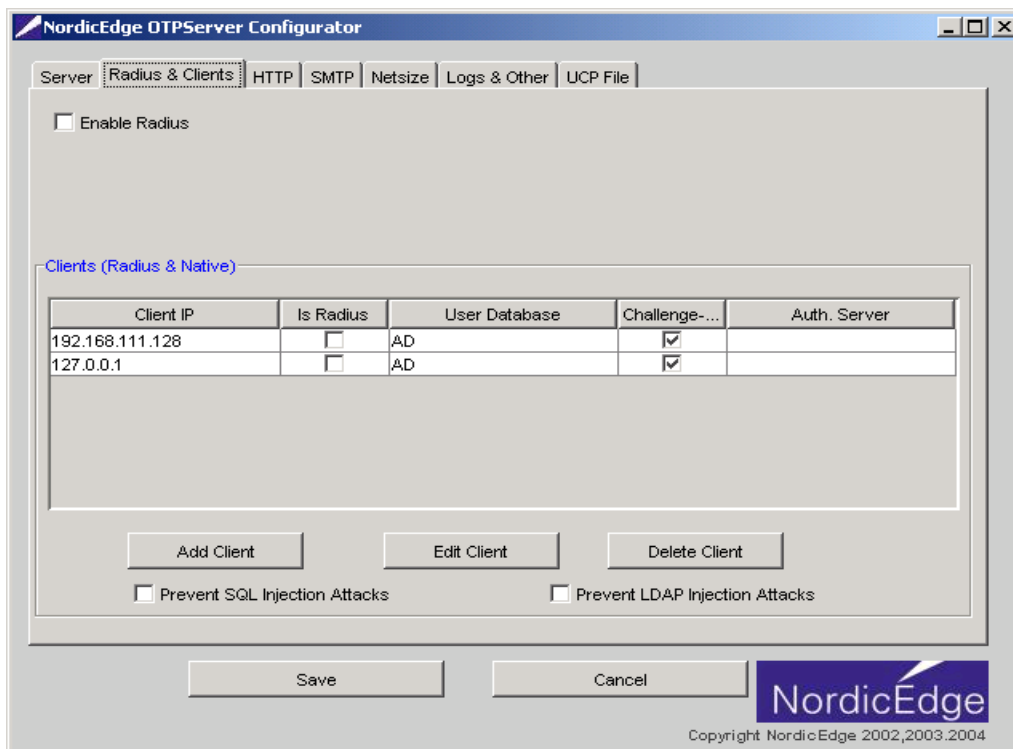
**Note! Due to basic authentication being used, web site should use HTTPS (SSL), since basic authentication type send user name and password in clear text over the internet.**

## 3.3 OTP Configuration

For the filter to communicate with the NordicEdge OTP Server correctly certain configuration parameters must be set on the NordicEdge OTP Server.

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

Detailed information about configuring the NordicEdge OTP Server please consult the NordicEdge One Time Password Server™ administration manual.



### 3.3.1 Client sample

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

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".

At the bottom of the dialog, there are two rows of buttons:

- Row 1: "New", "Edit", and "Delete" buttons.
- Row 2: "OK", "Options", and "Cancel" buttons.

---

### 3.3.2 Modify client sample:

---

For detailed information about Nordic Edge OTP server parameters, please consult the Nordic Edge One Time Password Server™ administration guide.

Editing AD UserDatabase

Database Display Name: AD

Database Type: LDAP

LDAP | JDBC | Database Group

**LDAP Settings**

**Host Settings**

Host Address: 192.168.111.128

Portnumber: 389  SSL  TLS

Admin DN: ator,CN=Users,DC=security,DC=ctx

Admin Password: \*\*\*\*\*)

Certificates Test LDAP Connection

**Account Settings**

OTP Attribute: mobile ...

Login Retries: 2

Inactive Attribute: ...

Inactive Value: ...

Disable OTP Attribute: pager ...

Disable OTP Value: nootp  Not

**OneTime Password Prefetch**

Enable OTP Prefetching Configure Prefetch OTP

**Search Settings**

Search Base DN: CN=Users,DC=security,DC=ctx ...

Search Scope: SUB Nr of Connections: 5

Search Filter Start: (&(cn= Samples

Search Filter End: )(objectclass=person))

Test LDAP Authentication

OK Cancel

### 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 Nordic Edge OTP Server. For detailed information about Nordic Edge OTP server parameters, please consult the Nordic Edge 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>.