

**NORDICEDGE ONE TIME  
PASSWORD SERVER™  
INTEGRATION MODULE**

**CITRIX ACCESS  
GATEWAY 4.5**

Copyright, NordicEdge®, 2008

# 1 Introduction

## NordicEdge One Time Password Server™ 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.

## Integration Module Overview

Citrix Access Gateway 4.5.x integration module for NordicEdge One Time Password Server™ enables strong authentication for Citrix Access Gateway.

Product Features:

- Works with stand-alone AAC and behind CAG appliance
- RADIUS configuration for CAG 4.5 Standard Edition
- Multiple serves for fail-over
- Select logonpoints to protect

## Pre-requisites & System requirements

---

### OS

---

Citrix Access Gateway integration module runs on the following Windows platforms:

Windows 2003 SP2 or higher

---

### Active Directory

---

Active Directory must be setup and configured for NordicEdge One Time Password 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.

---

### OTP Server

---

NordicEdge One Time Password Server™ 1.6 or higher.

---

### Citrix Access Gateway

---

Tested with CAG 4.5 and 4.5.5/4.5.6 Appliance.

Tested with CAG 4.5 AAC and with latest patch (AAC450W004). Note that the patch AAC450W001 patch can damage authentication. Check for more information on [www.citrix.com](http://www.citrix.com) and/or [www.nordicedge.se](http://www.nordicedge.se).

## 2 Installation

### Installing Citrix Access Gateway 4.5 Standard Edition and Advanced Edition integration module

#### Install Integration module for Advanced Access Control (Advanced Edition)

1. Download the latest package and the latest revision of this document from the NordicEdge One Time Password Server™ product site.
2. Backup the Citrix web root, c:\inetpub\wwwroot\CitrixLogonPoint (default location)
3. Unpack the zipfile contents to c:\inetpub\wwwroot\
4. Backup C:\inetpub\wwwroot\CitrixLogonPoint\web.config
5. Edit C:\inetpub\wwwroot\CitrixLogonPoint\web.config:

Add:

```
<add name="AGEHookup" type="Nordicedge.OtpServer.Citrix.AGEHookup,
Nordicedge.OtpServer.Citrix" />to <httpModules> section.
```

Add:

```
<add key="OtpServerList" value="127.0.0.1:3100" /> (ip address of the
NordicEdge One Time Password Server™)
```

```
<add key="ExcludedLogonPoints" value="SampleLogonPoint" /> (put any
logonpoints that should not use OTP here)
```

to <appSettings> section

Make sure that the key AuthenticationServiceUrl points to localhost and not the ip-address or DNS name of the server. This is not a OTP Server configuration, but a Citrix configuration.

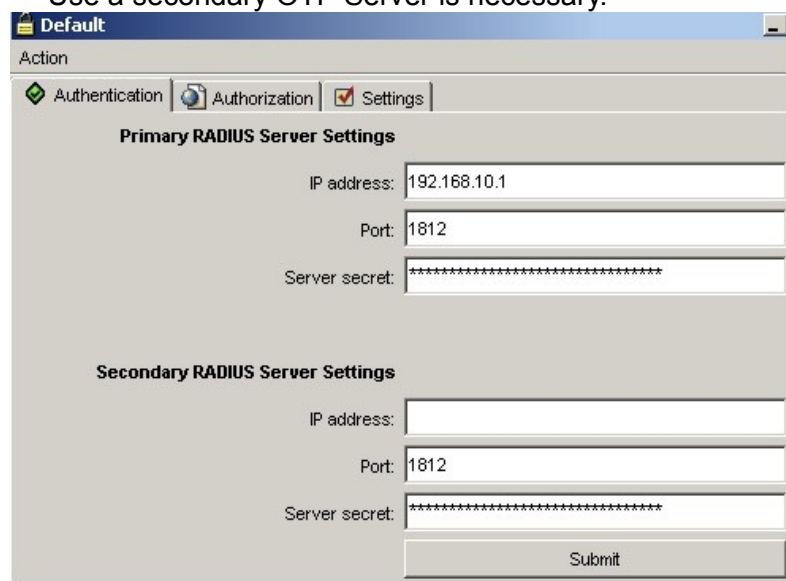
## NORDICEDGE OTP SERVER – INTEGRATION MODULE

6. Make sure the NordicEdge One Time Password Server™ is configured correctly and up and running.
7. Restart IIS Service.
8. Test

### Install Integration module for Standard Edition

This integration does not require any installation or downloads. In this case the OTP Server acts as a RADIUS server, which can be configured in the appliance administration tool.

1. Start the Access Gateway Administration Tool 4.5.
2. Make sure that under Advanced Options that “The Administration Tool Configures the Access Gateway only” is selected. Other wise use the installation instruction for Advanced Edition.
3. Select the authentication tab.
4. Add or change the default realm to use RADIUS authentication. Set the address to the OTP Server and set a shared secret. Use 1812 as the port. Use a secondary OTP Server is necessary.



The screenshot shows a web-based configuration interface for the Access Gateway Administration Tool. The window title is "Default". At the top, there are three tabs: "Authentication" (selected), "Authorization", and "Settings". Below the tabs, the "Primary RADIUS Server Settings" section contains three input fields: "IP address" with the value "192.168.10.1", "Port" with the value "1812", and "Server secret" with a masked value of "\*\*\*\*\*". Below this, the "Secondary RADIUS Server Settings" section contains three input fields: "IP address" (empty), "Port" with the value "1812", and "Server secret" with a masked value of "\*\*\*\*\*". A "Submit" button is located at the bottom right of the form.

## NORDICEDGE OTP SERVER - INTEGRATION MODULE

5. Make sure that RADIUS is turned on in the OTP Server. Change the port to 1812.

The screenshot shows the 'NordicEdge OTPServer Configurator' window. The 'Radius & Clients' tab is selected. Under 'Radius Settings', 'Enable Radius' is checked. The 'Portnr:' field is set to '1812' and 'Timeout:' is '0 (millsecs)'. 'Bind to This IP Address:' is set to 'All' and 'Debug Packets:' is unchecked. The 'Clients (Radius & Native)' table lists two clients: 127.0.0.1 and 192.168.10.10, both using 'Local ADAM' as the user database and having 'Challenge-...' checked. Below the table are 'Add Client', 'Edit Client', and 'Delete Client' buttons. At the bottom, 'Prevent SQL Injection Attacks' and 'Prevent LDAP Injection Attacks' are both checked. 'Save' and 'Cancel' buttons are at the bottom center, and the 'NordicEdge' logo and copyright information are at the bottom right.

Client IP	Is Radius	User Database	Challenge-...	Auth. Server
127.0.0.1	<input type="checkbox"/>	Local ADAM	<input checked="" type="checkbox"/>	
192.168.10.10	<input checked="" type="checkbox"/>	Local ADAM	<input checked="" type="checkbox"/>	

## NORDICEDGE OTP SERVER - INTEGRATION MODULE

6. Add the Gateway as a client in the OTP Server. Configure with the same shared secret and choose the response message.

The screenshot shows a dialog box titled "Native or Radius Client" with a subtitle "Modify Client '192.168.10.10'". The dialog contains the following fields and controls:

- Client IP Address:** A text box containing "192.168.10.10" and a checked checkbox labeled "Is RADIUS".
- Shared Secret:** A text box containing "\*\*\*\*\*".
- Uses Challenge/Response:** A checked checkbox.
- Response Message:** A text box containing "Please enter your one time password" and a small red ellipsis button to the right.
- User Database(s):** A section with a dropdown menu labeled "User Database:" showing "Local ADAM".
- Buttons:** "New", "Edit", and "Delete" buttons are located below the "User Database(s)" section. At the bottom of the dialog are "OK", "Options", and "Cancel" buttons.

7. Save the configuration and restart the OTP Server.
8. Test.

## 3 Configuration

### Configuration

This configuration guide is for Advanced Edition only.

---

#### web.config

---

In web.config it is possible to specify a number of application settings.

Value	Meaning
<b>OtpServerList</b>	This specifies a comma separated list of OTP Servers. Example; 127.0.0.1:3100, otp.company.com:3100
<b>ExcludedLogonPoints</b>	This specifies any logonpoint that should not be protected by OTP authentication. Default is to protect all logonpoints. Example; SampleLogonPoint, noOTPLogonPoint

---

#### Citrix Access Gateway

---

Configure logonpoints with default AD authentication.

If EPA is enabled, note that the EPA client is launched twice when OTP is enabled for a Logonpoint. This will be fixed in next release of this integration module. Also note that there can be problems if users can select multiple domains to logon to.