

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

**CITRIX WEB INTERFACE
4.0-4.2**

Copyright, NordicEdge®, 2006

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 Web Interface 4.0-4.2 integration module for NordicEdge One Time Password Server™ enables strong authentication for Citrix Web Interface.

Product Features:

- Use behind Citrix Secure Gateway if required
- Multiple serves for fail-over

Pre-requisites & System requirements

OS

Citrix Web Interface integration module runs on the following Windows platforms:

Windows NT 4 SP 6

Windows 2000 SP 4

Windows 2003 SP 1

IIS & Exchange

Citrix Web Interface integration module runs on the following Citrix versions:

4.0, 4.2

Active Directory

Active Directory or NDS 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™ 14C or higher.

2 Installation

Installing Citrix Web Interface integration module

Install Integration module

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\Citrix (default location)
3. Unpack the zipfile contents to c:\inetpub\wwwroot\Citrix
4. Register OtpW32.dll using regsvr32 OtpW32.dll (if you run the regsvr32 from the c:\inetpub\wwwroot\Citrix\MetaFrame\bin folder)
5. Make a copy of c:\inetpub\wwwroot\Citrix\MetaFrame\web.config
6. In web.config change `<add key=AUTH:AUTH_SUBDIR value=/auth/ />` to `<add key=AUTH:AUTH_SUBDIR value=/authOtp/ />`
7. Change

```
<add key="AUTH:UNPROTECTED_URLS"
```

```
value="/media/,/html/,/auth/loggedout.aspx,/auth/nocookies.aspx,/reloadConfiguration.aspx,/auth/help.aspx,/auth/certificateError.aspx"
```

```
/>
```

```
to
```

```
<add key="AUTH:UNPROTECTED_URLS"
```

```
value="/media/,/html/,/auth/loggedout.aspx,/authOtp/nocookies.aspx,/reloadConfiguration.aspx,/authOtp/help.aspx,/authOtp/certificateError.aspx"
```

```
/>
```

8. If the NordicEdge One Time Password Server™ is installed on another machine than the Web Interface, change `/metaframe/authOtp/serverscripts/otp.cs` to point to the correct server ip-address or hostname. It is configured to `127.0.0.1:3100` by default.

9. Make sure the NordicEdge One Time Password Server™ is started and configured with SMS or SMTP accounts. Contact sales@nordicedge.se for a NordicEdge SMS Gateway evaluation account.

3 Configuration

Configuration

web.config

In web.config it is specified which authentication sub-directory that should be used. It is possible to change layout to match company design guidelines.

Value	Meaning
AUTH:AUTH_SUBDIR	This specifies the authentication sub-directory. Must be changed from auth to authOtp.
AUTH:UNPROTECTED_URLS	This specifies any directory that should not be protected by authentication. This should be changed to reflect the new authentication directory. Except for the logout page, that must still use default auth directory.

NORDICEDGE OTP SERVER – INTEGRATION MODULE

otp.cs

In /metaframe/authOtp/serverscripts/otp.cs specific NordicEdge One Time Password Server™ parameters are configured.

Value	Meaning
OTP_HOSTNAME_LIST	This is a comma separated list of servers in the form; 127.0.0.1:3100 (default).
bOTPAuthenticationEnabled	This specifies if OTP authentication should be enabled or not. Can be true (default) or false .
allowNoneOTPAuthentication	This specifies if OTP server should be allowed to control if users should use OTP or not. Can be true (default) or false .