

OTP SERVER
INTEGRATION MODULE

NOVELL® ICHAIN™

Copyright, NordicEdge®, 2005

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 Novell® iChain™ integration Overview

NordicEdge® integration for Novell® iChain™ enables strong authentication for applications using the Novell iChain SSO framework.

1.3 Pre-requisites & System requirements

1.3.1 iChain

Novell iChain v2.1 SP1 or above

1.3.2 OTP Server

OTP Server 14C 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 LDAP v3 directory.

2 Installation

2.1 Installing the integration module

2.1.1 Files needed, iChain 2.1/2.2

Unzip the file sin otp4iChain.zip:

otpllogin.jar – The NordicEdge® OTP login servlet

otpllogin.properties – Sample properties file

login.jsp – Login page

login2.jsp – Response page

calograd.htm – Modified Novell® iChain radius login page

.gif,.jpg,style.css – style sheet and pictures used by login.jsp and login2.jsp

2.1.2 Files needed, iChain 2.3

The files can be found in the “/Integration Modules/iChain/2.3” directory of the NordicEdge® OTP Server installation.

calograd.htm – Modified Novell® iChain radius login page

radchaln.htm – Modified Novell® iChain challenge page

.gif,.jpg,style.css – style sheet and pictures used by calograd.htm and radchaln.htm

2.1.3 Integration method

The Novell® iChain 2.3 RADIUS client supports RADIUS challenge/response (not supported in Novell® iChain 2.1/2.2) and therefore the integration to NordicEdge OTP server is different depending on Novell® iChain version.

The integration servlet used in v 2.1/2.2 can still be used in 2.3. Follow the 'Install Novell® iChain 2.1/2.2' section, but with the following modifications:

1. Skip the 'Environment change:' under bullet nr 2.
2. Add a LDAP authentication profile named 'ldaprad', mention in section 2 k-t under 'Install Novell® iChain 2.3'.

2.1.4 Install Novell® iChain 2.1/2.2

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

1. Copy files:
Make a backup copy of the original radius login page,
`sys:\etc\proxy\data\calograd.htm`
Edit `calograd.htm`, and change the line where you find:
<http://neswalocal.demo.com/iChain/login.jsp>
this should be changed to match your environment (where you out the jsp files in section "Installing on servlet engine".
Copy `calograd.htm` to all iChain servers to the directory
`sys:\etc\proxy\data`
2. Environment change:
On the Novell® iChain proxy console, enter the following commands (replace O=MyOrg with your organization):
 - SET AUTHENTICATION ACLCHECK LDAP BINDANONYMOUS=NO
 - ADD AUTHENTICATION ACLCHECK LDAP SEARCHBASE = O=MyOrg
 - APPLY

2.1.5 Install Novell® iChain 2.3

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

1. Copy files:
On the iChain server, create a subdirectory named 'otp' in
`sys:\etc\proxy\data`

Make a backup copy of the original radius challenge page:

```
sys:\etc\proxy\data\radchain.htm
```

Copy calograd.htm, logo.gif, p0.gif, style.css and ne-logo.jpg from:

```
<otpinstallation>\iChain\2.3
```

to all iChain servers to the directory:

```
sys:\etc\proxy\data\otp
```

Copy radchain.htm and ne-logo.jpg from:

```
<otpinstallation>\iChain\2.3
```

to all iChain servers to the directory:

```
sys:\etc\proxy\data\
```

2.1.6 Installing on Servlet Engine (only version 2.1/2.2)

1. Copy files:

1. Copy the otplogin.jar from the NordicEdge® OTP-Server's iChain directory and the following files from the lib directory:

sunjce_provider.jar, jce1_2_1.jar, local_policy.jar and US_export_policy.jar to the authentication servlet server and add it to the class path of the servlet engine.

2. Create a directory named OTPLogin under the root directory of the servlet engine, and copy the otplogin.properties from the NordicEdge® OTP-Server's iChain directory to this directory.

Note! If you are unsure where the root is, the servlet will create the directory and a sample file if it can't find it.

3. Edit the following lines in login.jsp:

```
target = "http://ichain.demo.com/";
```

```
<FORM NAME=Login ACTION="/servlet/OTPLLogin" METHOD="POST"...
```

```
<input type=hidden name=radiusurl value="https://ichain.demo.com/ICSLogin/">
```

Make sure they all match your environment, where:

target - this should be the default URL of the protected resource and is only used if there is no target in the request.

ichain.demo.com – this should be the DNS name of the Novell® iChain server.

/servlet/OTPLLogin – this is the login servlet URL where the jsp will post to.

4. Edit the following line in login2.jsp:

```
<FORM NAME="Login" ACTION="http://ichain.demo.com/ICSLogin/auth-up"
```

```
MET....
```

Make sure they all match your environment, where:

ichain.demo.com – this should be the DNS name of the Novell® iChain server.

Also replace all “iChain/” with the directory where you copy the .gif, .jpg and style.css.

5. Copy login.jsp, login2.jsp, .gif, .jpg and style.css to a directory on the web server/servlet engine. The path where the login.jsp can be reach should be the URL entered in the calograd.htm.
2. Environment change:
 1. Add the otplogin.jar to the servlet engine class path.
 2. Edit the sample otplogin.properties file to match your environment.

3 Configuration

3.1 Configuration

The configuration depend on if standard RADIUS is used or the integration servlet for iChain 2.1/2.2. Follow the instructions in the correct section.

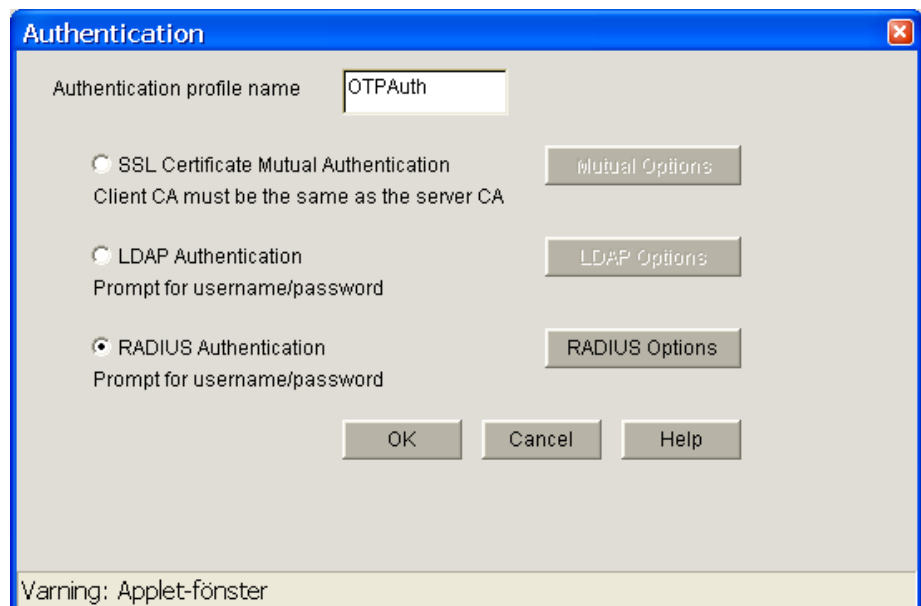
3.1.1 Parameters otplogin.properties

Parameters	Description
hostname	OTP Serverhost , all OTP server names and port, syntax "hostname:portnr;hostname2:portnr" etc.
loginpage	Login page URL , the URL to the login.jsp. Sample: /otp/login.jsp
encryption	OTP Encryption , if the login servlet should use encrypted communication to NordicEdge® OTP-Server OTP server. If set to NO, encryption will turned off.
responsepage	If the login servlet should preserve the user password and post it to iChain. IChain can then use this authenticate the user to other applications. Value YES/NO.
/jdk1.3/lib	JVMLibraryPath , The JVM library path.
debug	If the servlet should send out debug information. Value YES/NO.

3.2 iChain 2.3 Configuration

3.2.1 Administration

1. Start the Novell® iChain administration applet.
2. Go to “Configure” and “Authentication”.
3. Press “Insert”



4. Enter a name for the profile.
5. Chose “RADIUS Authentication”.
6. Press “RADIUS Options”.

RADIUS Options

RADIUS server address: 192 . 168 . 10 . 150

RADIUS server listening port: 1812

RADIUS shared secret: password

RADIUS server reply time in seconds: 7

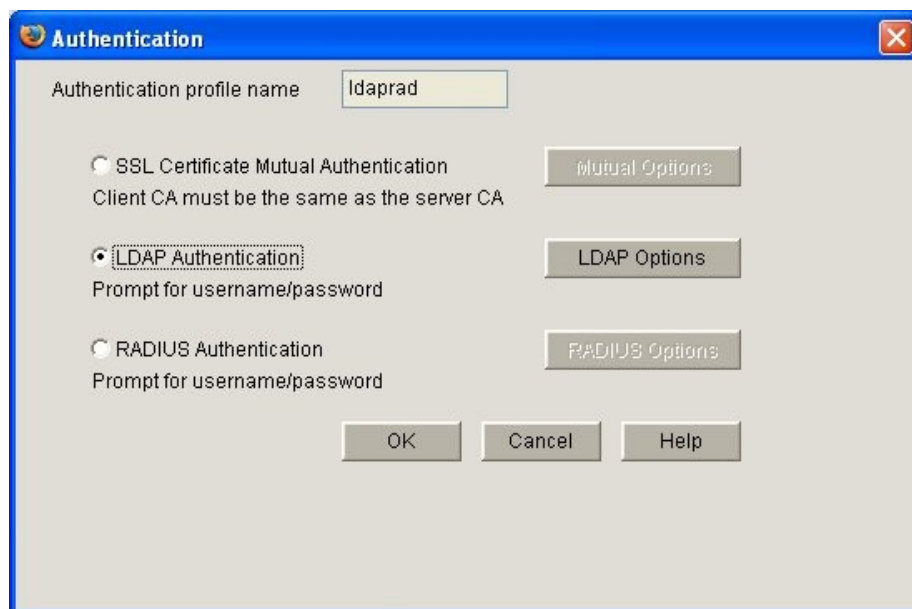
RADIUS re-send time in seconds: 2

OK Cancel Help

Varning: Applet-fönster

7. Enter the IP address of the OTP server.
8. Enter the port to be used for RADIUS communication with OTP server (must match the port configured in the OTP server)
9. Enter the RADIUS shared secret (must match the shared secret configured in the OTP server)
10. Press OK.
11. Press "Insert" to add a second profile.

Note! This LDAP profile is only used by iChain to find the RADIUS authenticated users, and should not be used in the accelerator.



12. Enter 'ldaprad' as name for the profile.
Note! The profile must be named 'ldaprad'.
13. Chose "LDAP Authentication".
14. Press "LDAP Options".

LDAP Options

Enable secure access to LDAP server

LDAP server listening port: 389

Server addresses: 192.168.10.52 [Insert] [Delete]

User name for LDAP searches: cn=admin,o=nordicedge Password: *****

Allow authentication through HTTP authorization header

- Use basic/proxy authentication
- Use iChain login page

Allow authentication through Netidentity

Netidentity Realm: []

LDAP login method:

- Build distinguished name
- Search on a single attribute
- Search using a query

LDAP search base list: o=NordicEdge [Insert] [Delete]

Search attribute: cn

[OK] [Cancel] [Help]

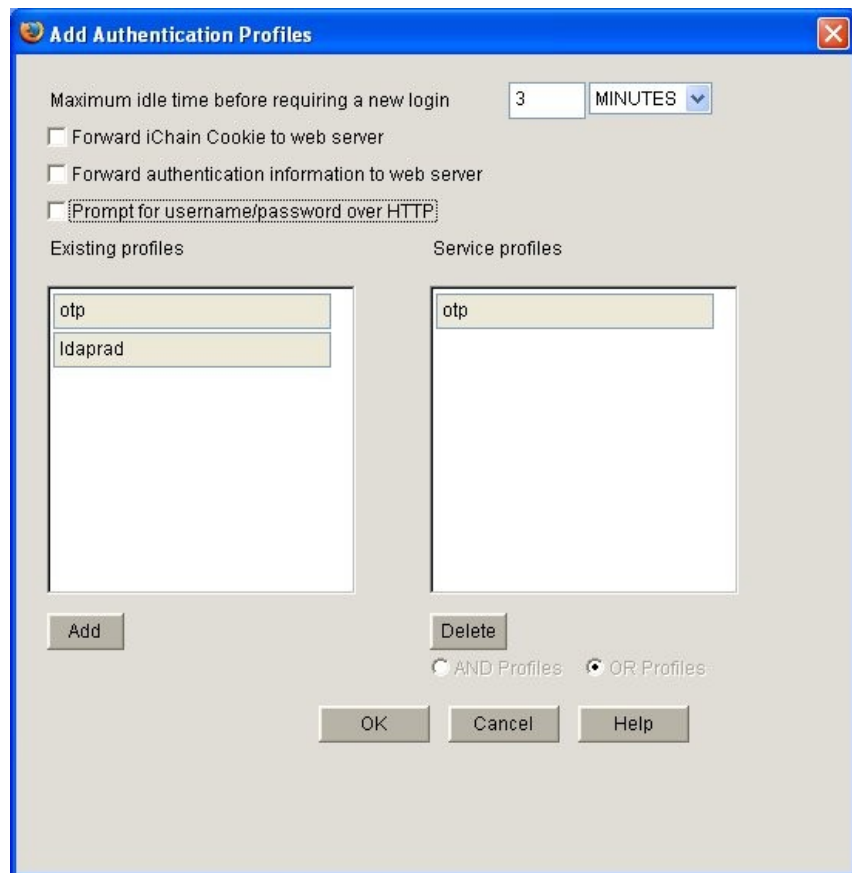
15. Enter the PORT and IP address of the eDirectory server used by iChain.
16. Enter a valid username and password to be used to search the directory.
17. On 'LDAP login method', select 'Search on a single attribute'.
18. Press 'Insert' and enter the base DN where to search for users.

OTP SERVER – INTEGRATION MODULE

19. Enter the search attribute. This must match the attribute configured for authentication in the OTP server RADIUS configuration.
20. Press OK.
21. Go to “Web Server Accelerator” tab.
22. Modify your accelerator.

The screenshot shows the 'Web Server Accelerator' configuration window. The 'Enable this accelerator' checkbox is checked. The 'Name' field contains 'otpdemo', 'DNS name' is 'www.nordicedge.info', and 'Cookie domain' is 'nordicedge.info'. The 'Alternate host name' radio button is selected with 'www.nordicedge.info' in the text box. The 'Return error if host name sent by browser does not match above DNS name' checkbox is checked. The 'Web server port' is set to 80, and the 'Web server addresses' list contains '192.168.10.52'. The 'Accelerator proxy port' is 80, and the 'Accelerator IP addresses' list contains '192.168.10.100'. The 'Enable authentication' checkbox is checked, and the 'Authentication Options' button is visible. Other options like 'Act as a tunnel', 'Forward browser IP address', and 'Enable logging' are unchecked. The 'Custom login page location' is set to 'otp'. Buttons for 'OK', 'Cancel', and 'Help' are at the bottom.

23. Make sure authentication is enabled.
24. Press “Authentication Options. Press “Authentication Options”.

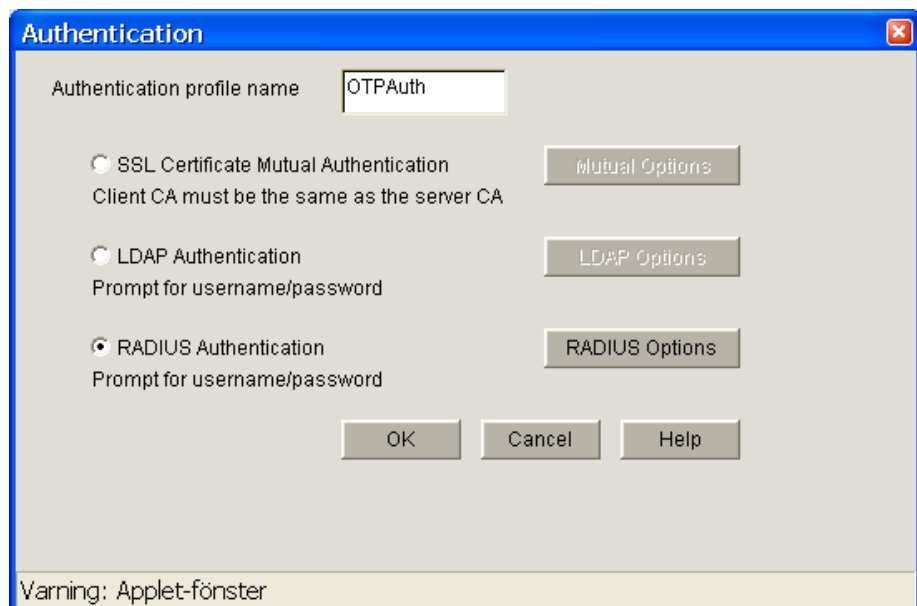


25. Remove any existing profiles, and add the profile just created in steps above.
Note! Do not add the profile name 'ldaprad'.
26. Press OK, and OK again. Finally press APPLY to update Novell® iChain server configuration.

3.3 IChain 2.1/2.2 Configuration

3.3.1 Administration

1. Start the Novell® iChain administration applet.
2. Go to “Configure” and “Authentication”.
3. Press “Insert”



4. Enter a name for the profile.
5. Chose “RADIUS Authentication”.
6. Press “RADIUS Options”.

RADIUS Options

RADIUS server address: 192 .168 .10 .150

RADIUS server listening port: 1812

RADIUS shared secret: password

RADIUS server reply time in seconds: 7

RADIUS re-send time in seconds: 2

OK Cancel Help

Varning: Applet-fönster

7. Enter the IP address of the OTP server.
8. Enter the port to be used for RADIUS communication with OTP server (must match the port configured in the OTP server)
9. Enter the RADIUS shared secret (must match the shared secret configured in the OTP server)
10. Press OK.
11. Go to “Web Server Accelerator” tab.

Web Server Accelerator

Name: test

DNS name: 1chain.demo.com

Cookie domain: demo.com

Use host name sent by browser (multi-homing web server)

Alternate host name: 1chain.demo.com

Return error if host name sent by browser does not match above DNS name.

Act as a tunnel Tunnel only ssl traffic

Forward browser IP address in Request Header [X-Forwarded-For]

Enable authentication

Enable logging for this accelerator

Enable Secure Exchange

SSL listening port: 443

Certificate: Auto

Enable multi-homing Multi-home master: [dropdown]

Custom login page location (blank to disable): [text box]

Web server port: 80

Web server addresses: 192.168.10.150

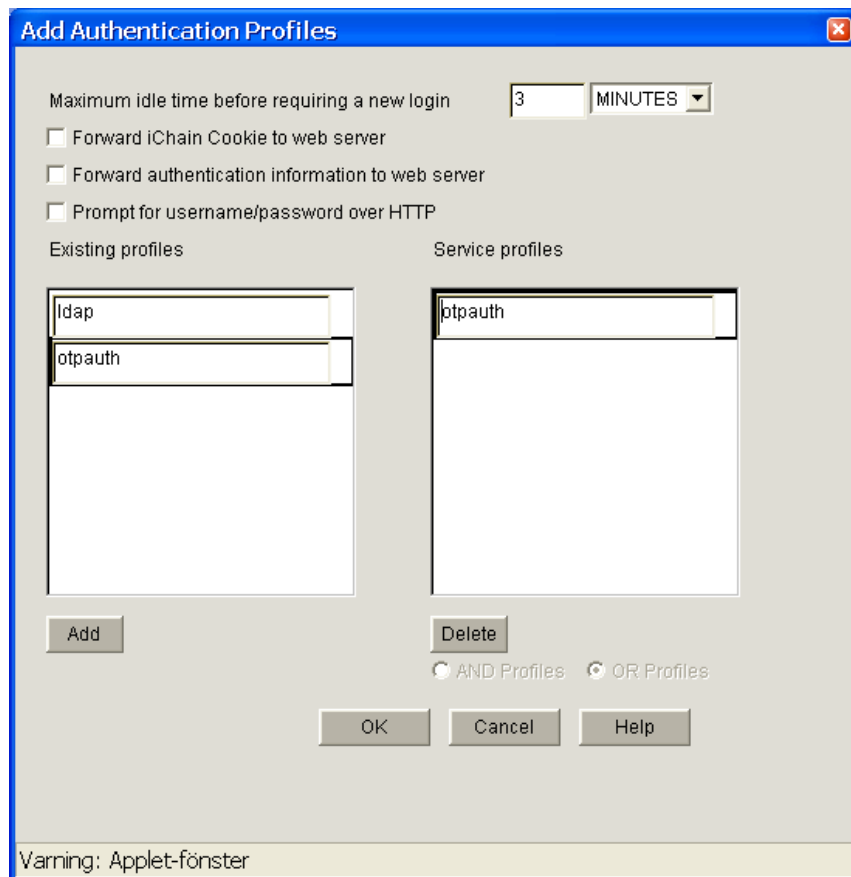
Accelerator proxy port: 80

Accelerator IP addresses: 192.168.10.161

Varning: Applet-fönster

12. Modify your accelerator.

13. Make sure authentication is enabled.



14. Press “Authentication Options. Press “Authentication Options”.
15. Remove any existing profiles, and add the profile just created in steps above.
16. Press OK, and OK again
17. Press APPLY to update Novell® iChain server configuration.

3.3.2 Configuring the NordicEdge® OTP-Server for Novell® iChain support

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

1. To set up the NordicEdge® OTP-Server to accept Novell® iChain login servlet (version 2.1/2.2) or RADIUS (version 2.3), go to the RADIUS tab, and enable it.

2. Make sure the “Portnr” match the port number set up in Novell® iChain authentication profile.
3. Press “Add Client”, and configure a RADIUS client:
Radius Client IP Address – This is the IP address of the iChain server
Shared Secret – This is the shared secret entered in the iChain authentication profile.
4. **If Novell® iChain 2.1/2.2:**
Deselect “Uses Challenge/Response”, and configure:
Auth. Server IP Address – This is the IP address of the server where the OTP authentication servlet is installed and running.

If Novell® iChain 2.3:

Make sure “Uses Challenge/Response” is selected, and configure ‘Response Message’ – This is the text that will show up on the challenge page (radchain.htm). Sample:

Please enter your one-time password

The screenshot shows a 'Radius Client' dialog box titled 'Modify Radius Client:192.168.10.100'. It contains the following fields and controls:

- Radius Client IP Address: 192.168.10.100
- Shared Secret: [Redacted]
- Uses Challenge/Response:
- Response Message: Please enter your one-time password
- Accept User Lookup only:
- User Database: Novell eDirectory

Buttons at the bottom include 'New', 'Edit', 'Delete', 'OK', 'Options', and 'Cancel'.

5. Press “New” to configure a new database:

Host Settings

Database Display Name – Enter a display name.

Host Address – The IP address to the LDAP directory.

Port number – The port number of the LDAP directory.

Admin DN – The admin DN.

Admin Password – The admin password.

Test LDAP Connection – Use this button to verify your LDAP settings.

Search Settings

Search Base DN – The DN where to start search for users.

Search Scope – What level of search, SUB, ONE or BASE.

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.

Note! If iChain version 2.3, this must match the attribute entered in the 'ldaprad' authentication profile.

Account Settings

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

Editing eDir Test OTP iChain UserDatabase

Database Display Name: Novell eDirectory

Database Type: LDAP

LDAP | JDBC

LDAP Settings

Host Settings

Host Address: 192.168.10.52

Portnumber: 389 SSL:

Admin DN: cn=admin,o=nordicedge

Admin Password: *****

Test LDAP Connection

Account Settings

OTP Attribute: title

Login Retries:

Disabled Attribute:

Disabled Value:

Disable OTP Attribute:

Disable OTP Value: Not

Search Settings

Search Base DN: o=NordicEdge

Search Scope: SUB Nr of Connections: 5

Search Filter start: (&(cn=

Search Filter End:)(objectclass=inetOrgPerson))

Test LDAP Authentication

OK Cancel

1. Press OK twice, and then Save.
2. Start the NordicEdge® OTP-Server. If you are running on NetWare, create a ncf start file based on the information in the otp.cmd.

4 Appendix A: Misc

4.1 Troubleshooting

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