

NordicEdge OTPServer for IBM Domino Installations notes

Prerequisites:

- Lotus Domino version 6 or higher installed.
- Microsoft Windows server 2003 or higher.
- NordicEdge OTPServer 2.0 or higher
- Apache with revproxy and otp module (included in the install package)
- The Domino database otp.nsf (included in the install package)

System architecture

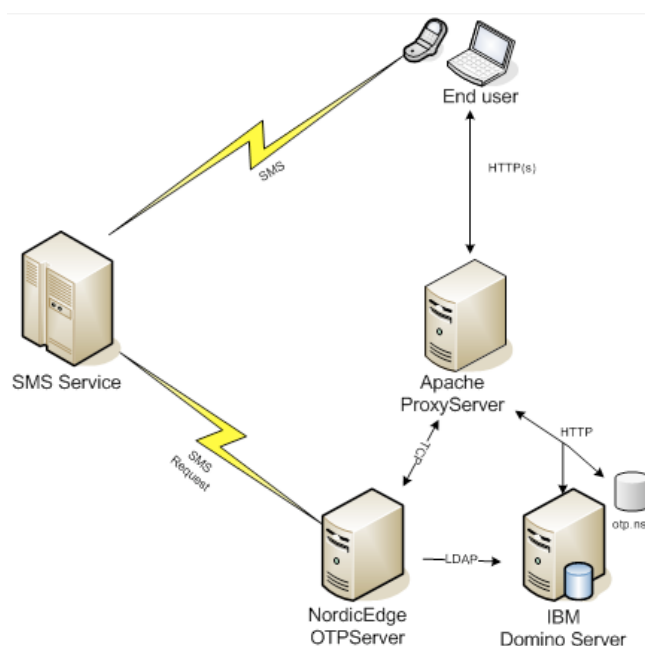
All user requests will pass through the Apache proxy server which will look for configured URLs to protect with OTP authentication.

Whenever a protected URL is detected and the user has not passed an OTP authentication but has authenticated in Domino the Apache server will call an agent in the otp.nsf database.

Example: <http://mydomino.acme.com:81/otp.nsf/GetName>

The agent then returns either the mobile number directly or a user name (for the OTPServer to make a look up through ldap).

The OTPServer then creates a onetime password (OTP) and sends it to the users



mobile phone or mail, the Apache server redirects the user to otp.html page for answering the

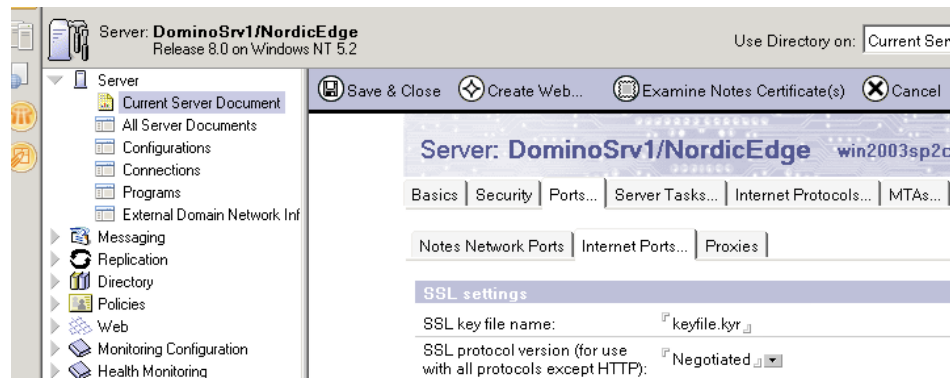
OTP request. When the user has correctly entered the OTP it's session gets flagged that it has passed OTP.

The main advantage of this technique is that it will use the standard Domino authentication and only force OTP whenever needed.

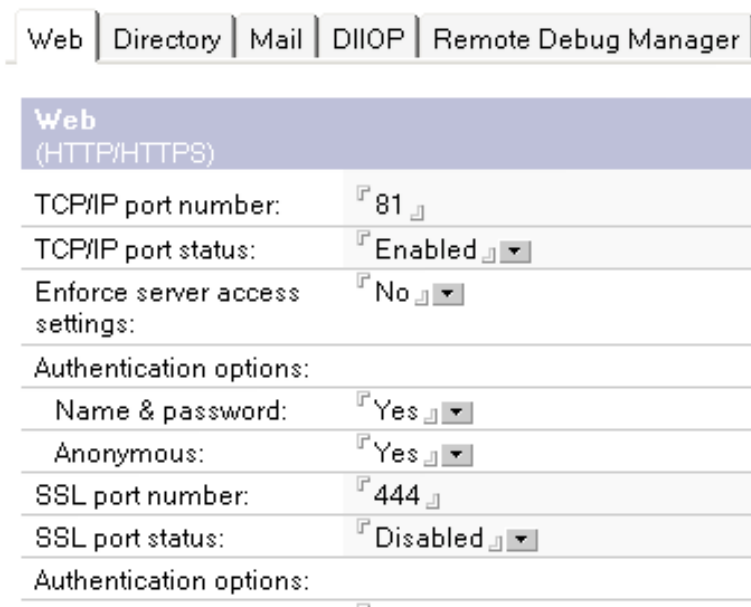


Prepare the Domino Web server.

If running the proxy server at the same machine as the IBM Domino server, the Domino web port numbers needs to be changed:



In this example, the standard port is changed from 80 to 81 and the SSL port is changed from 443 to 444.



Make sure that LDAP is configured enabled and accessible by the NordicEdge OTPServer

Install the proxy server

Run the installation of the Apache reversed proxy server.

Follow the onscreen instructions.

At the end of the installation several questions needs to be answered.



Enter requested information.
This will update the following files:
conf/ssl.conf
conf/httpd.conf
conf/otp.conf

Proxyserver's DNS name:

Proxyserver's TCP portnr:

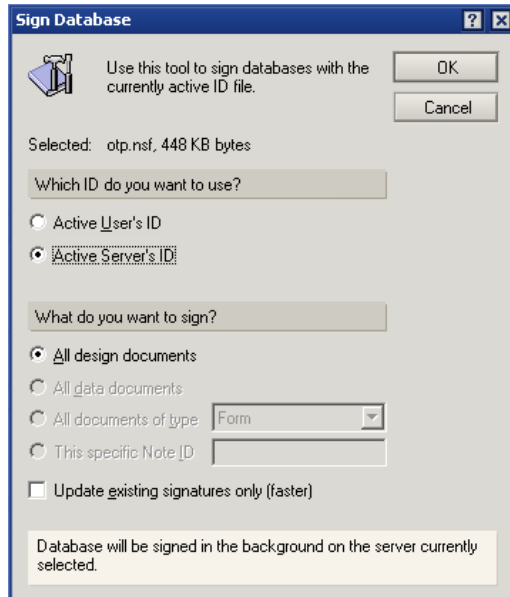
Proxyserver's SSL portnr:

Dominoserver's address:

Dominoserver using http or https?:

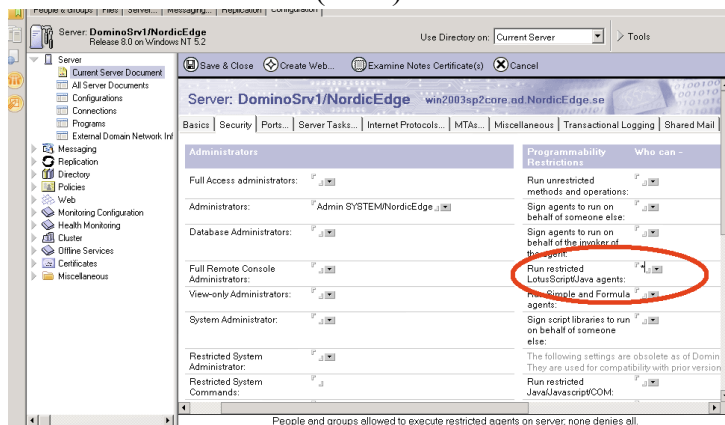
- **Proxyserver's DNS name**
This is the DNS name for this proxy server. This should be the address the end clients are using
- **Proxyserver's TCP portnr**
This is the unencrypted port number. Usually it is port 80 for http.
- **Proxyserver's SSL portnr**
This is the (https) encrypted port number. Usually it is port 443 for https.
- **Dominoserver's address**
This is the ipaddress and portnr of the dominoserver. If the Domino server is running on the same machine as the proxy server, enter 127.0.0.1:81
- **Dominoserver using http or https?**
If the Dominoserver is using http or https, enter either *http* or *https*
- **OTPServer address**
The ipaddress or DNS name of the OTPServer, if using several OTPServers for failover enter the addresses separated by comma, example:
192.168.0.33,192.168.0.75

Note, you must restart the Windows Server before continuing with the next step!



Enable “Run restricted LotusScript”

The otp.nsf database consists of just one agent named *GetName*. This agent extracts the username and makes it available to the proxyserver through HTTP. The user needs access to execute this agent. Open the Server document and select the Security tab and make sure all users (use *) have access to run restricted LotusScript:





Configure the Proxy server

Install the Proxy server as an Windows Service by enter the following command in the bin directory of the installation of the Apache server:

C:\Program Files\Apache2\bin>Apache.exe -k install

After this command has run, an service named **Apache2** has been created:

Name	Description	Status	Startup Type	Log On As
Alerter	Notifies selected us...		Disabled	Local Service
Apache2	Apache/2.0.61 (Wi...		Automatic	Local System
Application Experien...	Process application ...	Started	Automatic	Local System
Annlication Layer Ga...	Provides support fr...		Manual	Local Service

Selecting the Domino URLs to protect with OTP

All Domino URLs that is password protected are by default also OTP protected.

This can be changed by modifying the **otp.conf** file.

Open the file **otp.conf** located in the *C:\Program Files\Apache2\conf* directory with notepad or any texteditor. Go to **Location** section near the end.

```
# Example of a strongly authenticated Domino URL.
# Domino support requires a Java VM installed on the server.
# Make sure that the java directory is also copied into the
# Apache server root so that the plugin can find it.
<Location />
  AuthType      Basic
  AuthName      "NordicEdge OneTime Password Authentication Service"
  AuthAuthoritative off
  OTPAuthActiveDir on
  OTPAuthAuthoritativeDir on
  OTPAuthStrongDir on
  OTPAuthDominoDir on
  require valid-user
  OTPAuthDebugDir on
</Location>
```

Edit the line:

<Location />

to the URL that should be protected, for example all mail databases:

<Location /mail/>

If there are several different URLs that should be protected with OTP, just copy the Location section and create a new one:

```
<Location /mail/>
  AuthType      Basic
  AuthName      "NordicEdge OneTime Password Authentication Service"
  AuthAuthoritative off
  OTPAuthActiveDir on
  OTPAuthAuthoritativeDir on
  OTPAuthStrongDir on
  OTPAuthDominoDir on
  require valid-user
  OTPAuthDebugDir on
</Location>
<Location /company/>
  AuthType      Basic
  AuthName      "NordicEdge OneTime Password Authentication Service"
  AuthAuthoritative off
  OTPAuthActiveDir on
  OTPAuthAuthoritativeDir on
  OTPAuthStrongDir on
  OTPAuthDominoDir on
  require valid-user
  OTPAuthDebugDir on
</Location>
```



Create SSL certificate for the Apache Web server

The Apache web server comes with a bundled OpenSSL for Windows (see: <http://www.openssl.org/>)

- ✓ To create an SSL certificate, follow these instructions:
 - Start a command prompt
- ✓ Go to the Apache2\bin directory, example
cd C:\Program Files\Apache2\bin
- ✓ Create a private key by issuing the following command:
`openssl genrsa -out ..\conf\ssl.key\server.key 1024`
- ✓ Create a certificate signing request (CSR) with this command:
`openssl req -new -config ..\conf\openssl.cnf -key ..\conf\ssl.key\server.key -out ..\conf\ssl.csr\server.csr`

Answering the questions, make sure to answer the web server DNS address name for the question:

“Common Name (hostname, IP, or your name) []:”

example: *www.mycompany.com*

- ✓ **A)** Either send the CSR file *server.csr* located in the directory: *C:\Program Files\Apache2\conf\ssl.csr* to a Certificate Authority (CA) like VeriSign or Thawte and request a Apache certificate (crt) file.
Once the certificate file is returned, rename it to *server.crt* and replace the file located in the directory:
C:\Program Files\Apache2\conf\ssl.crt

B) Or create a self signed certificate (will not be automatically trusted by web browsers) issue this command:

```
openssl x509 -req -days 730 -in ..\conf\ssl.csr\server.csr -signkey ..\conf\ssl.key\server.key -out ..\conf\ssl.crt\server
```

Configuring the OTPServer for LDAP lookup

The Domino server must have LDAP configured and started (load ldap)

- Create a Native client with “Accept User Lookup only” enabled:
Make sure the Client IPAddress is the Apache servers ipaddress.

Native or Radius Client
Modify Client "127.0.0.1"

Client Display name: Domino Server

Client IPAddress: 127.0.0.1 Is RADIUS

Accept User Lookup only:

User Database(s)
User Database: LDAP Domino LDAP

New Edit Delete

OK Cancel

- Create an LDAP Database:

Editing Domino LDAP UserDatabase

Database Display Name: Domino LDAP Database Type: LDAP

Database is for OTP Mobile/Card users only!

LDAP | Database Group

Host Settings
Host Address: 127.0.0.1
Portnumber: 389 SSL TLS
Admin DN: admin
Password: *****
Test LDAP Connection

Account Settings
OTP Attribute: mobile
Login Retries: Accept Pwld change
Inactive Attribute:
Inactive Value:
Disable OTP Attribute:
Disable OTP Value: Not

Search Settings
Search Base DN:
Search Scope: SUB Nr of Connections: 5
Search Filter Start: (&(cn=...)
Search Filter End: (objectclass=inetOrgPerson) Samples
Test LDAP Authentication

Onetime Password Prefetch
 Enable OTP Prefetch
Configure Prefetch OTP

Pin code
 Enable Pin Code
Configure Pin Code

Advanced options
 External Databasehandler

OK Cancel