Installation guide for securing the authentication to your Bluecoat ProxySG solution with Nordic Edge One Time Password Server, delivering two-factor authentication via SMS to your mobile phone.

1 Summary

This is the complete installation guide for securing the authentication to your Bluecoat ProxySG solution with Nordic Edge One Time Password Server, delivering two-factor authentication via SMS to your mobile phone. You will be able to test the product with your existing SSL-VPN solution box and your LDAP user database, without making any changes affecting existing users. The guide will also allow you to make the complete installation efficiently, using a maximum of 1 hour. Nordic Edge provides several methods for delivering one time passwords, like e-mail, tokens, mobile clients, Pledge, prefetch, Yubikey etc. However in this test we are only going to use SMS.

This is a step-by-step guide covering the entire installation from A to Z. It is based on the scenario that you are running your SSL-VPN solution against Active Directory, and that you install the One Time Password Server on a Windows Server. The One Time Password Server is platform independent and works with all other LDAP user databases, like eDirectory, Sun One, Open LDAP etc. If you are not running Active Directory or Windows and if you have any questions regarding the slight differences in the installation process, you are most welcome to contact us.
at support@nordicedge.se and we will take you through the entire process.
# Table of Contents

1. Summary

Table of Contents

2. Prerequisites
   - Important information regarding communication

3. Getting started
   3.1 Register and download the software

4. Installation
   4.1 Start the installation
   4.2 Installing license

5. Configuring the One Time Password Server
   5.1 Start the OTP Configurator
   5.2 Configure the One Time Password Server
   5.3 Configure RADIUS
   5.4 Configure databases
   5.5 Configure LDAP Host Settings
   5.6 Configure the LDAP database settings
   5.7 Configure search filter
   5.8 Test LDAP Authentication

6. Configure the SSL-VPN client settings.

7. Configure Delivery Method

8. Restart the One Time Password Server as Windows Service

9. Add mobile phone number with Microsoft Management Console

10. configuring the Bluecoat ProxySG
   10.1 Authentication
   10.2 Policy - launch VPM
   10.3 For Admin Authentication create Admin Authentication Layer
   10.4 Create Admin Access for the appropriate access
10.5 For Web Access, Create Web Authentication Layer

Technical questions
Definitions

In this Step by Step guide the Bluecoat ProxySG is referred as “SSL-VPN Solution”

2 Prerequisites

You will need a server, for example a VMware virtual machine, with Windows Server 2003 or higher installed with Ethernet in bridge mode. The server must have a static ip-address configured and must also be able to reach your DNS-servers, your SSL-VPN solution and Active Directory. Since the software is quite small (315 mb) and easy to remove, you can also use any existing server from your network.

Important information regarding communication

The One Time Password Server is a software that can be installed on any existing server in your network or DMZ.

- The One Time Password Server must be able to communicate (Outbound traffic) with your LDAP or JDBC User Database. Default port for LDAP and Secure LDAP are TCP port 389 / 636.

- The SSL-VPN solution must be able to communicate (Outbound traffic) with the One Time Password Server via Radius, UDP port 1812 or 1645 (Outbound traffic).

- If you want to use the Nordic Edge SMS Gateway, the One Time Password Server must be able to communicate (Outbound traffic) with otp.nordicedge.net and otp.nordicedge.se with HTTPS on TCP port 443.

In the following test-scenario you will need to communicate with RADIUS port 1812 or 1645 and use the Nordic Edge SMS Gateway.
3 Getting started

3.1 Register and download the software

Go to www.nordicedge.net and click “PRODUCTS” and then “Downloads”
Type in your name and contact details to receive the software.
You will receive a link for downloading the software. A 30 days evaluation license will be sent via e-mail when you download the software.

Download the 32 or 64 bit version depending on your platform.
Nordic Edge OTPServer 3.0.9044 (April 2010)

Online Documentation

Installer created with InstallAnywhere® by Macrovision Corporation Copyright 2008. www.macrovision.com

Available Installers

<table>
<thead>
<tr>
<th>Platform</th>
<th>includes Java VM</th>
<th>without Java VM</th>
<th>Instructions</th>
</tr>
</thead>
<tbody>
<tr>
<td>MacOSX</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Windows32</td>
<td>Download (88.7M)</td>
<td></td>
<td>View</td>
</tr>
<tr>
<td>Windows64</td>
<td>Download (80.8M)</td>
<td></td>
<td>View</td>
</tr>
<tr>
<td>Linux32</td>
<td>Download (127.5M)</td>
<td></td>
<td>View</td>
</tr>
<tr>
<td>Linux64</td>
<td>Download (112.7M)</td>
<td></td>
<td>View</td>
</tr>
<tr>
<td>Linux</td>
<td></td>
<td>Download (69.6M)</td>
<td>View</td>
</tr>
<tr>
<td>Solaris</td>
<td></td>
<td>Download (69.6M)</td>
<td>View</td>
</tr>
<tr>
<td>Other Java-enabled Platforms</td>
<td></td>
<td>Download (58.7M)</td>
<td>View</td>
</tr>
</tbody>
</table>

4  Installation

4.1  Start the installation
Start the installation on the server where you want to install the One Time Password Server

Please note that if you are installing on a Windows 2008 Server you need to right click on the otp3install.exe using explorer and click on “Run as Administrator”.
Click Next
Installation and Use of OTPServer Requires Acceptance of the Following License Agreement:

END USER LICENSE AGREEMENT

The copyright in this software and its associated documentation is owned by Nordic Edge AB.
By opening this package you (an individual or legal entity) agree with Nordic Edge AB and its suppliers to
be bound by the terms of this Agreement which will govern your use of the Software.
If you do not accept these terms you may within 14 days of purchase return the Software,

☐ I accept the terms of the License Agreement
☐ I do NOT accept the terms of the License Agreement

Click Next
Click Next

4.2 Installing license
Choose the license.dat you received via e-mail.
Click Next
Step by Step Guide to implement SMS authentication to Bluecoat ProxySG

Click Next
Step by Step Guide to implement SMS authentication to Bluecoat ProxySG

Click Next
Click Install
Step by Step Guide to Implement SMS Authentication to Bluecoat ProxySG

1. Introduction
2. License Agreement
3. Choose Install Folder
4. Select license file
5. Install Windows Service
6. Choose Alias Folder
7. Pre-Installation Summary
8. Installing...
   - Install Complete
   - Start the OTPServer

Installing... Java Runtime Environment
Click Next
Step by Step Guide to implement SMS authentication to Bluecoat ProxySG

Leave default on Yes and click “Done”
Click Done
5  Configuring the One Time Password Server

5.1  Start the OTP Configurator

Start the OTP Configurator by clicking on the left button - “Configuration”

5.2  Configure the One Time Password Server
On the Server page you can set the length of the one time password and for how long it should be valid. Default is 5 minutes. You can also set a default country prefix, which means you will not need to set it in the mobile attribute. For more information regarding the optional setting please see One Time Password Server 3 - Administration manual.

For now, leave this page as default and go on to the next part - Configure RADIUS.

5.3 Configure RADIUS
Change to the RADIUS tab and configure the RADIUS port you want to use to communicate with your Bluecoat ProxySG server. In this example we are using RADIUS port nb 1645.
Click Save config.

5.4 Configure databases

In this setup we are going to use the Microsoft Active Directory LDAP database.

Change to the Databases tab and click on the LDAP Database button.
Select the type of database:

- LDAP Database
- ODBC or JDBC (SQL) Database
  - Oracle, Microsoft SQL, MySQL, Sybase etc.
- RADIUS Forward Database
  - Pass through to another RADIUS server
- Database Group
  - Group several databases together
5.5 Configure LDAP Host Settings

For this configuration we will use the active directory installed on the same server as the One Time Password Server. We will use the internal IP-address (127.0.0.1) as host address. We will use the standard LDAP port No. 389 to communicate with Active Directory. Admin DN will be the Administrator user to search for user objects in the Active Directory database. For now this user only need read rights to the user objects attributes but be aware that later you might
want to use options like disable accounts or the Pledge Enrollment concept from the Pledge Mobile Client. In this event the Admin DN need write rights to modify the disable account attribute and to store oath-keys into an optional user attribute.

Configure your LDAP host settings and click test. You should now get a messages saying “LDAP connection success”

Click OK and Save

Next step is to configure the LDAP database settings.
5.6 Configure the LDAP database settings
The BASE DN is the search base from where OTPServer will start looking for user objects. Click on the button with three dots at the right side of the Base DN field to browse your LDAP Database. Select an Organization Unit or Organization in Active Directory and click OK.

5.7 Configure search filter
Next step is to configure the search filter for One Time Password to search users via selected object classes and attributes according to the Microsoft Active Directory schema.

Click on the “Sample Button” and choose the filter template for MS Active Directory and click OK twice.

5.8 Test LDAP Authentication

Click on the Test LDAP Authentication button and type in the userid of a user you know exist in the directory.
Type in the password
If configuration is correct you will see the following success message.

6 Configure the SSL-VPN client settings.

Since One Time Password Server is also a RADIUS-server, the Cisco ASA 5500 is considered a client to the One Time Password Server.
Next step is to configure the settings for this client.
In the left pane click on "Clients"
Type in a name and ipaddress for your Bluecoat ProxySG.
Type in the RADIUS shared secret.
Choose the Active Directory you configured earlier as User Database.
Click Save
7 Configure Delivery Method

The Delivery Methods category is meant for enabling and configuring one or more delivery methods that can be used by the OTP Server to send one-time passwords.

One Time Password Server offers various methods like SMS, Oath Tokens, Instant Messaging, HTTP, Yubikey.

In this example we will use SMS with the Nordic Edge SMS-service as the SMS-provider.
During the evaluating phase we offer customers to use our Nordic Edge SMS-service free of charge for 30 days from the activation of the Demo Account.

In the left Pane, click “Delivery Methods” and then Nordic Edge SMS. In the right pane enable Nordic Edge SMS Gateway.

To Request a demo account click “Request a demo account”.

Click “Yes”
You should now get a success message and the Username and Password for the Nordic Edge SMS-gateway has automatically been filled in. Click OK and Save Config.
8 Restart the One Time Password Server as Windows Service

In the server panel for click “Shutdown”
In Windows Control Panel, open Administrative Tools / Services
Find the NordicEdge OTPServer Service, right click on that service and click “Start”.

In [Nordic Edge] One Time Password Server
Licensed to Test license for OTPServer 3 (Expires: 2010-04-25)
Copyright Nordic Edge AB 2002-2010. Version: 3.0 Build: 8987
Step by Step Guide to implement SMS authentication to Bluecoat ProxySG

Start service NordicEdge OTPServer 3.0 on Local Computer
9 Add mobile phone number with Microsoft Management Console

Add a mobile phone number to your test user mobile phone attribute by starting the Microsoft MMC, select the test user and enter the mobile phone number into the Mobile attribute.
10 configuring the Bluecoat ProxySG

10.1 Authentication

--> New RADIUS Realms
Configure as below
Note, Timeout value should be set to at least 15 seconds. The checkbox for OTP should be checked.
10.2 Policy - launch VPM

10.3 For Admin Authentication create Admin Authentication Layer
10.4 Create Admin Access for the appropriate access
10.5 For Web Access, Create Web Authentication Layer
Step by Step Guide to implement SMS authentication to Bluecoat ProxySG
Done.