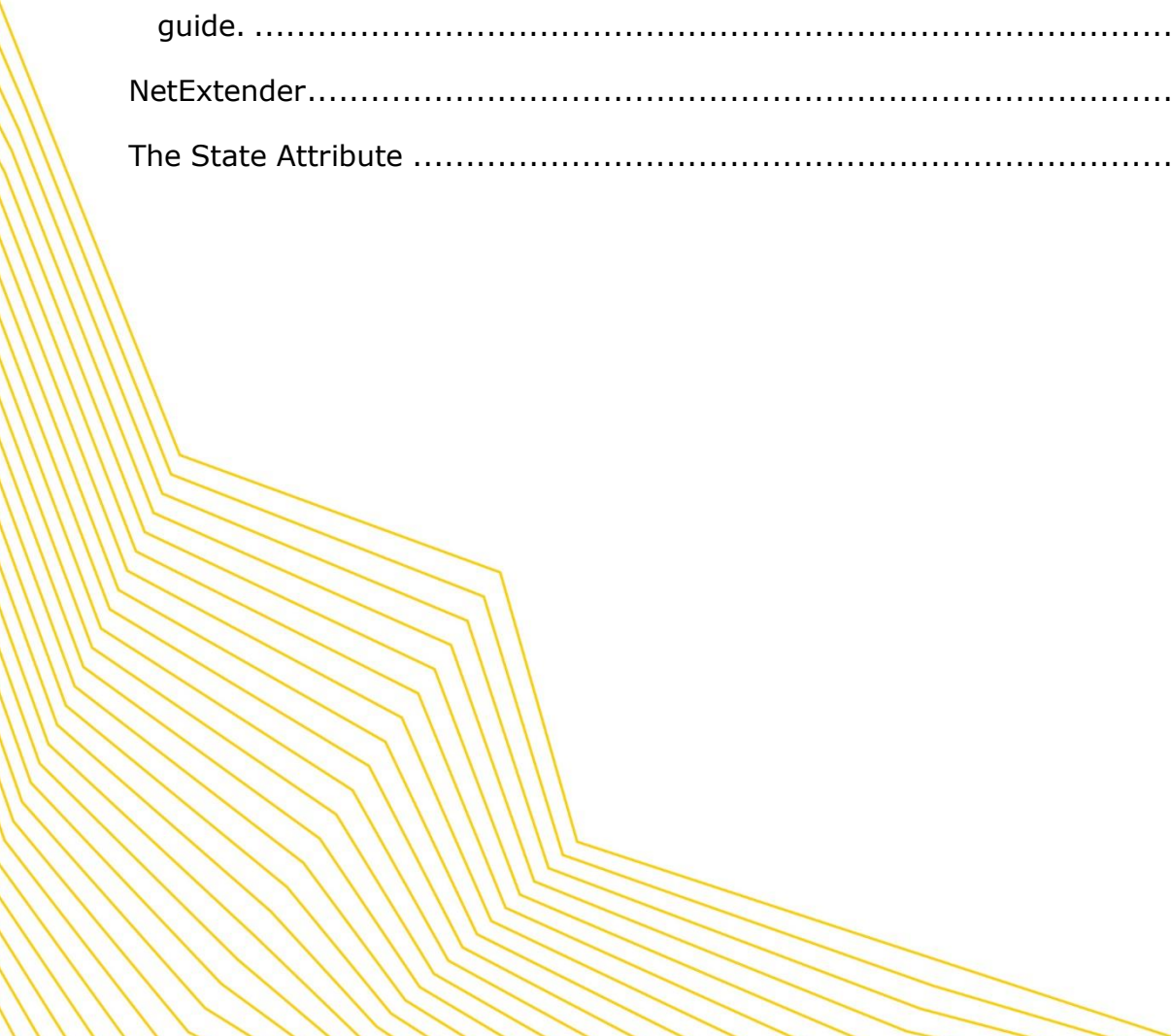




## Dell SonicWall MFA protection with SMS PASSCODE

### Contents

Configure the Radius server (NPS) according to the SMS PASSCODE Administrators guide. ....	1
NetExtender.....	3
The State Attribute .....	7





This guide will outline how to make a SonicWall work with CensorNet MFA.

Configure the Radius server (NPS) according to the SMS PASSCODE Administrators guide.

**Notice:**

When SMS PASSCODE has to Work with Radius challenge response with Sonicwall, it is important that the OS is NOT 6.2.5.1 or 6.2.5.2. There are bugs in these versions. These bugs have been fixed in OS version 6.2.5.3

The bug fixes only Works with the following clients:

1. SonicWALL Mobile Connect App (for iOS and Android)
2. SonicWALL Mobile Connect App (for Windows 10)
3. SonicWALL NetExtender version 8.6.257 (on Windows 7 and 10)

Please make sure that your SonicWall TZ/NSA/RSA is running with the newest general deployment (GD). This will benefit you with the newest version of the NetExtender client.

Configure your SonicWall for SSL-VPN clients, in a normal fashion. If in doubt, please consult the manual.



**DELL SonicWALL | Network Security Appliance**

Settings | **RADIUS Users** | Test

---

**Global RADIUS Settings**

RADIUS Server Timeout (seconds):  Retries:

---

**RADIUS Servers**

**Primary Server:**

Name or IP Address:

Shared Secret:

Port Number:

Send Through VPN tunnel

Configure user login to Radius+Local users. This will also make the local users (configured in the SonicWall) able to logon.

**DELL SonicWALL | Network Security Appliance**

Users / **Settings**

---

**User Authentication Settings**

User authentication method:

LDAP is selected for user group lookup for RADIUS/SSO users:

Single-sign-on method(s):

SSO Agent	<input type="checkbox"/>	<input type="button" value="Configure SSO..."/>
Terminal Services Agent	<input type="checkbox"/>	
Browser NTLM Authentication	<input type="checkbox"/>	
RADIUS Accounting	<input checked="" type="checkbox"/>	

Case-sensitive user names

Enforce login uniqueness

Force login per password change

Please test your login. If you use the built in test in the SonicWall, you will get error messages, as it does not support Radius Challenge Response.



Dell SonicWALL | Network Security Appliance

Settings RADIUS Users Test

### Test RADIUS Settings

To test the RADIUS settings, enter a valid RADIUS login name and password and click the Test button. Note that this will apply any changes that have been made.

User:

Password:

Test:  Password authentication  CHAP  MSCHAP  MSCHAPv2

Test Status:

**Got an access challenge from RADIUS - not supported by this test**

Returned User Attributes:

## NetExtender

Please find a computer with Windows 7 or 10. Download and install the Client for SonicWall NetExtender.

NetExtender

Dell SonicWALL | NetExtender

Server:

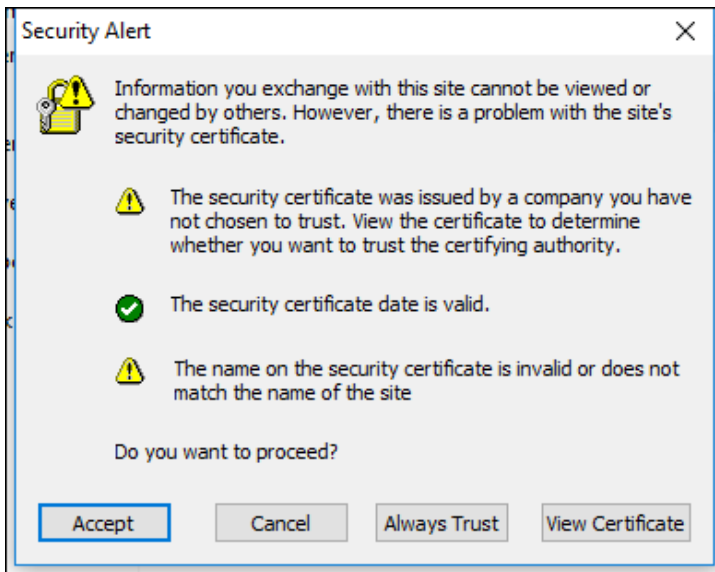
Username:

Password:

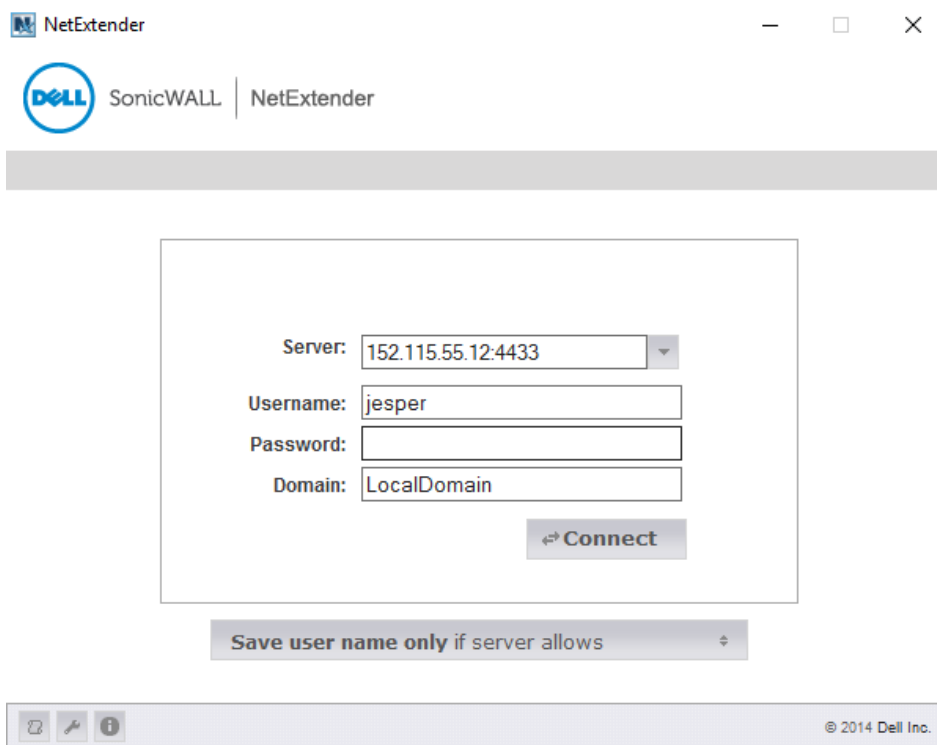
Domain:

Save user name only if server allows

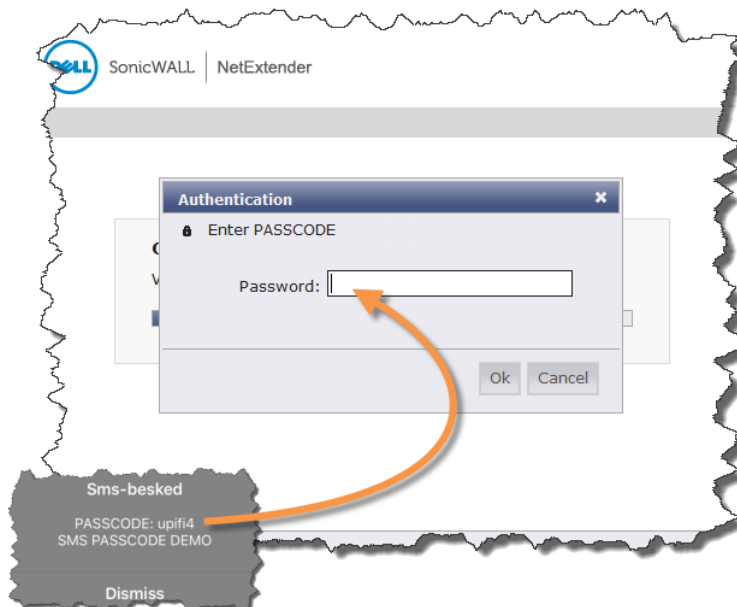
© 2014 Dell Inc.



Start the NetExtender client and configure with the SonicWall public IP and TCP port.



Please enter the username, password and domain and please click "Connect". This will prompt you for your One Time Passcode. This connects your computer. You will get a status window and the ability to disconnect again.





NetExtender

SonicWALL | NetExtender

User: jesper Connected: 0 Days 00:02:40

Status	Routes	DNS
<b>Server:</b>	152.115.55.12:4433	
<b>Client IP:</b>	192.168.168.10	
<b>Sent:</b>	55.95 KB	
<b>Received:</b>	365 bytes	
<b>Throughput:</b>	0 bytes/Sec	

© 2014 Dell Inc.



## The State Attribute

At every CENSORNET MFA protected Radius server, please add this registry key as DWORD: HKLM\SOFTWARE\SMS PASSCODE\Radius\Connection Request Policies \StateAttributeMaxLength and give it the value 30 (decimal) or 1e (HEX). For each listed connection request policy used by SonicWall, place the registry here as well. In example HKLM\SOFTWARE\SMS PASSCODE\Radius\Connection Request Policies \SonicWall\StateAttributeMaxLength

Please make sure that you got the latest NetExtender Client.

### Dell SonicWALL Notice Concerning Privilege Escalation Vulnerability in the Windows NetExtender client (CVE-2015-4173)

Dear Customer,

A vulnerability CVE-2015- 4173, affects a Registry key used by Dell SonicWALL NetExtender client for Windows exposes the system to a binary planting attack that can be triggered upon login. A malicious binary placed in a specific system folder by a low-privileged user could result in code execution upon an Administrator login.

#### Dell SonicWALL SMB SRA

NetExtender version	NetExtender 8.0.236 or earlier NetExtender 7.5.226 or earlier
Recommended Action	NetExtender 8.0.238 (or newer) is included in the SRA Firmware 8.0.0.3-23sv NetExtender 7.5.227 (or newer) is included in the SRA Firmware 7.5.1.2-40sv

#### Reported by

Andrew J. Smith, Security Analyst, Sword & Shield Enterprise Security (<http://www.swordshield.com>)

#### Additional Information

The latest 8.0 and 7.5 firmware versions are available for download on [www.mysonicwall.com](http://www.mysonicwall.com). Please contact Dell Tech Support for any issues in applying this security update.