Copyright © 2017 SonicWall Inc. All rights reserved.

SonicWall is a trademark or registered trademark of SonicWall Inc. and/or its affiliates in the U.S.A. and/or other countries. All other trademarks and registered trademarks are property of their respective owners

The information in this document is provided in connection with SonicWall Inc. and/or its affiliates' products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of SonicWall products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, SONICWALL AND/OR ITS AFFILIATES ASSUME NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL SONICWALL AND/OR ITS AFFILIATES BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF SONICWALL AND/OR ITS AFFILIATES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SonicWall and/or its affiliates make no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. SonicWall Inc. and/or its affiliates do not make any commitment to update the information contained in this document.

For more information, visit https://www.sonicwall.com/legal/.

Legend

⚠️ **WARNING:** A WARNING icon indicates a potential for property damage, personal injury, or death.

⚠️ **CAUTION:** A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

⚠️ **IMPORTANT, NOTE, TIP, MOBILE, or VIDEO:** An information icon indicates supporting information.

Mobile Connect User Guide
Updated - March 2017
Software Version - 1.0
232-003827-00 Rev A
# Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>About Mobile Connect</td>
<td>4</td>
</tr>
<tr>
<td>How Mobile Connect Works</td>
<td>4</td>
</tr>
<tr>
<td>Supported Platforms</td>
<td>4</td>
</tr>
<tr>
<td>Windows 10 Product Support</td>
<td>5</td>
</tr>
<tr>
<td>Upgrading from Windows 8.1</td>
<td>5</td>
</tr>
<tr>
<td>SonicWall Appliance Support</td>
<td>5</td>
</tr>
<tr>
<td>Required Network Information</td>
<td>6</td>
</tr>
<tr>
<td>Installing Mobile Connect</td>
<td>7</td>
</tr>
<tr>
<td>Configuring VPN Connections</td>
<td>9</td>
</tr>
<tr>
<td>Creating a Connection</td>
<td>9</td>
</tr>
<tr>
<td>Connecting to the VPN Server</td>
<td>11</td>
</tr>
<tr>
<td>Configuring Connections with PowerShell</td>
<td>12</td>
</tr>
<tr>
<td>Creating VPN Connections with PowerShell</td>
<td>13</td>
</tr>
<tr>
<td>Configuring VPN Connection Custom XML Settings</td>
<td>14</td>
</tr>
<tr>
<td>PowerShell Examples for Customizing VPN Connections</td>
<td>14</td>
</tr>
<tr>
<td>Configuring Advanced VPN Connection Settings</td>
<td>15</td>
</tr>
<tr>
<td>Configuring SMA 1000 Series / E-Class SRA Connection Settings</td>
<td>15</td>
</tr>
<tr>
<td>Configuring SMA 100 Series / SRA and Firewall Connection Settings</td>
<td>16</td>
</tr>
<tr>
<td>Configuring VPN Connection Triggers in Windows 10</td>
<td>16</td>
</tr>
<tr>
<td>Monitoring VPN Connections in Windows</td>
<td>18</td>
</tr>
<tr>
<td>Displaying VPN Connection Network Information</td>
<td>18</td>
</tr>
<tr>
<td>Displaying IPv4 Network Information</td>
<td>18</td>
</tr>
<tr>
<td>Displaying IPv6 Network Information</td>
<td>19</td>
</tr>
<tr>
<td>Displaying Routing Information</td>
<td>19</td>
</tr>
<tr>
<td>Displaying DNS Information</td>
<td>20</td>
</tr>
<tr>
<td>Monitoring Connections in the Windows Task Manager</td>
<td>21</td>
</tr>
<tr>
<td>Using the VPN Properties Window</td>
<td>23</td>
</tr>
<tr>
<td>General Tab</td>
<td>23</td>
</tr>
<tr>
<td>Options Tab</td>
<td>24</td>
</tr>
<tr>
<td>Security Tab</td>
<td>25</td>
</tr>
<tr>
<td>Networking Tab</td>
<td>26</td>
</tr>
<tr>
<td>Sharing Tab</td>
<td>27</td>
</tr>
<tr>
<td>Troubleshooting VPN Connections in Windows 10</td>
<td>28</td>
</tr>
<tr>
<td>SonicWall Support</td>
<td>29</td>
</tr>
</tbody>
</table>
SonicWall™ Mobile Connect for Windows 10 is an app that is available in the Windows Store. The app includes a VPN plug-in that enables secure mobile connections to private networks protected by SonicWall security appliances for devices running Windows 10.

Topics:
- How Mobile Connect Works on page 4
- Supported Platforms on page 4

How Mobile Connect Works

Modern business practices increasingly require that users be able to access any network resource (files, internal websites, etc.), anytime, anywhere. At the same time, ensuring the security of these resources is a constant struggle. While most users are aware that they must take care to protect computers from network security risks, this security awareness does not always extend to mobile devices. And yet, mobile devices are increasingly subject to security attacks. Furthermore, mobile devices often use insecure, untrusted, public Wi-Fi hotspots to connect to the Internet. It is therefore a challenge to provide secure, mobile access while still guarding against the inherent security risks of using mobile devices.

The SonicWall Mobile Connect for Windows 10 plug-in provides secure mobile access to sensitive network resources. Mobile Connect establishes a Secure Socket Layer Virtual Private Network (SSL VPN) connection to private networks that are protected by SonicWall security appliances. All traffic to and from the private network is securely transmitted over the SSL VPN tunnel.

To get started with Mobile Connect for Windows 10:

1. Ensure that the SonicWall SMA or firewall appliance to be used by Mobile Connect is connected to the network.
2. Configure the VPN connections within the Network & Internet > VPN section of the Windows 10 Settings app with the required information (connection name and server name).

   Mobile Connect establishes a SSL VPN tunnel to the SonicWall security appliance.

   You can now access resources on the private network. All traffic to and from the private network is securely transmitted over the SSL VPN tunnel.

Supported Platforms

The following sections describe supported platforms and network requirements for SonicWall Mobile Connect:

- Windows 10 Product Support on page 5
- Upgrading from Windows 8.1 on page 5
Windows 10 Product Support

SonicWall Mobile Connect for Windows 10 is supported on devices running the Windows 10 operating system from Microsoft. Microsoft is making Windows 10 available as free upgrade for qualified Windows 7, Windows 8.1, and Windows Phone 8.1 devices. See the following URL for more information:

Download SonicWall Mobile Connect for Windows 10 using the following URL:
http://microsoft.com/store/productid/9WZDNCRDSFKZ

Upgrading from Windows 8.1

VPN connections configured for the Mobile Connect inbox plug-in in Windows 8.1 will not work after upgrading to Windows 10 until the Mobile Connect app has been downloaded and installed from the Windows Store. The VPN connection will still appear in the Settings app, however, clicking Connect will show the error “Application Not Found.”

In this case, the Store app will be automatically launched and the Mobile Connect app page will be displayed. Once Mobile Connect has been successfully installed, clicking Connect on the VPN connection will now work as expected.

SonicWall Appliance Support

SonicWall Mobile Connect is a free app available for download from the Windows Store, but requires a concurrent user license on one of the following SonicWall solutions to function properly:

- SonicWall firewall appliances including the TZ, NSA, E-Class NSA, and SuperMassive™ 9000 Series running SonicOS 5.8.1.0 or higher
• SonicWall Secure Mobile Access 100 Series / SRA appliances running 7.5 or higher
• SonicWall Secure Mobile Access 1000 Series / E-Class SRA appliances running 10.7 or higher

Required Network Information

To use Mobile Connect, you will need the following information from your network administrator or IT Support:

• **Server name or address**—This is either the IP address or URL of the SSL VPN server that you will connect to.

• **Username and password**—Typically, you will be required to enter your username and password, although some connections may not require this.

• **Domain or Login Group name**—The domain or login group name of the SSL VPN server. Mobile Connect may be able to automatically determine this when it first contacts the server, or there may be multiple domains that can be selected.

DNS Domain Settings on SonicWall Appliances

Before Mobile Connect users will be able to access the private network, the network administrator must configure the DNS Domain on the SonicWall appliance. When the Mobile Connect user accesses a URL on the private network, the configured DNS domain is used to resolve the hostname lookup. For public domains that do not match the configured DNS domain, the DNS server for the Wi-Fi or 3G/4G network is used.

**NOTE:** The Mobile Connect user does not need to perform any configuration tasks related to DNS.

The following information is for SonicWall network administrators:

The DNS Domain configuration process varies, depending on the type of SonicWall appliance being used:

• **SonicWall firewall appliances** — On the SSL VPN > Client Settings page, enter the DNS domain name in the DNS Domain field.

• **SonicWall SMA 100 Series / SRA appliances** — The DNS domain can be configured either globally, at the group level, or at the individual user level:
  - **Global level:** On the Network > DNS page, enter the DNS domain name in the DNS Domain field.
  - **Group level:** On the Users > Local Groups page, click the edit icon for the group. Click on the NetExtender/Mobile Connect tab and enter the DNS domain the DNS Domain field.
  - **User level:** On the Users > Local Users page, click the edit icon for the user. Click on the NetExtender/Mobile Connect tab and enter the DNS domain the DNS Domain field.

• **SonicWall SMA 1000 Series / E-Class SRA appliances** — The DNS domain can be configured either globally or for specific IP address pools:
  - **Global level:** From the main navigation menu in the Appliance Management Console (AMC), click Network Settings. In the Name resolution area, click Edit. The Configure Name Resolution page appears. Enter the DNS domain name in the Search domains field.
  - **IP address pool level:** From the main navigation menu in AMC, click Services. Under Access services, in the Network tunnel service area, click Configure. The Configure Network Tunnel Service page appears. Click the name of the IP address pool you want to edit. The Configure IP Address Pool page appears. To the right of the Advanced heading, click the arrow icon. Select the Customize default settings check box and enter the DNS domain name in the Search domains field.

Installing Mobile Connect

This section describes how to install Mobile Connect. SonicWall Mobile Connect for Windows 10 is installed from the Windows Store.

To install Mobile Connect:

1. On your Windows 10 device, launch the Store app.

2. In the search field, type in SonicWall Mobile Connect and click Enter.

3. In the search results, select SonicWall Mobile Connect.
4 Select **Install**. The app will begin downloading and install on your device.

![Image of SonicWall Mobile Connect app downloading](image1.png)

5 When installation is complete, the SonicWall Mobile Connect icon will appear in the list of applications on your Windows 10 device.

![Image of SonicWall Mobile Connect icon](image2.png)
Configuring VPN Connections

This section describes how to configure and initiate a VPN connection using SonicWall Mobile Connect for Windows 10.

Topics:
- Creating a Connection on page 9
- Connecting to the VPN Server on page 11
- Configuring Advanced VPN Connection Settings on page 15
- Configuring VPN Connection Triggers in Windows 10 on page 16

Creating a Connection

In Windows 10, VPN connections can be created in the Settings app.

To create a VPN connection:
1. Launch the Settings app and navigate to Network & Internet > VPN.
2. Under VPN, select Add a VPN connection.
3 In the Add a VPN connection window, select **SonicWall Mobile Connect** as the VPN provider.

4 After entering all the required information, click **Save**.

**IMPORTANT:** If a custom port is required, then the server name must be entered in URL format in the **Server name** field, for example **https://vpn.example.com:4433**.

Once the VPN connection is successfully created, the VPN connection name appears in the list of connections and in the VPN section.
Connecting to the VPN Server

To establish a Mobile Connect VPN session:

1. In the Action Center, select the VPN to open the Settings app and connect the VPN by selecting Connect.

2. Enter your username and password when prompted and tap OK. Note that the Windows Sign In screen accepts the SonicWall SMA 100 Series / SRA or Firewall appliance domain or the SonicWall SMA 1000 Series / E-Class SRA Login Group value as the Microsoft domain portion of the username:

   Username@Domain OR Username@LoginGroup
   Domain\Username OR LoginGroup\Username

   Example 1: jdoe@SRA-DEMO or SRA-DEMO\jdoe, where SRA-DEMO is the name of the domain for the SMA 100 Series / SRA appliance.
   Example 2: jdoe@CORP or CORP\joe, where CORP is the Login Group for the SMA 1000 Series / E-Class SRA appliance.
When the connection is successfully established, the Status changes to Connected and the Disconnect button replaces the Connect button.

Once connected, you can access the remote network. The Networks screen shows the status of the VPN connection.

If the VPN connection is interrupted, the VPN icon shows as disconnected and you will no longer be able to access the remote network. Return to the Networks screen to reestablish the VPN connection. Windows 10 will automatically attempt to reestablish interrupted connections. VPN connections in Windows 10 also can be managed using PowerShell.

**Configuring Connections with PowerShell**

This section includes the following topics:

- [Creating VPN Connections with PowerShell](#) on page 13
- [Configuring VPN Connection Custom XML Settings](#) on page 14
- [PowerShell Examples for Customizing VPN Connections](#) on page 14
Creating VPN Connections with PowerShell

To create a VPN connection, use the PowerShell command `Add-VpnConnection` (see [http://technet.microsoft.com/en-us/library/jj554824.aspx](http://technet.microsoft.com/en-us/library/jj554824.aspx)). The PluginApplicationID for the SonicWall Mobile Connect VPN plugin is `SonicWALL.MobileConnect_e5kpm93dbe93j`. In the example below, a VPN connection to vpn.example.com is created with default options. This is equivalent to using the Settings app on the Windows 10 device.

The following is an example of the PowerShell commands for creating a connection:

```powershell
PS C:\> $xml = "<MobileConnect/>
PS C:\> $sourceXml=New-Object System.Xml.XmlDocument
PS C:\> $sourceXml.LoadXml($xml)
PS C:\> Add-VpnConnection -NameVPN -ServerAddress vpn.example.com -SplitTunneling $True -PluginApplicationID SonicWALL.MobileConnect_e5kpm93dbe93j -CustomConfiguration $sourceXml
```

To delete a VPN connection, use the PowerShell command `Remove-VpnConnection`, specifying the VPN connection using the `-name` option. For example:

```
PS C:\> Remove-VpnConnection -Name VPN
```
Configuring VPN Connection Custom XML Settings

Using PowerShell, it is possible to configure advanced settings for the Mobile Connect VPN plug-in. This section describes each individual custom XML option and provides examples of how to configure these settings using PowerShell.

- **Server Port**—<Port>4443</Port> - server port (optional, default is 443)
- **Debug Logging**—<DebugLogging>true</DebugLogging> - enable debug logging in plug-in (optional, default false).

  - **NOTE:** If DebugLogging is enabled, logs are written to the following file:
    C:\Users\<userName>\AppData\Local\Packages\SonicWALL.MobileConnect_e5kpm93dbe93j\LocalState\Logs\MobileConnect.log

- **Packet Capture**—<PacketCapture>true</PacketCapture> - enable packet capture (optional, default false)

  - **NOTE:** If Packet Capture is enabled, the packet capture is in the following files:
    Connections to SMA 1000 Series / E-Class SRA appliances:
    C:\Users\<userName>\AppData\Local\Packages\SonicWALL.MobileConnect_e5kpm93dbe93j\LocalState\Logs\MobileConnect.pcap
    Connections to SMA 100 Series / SRA and Firewall appliances:
    C:\Users\<userName>\AppData\Local\Packages\SonicWALL.MobileConnect_e5kpm93dbe93j\LocalState\Logs\MobileConnect.ppp.pcap

- **Windows Native Authentication UI**—<WindowsAuthUI>false</WindowsAuthUI> - disable Windows native authentication UI (optional, default true).
- **Parse Domain from Username field**—<UsernameHasDomain>false</UsernameHasDomain> - Parse out Domain field from Username field in Windows Auth dialog (optional, default true). Username should be entered in the format <Username>@<Domain> or <Domain><Username>. For SMA 100 Series / SRA and Firewall connections, the Domain portion is used for the Domain field.

  - **NOTE:** <UsernameHasDomain> only applies if WindowsAuthUI is enabled

- **Windows Single Sign On**—<SingleSignOn>false</SingleSignOn> - Do not set SSO flag to RequestCredentials() (optional, default true).

  - **NOTE:** <SingleSignOn> will not apply for the username & password custom authentication prompt (WindowsAuthUI set to false)

PowerShell Examples for Customizing VPN Connections

Enable debug logging:

```
PS C:\> $xml = "<MobileConnect><DebugLogging>true</DebugLogging></MobileConnect>"
PS C:\> $sourceXml=New-Object System.Xml.XmlDocument
PS C:\> $sourceXml.LoadXml($xml)
PS C:\> Add-VpnConnection -Name VPN -ServerAddress vpn.example.com -SplitTunneling $true -PluginApplicationID SonicWALL.MobileConnect_e5kpm93dbe93j -CustomConfiguration $sourceXml
```
Enable debug logging and packet capture:

```powershell
PS C:\> $xml = "<MobileConnect><DebugLogging>true</DebugLogging><PacketCapture>true</PacketCapture></MobileConnect>
" PS C:\> $sourceXml=New-Object System.Xml.XmlDocument PS C:\> $sourceXml.LoadXml($xml) PS C:\> Add-VpnConnection -Name VPN -ServerAddress vpn.example.com - SplitTunneling $True -PluginApplicationID SonicWALL.MobileConnect_e5kpm93dbe93j -CustomConfiguration $sourceXml
```

Specify Non-standard port for VPN connection:

```powershell
PS C:\> $xml = "<MobileConnect><Port>4433</Port></MobileConnect>
" PS C:\> $sourceXml=New-Object System.Xml.XmlDocument PS C:\> $sourceXml.LoadXml($xml) PS C:\> Add-VpnConnection -Name VPN -ServerAddress vpn.example.com - SplitTunneling $True -PluginApplicationID SonicWALL.MobileConnect_e5kpm93dbe93j -CustomConfiguration $sourceXml
```

Configuring Advanced VPN Connection Settings

This section includes the following topics:

- Configuring SMA 1000 Series / E-Class SRA Connection Settings on page 15
- Configuring SMA 100 Series / SRA and Firewall Connection Settings on page 16

Configuring SMA 1000 Series / E-Class SRA Connection Settings

The following settings are applicable to VPN connections with SMA 1000 Series / E-Class SRA appliances:

- **Encapsulated Security Payload**— `<ESP>true</ESP>` - Enable ESP mode (optional, default false)
- **Compression**— `<Compression>false</Compression>` - Disable lz4 compression (optional, default true)
- **Network Conflict Resolution Mode**— `<NCR>Local</NCR>` - Set Network Conflict Resolution (NCR) mode (optional, default 'Admin', other values 'Remote' or 'Local')
- **Login Group Caching**— `<CacheLoginGroup>true</CacheLoginGroup>` - Enable Login Group selection caching (optional, default false)
Configuring SMA 100 Series / SRA and Firewall Connection Settings

The following settings are applicable to VPN connections with SMA 100 Series / SRA or Firewall appliances:

- **Case-sensitive Domain Matching**—<DomainMatchCaseSensitive>true</DomainMatchCaseSensitive> - Perform case-sensitive match for user entered Domain field against VPN server Domain (optional, default false)

  ![NOTE:](image)

  Default behavior is that a case-insensitive match is performed. Only applies if <WindowsAuthUI> is enabled and <UsernameHasDomain> is enabled.

- **Max Login Retries**—<MaxLoginRetries>0</MaxLoginRetries> - (optional, default 2 - total of 3 login attempts allowed)

- **Require Smart Card Certificate**—<SmartCardRequired>true</SmartCardRequired> - require client certificate to be Smart Card (CertificateQuery>HardwareOnly flag must be set) (optional)

- **Client Certificate Issuer CA**—<ClientCertIssuerCA>testing.testsslvpn.com</ClientCertIssuerCA> - filter set of client certificates installed on Windows 10 by the Issuer CA (optional)

  ![NOTE:](image)

  The WinRT StreamSocket API in Windows 10 does not currently provide the list of Issuer CA certificates from the SSL server, so this may be used as a workaround to filter the list.

- **Automatically Select Client Certificate**—<ClientCertAutoSelect>true</ClientCertAutoSelect> - automatically select a single client certificate without prompting the user for verification (optional, default false)

- **Client Certificate Thumbprint**—

  ![image]

  automatically select the client certificate that matches the given certificate Thumbprint (optional)

Configuring VPN Connection Triggers in Windows 10

VPN connection triggers can be configured using PowerShell to automatically connect a VPN connection when an application is launched, or when a client attempts to access a resource within a specified DNS namespace. In addition, trusted networks can be configured to prevent a VPN connection from being initiated when client devices are already within the trusted network and the VPN is not needed. Please refer to Microsoft’s documentation on the following commands:


  The Add-VpnConnectionTriggerApplication command adds applications to a VPN connection object. The applications automatically trigger a VPN connection when launched.


  The Add-VpnConnectionTriggerDnsConfiguration command adds a DNS suffix or name to the DNS trigger properties for a client. If you specify a DNS IP address for the suffix or name, when the client accesses a resource within the suffix, the client starts a VPN connection. If you do not specify a DNS IP address for a DNS suffix or name, accessing the suffix or name does not trigger the VPN connection.
• **Add-VpnConnectionTriggerTrustedNetwork**
  

  The `Add-VpnConnectionTriggerTrustedNetwork` command adds DNS suffixes as trusted networks to the VPN profile. When a DNS suffix that you add to the VPN profile is present on the physical interface on the client, the VPN connection does not start even if the client tries to access an application that is part of triggering properties or tries to access a resource that is part of DNS suffix configured for triggering.
Monitoring VPN Connections in Windows

VPN connections can be monitored in Windows 10 using the native set of Windows utilities, including CMD shell commands, such as `ipconfig` and `route`, and applications such as Task Manager, Resource Monitor, and the Event Viewer.

This section includes the following topics:

- [Displaying VPN Connection Network Information](#) on page 18
- [Monitoring Connections in the Windows Task Manager](#) on page 21

Displaying VPN Connection Network Information

The following sections include examples using command line utilities to show detailed network information:

- [Displaying IPv4 Network Information](#) on page 18
- [Displaying IPv6 Network Information](#) on page 19
- [Displaying Routing Information](#) on page 19
- [Displaying DNS Information](#) on page 20

Displaying IPv4 Network Information

The following is an example showing IPv4 network information:

```
C:\> ipconfig /all
Windows IP Configuration
PPP adapter VPN

  Connection-specific DNS Suffix. : example.com
  Description . . . . . . . . . . . . . : VPN
  Physical Address . . . . . . . . . : 
  DHCP Enabled . . . . . . . . . . . : No
  Autoconfiguration Enabled . . . . : Yes
  IPv4 Address . . . . . . . . . . . : 192.168.200.61(Preferred)
  Subnet Mask . . . . . . . . . . . . : 255.255.255.255
  Default Gateway . . . . . . . . . : 
  NetBIOS over Tcpip . . . . . . . . : Enabled
  Connection-specific DNS Suffix Search List : example.com
```
Displaying IPv6 Network Information

The following is an example showing IPv6 network information:

C:\> ipconfig /all
Windows IP Configuration
PPP adapter VPN

  Connection-specific DNS Suffix. . : example.com
  Description . . . . . . . . . . : VPN
  Physical Address. . . . . . . . : 
  DHCP Enabled. . . . . . . . . . : No
  Autoconfiguration Enabled . . . : Yes
  Subnet Mask . . . . . . . . . : 255.255.255.255
  Default Gateway . . . . . . . : 
  DHCPv6 IAID. . . . . . . . . . : 452990301
  DHCPv6 Client DUID . . . . . : 00-01-00-1-BD-D7-43-00-15-5D-7E-C4-43
  NetBIOS over Tcpip. . . . . . : Enabled
  Connection-specific DNS Suffix Search List : example.com

Displaying Routing Information

The following is the command to show routing information:

C:\> route PRINT
Displaying DNS Information

**NOTE:** The proper DNS information for the VPN connection is displayed using the `netsh name show effective policy` command. The `ipconfig` command does not show the complete set of DNS information and should not be relied upon.

The following is an example showing DNS information:

```bash
C:\> netsh name show effectivepolicy
DNS Effective Name Resolution Policy Table Settings
Note: DirectAccess settings are inactive when this computer is inside a corporate network.

Settings for .example.com
----------------------
Generic (DNS Servers):
192.168.200.20
192.168.200.21

Generic (VPN Trigger): disabled
Settings for vpn.example.com
----------------------
Generic (DNS Servers):
Generic (VPN Trigger): disabled
```
Monitoring Connections in the Windows Task Manager

When the VPN is connected, the process *SonicWall Mobile Connect* will appear in the list of processes. Right-click on the *SonicWall Mobile Connect* process and select *Properties*.

![Task Manager screenshot](image)

<table>
<thead>
<tr>
<th>Name</th>
<th>1% CPU</th>
<th>50% Memory</th>
<th>0% Disk</th>
<th>0% Network</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cortana Background Task Host</td>
<td>0%</td>
<td>13.7 MB</td>
<td>0 MB/s</td>
<td>0 Mbps</td>
</tr>
<tr>
<td>Microsoft Windows Search Indexer</td>
<td>0%</td>
<td>13.4 MB</td>
<td>0 MB/s</td>
<td>0 Mbps</td>
</tr>
<tr>
<td>Service Host: Local Service (11)</td>
<td>0%</td>
<td>11.8 MB</td>
<td>0 MB/s</td>
<td>0 Mbps</td>
</tr>
<tr>
<td>Task Manager</td>
<td>0.4%</td>
<td>11.7 MB</td>
<td>0 MB/s</td>
<td>0 Mbps</td>
</tr>
<tr>
<td>Service Host: Local Service (Network R...)</td>
<td>0%</td>
<td>9.9 MB</td>
<td>0 MB/s</td>
<td>0 Mbps</td>
</tr>
<tr>
<td>Application Frame Host</td>
<td>0%</td>
<td>9.2 MB</td>
<td>0 MB/s</td>
<td>0 Mbps</td>
</tr>
<tr>
<td>SonicWall Mobile Connect</td>
<td>0%</td>
<td>8.6 MB</td>
<td>0 MB/s</td>
<td>0 Mbps</td>
</tr>
<tr>
<td>WMI Provider Host</td>
<td>0%</td>
<td>7.0 MB</td>
<td>0 MB/s</td>
<td>0 Mbps</td>
</tr>
<tr>
<td>Service Host: DCOM Server Process L...</td>
<td>0%</td>
<td>6.5 MB</td>
<td>0 MB/s</td>
<td>0 Mbps</td>
</tr>
<tr>
<td>Service Host: Network Service (5)</td>
<td>0%</td>
<td>6.1 MB</td>
<td>0 MB/s</td>
<td>0 Mbps</td>
</tr>
<tr>
<td>Host Process for Setting Synchronization...</td>
<td>0%</td>
<td>5.7 MB</td>
<td>0 MB/s</td>
<td>0 Mbps</td>
</tr>
<tr>
<td>Service Host: Remote Procedure Call (2)</td>
<td>0%</td>
<td>5.2 MB</td>
<td>0 MB/s</td>
<td>0 Mbps</td>
</tr>
<tr>
<td>Service Host: Unistack Service Group (5)</td>
<td>0%</td>
<td>5.2 MB</td>
<td>0 MB/s</td>
<td>0 Mbps</td>
</tr>
<tr>
<td>appmodel (2)</td>
<td>0%</td>
<td>5.2 MB</td>
<td>0 MB/s</td>
<td>0 Mbps</td>
</tr>
<tr>
<td>Windows Audio Device Graph Isolation</td>
<td>0%</td>
<td>5.1 MB</td>
<td>0 MB/s</td>
<td>0 Mbps</td>
</tr>
</tbody>
</table>

In the Mobile Connect VPN Plugin App Properties dialog, select the Details tab to view the plugin version and copyright information.

Additionally, in the Task Manager Details tab, MobileConnectVpnPluginApp.exe will appear in the list of process names. Right-click on the MobileConnectVpnPluginApp.exe process and select Properties to bring up the same Properties dialog.

**NOTE:** Mobile Connect copyright and third-party open source software license information can be found in the LICENSE.txt file at C:\Windows\vpnplugins\sonicwall\LICENSE.txt
Using the VPN Properties Window

The Mobile Connect VPN Properties window allows you to edit or change settings specific to VPN Properties. Navigate to the Network Connections > VPN Properties page. See the following sections for more information:

- General Tab on page 23
- Options Tab on page 24
- Security Tab on page 25
- Networking Tab on page 26
- Sharing Tab on page 27

General Tab

The VPN Properties > General tab allows you to edit the Hostname or IP address of destination. Note that you can enter an IPv4 or IPv6 address.

You can also enable First Connect, which allows Windows to first connect to a public network before attempting to establish the VPN connection. If you wish to enable First Connect, select the Dial another connection first check box, then specify the connection in the field below.
Options Tab

The VPN Properties > Options tab allows you to select the Remember my credentials check box for ease of logging in to the VPN connection. You can specify the Idle time before hanging up from the drop-down list. Click the PPP Settings button to configure settings for PPP.
Security Tab

The VPN Properties > Security tab allows you to configure the following:

- **Type of VPN**—Select the type of VPN connection from the drop-down list. For more options, click the Advanced Settings button.

- **Data Encryption**—Select the type of data encryption from the drop-down list.

- **Use Extensible Authentication Protocol (EAP)**—Select this option if you wish to use EAP. For more information, click the Properties button.

- To use any of the listed authentication protocols, select the **Allow these protocols** option, then select the checkbox(es) of the available choices.
Networking Tab

The VPN Properties > Networking tab allows you to edit the settings for the different connections to the VPN.
Sharing Tab

The **VPN Properties > Sharing** tab allows you to configure Internet Connection Sharing options. For more information, click the **Settings** button.
Troubleshooting VPN Connections in Windows 10

If you are unable to connect to the SonicWall VPN server, perform the following steps to troubleshoot the connection.

1. Double check that you have entered the server name properly in the connection configuration.

2. Open a Web browser on your Windows 10 device and attempt to navigate to the user portal on the SMA 100 Series / SRA, SMA 1000 Series / E-Class SRA, or Firewall appliance. This could be the Virtual Office portal on SMA 100 Series / SRA, the WorkPlace portal on SMA 1000 Series / E-Class SRA, or the NetExtender connection to the firewall.

3. If you are unable to load the Web portal, the problem is with your network connection or possibly the SonicWall appliance. Contact your network administrator if the problem persists.

4. If the Web portal loads successfully on your browser and you still cannot establish a VPN connection, notify your network administrator.

5. Double check the VPN connection properties on the Network Connections page. Right-click the VPN Connection, and select Properties. The VPN Properties window displays. For more information, see Using the VPN Properties Window on page 23.
Technical support is available to customers who have purchased SonicWall products with a valid maintenance contract and to customers who have trial versions.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. To access the Support Portal, go to https://support.sonicwall.com.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. In addition, the Support Portal provides direct access to product support engineers through an online Service Request system.

The Support Portal enables you to:

- View knowledge base articles and technical documentation
- Download software
- View video tutorials
- Collaborate with peers and experts in user forums
- Get licensing assistance
- Access MySonicWall
- Learn about SonicWall professional services
- Register for training and certification

To contact SonicWall Support, refer to https://support.sonicwall.com/contact-support.

To view the SonicWall End User Product Agreement (EUPA), see https://www.sonicwall.com/legal/eupa.aspx. Select the language based on your geographic location to see the EUPA that applies to your region.