1NET V2.5 ADMINISTRATION AND INSTALLATION GUIDE

Document Version 2.2.0

ACCESSITY PTY LTD

ABN: 18 120 507 137

WWW.ACCESSITY.COM.AU

Contents

OPERATIONAL OVERVIEW

1NET is designed to ensure that computers connected to a Windows Domain Network are not also connected to any other untrusted third party network.

1NET integrates seamlessly with Microsoft Windows 7 and Microsoft Windows 8 providing a seamless experience for end users. 1NET is simple to deploy and provides a number of ways to administer it providing flexibility for system administrators.

1NET utilises the Windows Network List Manager to identify Domain and Non Domain networks.

1NET can be configured to disconnect from your corporate wireless network while connected to the corporate Domain network by a wired LAN connection and then reconnect to the wireless network when the wired connection is disconnected. Or it can be configured to allow connections to the Domain network by both the wireless and wired network adapters at the same time.

1NET can be used on computers such as desktops, which must only ever be connected to the Domain network. If a user disconnects from the Domain network and attempts to connect to a non-Domain network (i.e. a Public/untrusted network), 1NET will prevent this.

1NET works with Microsoft DirectAccess and VPNs. 1NET can provide additional protection while using DirectAccess or a VPN by ensuring that the computer only has one network adapter on a public network. E.g. if a computer is accessing your network by VPN over a wired ADSL link and the user then establishes a 3G/4G connection, 1NET can disconnect this second connection.

1NET supports any wired or wireless network adapter installed and any Mobile Broadband devices that integrates with the Windows 7/8 WWAN Service and the Windows 7/8 Mobile Broadband Connection Manager. Third party broadband connection managers are not supported and should be tested with 1NET by the customer.

CHANGES IN V2.5

1NET v2.5 is a minor release which adds the ability to restrict a computer to only Domain networks. This new feature is intended for Desktop computers which should only ever be on the corporate Domain network. This release includes stability updates, improved SSL VPN detection and logging improvements.

CHANGES IN V2.4

1NET v2.4 is a minor release which adds the ability for 1NET to restrict the number of public networks a computer can connect to when it is off the Domain network. Improvements to 1NET's VPN detection to better detect common SSL VPN's. Depreciated 'ExcludeVPNAdapters' setting, this behaviour is default if remote access VPNs are permitted. Updated ADMX files.

CHANGES IN V2.3

1NET v2.3 is a minor release which adds the ability to use the existing 'Exclude Network Adapters List' setting to exclude VPN connections which are not recognised by Windows as VPN adapters.

CHANGES IN V2.2

1NET v2.2 is a minor enhancement which enables 1NET to automatically reconnect to the corporate wireless network when the computer is disconnected from the wired corporate network by the user.

CHANGES IN V2.1

1NET v2.1 is a minor release which improves the detection of Remote Access VPNs and Tunnels. Includes updated Group Policy to disable the detection of Remote Access VPNs and Tunnels.

CHANGES IN V2.0

1NET v2.0 is an incremental update, building and improving on the previous version. Many of the new features are based on customer requests.

Notable changes include:

- Ability to automatically disable Domain wireless connections when connected to the Domain with the wired connection.
- By default adapters associated with desktop virtualisation software (e.g. VMWare Workstation, Microsoft Loop Back Adapter etc) will be excluded from being disconnected by 1NET.
- Ability to exclude other network adapters from being disconnected by 1NET
- Now multithreaded meaning 1NET can respond even faster to network changes when on the Domain network
- New Group Policy template to control the new features
- Improved logging

KNOWN ISSUES

Issue 1: 1NET service may not start after a reboot if McAfee Agent 4.8 is installed

Versions Affected: All 1NET versions

Fix: This is a McAfee issue. Install McAfee 4.8 Patch 1

More information on changes in 1NET versions can be found in the Release Notes.

INSTALLATION

1NET is distributed as a Windows Installer package and is easily deployed using software deployment systems such as Microsoft System Center Configuration Manager (SCCM) or Group Policy Software Installation etc.

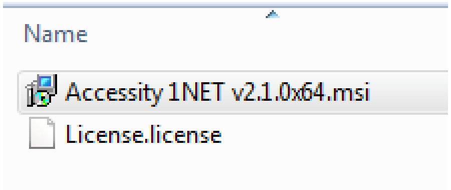
1NET can be installed in a reference/master operating system image or deployed to existing computers.

System Requirements

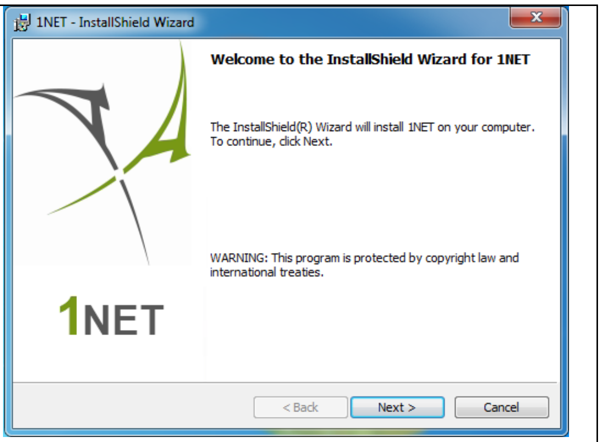
- Microsoft Windows 7 or Microsoft Windows 8 (32bit or 64bit)
- Computers must be a member of a Windows Domain
- Microsoft .NET Framework 4.0 *(The Microsoft .NET Framework 4.0 is **not** included in the 1NET installation and must be installed prior to installing 1NET. The Microsoft .NET Framework 4.0 redistributable can be downloaded from here http://msdn.microsoft.com/en-us/netframework/aa569263)*
- Mobile broadband modems must be Windows 7/8 compatible and support the Windows 7/8 WWAN Service.
- Windows Installer

NOTE: It is not supported to install the 32bit version of 1NET onto a 64bit system.

Interactive Installation

1. **Copy the License File** If you have **purchased** 1NET, copy the Accessity supplied license file (named '**License.License**') into the same directory as the installer MSI. The installer will copy this file to the system. **If the License.License file is not present, 1NET will function as 45 day fully featured trial.**	 Name Accessity 1NET v2.1.0x64.msi License.license **Shows License File Ready for Installation**
2. Logon to the computer with an **Administrator** account and Launch appropriate MSI for your Windows 7 architecture	***Intentionally Left Blank***
3. **Install Wizard – Welcome** The installer welcome screen will be displayed.	

Click ‘**Next**’ to continue



1NET - InstallShield Wizard

Welcome to the InstallShield Wizard for 1NET

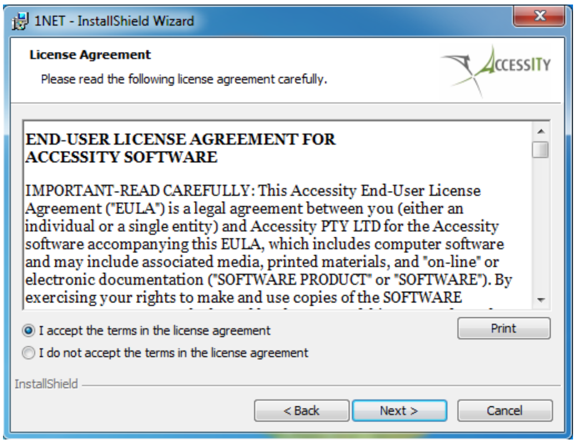
The InstallShield(R) Wizard will install 1NET on your computer. To continue, click Next.

WARNING: This program is protected by copyright law and international treaties.

Welcome Screen

4. **Install Wizard – License Agreement**

The License Agreement/EULA will be displayed. Accept the agreement and click ‘**Next**’ to continue.



1NET - InstallShield Wizard

License Agreement

Please read the following license agreement carefully.

END-USER LICENSE AGREEMENT FOR ACCESSITY SOFTWARE

IMPORTANT-READ CAREFULLY: This Accessity End-User License Agreement ("EULA") is a legal agreement between you (either an individual or a single entity) and Accessity PTY LTD for the Accessity software accompanying this EULA, which includes computer software and may include associated media, printed materials, and "on-line" or electronic documentation ("SOFTWARE PRODUCT" or "SOFTWARE"). By exercising your rights to make and use copies of the SOFTWARE

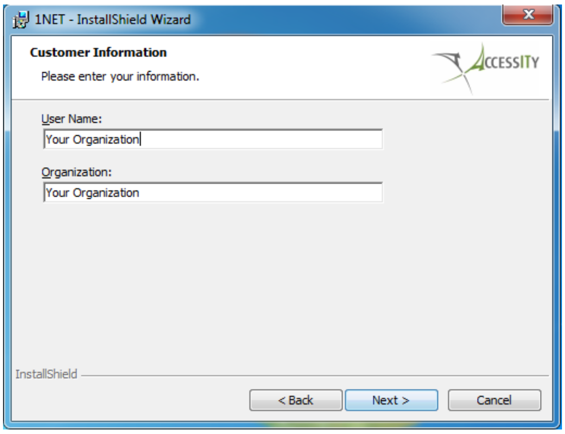
● I accept the terms in the license agreement

○ I do not accept the terms in the license agreement

License Agreement

5. Install Wizard – User Information

Enter information to personalise the installation. Click ‘**Next**’ to continue



1NET - InstallShield Wizard

Customer Information

Please enter your information.

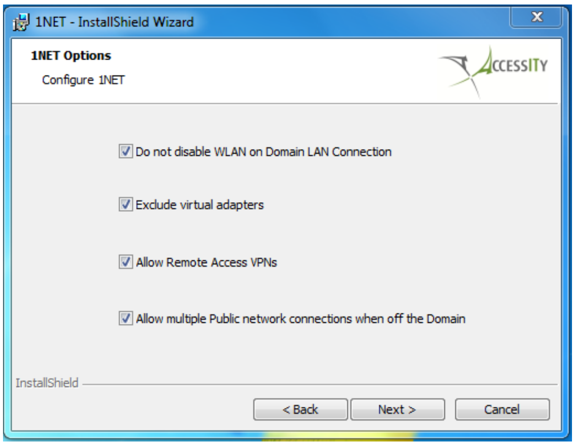
User Name: Your Organization

Organization: Your Organization

Company Information

6. Install Wizard – 1NET Options

The default 1NET behaviour is shown on this screen. You may configure these options for your organisation’s needs. Click ‘**Next’** to continue.



1NET - InstallShield Wizard

1NET Options

Configure 1NET

☑ Do not disable WLAN on Domain LAN Connection

☑ Exclude virtual adapters

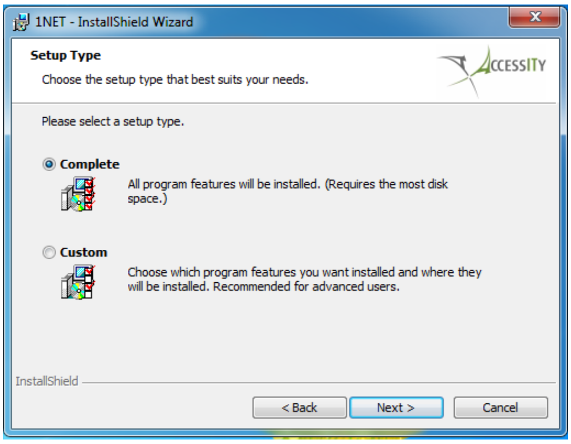
☑ Allow Remote Access VPNs

☑ Allow multiple Public network connections when off the Domain

1NET Options

7. Install Wizard – Setup Type

Please leave the default of **Complete**. Click ‘**Next’** to continue.



1NET - InstallShield Wizard

Setup Type

Choose the setup type that best suits your needs.

Please select a setup type.

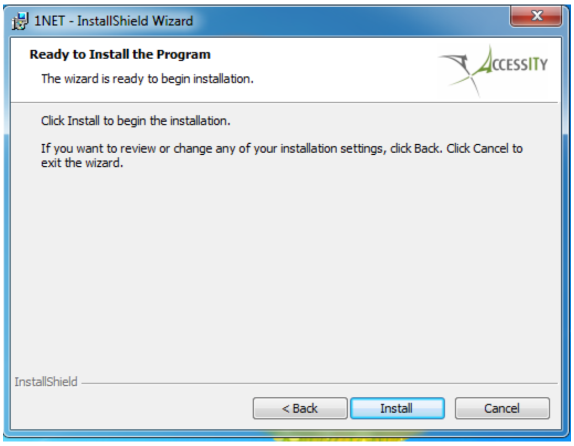
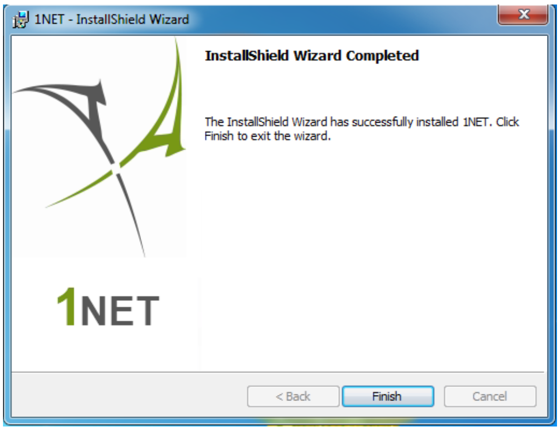
● **Complete**

All program features will be installed. (Requires the most disk space.)

○ **Custom**

Choose which program features you want installed and where they will be installed. Recommended for advanced users.

Setup Type

8. **Install Wizard – Ready to Install** The installation is ready to begin. Click ‘**Next**’ to begin the installation	 1NET - InstallShield Wizard **Ready to Install the Program** The wizard is ready to begin installation. Click Install to begin the installation. If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard. Ready to Install
9. **Install Wizard – Finish** The install is now complete. 1NET is running	 1NET - InstallShield Wizard **InstallShield Wizard Completed** The InstallShield Wizard has successfully installed 1NET. Click Finish to exit the wizard. Finish

Upgrading from a Previous Version

1NET supports upgrading from previous versions. The 1NET installer can be run on systems that have a previous version installed in order to upgrade.

The Group Policy ADMX files have been updated in v2.5 to version v1.5. These ADMX files support all 1NET versions greater than 1NET v2.0. These can be upgraded by simply copying over the previous files in the Central Policy Store.

Silent Installation

1NET supports standard Windows Installer command line switches.

A sample silent install

1NET 32bit

```
Msiexec /I “<path to installer>\Accessity 1NET v2.5.0x86.msi” /qb
```

1NET 64bit

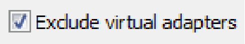
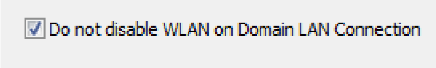
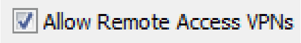
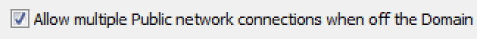
```
Msiexec /I "<path to installer>\Accessity 1NET v2.5.0x64.msi" /qb
```

Optional Parameters

The following optional parameters can be used to customise 1NET functionality. If the parameters are not specified, the default option will be used.

Please see the '**Configuring 1NET**' section of this document for more information on configuring 1NET.

These parameters are case sensitive.

PARAMETER	VALUE	DESCRIPTION	INSTALLER GUI
EXCLUDEVIRTUALADAPTERS	Y (Default) / N	Controls if adapters associated with virtualisation software will be managed by 1NET By default virtual adapters are not managed by 1NET.	 ☑ Exclude virtual adapters
ALLOWWLANONDOMAIN	Y (Default) / N	Controls if computers can be connected to the Domain network by wireless if they are also connected by the wired/LAN. By default computers can be connected to the Domain by both wired and wireless connections.	 ☑ Do not disable WLAN on Domain LAN Connection
ALLOWVPN	Y (Default) / N	Controls if Remote Access VPNs are permitted. Remote Access VPNs are used by users to remotely access your corporate network. Some VPNs and configurations appear as 'Domain' networks, this setting prevents the VPN connection being managed by 1NET.	 ☑ Allow Remote Access VPNs
SINGLEREMOTEADAPTER	Y / N (Default)	Controls if computers can be connected to multiple public networks when off the	 ☑ Allow multiple Public network connections when off the Domain

		Domain. By default 1NET assumes your VPN will control network traffic while off the corporate network. This setting can used for additional protection.	

Sample Command Line

You can use multiple properties on a single command line.

```
Msiexec /I "<path to installer>\Accessity 1NET v2.5.0x64.msi"
ALLOWWLANONDOMAIN=N /qb
```

License File

Upon purchase of 1NET, ACCESSITY will generate a License File ('**License.License**'). This file will license the product and remove the trial period.

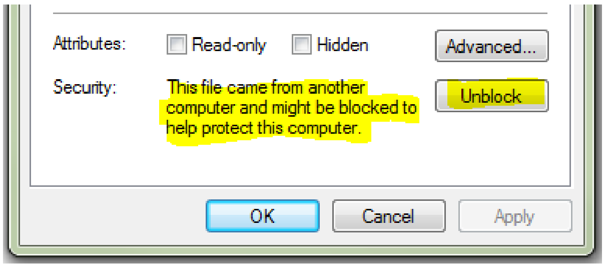
This license file must be copied into the same directory where 1NET has been installed.

The default location for the file is
%ProgramFiles%\Accessity\1NET\

Automatic License Installation

The 1NET 2.x installer will copy this file during the installation. In order for this license file to be automatically installed, the 'License.License' file must be located in the same directory as the installer (MSI file).

NOTE: For automatic license installation to work, any Internet Zone Identifies on the 'License.license' file must be removed. i.e.



Attributes: □ Read-only □ Hidden

Security: This file came from another computer and might be blocked to help protect this computer.

Figure 1 Shows the Zone Identifiers

Manual License Installation

This file can be copied using any method, e.g. wrapper script, batch file etc.

UPGRADING FROM THE TRIAL

If a license file (‘License.License’) is not present, 1NET will run in a full featured 45 day trial mode.

To upgrade from the trial version simply copy the supplied ‘License.License’ into the directory where 1NET is installed. Alternatively you can uninstall and reinstall 1NET with the ‘License.License’ in the same directory as the installer.

1NET will look for a ‘License.License’ when the service starts. When upgrading a system running in trial mode by manually copying the license file, you may wish to restart the 1NET service or reboot the computer to ensure the license file is processed instantly.

REMOTE ACCESS VPN SUPPORT

1NET supports IPSEC and SSL Remote Access VPNs. If you use a Remote Access VPNs with 1NET, you need to ensure that 1NET is aware of the VPN's network adapter.

If 1NET is not aware of the VPN adapter, it may attempt to disconnect it.

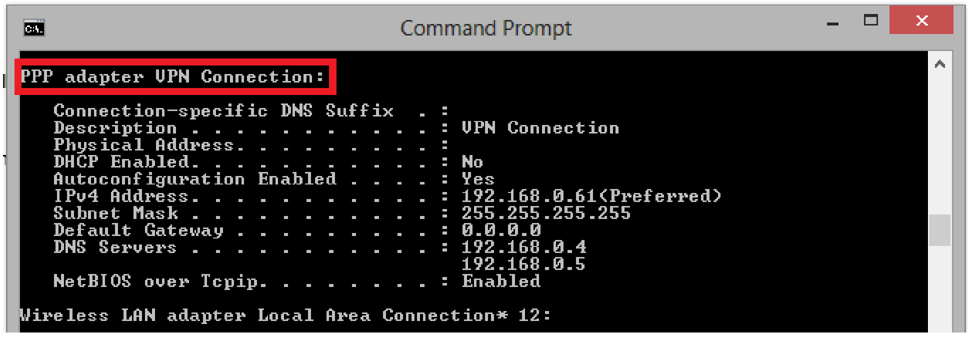
VPN Auto Detection

1NET's default behaviour is to automatically detect VPN adapters. In order for 1NET to identify a VPN adapter, it must be registered in Windows as a VPN adapter. Common SSL VPN's should also be detected automatically.

More information on controlling this behaviour can be found under Allow Remote Access VPNs in the Configuring 1NET section of this document.

You can quickly examine the network adapters on your system to see if 1NET will detect them.

To do this run the command `ipconfig /all` and see if your VPN is listed as a "**VPN Connection**".



```
PPP adapter VPN Connection:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : VPN Connection
   Physical Address. . . . . . . . . :
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   IPv4 Address. . . . . . . . . . . : 192.168.0.61(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.255
   Default Gateway . . . . . . . . . : 0.0.0.0
   DNS Servers . . . . . . . . . . . : 192.168.0.4
                                       192.168.0.5
   NetBIOS over Tcpip. . . . . . . . : Enabled

Wireless LAN adapter Local Area Connection* 12:
```

Figure 2- Shows a supported auto detected VPN adapter

Manually Defining a VPN Adapter

Some additional configuration of 1NET might be needed to ensure that 1NET can identify your VPN. This is typical for some **SSL** VPNs.

Steps on performing this can also be found under **Exclude Network Adapters** in the **Configuring 1NET** section of this document.

The following describes the process of excluding a VPN adapter which was **not** automatically identified. 1NET can be configured using **Group Policy** (**Option 1** - below) or by editing the **Registry** (**Option 2** - below).

Option 1: Configure 1NET using Group Policy

a. Install the ADMX/ADML files into the central policy store

b. Enable the Group Policy Setting '**Allow Remote Access VPN Connections**'

c. Obtain the '**PNP Device ID**' of the **VPN Adapter** and add it to the Group Policy setting **'Exclude Network Adapters List'**

d. Apply the Group Policy to the computer, and reboot the computer or restart 1NET service

Option 2: Configure 1NET using the Registry

a. Ensure the registry key to enable Remote Access VPN support is set to '1' or does not exist
Key: HKLM\Software\Accessity\1Netv2
Value Type: DWORD
Value Name: AllowVPN
Data: 1

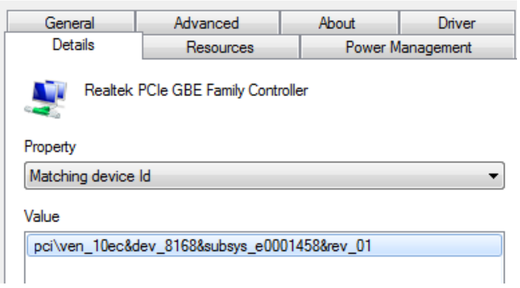
b. Add the registry key
Key: HKLM\Software\Accessity\1Netv2
Value Type: REG_SZ
Value Name: ExcludeAdaptersList
Data: The 'Device ID' if the VPN Adapter.

c. Restart the 1NET service or the computer to pick up the settings.

Obtaining the PNP Device ID

In order to exclude a VPN adapter, you need to obtain is **PNP Device ID**. There are several way to do this

1. The 1NET **Debug Logging** will log the PNP Device ID for any adapter it is disconnected. You can retrieve the PNP Device ID from the 1NET Debug Log.
2. Through **Windows Device Manager**. (You may need to select 'View -> Show hidden devices')



Realtek PCIe GBE Family Controller

Property: Matching device Id

Value: pci\ven_10ec&dev_8168&subsys_e0001458&rev_01

3. Using the following PowerShell command. Substituting "`<YourSSLVender>` for your VPN vendor e.g. `Cisco`

```
Get-WmiObject win32_pnpentity | where {$_.Name -match
"<YourSSLVender>"}
```

NETWORK ADAPTERS

The following network adapter types and configurations are supported by 1NET.

Ethernet and Wireless Adapters

1NET supports the management of network connections which appear as 'Local Area Connection' or 'Wireless Network Connections'.

WWAN/Mobile Broadband Modems

1NET supports Mobile Broadband Modems that integrate with the Windows 7/8 Mobile Broadband Connection Manager and WWAN Service.

Mobile Broadband Modems often come bundled with proprietary Connection Managers or Watchers. These can often be configured in a way that prevents them from being managed by the Windows Mobile Broadband Connection Manager. ACCESSITY strongly recommends that proprietary connection managers and watches should **not** be installed.

Typically Windows Compatible Mobile Broadband Modems have a 'driver only' install available or guidance on enterprise deployments.

Mobile Phone Tethering

Tethered Mobile Phones which are connected to the computer via USB and appear as a 'Local Area Connection' are supported by 1NET.

Using a mobile phone as a 'wireless hotspot' or 'wireless router/access point' is supported by 1NET.

Remote Access

1NET supports most typical IPSEC and SSL VPN adapters. 1NET will attempt to identify your remote access VPN, if it cannot, this can be manually configured. More information on Remote Access VPNs can be found in the **Remote Access VPN Support** section of this document.

1NET supports Microsoft DirectAccess. No additional configuration is required to support this remote access technology.

Virtual Adapters

The following network adapters associated with client virtualisation software will be automatically excluded from being managed by 1NET.

Oracle Virtual Box
VMware Adapters
Microsoft Hyper-V
Microsoft Loopback Adapter

CONFIGURING 1NET

1NET features can be configured in a number of ways. Choose the method which best suits your organisation. It is not necessary to configure all or any features, typically the defaults will be sufficient for most organisations.

1. Installer Parameters *(limited settings)*
2. Using Group Policy and the 1NET ADMX.
3. Registry Keys

Disconnect Wireless When Connected by Ethernet

By default, 1NET allows computer to be connected to the Domain network using both the wired and wireless Domain connections simultaneously.

1NET can be configured to automatically disconnect any wireless Domain connections when connected to the Domain by the wired/LAN connection and to automatically reconnect to the Domain wireless network when disconnected from the Domain wired/LAN.

This setting will ensure that computers are only connected to the Domain by wired connection.

Default Behaviour	**Disabled**. Computers may be connected to the Domain using both wired and wireless network connections simultaneously.	
Installer Parameter	ALLOWWLANONDOMAIN=Y	Allows both wired and wireless connections
	ALLOWWLANONDOMAIN=N	Disconnects wireless if connected to the Domain by the wired connection
Registry Keys	**Key:** HKLM\Software\Accessity\1Netv2 **Value Type:** DWORD **Value Name:** DisconnectWLANonDomain	
	Value: 1	**Enabled**: Disconnects wireless if connected to the Domain by the wired connection
	Value: 0 *Or not set*	**Disabled**: Allows both wired and wireless connections
	Key: HKLM\Software\Accessity\1Netv2 **Value Type:** DWORD **Value Name:** DisableWLANReconnect	
	Value: 1	**Enabled**: 1NET will not auto reconnect to the corporate wireless network
	Value: 0 *Or not set*	**Disabled:** 1NET will auto reconnect to the corporate wireless network
Group Policy	Computer Configuration -> Administrative Templates -> Accessity -> 1NET -> v2 -> **Disconnect WLAN on Domain**	

	Enabled	Disconnects wireless if connected to the Domain by the wired connection
	Disabled	Allows both wired and wireless connections
	Not Configured	Allows both wired and wireless connections
	Computer Configuration -> Administrative Templates -> Accessity -> 1NET -> v2 -> **Disable WLAN Reconnect**	
	Enabled	1NET will not auto reconnect to the corporate wireless network
	Disabled	1NET will auto reconnect to the corporate wireless network
	Not Configured	1NET will auto reconnect to the corporate wireless network

Single Remote Adapter

Single Remote Adapter will restrict computers off the Domain network to only one public network. By default, 1NET will allow a computer off the Domain network to connect to multiple public networks and relies on DirectAccess or VPNs to control the traffic routing and control tunnelling.

A computer must have one network adapter on a public network in order to use a VPN/DirectAccess etc. Enabling this setting will prevent subsequent connections to public networks. This setting can help reduce risk, but should be considered carefully before enabling

Default Behaviour	**Disabled**. While a computer is not connected to the Domain network it is permitted to connect to multiple public networks.	
Installer Parameter	SINGLEREMOTEADAPTER=Y	While off the Domain network, the computer can only connect to one network
	SINGLEREMOTEADAPTER =N	While off the Domain network, the computer can connect to multiple networks
Registry Keys	**Key:** HKLM\Software\Accessity\1Netv2 **Value Type:** DWORD **Value Name:** SingleRemoteAdapter	
	Value: 1	**Enabled**: While off the Domain network, the computer can only connect to one network
	Value: 0 *Or not set*	**Disabled**: While off the Domain network, the computer can connect to multiple networks
Group Policy	Computer Configuration -> Administrative Templates -> Accessity -> 1NET -> v2 -> **Single Remote Adapter**	
	Enabled	While off the Domain network, the computer can only connect

		to one network
	Disabled	While off the Domain network, the computer can connect to multiple networks
	Not Configured	While off the Domain network, the computer can connect to multiple networks

Disconnect Virtual Adapters

By default, 1NET will not manage virtual adapters associated with some specific client side virtualisation software. See the '**Network Adapters**' section for a list of supported products.

This setting is intended for organisations that have users that run client side virtualisation software and wish to support this usage. For organisations that don't use client side virtualisation and wish to discourage its usage, enabling this setting will cause 1NET to disconnect these adapters.

Typically network adapters associated with client side virtualisation software will appear to the Windows 7 host as being on a '**Public**' or '**Unclassified**' network and as such, 1NET will disconnect them.

Default Behaviour	**Disabled**. Network adapters associated with specific client side virtualisation software will not be managed (disconnected) by 1NET	
Installer Parameter	EXCLUDEVIRTUALADAPTERS=Y	Excludes network adapters associated with virtualisation software
	EXCLUDEVIRTUALADAPTERS=N	Disconnects network adapters associated with virtualisation software
Registry Keys	**Key:** HKLM\Software\Accessity\1Netv2 **Value Type:** DWORD **Value Name:** DisconnectVirtualAdapters	
	Value: 1	**Enabled**: Disconnects network adapters associated with virtualisation software
	Value: 0 *Or not set*	**Disabled**: Excludes network adapters associated with virtualisation software
Group Policy	Computer Configuration -> Administrative Templates -> Accessity -> 1NET -> v2 -> **Disconnect Virtual Adapters**	
	Enabled	Disconnects network adapters associated with virtualisation software
	Disabled	Excludes network adapters associated with virtualisation software
	Not Configured	Excludes network adapters

		associated with virtualisation software

Exclude Network Adapters

This allows organisations to exclude specific adapters from being managed by 1NET. This setting should allow maximum flexibility to organisations.

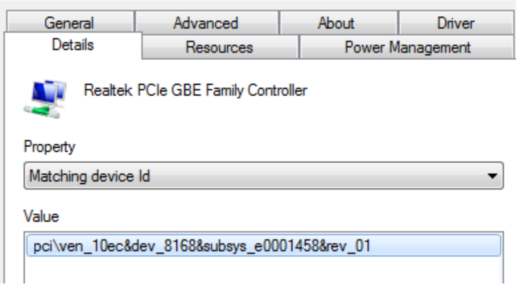
This option has two settings. You can set one or both

1. **Exclude Network Adapters**
   If you wish to have a computer connected to the **Domain** network and use an additional network adapter to legitimately connect to another **Non Domain** network. Enable this setting **and** add the '**Device ID'** of the additional network adapter to the **'Exclude Network Adapters List**'

2. **Exclude VPN Adapters**
   Excludes Remote Access VPNs which appear to Windows as a **standard** network adapter and **not** a VPN adapter. 1NET will automatically detect VPNs but if Windows does not know it's a VPN, 1NET also does not know. In this scenario. Enable this option **and** add the **'PNP Device ID**' of the VPN's network adapter to the **'Exclude Network Adapters List'**

Exclude Network Adapters List

To exclude any adapter, you will require the devices '**PNP Device ID**' which can be obtained a number of ways, including through **Windows Device Manager**. (You may need to select 'View -> Show hidden devices')



Realtek PCIe GBE Family Controller

Property

Matching device Id

Value

pci\ven_10ec&dev_8168&subsys_e0001458&rev_01

Figure 3- Shows 'Device ID' through Device Manager

Default Behaviour	**Disabled**. No adapters are excluded	
Installer Parameter	N/A	
Registry Keys	**Key:** HKLM\Software\Accessity\1Netv2 **Value Type:** DWORD **Value Name:** ExcludeNetworkAdapters	
	Value: 1	**Enabled**: The specified network adapters will be excluded from 1NET

	Value: 0 *Or not set*	**Disabled**: All network adapters will be managed by 1NET.
	Key: HKLM\Software\Accessity\1Netv2 **Value Type:** REG_SZ **Value Name:** ExcludeAdaptersList	
	Value: Comma separated list of 'Device IDs'	The adapters specified in this registry key will be excluded from 1NET or identified as VPNs
Group Policy	Computer Configuration -> Administrative Templates -> Accessity -> 1NET -> v2 -> **Exclude Network Adapters**	
	Enabled	The specified network adapters will be excluded from 1NET
	Disabled	All network adapters will be managed by 1NET.
	Not Configured	All network adapters will be managed by 1NET.
	Computer Configuration -> Administrative Templates -> Accessity -> 1NET -> v2 -> **Exclude Network Adapters List**	
	Enabled Comma separated list of **'Device IDs'**	The specified network adapters will be excluded from 1NET or identified as VPNs
	Disabled	All network adapters will be managed by 1NET.
	Not Configured	All network adapters will be managed by 1NET.

Network Identification Timeout

This allows organisations to manage the amount of time 1NET will wait for Windows to classify the network connection. This is intended to help tune 1NET for an organisation's network. However, it is expected the default setting will be sufficient for most environments.

If this timeout is configured too low, it will make 1NET more responsive, but will risk the Domain network being disconnected if the network is slow to be classified. Setting the timeout too high could leave your network unprotected by 1NET for longer.

1NET will check to see if the Windows Network Location Manager has classified the network every 5 seconds up to this specified timeout value. i.e. 5 secs x <TimeOut> = Total Identification Time.

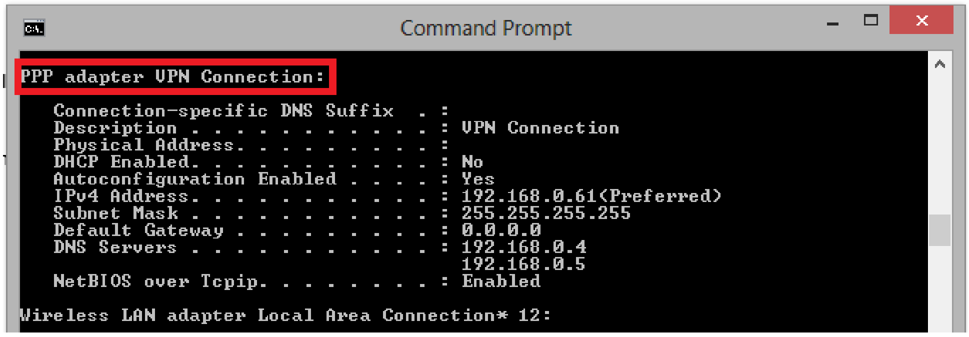
Default Value	**24** 1NET will wait 24 x 5 = 120 secs (2 mins)	
Installer Parameter	N/A	
Registry Keys	**Key:** HKLM\Software\Accessity\1Netv2 **Value Type:** REG_SZ **Value Name:** IDTimeOut	
	Value: the TimeOut value	1NET will check with the NLM

		every 5 secs up to the number of times specified in this value
	Not Set	The default of 24 will be used.
Group Policy	Computer Configuration -> Administrative Templates -> Accessity -> 1NET -> v2 -> **Network Identification Timeout**	
	Enabled The TimeOut value	1NET will check with the NLM every 5 secs up to the number of times specified in this value
	Disabled	The default of 24 will be used.
	Not Configured	The default of 24 will be used.

Allow Remote Access VPNs

Controls if 1NET will **allow** or **disallow** remote access VPNs. Any VPN connections detected by Windows as VPNs are supported by 1NET. This setting prevents the host adapter being disconnected when a VPN connection is established.

The following image shows how a Windows supported VPN adapter appears when you run the command `ipconfig /all`



```
PPP adapter VPN Connection:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : VPN Connection
   Physical Address. . . . . . . . . :
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   IPv4 Address. . . . . . . . . . . : 192.168.0.61(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.255
   Default Gateway . . . . . . . . . : 0.0.0.0
   DNS Servers . . . . . . . . . . . : 192.168.0.4
                                       192.168.0.5
   NetBIOS over Tcpip. . . . . . . . : Enabled

Wireless LAN adapter Local Area Connection* 12:
```

Figure 4- Shows a supported auto detected VPN adapter

If your VPN adapter is not detected by Windows as a VPN, you can exclude it from 1NET using the by adding it to the 'Exclude Network Adapters List'. See the *Exclude Network Adapters* setting for more information.

Default Value	**Enabled**	
Installer Parameter	ALLOWVPN=Y	Automatically Detected Remote Access VPNs will be permitted.
	ALLOWVPN=N	Automatically Detected Remote Access VPNs will not be permitted.
Registry Keys	**Key:** HKLM\Software\Accessity\1Netv2 **Value Type:** DWORD	

	Value Name: AllowVPN	
	Value: 1 *Or not set*	Automatically Detected Remote Access VPNs will be permitted.
	Value: 0	Automatically Detected Remote Access VPNs will not be permitted.
Group Policy	Computer Configuration -> Administrative Templates -> Accessity -> 1NET -> v2 -> **Allow Remote Access VPN Connections**	
	Enabled	Remote Access VPNs will be permitted.
	Disabled	Remote Access VPNs will not be permitted
	Not Configured	Remote Access VPNs will be permitted.

Allow Tunnel Adapters

Controls if 1NET will **allow** or **disallow** network tunnels. Enabling this setting will prevent 1NET disconnecting the host adapter when a network tunnel is used for remote access. Network tunnel are typical for SSL VPNs and ISATAP connections.

Default Value	**Disabled**	
Installer Parameter	N/A	
Registry Keys	**Key:** HKLM\Software\Accessity\1Netv2 **Value Type:** DWORD **Value Name:** Tunnels	
	Value: 1	1NET will manage Tunnel Adapters
	Value: 0 *Or not set*	1NET will not manage Tunnel Adapters
Group Policy	Computer Configuration -> Administrative Templates -> Accessity -> 1NET -> v2 -> **Allow Tunnel Adapters**	
	Enabled	1NET will manage Tunnel Adapters
	Disabled	1NET will manage Tunnel Adapters
	Not Configured	1NET will manage Tunnel Adapters

Debug Logging

The debug logging is used to help troubleshoot and monitor 1NET activity. This logging is very verbose, so should be enabled selectively and while troubleshooting.

Log File: %windir%\Temp\1NET_Debug.log

Default Value	**Disabled**	
Installer Parameter	N/A	
Registry Keys	**Key:** HKLM\Software\Accessity\1Netv2 **Value Type:** DWORD **Value Name:** DebugLog	
	Value: 1	Logging will be enabled
	Value: 0 *Or not set*	Logging will not be enabled.
Group Policy	Computer Configuration -> Administrative Templates -> Accessity -> 1NET -> v2 -> **Enable Debug Logging**	
	Enabled	Logging will be enabled
	Disabled	Logging will not be enabled.
	Not Configured	Logging will not be enabled.

Domain Connections Only

Controls if computers can only connect to the corporate Domain Network. This setting is NOT intended for laptops/portable computers that may need to connect to Public networks in order to use VPNs or other remote access technologies.

This setting is computers such as desktop computers which should only ever be used on networks other than the corporate Domain network.

This setting prevents users from disconnecting their computer from the corporate Domain network and connecting to a Public/untrusted network.

Default Value	**Disabled**	
Installer Parameter	N/A	
Registry Keys	**Key:** HKLM\Software\Accessity\1Netv2 **Value Type:** DWORD **Value Name:** DomainOnly	
	Value: 1	When the computer is off the Domain network, any Public connections will be disconnected
	Value: 0 *Or not set*	When the computer is off the Domain network, any Public connections will be permitted

Group Policy	Computer Configuration -> Administrative Templates -> Accessity -> 1NET -> v2 -> **Domain Connections Only**	
	Enabled	When the computer is off the Domain network, any Public connections will be disconnected
	Disabled	When the computer is off the Domain network, any Public connections will be permitted
	Not Configured	When the computer is off the Domain network, any Public connections will be permitted

TROUBLESHOOTING TIPS

1NET Logging

Logging can be enabled by setting the following registry entry. This logging is very verbose, so should be enabled selectively and while troubleshooting.

> **Path:** HKLM\Software\Accessity\1Netv2
> **Value Type:** DWORD
> **Value Name:** DebugLog
> **Value:** 1

Log File: %windir%\Temp\1NET_Debug.log

NOTE: The 1NET service must be restarted after setting this registry key in order to begin logging.

Network Classification Issues

1NET requires Windows 7 to classify networks correctly as either Domain, Public or Private networks and to do this in a timely manner. The default is 2 minutes, but this can be tuned. See the '**Configuring 1NET**' section of this document.

The Windows 7 Event Log **<Event Viewer>\Application and Services Logs\Microsoft\Windows\NetworkProfile** will help in troubleshooting network classification issues.

Issues with this Windows 7 feature should be investigated with the help of Microsoft Support.

Restrict Users from Changing a Network Location

You may wish to restrict user's ability to change the location for a specific network.

This can be controlled through the following Group Policy Setting
Computer Configuration\Windows Settings\Security Settings\Network List Manager Policies\All Networks

Stop Administrators Disabling 1NET

Typically in most organisations, standard users do not have Administrator access on their system and as such cannot disable 1NET, this is best practice. If a user is an Administrator, they can stop/disable 1NET. Users with Administrator access have almost unrestricted access to the system preventing Administrators from doing something is largely pointless. However, if you wish to make it more difficult for Administrators to disable 1NET here are some steps.

NOTE: Please follow steps with caution and test this configuration. Accessity does not accept responsibility for any damages this configuration may cause.

1. Log on to a machine that has the particular service installed using an account with sufficient rights to create group policy objects. (for instance a Domain Admin)
2. Install the Group Policy Management Console (GPMC) available here.
3. Start the Group Policy Management MMC (gpmc.msc)
4. Select the Organization Unit (OU) where you've placed your client computers
5. Right click the OU and select the Create and link a new gpo here... option from the menu
6. Give the new Group Policy object (GPO) a distinctive name (like 'Policy to enable 1NET')
7. Select the Group Policy Object itself, right click it and select the Edit option from the menu
8. Navigate to the Computer Configuration\Window Settings\Security Settings\System Services part of the GPO.
9. A list of Services on the local computer should show up.
10. Search the service you want to be forced and select it.
11. Double click the Service Name
12. Click Define this policy.
13. Change the security setting to only enable a group of 'real' or '1Net' administrators to overrule these settings. If this group does not exist, create it now.
14. Set the Service startup mode as Automatic.
15. Click OK
16. Close the Group Policy Management Console
17. Log off

Monitoring the 1NET Service

1NET itself does not contain any centralised monitoring capability. Most organisations would prefer not to have multiple management systems polling their systems or that they have to run. 1NET is intended to be very lightweight and simple to deploy, and built in centralised management would be contrary to this goal.

The 1NET service can be monitored by third party tools that are commonly used in most large organisations. Such tools include Microsoft System Center Operations Manager and Microsoft System Center Configuration Manager using the Desired Configuration Management tools.

E.g. Microsoft System Center Configuration Manager using the Desired Configuration Management can be used to monitor the 1NET service and report on system where the service is not running.

Users gets disconnected when the access your network over VPN

If users immediately get disconnected when they attempt to access your corporate network over a remote access VPN, it may be that 1NET is not aware of the VPN adapter and is disconnecting it once the VPN tunnel to the Domain has been established. See the **Remote Access VPN Support** section of this document for more information.

1NET service does not start

If the 1NET the 1NET service will not start the following maybe the cause

1. The trial period has expired. Please note that the trial period began on a computer when the first instance of 1NET was installed. This includes any previous versions of 1NET.
2. The License.License file is not installed correctly. See the
3.
4. **License** File section of this document.
5. The Microsoft .NET Framework 4.0 is not installed or is not working correctly
6. 1NET is installed on an operating system other than Microsoft Windows 7 or Microsoft Windows 8
7. 1NET depends on the Windows services “**Network List Service**” and the “**Network Location Awareness**” service. Ensure that these are running correctly

TRADEMARK NOTICES

Microsoft, .NET Framework, DirectAccess, System Center, Configuration Manager, and Windows are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.