

EdgeXOS Platform Notes

XRoads Networks

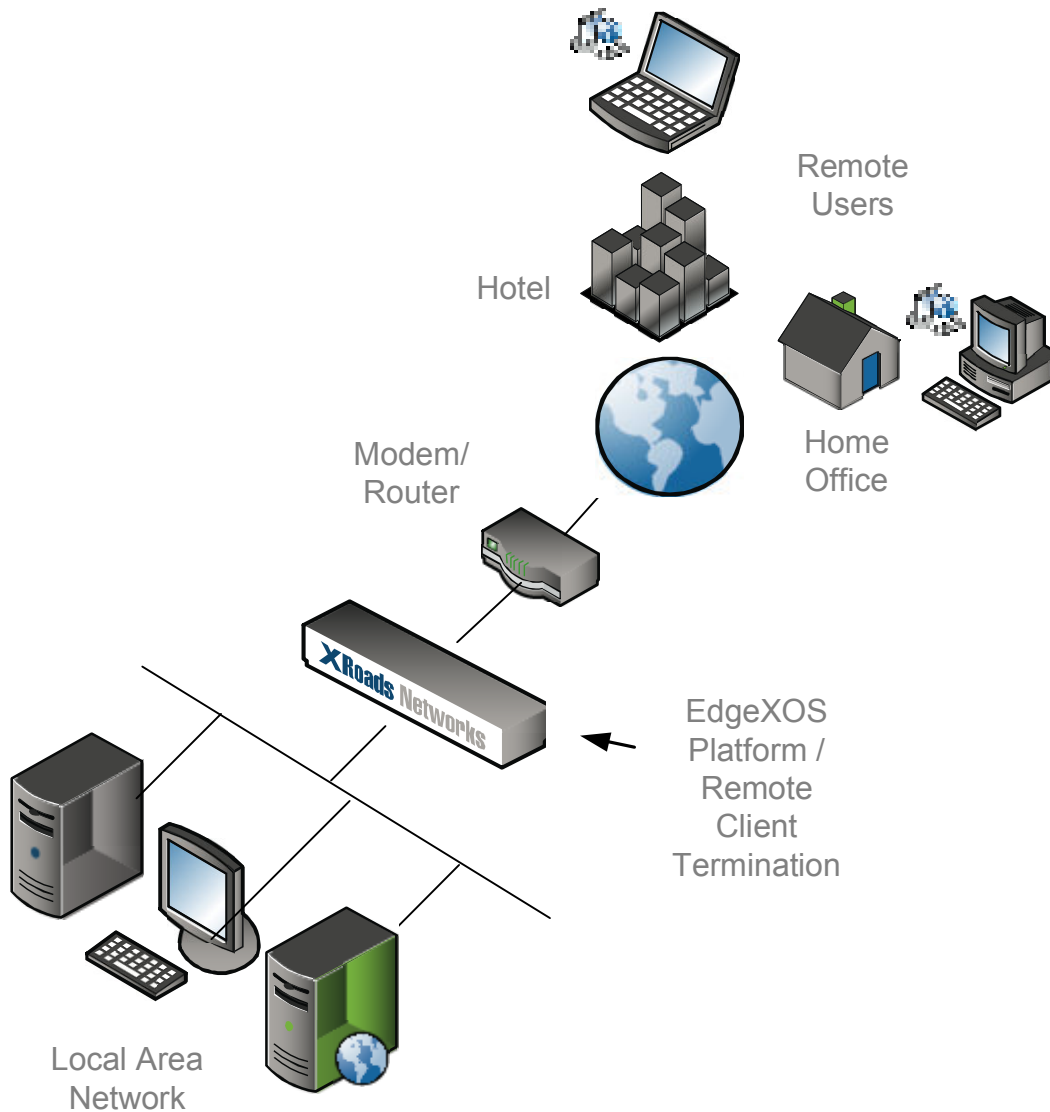
Edge Network Appliance Platform Notes

EdgeXOS Setting Up Site2Site Client Connectivity

How To Easily Setup Site2Site Clients

This document provides an overview of how you can easily setup our Site2Site client on any MS Windows-based system. The client is designed to be deployed on remote workstations, laptops, or home office systems which need secure remote access.

Overview: The Site2Site clients allow remote workers to easily access corporate resources by setting up a secure encrypted tunnel back to the central office EdgeXOS appliance. Our Site2Site tunnels utilize SSL-based tunneling technology, but do not require a browser or any browser based services. Our tunnels provide full Layer-3 connectivity with 3DES encryption built-in.



Authentication is based on certificates and a username / password authentication system. If either is missing the remote user will not be granted access.

Additional restrictions on remote users can be applied by using firewall rules.

Downloading the Client: In order to download the client, go to the NAS Firewall tab select the Site2Site Client Termination menu. From here you will see a link which goes to the client download site. Click on the link, fill out the registration form and get ready to install the client.

Setting Up The Server Side: To setup the server side, the first step is to enable the Site2Site client termination and enter the virtual tunnel IP address range. This can be done under the NAC Firewall tab Site2Site Client Termination menu. The virtual tunnel IPs are used to connect the clients to the EdgeXOS appliance.

NOTE: The Site2Site Client Network addresses can NOT be the same as your LAN addresses. These addresses could be a private address range (i.e. 192, 10, or 172 space), or any range which is not currently being used. Again, these addresses should NOT be within any ranges that are use within your existing network.

The following is an example of how to setup simple remote Site2Site client access:

Enabled Disabled (Enables Site2Site Client Termination)

Enabled Disabled (Direct Client-to-Client Communications)

Enabled Disabled (Force Default Gateway)

. . .0 Site2Site Client Network (Examples: 192.168.1.0 or 10.10.0.0)

Server Port (Default XRLogin Port 1104)

If you want the clients to be able to communicate directly with one another, enable the Direct Client-to-Client Communications.

If you want to force ALL remote user traffic, including any Internet-based traffic through the tunnel, enable the Force Default Gateway option. You may also need to do this if you have multiple LAN networks to which the user must connect.

Finally, if you wish to use a different default port then enter that port number instead of the default 1104 port (XRL).

Once the Site2Site Client Termination menu has been configured it is now time setup the remote users. This is done under the User/Device Management menu (now found under the NAS Firewall tab, was previously under the Shaping tab).

To add a new user simply click the Add User/Device button and enter the required information. The user will be assigned a dynamic address from the client network pool so do not assign an IP address here.

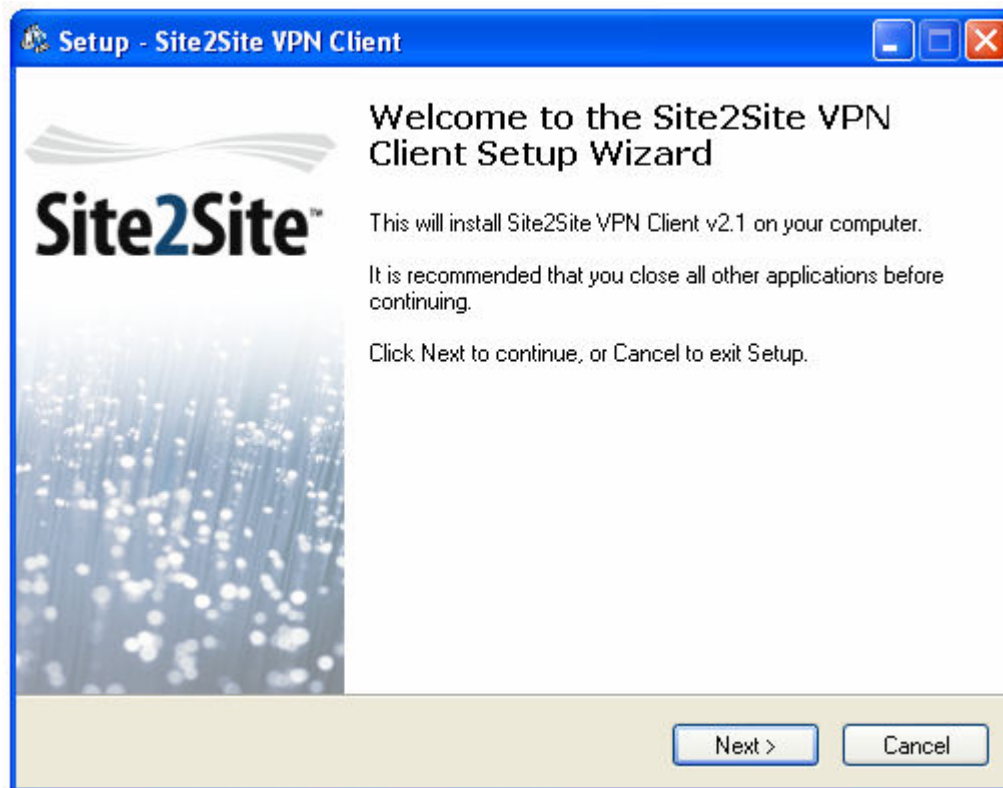
Required Information:

- 1) Name for this user/device.
- 2) Authentication Password
- 3) Confirmation of Authentication Password

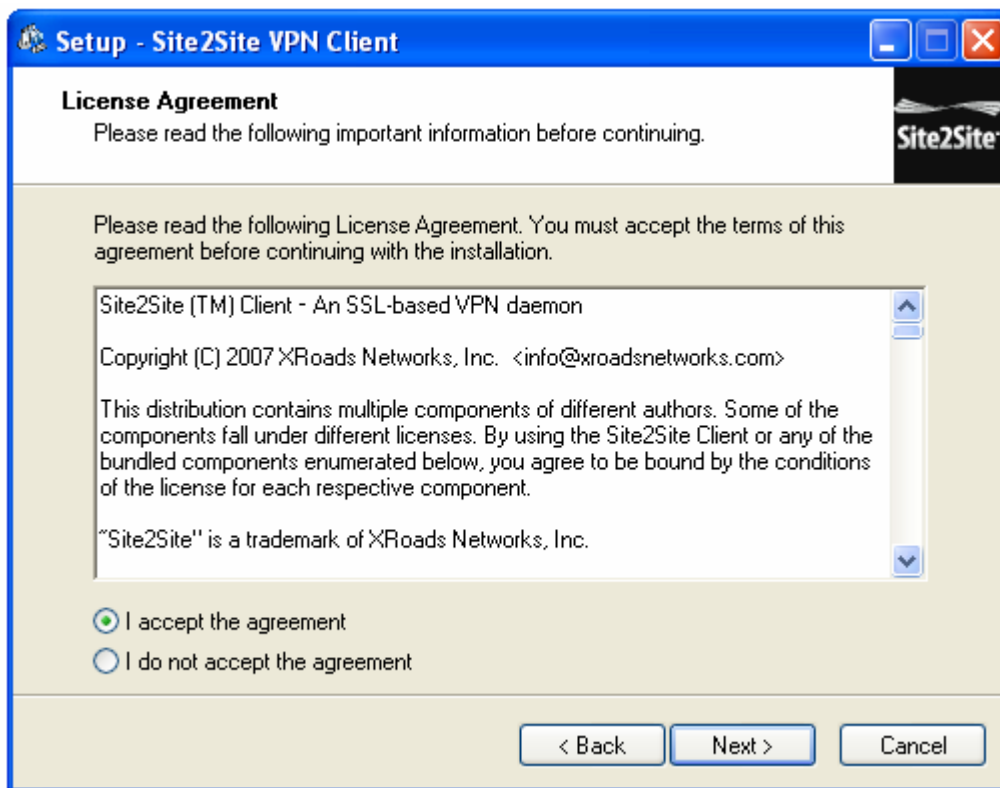
Once the users have been added, make sure that there are no firewalls which may block inbound access to the clients. By default the an allow rule is created when the Site2Site client termination is enabled, however this rule can be overridden by other rules created by the network administrator, so check your rules carefully if you have problems.

Setting Up The Client Side: To setup the client side, the first step is to install the small Site2Site client application. This client application is used to improve the authentication process and provide full Layer-3 connectivity.

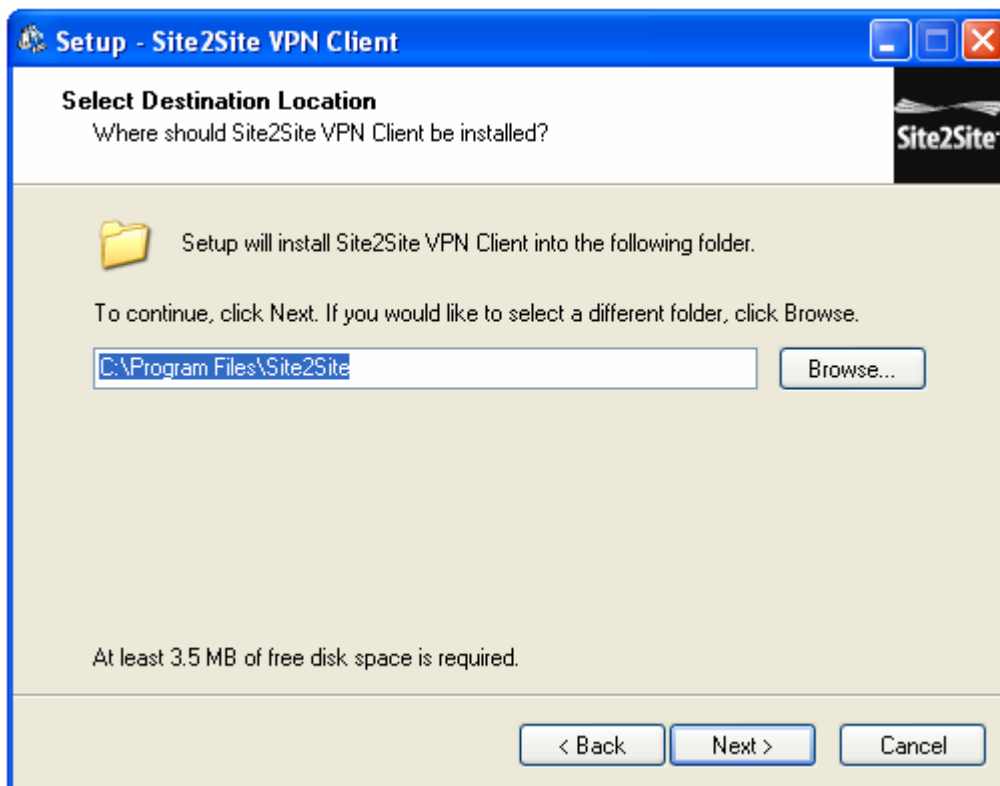
To install the client simple double-click on the executable which was downloaded and follow the instructions. During the installation you will be asked to approve the installation of a new network driver.



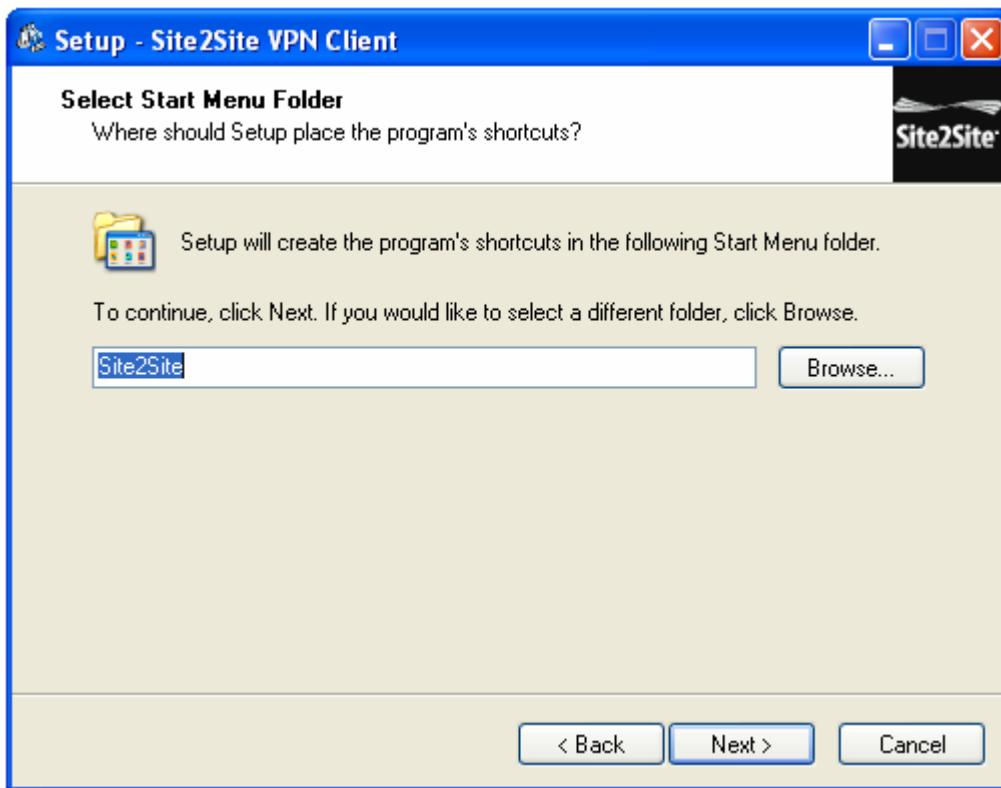
Click Next



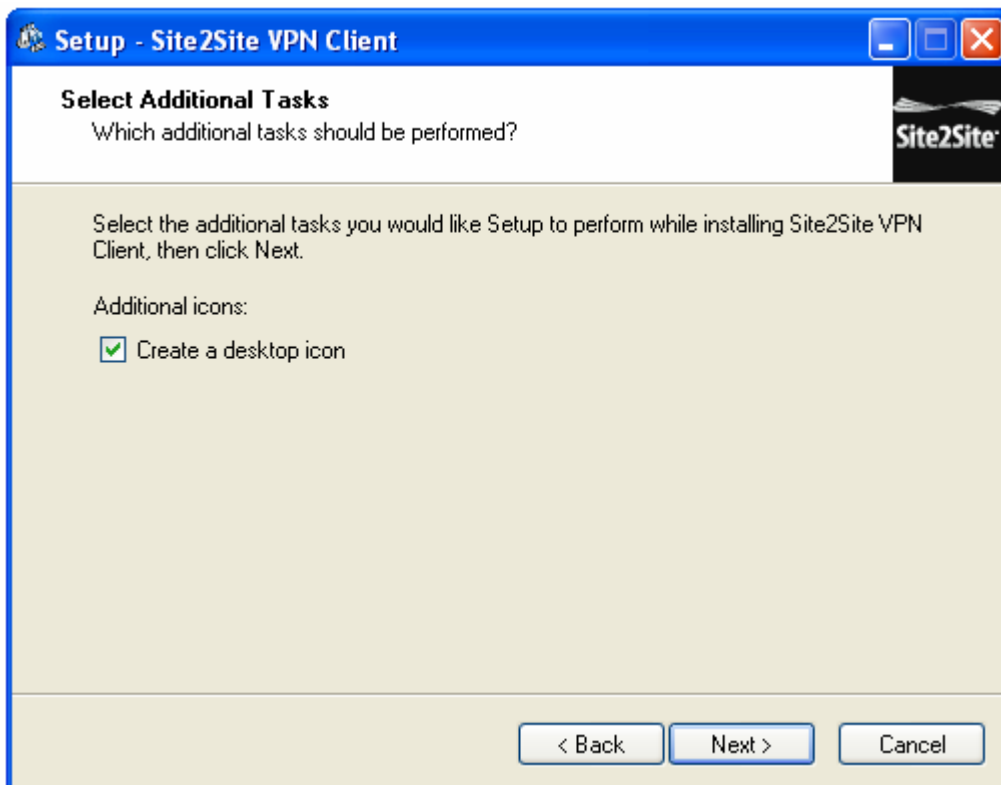
Accept the License Agreement and click Next



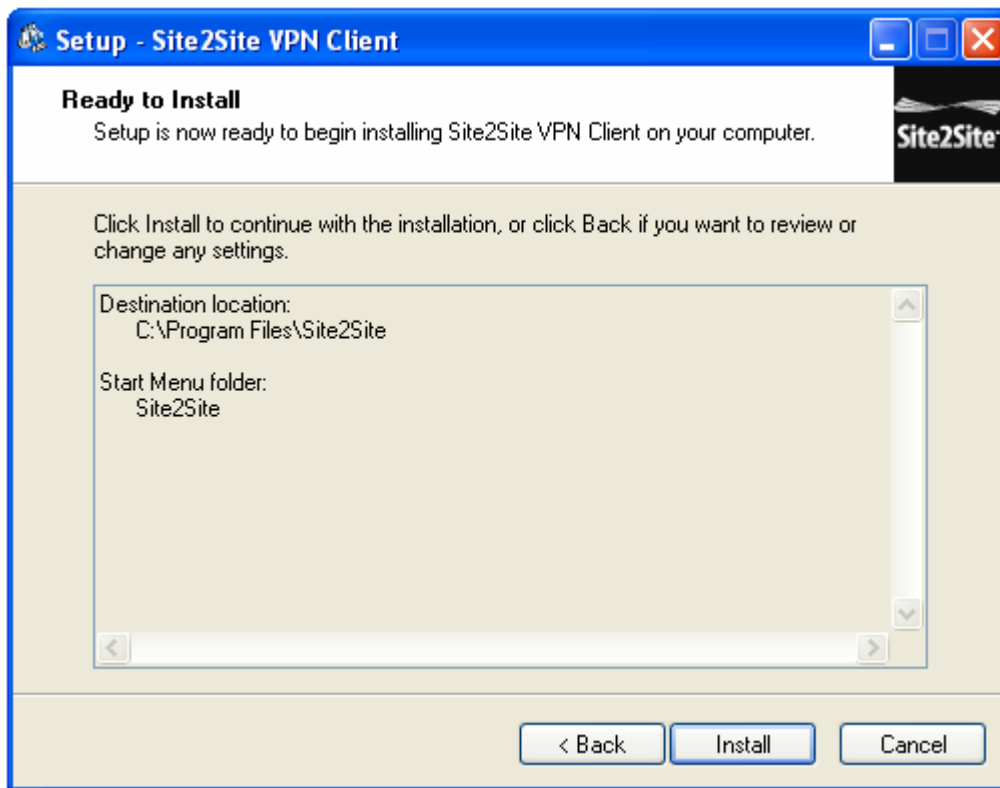
Enter the folder location or accept the default and click Next



Enter the folder to be used under the Start menu and click Next



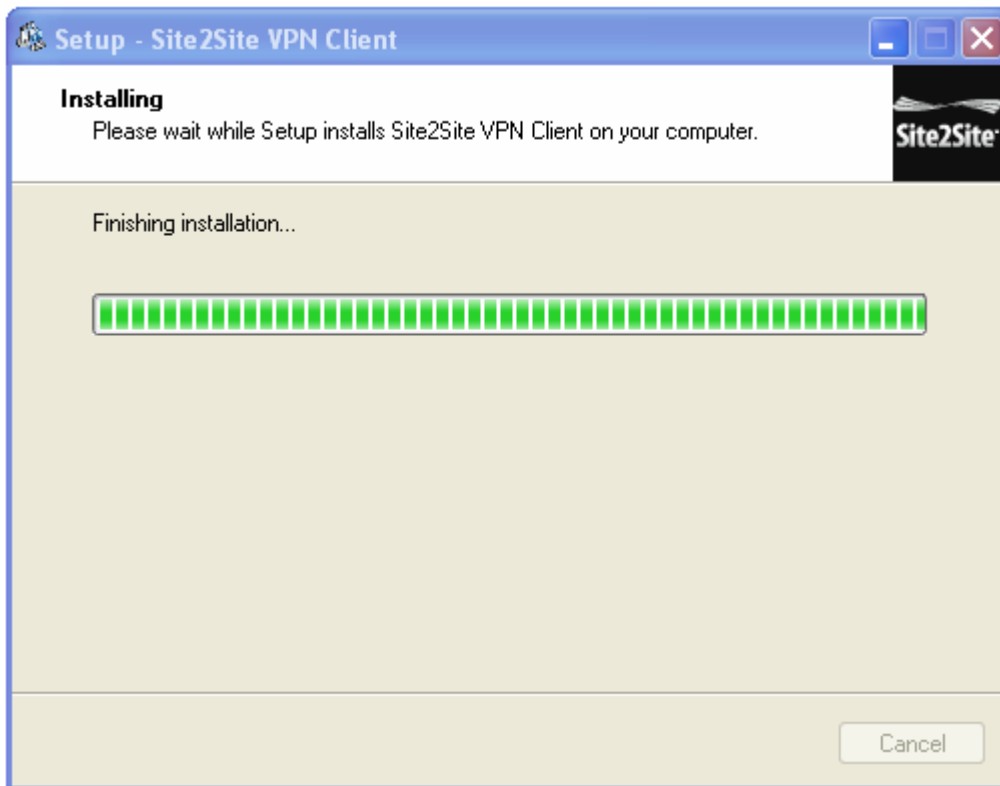
Add a desktop icon if you want to start the tunnel from the desktop, then click Next



Then click the Install button to begin the installation process.

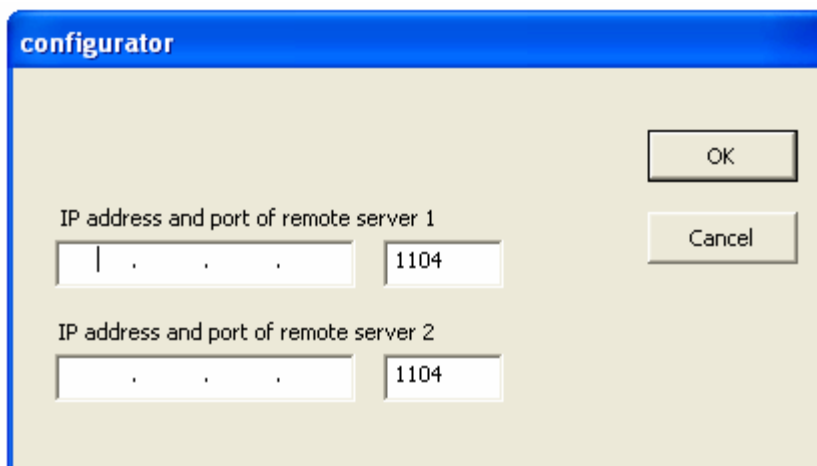


You will be prompted to install this driver, select 'Continue Anyway'

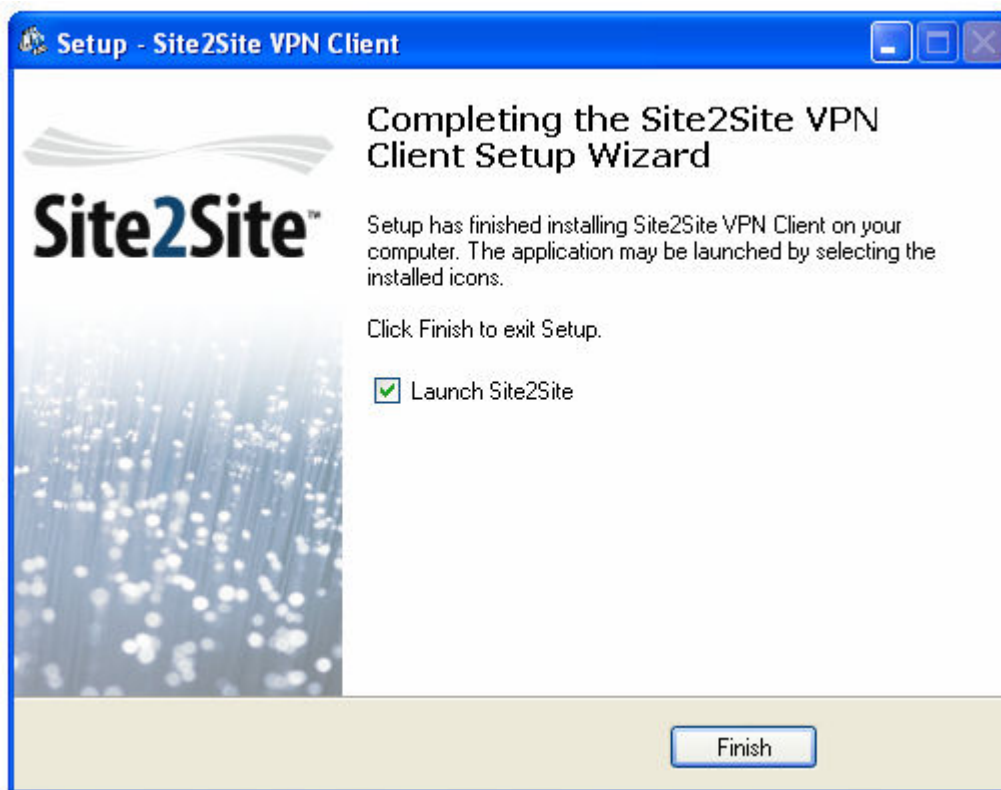


It will finish the installation process and then prompt you for the EdgeXOS contractors IP address, this is the WAN address of the remote EdgeXOS appliance.



Automated Failover Option: Our Site2Site clients are one of the few VPN clients today which provide automated failover capabilities for remote office connectivity. Unlike many IPsec based solutions, our simple remote client requires no dual SA setup, or other cumbersome configuration parameters. Simply enter the secondary WAN interface of the remote EdgeXOS appliance and you are ready to go with full resiliency.



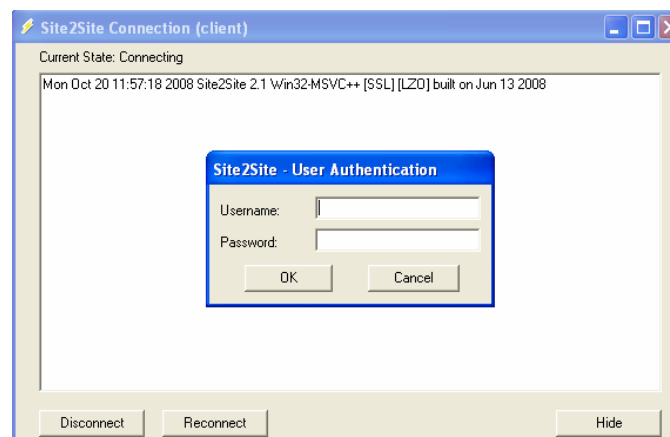
Enter the WAN1 and WAN2 addresses, along with the correct port (if not the default) and click the OK button.



The setup is now finished and you are ready to connect.

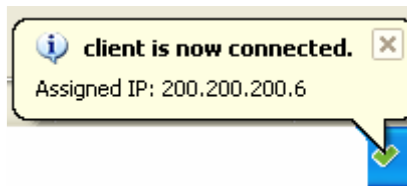
Once the client is installed it will display a small icon within the task bar. When the tunnel is down, it will appear as  when the tunnel is connected it will appear as .

To start the tunnel simply double-click the , which will open this screen:

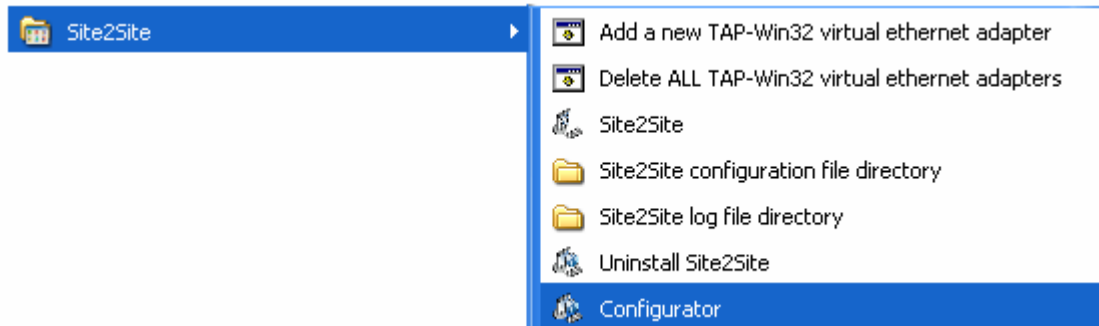


Enter a username and password added to the User/Device Management menu.

If the username and password are correct you will see the following:



If the username and password is not correct then you will be re-promoted for the correct username and password. If the connection fails because the address or port number for the remote EdgeXOS platform is incorrect then this can be changed by going to the Start Menu and selecting the Site2Site Configurator option:



NOTE TO MS VISTA USERS: You must first turn off Control Panel > User Account Control in order to disable window folder locking.

This will ask you to re-enter the IP address and port number to be used when connecting to the EdgeXOS platform.

Troubleshooting: Always make sure that you have the correct remote IP address (which is pingable), and the correct port number (must match the server side). Then check the username and password with the User Management and firewall rules. If problems persist, try disabling the firewall altogether and/or contract support.

NOTE: If you need to remove the Site2Site client, you can simply un-install the application by selecting the Uninstall Site2Site option via the Start menu.

