SonicWall® Directory Connector with SSO 4.1

Administration Guide

SONICWALL®

Contents

Part 1. Introduction

Part 2. Installation and Configuration

Part 3. Appendices

Part 1

Introduction

- About Directory Connector and this Guide
- Directory Connector and SSO Overview

1

About Directory Connector and this Guide

The *SonicWall® Directory Connector with SSO Administration Guide* provides information about installing and configuring the SonicWall Single Sign-On Agent and other elements of Directory Connector.

This section provides links to and a summary of the main sections in this guide.

Always check https://www.sonicwall.com/support/technical-documentation for the latest version of this manual as well as other SonicWall products and services documentation.

See the following sections for additional information:

Directory Connector and SSO Overview

This section provides an overview of Directory Connector and SSO. It includes an introduction to SSO, information about user identification methods, and platform compatibility information.

Installing Directory Connector and the SSO Agent

This section provides installation procedures for Directory Connector and the SSO Agent on Windows and Linux.

Viewing and Configuring SSO Agents

This section provides configuration procedures for the SSO Agent using the Directory Connector Configuration Tool.

Adding Firewalls, Servers and Remote Agents

This section provides configuration procedures for SonicWall network security appliances, remote SSO Agents, and servers including domain controllers, terminal servers, Exchange servers, and Novell eDirectory servers using the Directory Connector Configuration Tool.

Licensing Information

This section provides Open Source code information and the End User Product Agreement.

SonicWall Support

This section provides information about the support portal and contacting SonicWall Support.

2

Directory Connector and SSO Overview

This section provides an overview of SonicWall Directory Connector with SSO. It includes an introduction to Directory Connector and the SSO Agent, along with the supported user identification methods and platform compatibility.

Topics:

About Directory Connector

SonicWall Directory Connector with SSO provides the Configuration Tool as the administrative interface. It includes configuration screens for local and remote SonicWall Single Sign-On Agents (SSO Agents), SonicWall network security appliances, and the various types of servers that the SSO Agent needs to access. The SSO Agent provides centralized user identification to SonicWall network security appliances, interacting with the SonicOS and SonicOSX (SonicOS/X) Single Sign-On feature. Directory Connector provides integration with both Active Directory and Novell eDirectory for user identification.

The following SonicWall network security platforms support Directory Connector and the SSO Agent:

1. SonicWall NSv series, SuperMassive™ series, NSsp series, E-Class NSA series, NSA series, NSa series, TZ series, and SOHO series appliances are supported for transparent, automated Single-Sign-On integration with both Active Directory and Novell eDirectory.

   Refer to SonicWall Appliance/Firmware Compatibility on page 14 for more information.

2. SonicWall PRO and TZ 190/180 series appliances are supported for Single-Sign-On integration with Active Directory.

SonicOS/X and the SSO Agent can use Active Directory or Novell eDirectory to authenticate users and determine the filtering policies to assign to each user or user group. The SSO Agent identifies users by IP address and automatically determines when a user has logged out to prevent unauthorized access.

Along with the username information, the SSO Agent sends the following information to the appliance:

- The Domain Controller on which information about logged in users is found.
- The User Detection mechanism used by the Agent to find logged in users.

The SSO Agent can work both passively and actively. In the default configuration, both methods are used. In passive mode, SonicOS/X on the SonicWall network security appliance sends a request that contains an IP address to the SSO Agent. The SSO Agent identifies the username associated with the IP address and then sends the result back to SonicOS/X. In active mode, the SSO Agent attempts to detect user logon and logoff events and sends notifications to SonicOS/X.

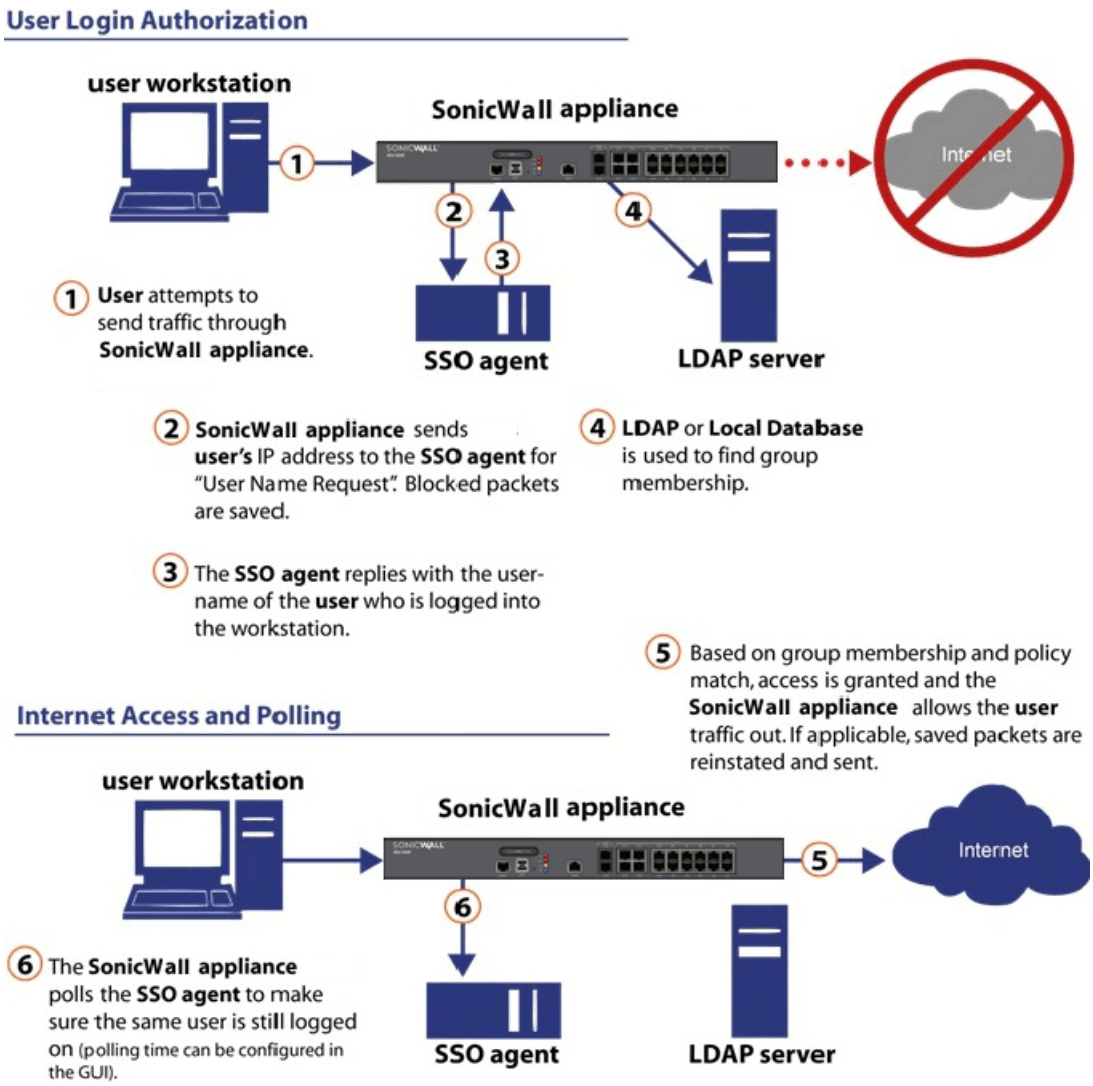
About Single Sign-On and the SSO Agent with Active Directory

Single Sign-On (SSO) is a transparent user-authentication mechanism that provides privileged access to multiple network resources with a single workstation login. SonicWall security appliances provide SSO functionality using the SonicWall Single Sign-On Agent (SSO Agent) to identify user activity based on workstation IP address.

SSO is configured in the **Users > Settings** page of the SonicOS/X management interface. SSO is separate from the authentication method for login settings that can be used at the same time for authentication of VPN/L2TP client users or administrative users.

The SonicWall SSO Agent identifies users by polling/monitoring the security log in an Active Directory server (the Domain Controller) and sends user login/logout notification to the appliance when it detects user login/logout. See the Identifying users diagram. Based on data from the SSO Agent, the SonicWall security appliance queries LDAP or the local database to determine group membership. Memberships are optionally checked by firewall policies to control who is given access, and can be used in selecting policies for Content Filtering and Application Control to control what they are allowed to access.

Identifying users



User names learned through SSO are reported in the SonicWall appliance logs of traffic and events from the users. The configured inactivity timer applies with SSO, but the session limit does not, though users who are logged out are automatically and transparently logged back in when they send further traffic.

Users logged into a workstation directly, but not logged into the domain, cannot be authenticated. For users that are not logged into the domain, an Authentication Required screen displays, indicating that a manual login is required for further authentication. If the workstation joins the Windows domain, the logged on user can be detected by WMI/NetAPI. The returned user name includes a Local: prefix. For example, Local:user01.

Users that are identified, but lack the group memberships required by the configured policy rules, are redirected to an Access Barred page.

About User Identification Methods

The SSO Agent supports the user identification methods described in the following sections:

About Client Probing

Client Probing includes both Windows Management Instrumentation (WMI) and NetAPI probing methods.

WMI is the infrastructure for management data and operations on Windows-based operating systems. The SSO Agent sends a WMI request to the client, and then determines the username and domain name by examining certain processes on the client machine.

NetAPI is another interface based on Windows DCE-RPC service. In this case, the SSO Agent sends a request that lists the users logged into the client workstation. This list includes interactive, service and batch log ons. The SSO Agent then determines the correct user name in this list. The NetAPI method is much faster than the WMI method, but might not always yield a correct username.

CAUTION: NetAPI has known security vulnerabilities on Windows and SonicWall does not recommend enabling it. If you do use it, create a dedicated account for it with the minimum necessary administrative privileges.

Windows Firewall might block both methods by default. To enable:

- WMI methods in the Windows Firewall, you can select *Windows Management Instrumentation* in the Control Panel > All Control Panel Items > Windows Firewall > Allowed Programs.
- The NetAPI method in Windows Firewall, you can select *File and Printer Sharing*.

Because the Windows API does not provide an interface to set the timeout for both probing methods, the default timeout is set to three seconds when the IP address is not accessible or when the connection is dropped by the Windows Firewall. The SSO Agent first creates a TCP connection to the target machine to check the connectivity. For WMI, the port is 445. For NetAPI, the port is 135. The default timeout is **3** seconds for both methods.

If a user logs onto a machine using a local account instead of a Windows domain account, the SSO Agent can only identify this user through a Client Probing method. This is because the other methods all involve Active Directory. When the administrator enables the *WMI/NetAPI Scanner* option in Directory Connector, the SSO Agent will repeatedly probe these IP addresses using Client Probing methods. The SSO Agent can detect when the user has logged off, and it sends a log off notification to SonicOS/X.

About Domain Controller Querying

The Domain Controller (DC) is a server that responds to security authentication requests (logging in, checking permissions, and so on), within the Windows Server domain. Two methods are supported that identify users who log on to the Windows domain. They are the DC Security Log and Server Session methods.

Topics:

About DC Security Logs

In Microsoft Windows, the Security Log contains records of log in and log out activity or other security-related events specified by the system's audit policy. When a domain user tries to log in to the domain network, the domain controller logs a message in the security log. The SSO Agent monitors event messages with specific Event IDs, and notifies SonicOS/X of the user information and logoff status.

Event ID 4661 is associated with user logoff. If this Event ID is not enabled in the DC group policy for some reason, the SSO Agent will not receive user logoff notifications via the DC Security Log method. In this case, the user cache refresh mechanism is used to determine user logoff upon expiration of the cache duration.

About Server Sessions

Any connection to a file or print service creates a “session” in the server’s session table. In the normal operation of an AD domain, users on Windows systems connect to the sysvol share on the domain controller to check for new Group Policy Objects every one to two hours. The user appears in the session table for about five minutes each time. Log out messages are sent to the firewall when the SSO Agent cannot find the user after two hours.

Usually, Server Sessions is a more efficient method than DC Security logs, but sometimes, Server Sessions is not as accurate. In multiple domain environments, incorrect domain names might be reported. If the user switches between two logged on usernames, the SSO Agent cannot detect it.

About Enabling Audit Logs in DC Policy

Audit Logon is disabled by default in Windows Server. Steps to enable Audit Logon are provided in the following sections:

About Using Non-Admin Accounts to Access the DC Security Logs for SSO

SSO Agent service users do not have to be domain administrators. You can also use a normal domain user with some additional permissions granted, for access. For more information, refer to the following knowledge base article: https://www.sonicwall.com/en-us/support/knowledge-base/171004124849942.

About Terminal Servers

Terminal Server IP Virtualization is supported beginning in SonicWall Directory Connector with SSO 4.1. This feature provides an alternative method of identifying users logged into Terminal Servers which is expected to replace the SonicWall Terminal Server Agent in future releases.

It is supported on Windows Server 2008 R2 and higher, and is based on Remote Desktop IP Virtualization technology by Microsoft. Remote Desktop IP Virtualization allows IP addresses to be assigned to remote desktop connections on a per session or per program basis. This can be useful if a program communicates with a server that only allows one connection per IP address. Prior to Windows Server 2008 R2, every session on a Remote Desktop Session Host server was assigned the same IP address. With Windows Server 2008 R2, Remote Desktop IP Virtualization provides a way to assign IP addresses on a per session or per program basis. If IP addresses are assigned for multiple programs, they will share a per session IP address. If there is more than one network adapter on the server, one must be designated for Remote Desktop IP Virtualization.

The SonicOS/X user authentication module uses this feature to accomplish the same functionality as the SonicWall Terminal Server Agent (TSA), from within the SonicWall SSO Agent. Once a user logs into the terminal server with an RDP session, the Windows Server assigns a unique IP address to the session and logs an application event in the Windows event log. The SSO Agent reads the log remotely and notifies the firewall, allowing the user to be identified by SonicOS/X.

IP Virtualization is disabled by default in Windows Server. Steps to enable IP Virtualization are provided in the following sections:

- Enabling IP Virtualization in Windows Server 2008 R2 on page 66
- Enabling IP Virtualization in Windows Server 2012 on page 68

About Exchange Servers

When a user logs on to a computer that is not in the domain, the DC server does not have the user and IP address information. Typically, this is handled by the Client Probing method. You can also use the Exchange Server to identify the user.

This works only as a supplement to the Domain Security Log method. Although it works for machines not joined to a domain, it only works if users use Microsoft Outlook after logging in.

If the user opens Outlook to send or receive mail using a domain user name and credentials, both the DC and Exchange Server log events for this activity. On the DC, the event is logged, but the IP address given is not the real source. Instead, it points to the Exchange Server. On the Exchange server, a security log entry is made that contains both the user name and the source IP address. Each time Outlook receives email; there is also an event recorded by the Exchange server. The SSO Agent can monitor these events in the Exchange security log.

About Novell eDirectory

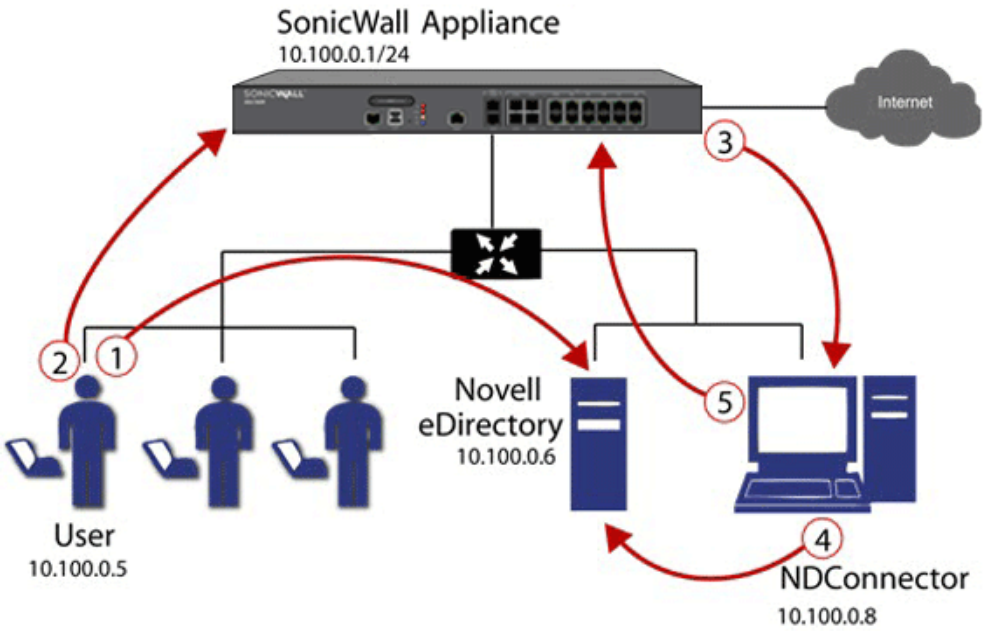
Novell eDirectory (formerly known as Novell Directory Services (NDS), sometimes referred to as NetWare Directory Services) is an X.500-compatible directory service software product initially released in 1993 by Novell

for centrally managing access to resources on multiple servers and computers within a given network. eDirectory is a hierarchical, object oriented database used to represent certain assets in an organization in a logical tree, including organizations, organizational units, people, positions, servers, volumes, workstations, applications, printers, services, and groups.

When a user logs on to an eDirectory network, the user's IP address is added to the networkAddress field in the user's record. If the user logs on to the eDirectory network multiple times from different machines, there will be multiple networkAddress fields. If the user logs off the eDirectory network properly, the corresponding networkAddress field is removed immediately. Otherwise the field is kept for some time before it is removed.

For this user identification method, the SSO Agent repeatedly queries the eDirectory using the LDAP protocol; see User identification with eDirectory.

User identification with eDirectory



The sequence of events shown in User identification with eDirectory is:

1 The user logs into the network and authenticates with eDirectory.

2 The user initiates a request for an Internet resource (such as a Web page, an audio or video stream, or a chat program). The SonicWall network security appliance detects the request.

3 The SonicWall appliance queries the SSO Agent.

4 The SSO Agent queries the eDirectory server about the user.

The SSO Agent communicates the user's content filtering policies to the SonicWall appliance, based on the user's individually assigned policies and any policies inherited from groups and from organizational units. The SonicWall appliance allows, logs, or blocks the user's request, based on the user's content filtering policies.

About Using Samba on Linux/UNIX Clients

Samba 3.0 or newer can be installed on Linux/UNIX clients for use with SonicWall SSO Agent running on a Windows Server machine. However, the SonicWall SSO Agent running on a Linux machine is supported in SonicWall Directory Connector with SSO 4.1.6 and higher, and provides a better interface for Linux clients.

Samba is a software package used on Linux/UNIX machines to give them access to resources in a Windows domain (by way of Samba's *smbclient* utility). A user working on a Linux PC with Samba in a Windows domain can be identified through SSO, but it requires proper configuration of the Linux PC, and possibly some reconfiguration of the appliance, as described in the *Using Single Sign-On with Samba* technote.

The NetAPI, WMI, and DC Security Log authentication methods used by the SSO Agent all depend on Samba, and most Linux distributions support Samba natively. However, without Samba, Linux PCs would normally not work with NetAPI or WMI client probing methods. Linux users can still get access, but they need to log in to do so. They can be redirected to the login prompt if policy rules are set to require authentication.

In SonicWall Directory Connector with SSO version 4.1 and higher, the elements of Samba are packaged into the installation folder. Thus, even if Samba is not installed on a Linux PC, NetAPI, WMI, and DC Security Log methods will still work to authenticate Linux users with the 4.1 SSO Agent.

About NetBIOS Name Support

Windows provides support for applications that use the NetBIOS networking APIs and the flat NetBIOS names. This allows identification of Windows domains for computers that are running Windows. A fully qualified domain name (FQDN), sometimes also referred to as an absolute domain name, is a domain name that specifies its exact location in the tree hierarchy of the Domain Name System (DNS). It specifies all domain levels, including the top-level domain and the root zone.

Both the NetBIOS name and the FQDN domain name can be found through an LDAP search. The SSO Agent connects to the DC using these service credentials and completes the LDAP search.

The SSO Agent remembers these names and sends the correct domain name to the firewall according to the administrator's configuration of the SSO Agent. By default, it sends the NetBIOS name.

Platform Compatibility

To use SonicWall Single Sign-On, it is required that the SSO Agent be installed on a server that can communicate with the Active Directory or eDirectory server and with clients and the SonicWall security appliance directly using the IP address or using a path, such as VPN. The following requirements must be met in order to run the SSO Agent:

- Port 2258 must be open; the firewall uses UDP port 2258 by default to communicate with the SSO Agent; if a custom port is configured instead of 2258, then this requirement applies to the custom port
- Windows Server, with latest service pack
- .NET Framework 4.5 or above
- NetAPI or WMI (unless using DC Windows Security Log as the Client Probing Method)
- The SSO Agent must run under Domain Admin privileges

SonicWall Directory Connector with SSO and the SSO Agent runs as either a 32-bit or 64-bit application. This improves the performance of 64-bit agent machines, especially in cases where the agent is set to use NetAPI or WMI as the Client Probing Method.

Topics:

SSO Agent Platform Compatibility

NOTE: For best performance, SonicWall recommends installing the SSO Agent on a dedicated system.

Supported Windows Platforms

SonicWall Directory Connector with SSO is supported for installation on 32-bit and 64-bit Windows systems running the following operating systems:

- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2
- Windows Server 2008

On all Windows 32-bit and 64-bit servers, a .NET Framework must be installed. The following version of.NET Framework is supported:

- .NET Framework 4.5

Supported Linux Platforms

On Linux, SonicWall Directory Connector with SSO 4.1 software is supported for installation on 64-bit platforms running the following operating systems:

- CentOS 7
- CentOS 6
- Ubuntu 16.04
- Ubuntu 14.04
- Redhat 7
- Redhat 6

Virtual Environment Compatibility

Recommended Virtual Environments for Directory Connector include:

- VMware ESX 6.7
- VMware ESX 6.5
- VMware ESX 6.0

- VMware ESX 5.x
- VMware ESX 4.x
- Microsoft Hyper-V on Windows Server 2016
- Microsoft Hyper-V on Windows Server 2012 R2
- Microsoft Hyper-V on Windows Server 2008 R2

Virtual Machine host configuration requirements:

- OS - Windows Server 2008 / 2008R2 / 2012 / 2012R2 / 2016 — 32-bit/64-bit
- CPU – Intel Xenon (4 processors)
- Memory - 4GB

SonicWall Appliance/Firmware Compatibility

SonicWall Directory Connector with SSO is a supported release for use with the following SonicWall platforms:

- NSv all platforms running SonicOS Virtual 6.5.4 and above
- NS*v* all platforms running SonicOSX 7.0.0 and above
- SuperMassive 9200 / 9400 / 9600 running SonicOS 6.1 and above
- SuperMassive 9800 running SonicOS 6.2.7.7 and above
- SuperMassive E10200 / E10400 / E10800 running SonicOS 6.0.x
- NSsp 15700 running SonicOSX 7.0.0 and above
- NSsp 12400 / 12800 running SonicOS 6.4
- NSa 2700 and other x700 models running SonicOS/X 7.0.0 and above
- NSa 2650 running SonicOS 6.5 and above
- NSa 2600 / 3600 / 4600 / 5600 / 6600 running SonicOS 6.1 and above
- NSA E-Class E5500 / E6500 / E7500 / E8500 / E8510 running SonicOS 5.0 and above
- NSA 240 / 2400 / 3500 / 4500 / 5000 running SonicOS 5.0 and above
- NSA 220 / 220W / 250M / 250MW running SonicOS 5.8.1 and above
- SOHO running SonicOS 5.9.1.3 and above
- SOHO W running SonicOS 6.2.4.0 and above
- SOHO 250 / SOHO 250W running SonicOS 6.5.4 and above
- TZ670, TZ570/570W/570P, TZ470/470W, TZ370/370W, TZ270/270W running SonicOS/X 7.0.0 and above
- TZ600P / TZ300P / TZ350 / TZ350W running SonicOS 6.5.4 and above
- TZ600 / TZ500 / TZ400 / TZ300 running SonicOS 6.2.3.1 and above
- TZ500W / TZ400W / TZ300W running SonicOS 6.2.4.0 and above
- TZ 215 / 215W / 205 / 205W / 105 / 105W running SonicOS 5.8.1 and above
- TZ 210 / 210W / 200 / 200W / 100 / 100W running SonicOS 5.0 and above
- TZ 190 / 190W / 180 / 180W running SonicOS 4.0 and above
- PRO 2040 / 3060 / 4060 / 4100 / 5060 running SonicOS 4.0 and above

NOTE: SonicOS 5.5 or newer is required for Novell eDirectory Support.

NOTE: SSO Agent performance is sensitive to the round trip network time during frequent information exchanges with the network security appliance. The Agent machine should be as close as possible to the appliance for a recommended round-trip time of less than 1 ms.

Exchange Server Compatibility

SonicWall Directory Connector with SSO is supported for use with the following exchange servers:

- Exchange server 2016
- Exchange server 2013
- Exchange server 2010

Domain Controller Server Compatibility

SonicWall Directory Connector with SSO is supported for use with Domain Controllers running the following operating systems:

- Windows Server 2019 – 64-bit
- Windows Server 2016 – 64-bit
- Windows Server 2012 – 64-bit
- Windows Server 2012 R2 – 64-bit
- Windows Server 2008 R2 – 64-bit

It is recommended to run the SSO Agent service using a domain administrator account. An account with fewer permissions, such as a domain user account, does have sufficient privileges for all service components to interact with the Domain Controller.

Novell eDirectory Server Compatibility

SonicWall Directory Connector with SSO is supported for use with the following Novell eDirectory versions:

- Novell eDirectory 9.1 – 64-bit
- Novell eDirectory 8.8 – 64-bit

Terminal Server Compatibility

SonicWall Directory Connector with SSO version 4.1.6 and higher software is supported for use with the following platforms configured as Terminal Servers:

- Windows Server 2012 R2 – 64-bit
- Windows Server 2012 – 64-bit
- Windows Server 2008 R2 – 64-bit

Client Compatibility

Directory Connector is compatible with the following client operating systems for the purpose of determining the logged in user name and other information necessary for user authentication:

- Windows 10 – 32/64-bit
- Windows 8 – 32/64-bit
- Windows 7 – 32/64-bit

Part 2

Installation and Configuration

- Installing Directory Connector and the SSO Agent
- Viewing and Configuring SSO Agents
- Adding Firewalls, Servers and Remote Agents

3

Installing Directory Connector and the SSO Agent

This section provides information about installing Directory Connector and the SSO Agent.

Install the SonicWall SSO Agent on a host on your network that has access to the authentication server such as Active Directory, the SonicWall network security appliance, and all client workstations.

NOTE: For best performance, SonicWall recommends installing the SSO Agent on a dedicated system.

When using NetAPI or WMI, one SSO Agent can support up to approximately 2500 users, depending on the performance level of the hardware that it is running on, how it is configured on the firewall and other network-dependent factors. When configured to read from domain controller security logs, one SSO Agent can support a much larger number of users identified via that mechanism, potentially 50,000+ users depending on similar factors.

Topics

Installing the SSO Agent on Linux

The Linux SSO Agent installer package is available in two types, both requiring root permission to install:

- SSOAgent-4.1.x.deb – the DEBIAN installer
- SSOAgent-4.1.x.rpm – the RPM installer

Note that “4.1.x” represents the actual version of the software, such as “4.1.17”.

For the list of Linux platforms that are compatible with the SSO Agent, see Supported Linux Platforms on page 13.

Topics:

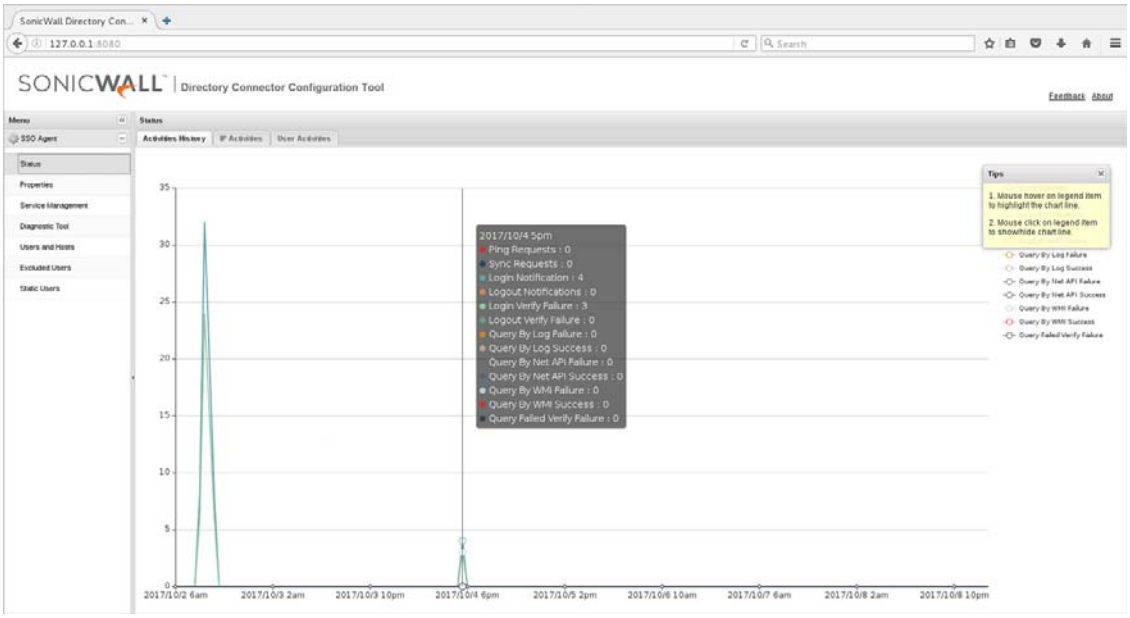
Installing the Linux SSO Agent

To install SonicWall Directory Connector with SSO on a Linux machine:

1 Download the appropriate installer for your version of Linux and place it into `/usr/local/bin` or another directory of your choice.

2 From the command line, execute the appropriate command to perform the installation, such as: `sudo dpkg -i /usr/local/bin/SSOAgent-4.1.x.deb` on Ubuntu.

Once the installation completes and the service daemon is started, you can connect to the Directory Connector Configuration Tool (the web based interface), by pointing your browser to: `http://127.0.0.1:8080`



By default, the web management interface can only be accessed locally.

Installed Files on Linux

Topics:

Program Files

The installer places all the program files into `/opt/ssoagent/` by default, and starts a service daemon `ssoagentd`. The following files are placed in `/opt/ssoagent/`:

- `config.xml` is the main configuration file.
- `chroot\*` are all the dependency `so` files.
- `chroot-wmi\*` are all the dependency `so` files for WMI.
- `HttpRequest.py` is a tool to send HTTP requests by the SSO Agent.

- `Plugins\libSSOAgent.so` is a part of the service program.
- `ssoagentd` is the service daemon startup script.
- `SSOAgentService` is the service program.
- `SSOAPI` is a tool program.
- `version` is a text file that contains the version of the SSO Agent.
- `webui\*` are resources needed by the SonicWall Directory Connector with SSO user interface.
- `webui\SSOHttpServer.py` is a simple HTTP server by Python.
- `WMIDCIpQuery` is a command line to get the domain controller IP address when given the IP address of a machine in the domain.
- `WMIDCValidateQuery` is a command line tool to verify user name and password on the domain controller.
- `WMIGroupPolicyIdQuery` is a command line tool to get the default group policy ID of the domain controller.
- `WMIRemoteOSVersionQuery` is a command line tool to get a remote machine's OS version.
- `WMIUserQuery` is a command line tool to send a WMI query to an IP address.
- `WMIValidateGroupPolicyQuery` is a command line tool to check whether the specified group policy is defined and which value is set.

Log Files

The log files can be found in the `/opt/ssoagent/log` folder. The files stored in the `log` folder include:

- `SSOAgentService.log`
- `SSOAgent.log`
- `SSOPacket.log`
- `Rpc.log`
- `SessionTable.log`
- `SecurityEvent.log`

Several CSV files are also stored in the `log` folder. These files contain statistics information displayed in the **Status** page of the SSO agent user interface. The files are updated every 30 minutes.

- `IpStatistics.csv` – stores information displayed in **IP Activities** screen
- `UserStatistics.csv` – stores information displayed in **User Activities** screen
- `UTMStatistics.csv` – stores information displayed in **Activities History** screen

Installing the SSO Agent on Windows

To run the SSO Agent on a Windows machine, .NET Framework v4.5 must be installed. If it is not installed, an error message appears.

For the list of Windows platforms that are compatible for running the SSO Agent, see Supported Windows Platforms on page 13.

Topics:

Installing the Windows SSO Agent

To install the SonicWall SSO Agent on Windows, for use with Active Directory:

1 Download one of the following installers, depending on your computer:

For 32-bit:

- `SSOInstaller.4.1.17.x86.msi`

For 64-bit:

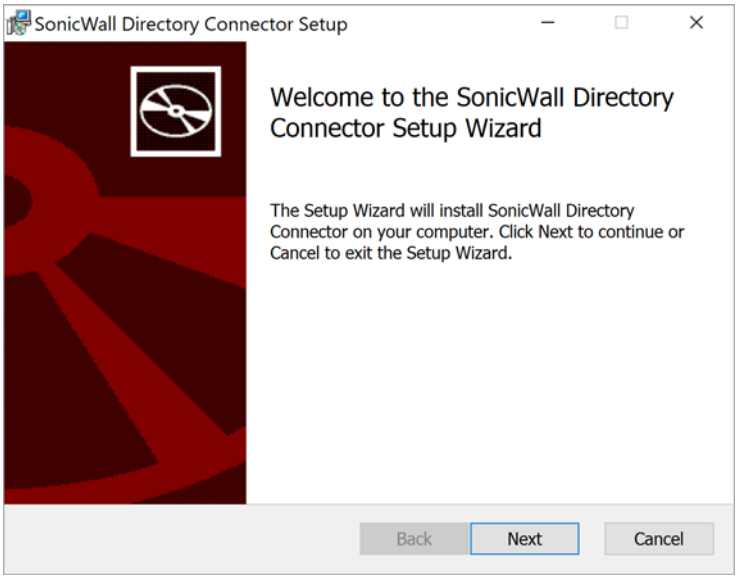
- `SSOInstaller.4.1.17.x64.msi`

You can find these on https://www.mysonicwall.com under **Directory Connector**. The installer is an MSI file signed by SonicWall Inc.

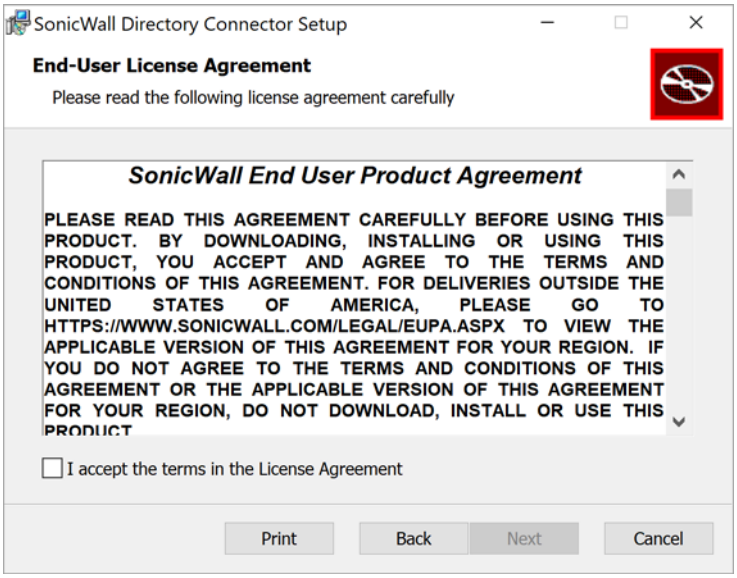
2 To begin installation, double-click the installer.

The installer automatically uninstalls any previous version of the SSO Agent.

3 In the **Welcome** screen, click **Next** to continue the installation.



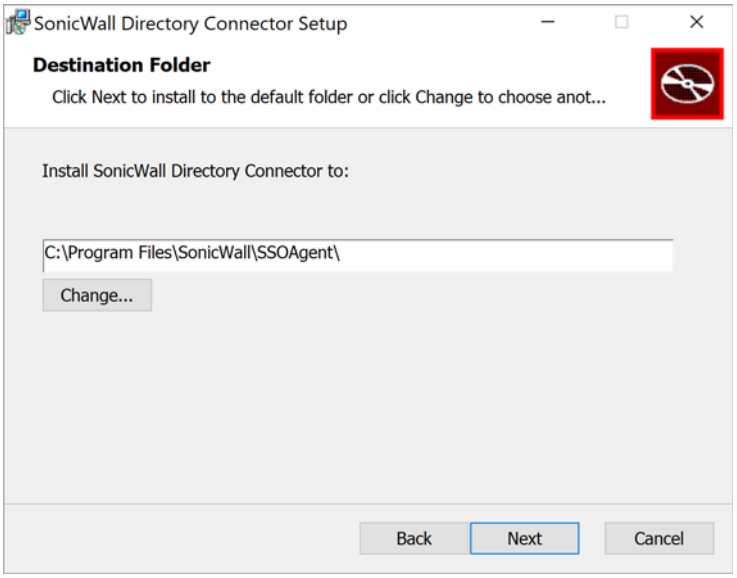
The **License Agreement** screen displays.



4 Accept the terms of the license agreement, and then click **Next**.

TIP: To print a copy of this agreement, click **Print**.

The **Destination Folder** screen displays.

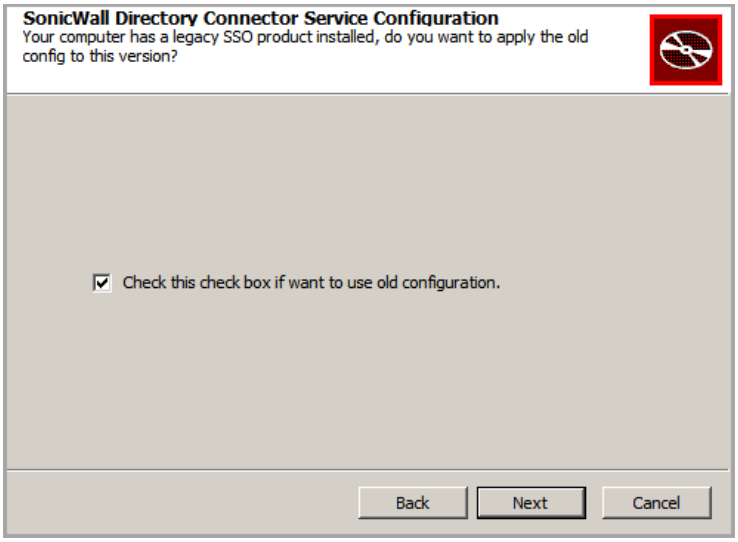


5 Select the destination folder:

- To use the default folder, `C:\Program Files\SonicWall\SSOAgent\`, click **Next**.
- To specify a custom location, click **Change**, select the folder, and then click **Next**.

What displays next, depends on whether this is a new installation or an upgrade:

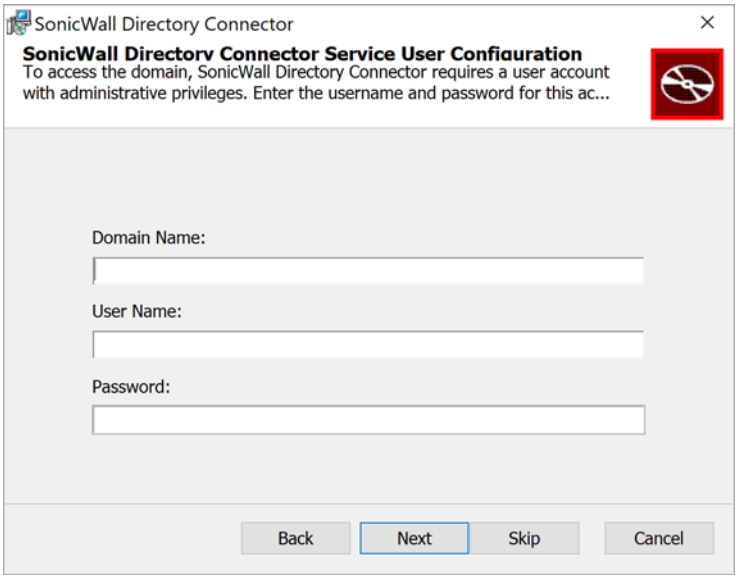
- For new installations, the **Service User Configuration** screen displays. Go to Step 7.
- If your system has an older version of Directory Connector, a **Service Configuration** screen displays asking if you want to use the existing configuration. The **Check this check box if want to use old configuration** checkbox is selected by default.



6 Do one of the following:

- To use the old configuration, click **Next**. The **Service User Configuration** screen displays. Go to Step 7.
- To reconfigure SonicWall Directory Connector with SSO, clear **Check this check box if want to use old configuration** and then click **Next**.

7 Use the **Service User Configuration** screen to configure a common service account that the SSO Agent will use to log into a specified Windows domain.



TIP: This section can be configured at a later time. To skip this step and configure it later, click **Skip**. Go to Step 8.

a Enter the domain name of the account in the **Domain Name** field.

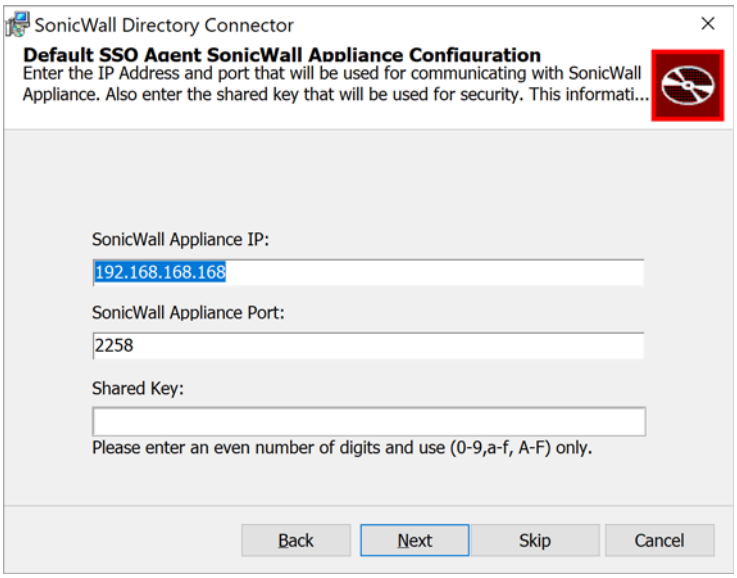
b Enter the username of an account with administrative privileges in the **Username** field.

c Enter the password for the account in the **Password** field.

d Click **Next**.

The **Appliance Configuration** screen displays.

8 Use the **Appliance Configuration** screen to configure the IP address and port used for communication with the firewall.



TIP: This section can be configured at a later time. To skip this step and configure it later, click **Skip**. Go to Step 9.

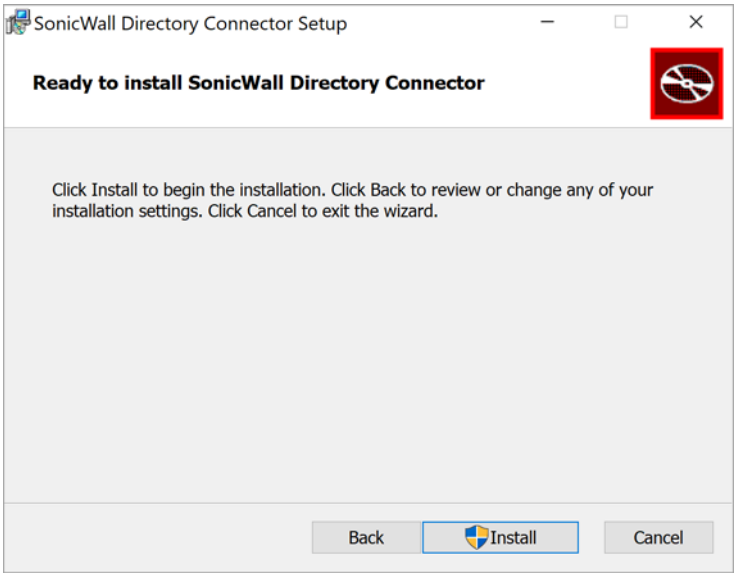
a Enter the IP address of your SonicWall security appliance in the **SonicWall Appliance IP** field. The default is 192.168.168.168, which is the default X0 IP address.

b Type the port number for the same appliance into the **SonicWall Appliance Port** field. The default port number is **2258**.

c Enter the hexadecimal representation (an even number of digits using only hexadecimal numbers) of the shared key in the **Shared Key** field.

d Click **Next**.

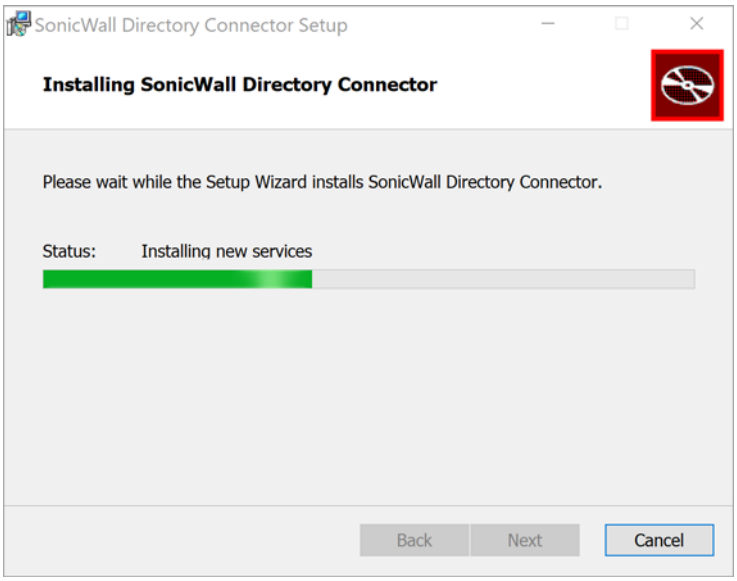
The **Install** screen displays.



9 Click **Install** to begin the installation. A warning screen requesting permission to install files may display; if so, click **Yes**.

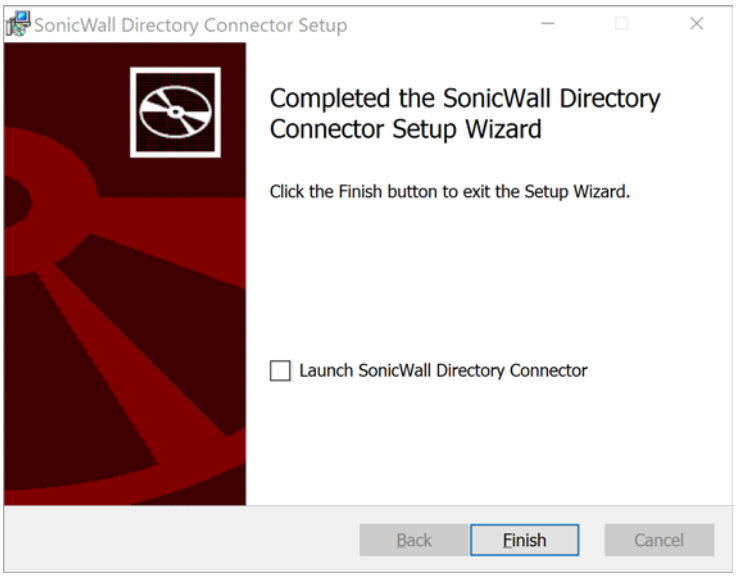
10 An **Installing** progress screen displays. Wait for the installation to complete.

The status bar displays while the SonicWall SSO Agent installs.



Program and service files are installed, including the *SSOAgentService*. The installer starts the newly installed service automatically.

A **Completed** screen displays.



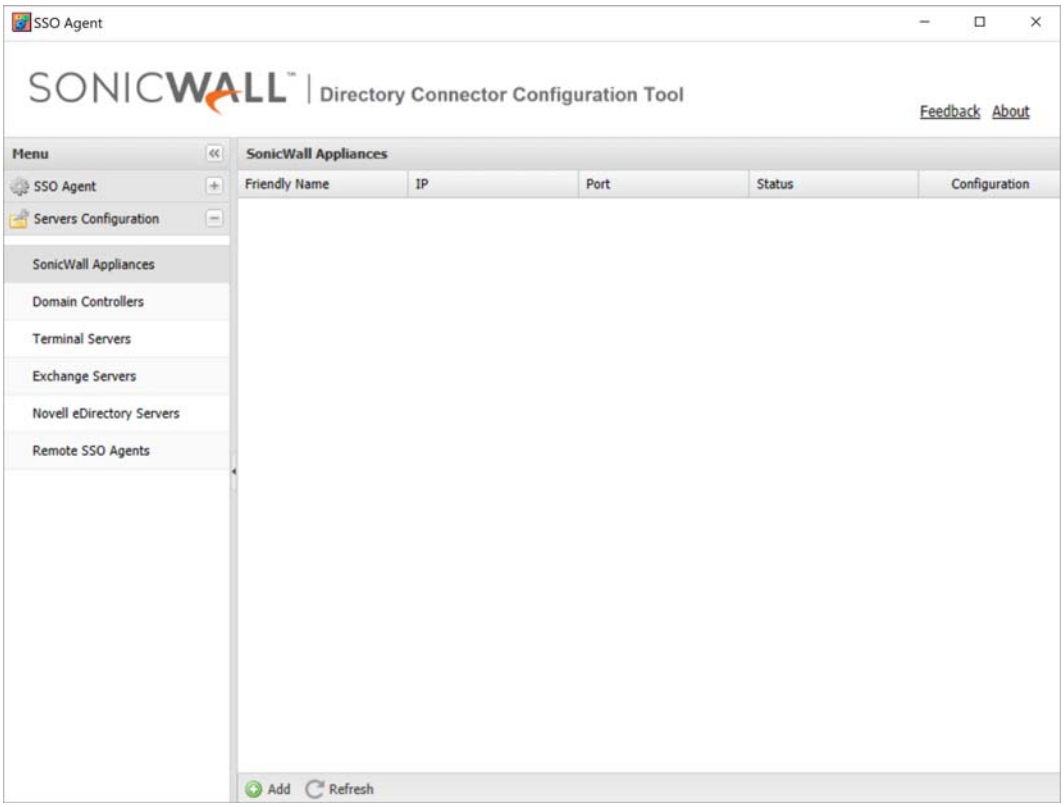
IMPORTANT: To run the SSO Agent, .NET Framework v4.5 must be installed. If it is not installed, an error message appears.

11 When the installation is complete, optionally select the **Launch SonicWall Directory Connector** checkbox to launch the SonicWall Directory Connector Configuration Tool. This option is not selected by default.

12 Click **Finish**. A warning screen requesting permission to make changes to the computer may display; if so, click **Yes**.

The installer creates a desktop shortcut for the SonicWall Directory Connector Configuration Tool.

If you selected the **Launch SonicWall Directory Connector** checkbox, the Directory Connector Configuration Tool displays.



Installed Files on Windows

Topics:

Program Files

The installer places all the program files into `C:\Program Files\SonicWall\SSOAgent` or `C:\Program Files (x86)\SonicWall\SSOAgent` by default:

- `SSOAgentService.exe` is the service program.
- `SSOAgentWindowsUI.exe` is the configuration user interface program.

- `SSOAgentWindowsUI.exe.config` is an XML file that specifies the Windows service port and the path to the web UI resource files.
- `SSOAPI.exe` is a command line tool program.
- `Plugins\SSOAgent.dll` is a part of the service program.
- `webui\*` are resources needed by the SonicWall Directory Connector with SSO user interface.

The following data files are placed into `C:\ProgramData\SonicWall\SSOAgent`:

- `config.xml` is the main configuration file.

  NOTE: In Directory Connector/SSO 4.1.17, the location for config.xml is changed from `C:\Program Files\SonicWall\SSOAgent` to `C:\ProgramData\SonicWall\SSOAgent`.

  If you are upgrading from a previous version, you can use “Run as different user” or “Run as administrator” to ensure that the installer migrates the existing `config.xml` into the new location.

  1 Download installer MSI file.
  2 Hold the Shift key while right-clicking on the installer MSI.
  3 Click on “Run as different user” or “Run as administrator”.
  4 A Windows Security prompt appears. Enter the credentials for an administrative user.

- `static.csv` is used for persistence of static users imported from a local file or added via the Directory Connector Configuration Tool. This feature is also used for automation load testing.
- `Users.xml` is the user list that is saved during service restart.

The installer also creates short cuts in the Start menu and on the desktop.

Log Files

Log files and crash dump files are placed in `C:\ProgramData\SonicWall\SSOAgent\log`. The files stored in the `log` folder include:

- `SSOAgentService.log`
- `SSOAgent.log`
- `SSOPacket.log`
- `Rpc.log`
- `SessionTable.log`
- `SecurityEvent.log`

Several CSV files are also stored in the `log` folder. These files contain statistics information displayed in the **Status** page of the SSO agent user interface. The files are updated every 30 minutes.

- `IpStatistics.csv` – stores information displayed in **IP Activities** screen
- `UserStatistics.csv` – stores information displayed in **User Activities** screen
- `UTMStatistics.csv` – stores information displayed in **Activities History** screen

Using the Feedback and About Options

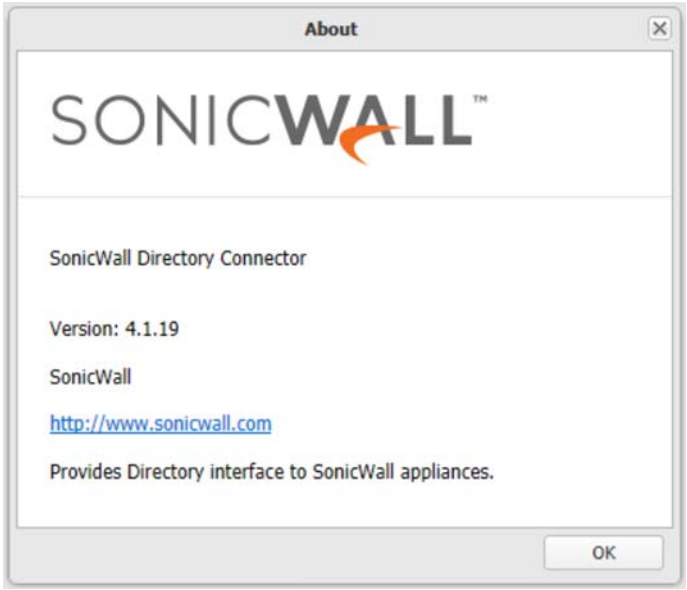
The top banner of the Directory Connector Configuration Tool has two options:

- **Feedback**

  Click **Feedback** to display a popup window in which you can enter feedback about Directory Connector and the SSO Agent and send it to the Support team. Fill in the **Subject**, **Email Address** (your email address), **Name** (your name), and **Comment** fields, and then click **Submit**.

- **About**

  Click **About** to display a popup dialog with the installed version number of Directory Connector and the SSO Agent.



4

Viewing and Configuring SSO Agents

This section provides information about using the Directory Connector Configuration Tool to view and configure an SSO Agent, including the status dashboard, properties and settings, service logon credentials, static users, and excluded users. The Users and Hosts status page and diagnostic tools are also described.

Topics

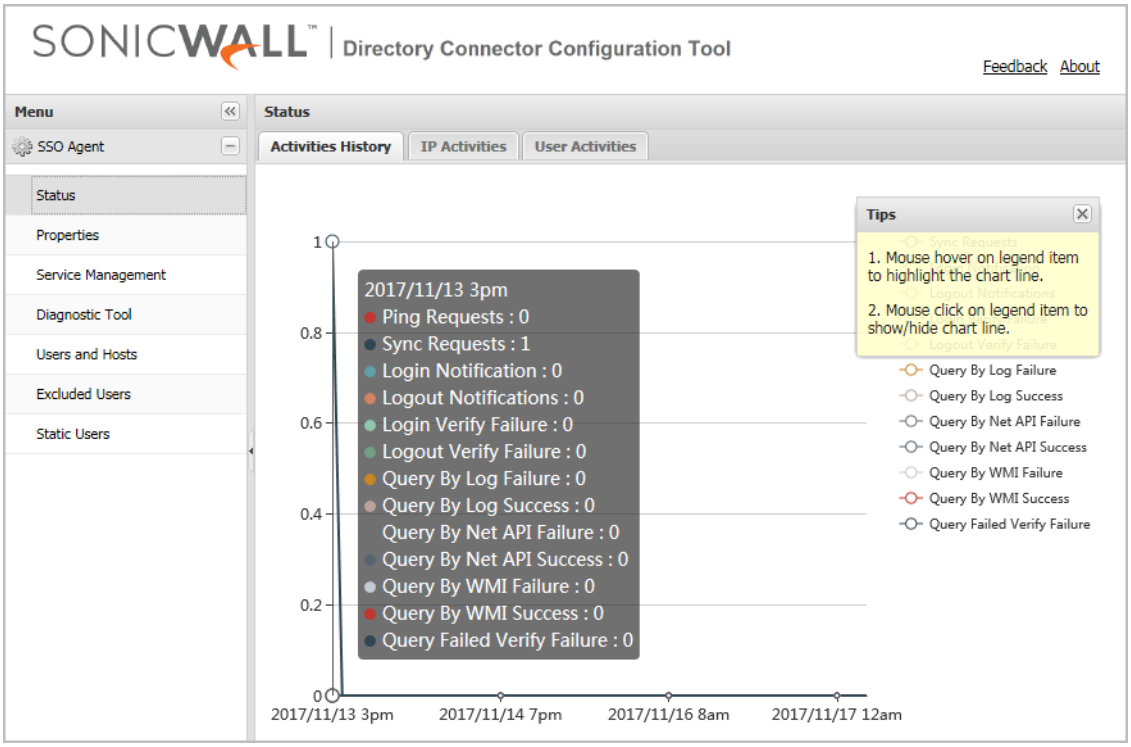
Viewing the SSO Agent Status Page

The **Status** page of the SSO Agent user interface displays a dashboard with a graph of the activities over the past seven days. You can view the full activities history, per-IP activities, and per-user activities in different tabs. A list of statistics is also displayed on the dashboard. You can click the legend to show or hide a particular counter, and click the column header to sort the result.

To view the Status page:

1 Launch the Directory Connector Configuration Tool:
   - On Windows, either from the Start menu or by double-clicking the desktop shortcut
   - On Linux, by pointing your browser to `http://127.0.0.1:8080`

2 Under **SSO Agent** in the left pane, click **Status** to display the dashboard and information in the right pane.



3 On the **Activities History** tab:

- Hover your mouse pointer anywhere on the chart to display the related list of statistics.
- Hover your mouse pointer on an item in the legend to highlight the related event line in the chart.
- Click on the item in the legend to show or hide the associated chart line.

4 Click the **IP Activities** tab to display a table with the following information for each IP address being tracked by the SSO Agent:

- **IP** – the IP address of the user's workstation or terminal server session
- **WMI** – Windows Management Instrumentation information for the IP address
- **NetAPI** – Windows networking API information for the IP address
- **DC Log** – Domain Controller event log information from the **DC Security Log Subscription** server monitoring method for the IP address
- **Exchange Log** – Exchange server log event information from the **Event Subscription** server monitoring method for the IP address
- **Polling DC Log** – information about the IP address obtained by polling the Domain Controller log
- **Polling Exchange Log** – information about the IP address obtained by polling the Exchange server log
- **Polling DC Session** – information about the IP address obtained by polling the Domain Controller's session table
- **Polling EDirectory** – information about the IP address obtained by polling the Novell eDirectory server

5 Click the **User Activities** tab to display a table with the following information for each user being tracked by the SSO Agent:

- **User Name** – the user name

- **WMI** – Windows Management Instrumentation information for the user
- **NetAPI** – Windows networking API information for the user
- **DC Log** – Domain Controller event log information from the **DC Security Log Subscription** server monitoring method for the user
- **Exchange Log** – Exchange server log information from the **Event Subscription** server monitoring method for the user
- **Polling DC Log** – information about the user obtained by polling the Domain Controller log
- **Polling Exchange Log** – information about the user obtained by polling the Exchange server log
- **Polling DC Session** – information about the user obtained by polling the Domain Controller's session table
- **Polling EDirectory** – information about the user obtained by polling the Novell eDirectory server
- **IPs** – the IP address of the user's workstation or terminal server session

Configuring SSO Agent Properties

The SonicWall SSO Agent communicates with workstations using NetAPI or WMI, which both provide information about users logged into a workstation, including domain users, local users, and Windows services. Be sure that WMI or NetAPI is installed prior to configuring the SonicWall SSO Agent.

NOTE: When using Single Sign-on, the Windows SSO Agent tries to identify the logged in user by querying the workstations using the NetAPI or WMI protocols. NetAPI and WMI require *File & print sharing* enabled on the client workstations.

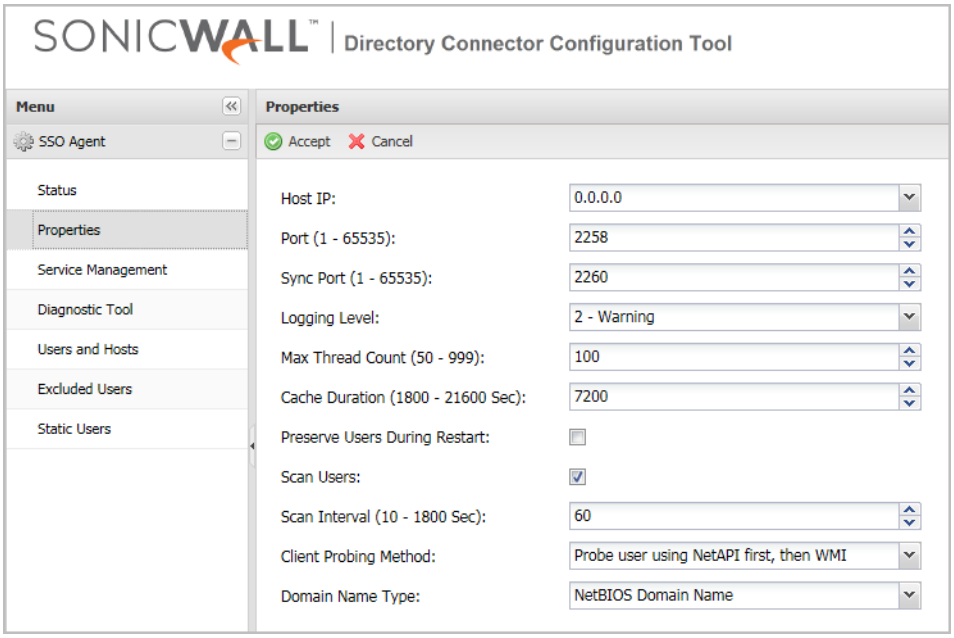
CAUTION: **NetAPI has known security vulnerabilities on Windows and SonicWall does not recommend enabling it. If you do use it, create a dedicated account for it with the minimum necessary administrative privileges.**
Refer to Creating a Dedicated Domain User with Minimum Privileges for SSO Agent on page 49.

NOTE: The Configuration Tool communicates with the SSO Agent service through JSON RPC. The RPC port is `127.0.0.1:12348`. If the service is stopped, the Configuration Tool tries to start the service first.

To configure the properties of the SonicWall SSO Agent:

1 Launch the Directory Connector Configuration Tool:
   - On Windows, either from the Start menu or by double-clicking the desktop shortcut
   - On Linux, by pointing your browser to `http://127.0.0.1:8080`

2 Under **SSO Agent** in the left pane, click **Properties** to display the configuration fields in the right pane.



3 For **Host IP**, select an IP address from the drop-down menu. The default IP address is **0.0.0.0**.

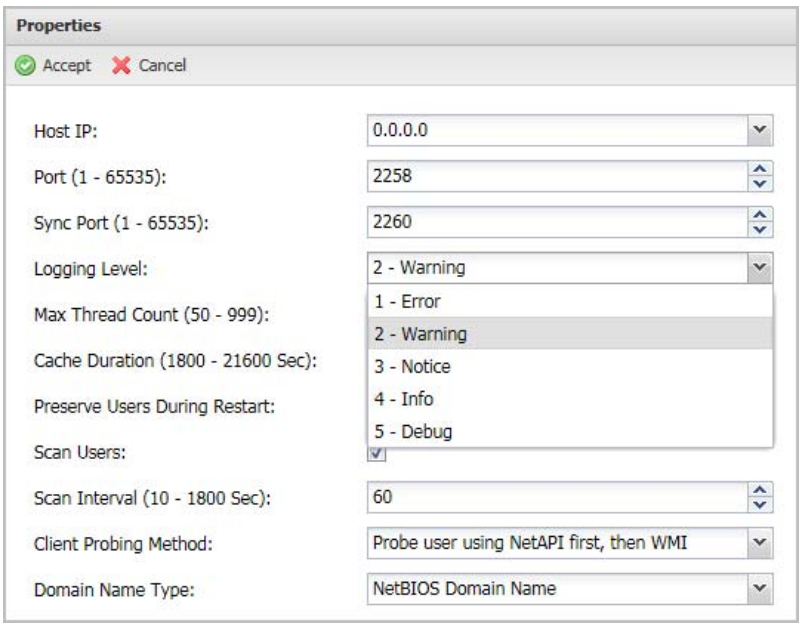
The SSO Agent binds the UDP socket at this IP address and the port number specified in the **Port** field. The Agent receives the SSO protocol packets from the firewall on this socket.

NOTE: If the Host IP address is `0.0.0.0`, the SSO Agent accepts packets from any interface.

4 In the **Port** field, accept the default port or type in a custom port. By default, the SSO Agent uses UDP port **2258** to receive the SSO protocol packets.

5 In the **Sync Port** field, accept the default port or type in a custom port. By default, the SSO Agent uses TCP port **2260** to receive the agent synchronize datagrams.

6 From the **Logging Level** the drop-down menu, select the level of events to be logged in the log file in the program data directory. The log file is useful for diagnostics and debugging. The default logging level is **2 - Warning**.



7 In the **Max Thread Count** field, accept the default of **100** or type in a custom value within the indicated range.

The SSO Agent starts the configured number of threads at run time. Most of the threads are used for client probing. These threads periodically query the IP addresses that are present in the Scanner queue. After completing each query, the agent adds or updates the user or error information in its cache. The thread count adjusts the trade off between simultaneity and overall performance.

8 In the **Cache Duration** field, accept the default of **7200** seconds (2 hours) or type in a custom value within the indicated range.

If a user does not log off the computer properly, for example by pulling the power plug or if the DC group policy for enabling Event ID 4661 is not set, the SSO Agent does not receive a log-off message for the user. In this case, the SSO Agent keeps the user information in its cache. After the cache duration time expires, the SSO Agent removes the user from the cache and sends a log-out notification to the firewall. The default time of **2** hours is based on the typical duration after which the log-in status is refreshed on the Domain Controller. Cache duration functions only apply to users whose session ID is not equal to zero.

Upon a user information request for any IP address from the appliance, the SSO Agent checks for the IP address in its cache. If the IP address is not present in the cache, the SSO Agent treats the request as the first request for that IP Address and adds the IP Address to its Scanner queue for further processing.

9 To save information about previously identified users when the SSO Agent service is restarted, select the **Preserve Users During Restart** checkbox. This option is not selected by default.

Because the SSO Agent must be restarted for Properties changes to take effect, this option allows the Agent to maintain current user information across these restarts. The SSO Agent saves the user information in an XML file that contains a timestamp. If the file is less than 15 minutes old when the SSO Agent restarts, it uses this file to fill its cache; otherwise, the SSO Agent ignores the file to avoid restoring outdated information.

10 The **Scan Users** checkbox is selected by default.

If **Scan Users** is enabled and a user is identified with a Client Probing method, the SSO Agent probes this user repeatedly until the user logs off the computer or the SSO Agent can identify this user using another

method, such as DC Security Log or Server Session. When the SSO Agent detects that the user has logged off the computer, it sends a log-off notification to the firewall.

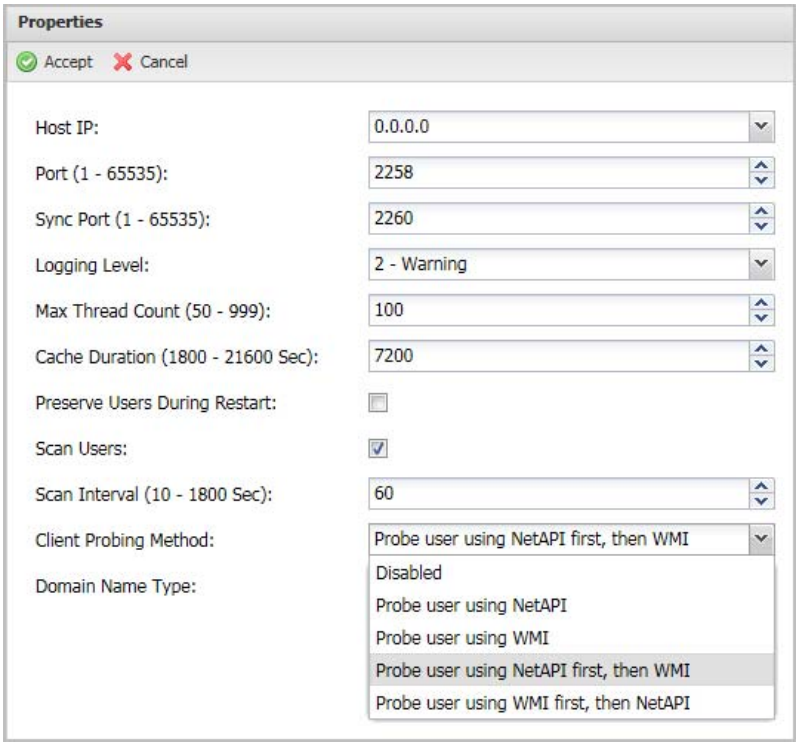
If the query returns an error for any IP address and the SSO Agent is not able to identify the user information, the agent treats the IP address as a Bad IP. This can occur for network devices such as printers, non-Windows computers, or other workstations that do not understand the query options. While processing requests in the Scanner queue, the agent skips any Bad IP addresses and adds the IP address to the back of the queue for the next fetch.

To ensure that the agent does not process any IP address that has not been polled from the appliance for a considerable amount of time, the agent maintains the session time and the time of the last request from the appliance for each IP address. This allows the agent to minimize the queue size, ensures that threads are not wasted, and prevents unnecessary traffic from the agent for IP addresses that are not polled from the appliance. The session time can be modified from Windows registry settings using the registry value, `SESIONTIME`.

11 In the **Scan Interval** field, accept the default of **60** seconds or type in a custom value within the indicated range.

12 For **Client Probing Method**, select one of the following options from the drop-down menu:

- **Disabled**
- **Probe user using NetAPI**
- **Probe user using WMI**
- **Probe user using NetAPI first, then WMI** (this is the default option)
- **Probe user using WMI first, then NetAPI**



When the SSO Agent receives an IP Address request from the firewall and the user is not found in its cache, it uses the selected Client Probing Method to identify the username.

NOTE: NetAPI provides faster, though possibly slightly less accurate, performance. With NetAPI, Windows reports the last login to the workstation whether or not the user is still logged in. This means that after a user logs out from his computer, the appliance still shows the user as logged in when NetAPI is used. If another user logs onto the same computer, then at that point the previous user is logged out from the SonicWall appliance.

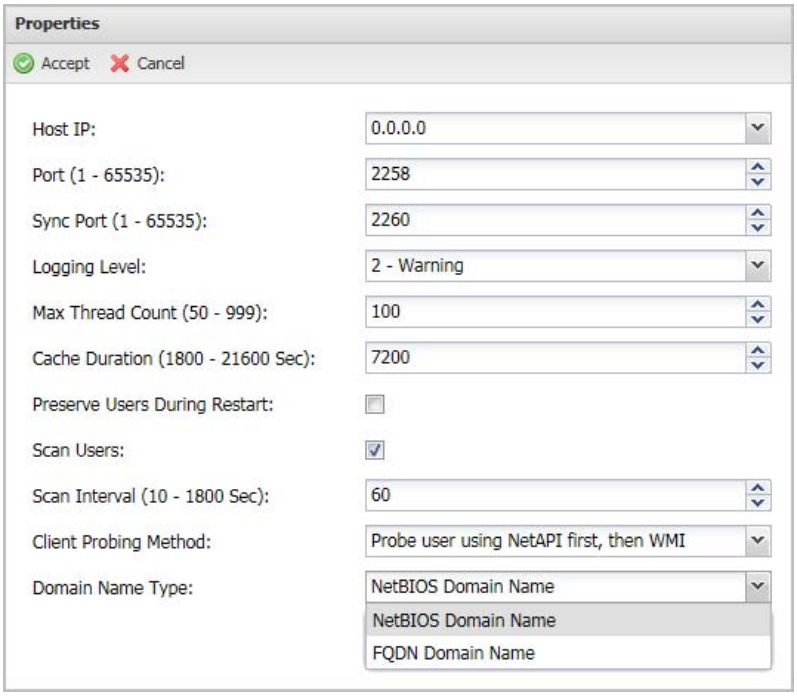
CAUTION: NetAPI has known security vulnerabilities on Windows and SonicWall does not recommend enabling it. If you do use it, create a dedicated account for it with the minimum necessary administrative privileges.

The handling of non-responsive workstations to queries from WMI and NetAPI is optimized in the SSO Agent. The appliance repeatedly polls the SSO Agent with multi-user requests, and often sends more than one such request at a time. The number of concurrent requests increases when workstations do not respond to the requests, potentially overloading the Agent. To avoid this, a time-out mechanism is included in multi-user requests from the appliance. If the request does not complete within this time, the agent silently aborts it.

13 For **Domain name type**, select one of the following options from the drop-down menu:

- **NetBIOS Domain Name**
- **FQDN Domain Name**

SonicOS/X can handle both domain name types. The default option is **NetBIOS Domain Name**.



14 Click **Accept** at the top of the screen.

15 Click **OK** in the update status dialog.

Configuring Service Management and Restarting

The **SSO Agent > Service Management** page displays the current Service Logon User credentials and allows you to configure them. This page also provides a way to restart the Windows SSO Agent service program.

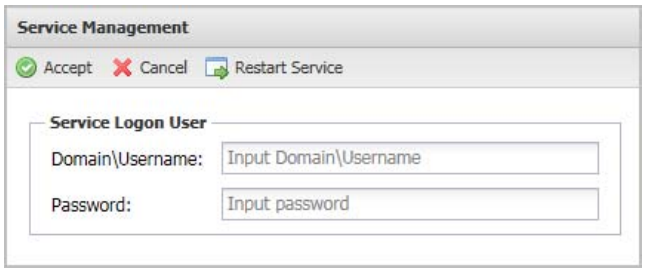
Topics:

Configuring Service Logon User Credentials

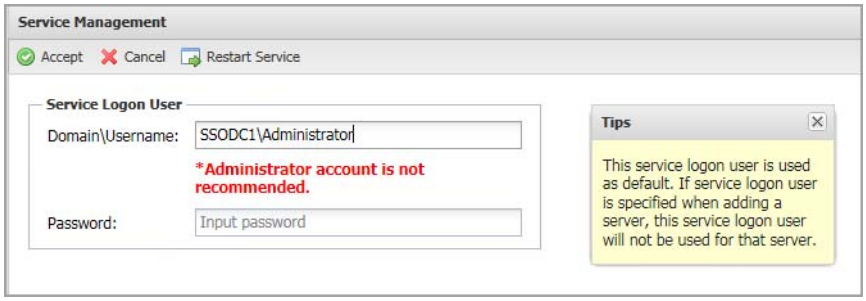
The Service Logon User credentials configured on this page are used as default credentials for the SSO Agent to do WMI queries and NetAPI queries and to access the domain controller.

You can input specific credentials for the domain controller, terminal server, or Exchange server when adding or editing these servers. These credentials are independent of one another and do not have to be in the same domain. If credentials are specified for any of these servers, the default Service Logon User is not used to access that server.

The WMI, NetAPI, and DC Security Log server access methods all require some level of domain administrator privileges. SonicWall recommends creating a dedicated domain user account with the minimum required privileges to run the SSO Agent service. Refer to Creating a Dedicated Domain User with Minimum Privileges for SSO Agent on page 49 for information.



CAUTION: Using a domain administrator account as the Service Logon User is not recommended. If you input a domain administrator account as the Service Logon User, there will be a warning.



To configure the default Service Logon User credentials:

1 Launch the Directory Connector Configuration Tool:

- On Windows, either from the Start menu or by double-clicking the desktop shortcut
- On Linux, by pointing your browser to `http://127.0.0.1:8080`

2 Under **SSO Agent** in the left pane, click **Service Management** to display the configuration fields in the right pane.

3 Under **Service Logon User** in the **Domain\Username** field, enter the domain and user name for the account, separated by a backslash '\'.

4 In the **Password** field, enter the account password.

> **CAUTION: For best security, the password should be a complex string of at least 20 characters using upper and lower case characters, numbers, and special characters.**

5 Click **Accept** to save the changes.

6 Restart the SSO Agent service. After configuring the **Service Logon User**, it is required to restart the SSO Agent service.

Restarting the SSO Agent Service

The Service Management page provides a way to start and stop the Windows service for the SSO Agent.

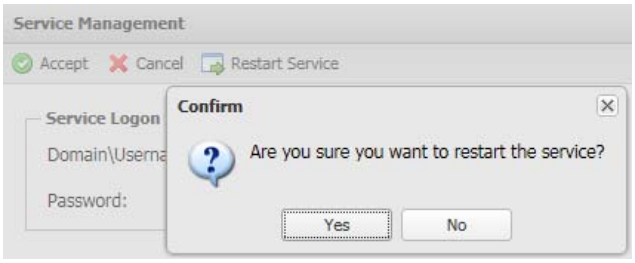
> **NOTE:** The Linux SSO Agent service can be restarted from the command line using a command such as `service ssoagentd restart` or `systemctl restart ssoagentd`.

To restart the Windows SSO Agent service:

1 Launch the Directory Connector Configuration Tool and navigate to the **SSO Agent > Service Management** page.

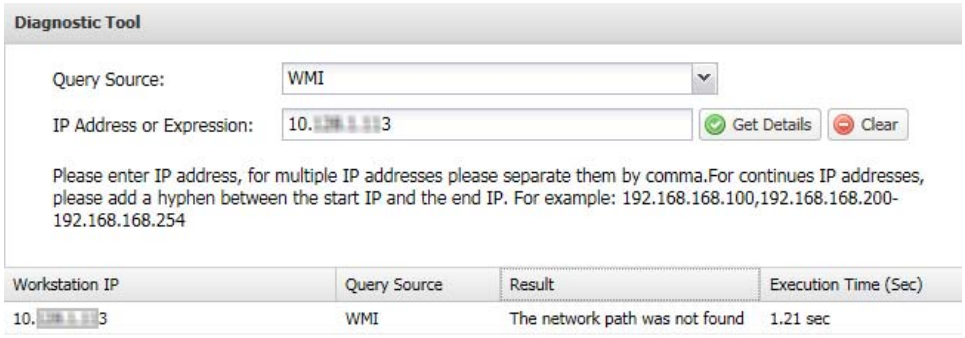
2 At the top of the right pane, click the **Restart Service** button.

3 Click **Yes** in the confirmation dialog.



Using the Diagnostic Tool

The **SSO Agent > Diagnostics Tool** page of the Directory Connector Configuration Tool provides a way to find logged in user information for remote workstations. You can manually identify IP addresses using the WMI, NetAPI, or NetAPI-Workstation Info method. NetAPI-Workstation Info will query the computer name and domain name of the IP address specified.



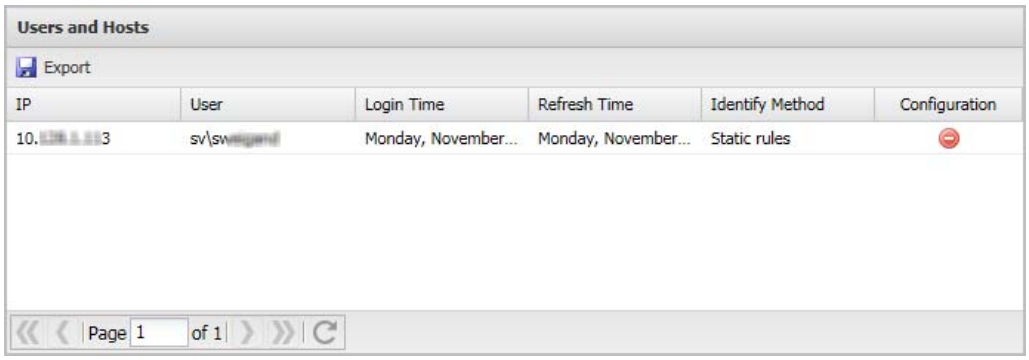
To use the diagnostic tool:

1. Launch the Directory Connector Configuration Tool and navigate to the **SSO Agent > Diagnostic Tool** page.
2. For **Query Source**, select one of:
   - **WMI**
   - **NetAPI**
   - **NetAPI-Workstation Info**
3. In the **IP Address or Expression** field, enter one of the following:
   - An IP address
   - Multiple IP addresses separated by commas
   - An IP address range using a hyphen
4. Click **Get Details**.

   The information is displayed in the **Result** column and the time taken by the query is displayed in the **Execution Time (Sec)** column.
5. To repeat for a different IP address or range, click the **Clear** button and enter the new address(es) in the **IP Address or Expression** field, then click **Get Details** again.

Displaying Users and Hosts Statistics

The **SSO Agent > Users and Hosts** page of the Directory Connector Configuration Tool displays some user statistics and all users in the SSO Agent cache. The page displays the IP address, user name, user login time, time of last refresh, and the method used to identify the user. The **Configuration** column displays the *Remove User and Host* button.



You can sort the users by clicking the column heading, manually remove a user from the cache, and export the whole user list to a CSV file.

To display the user information:

1. Launch the Directory Connector Configuration Tool and navigate to the **SSO Agent > Users and Hosts** page.
2. On deployments with many users, use the following **Page** functions at the bottom of the page to display additional users:
   - Enter the desired page number and press Enter.
   - Click the single arrow buttons to scroll forward or backward one page.
   - Click the double arrow buttons to jump to the beginning or end of the list.

To export the user list:

1. Click the **Export** button at the top of the page.
2. Click **Save** in the popup dialog.

   On Windows machines, the `users.csv` file is saved in your `Downloads` folder.

To remove a user from the cache:

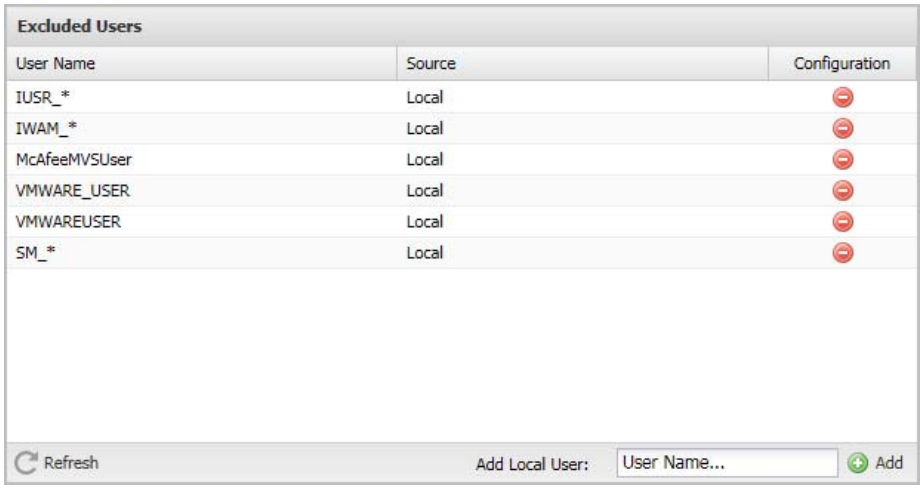
1. Click the *Remove User and Host* button in the **Configuration** column of the row with the user you want to remove.
2. Click **OK** in the confirmation dialog.

To sort the user list:

1. Click a column heading to sort the list in ascending or descending order based on that column.

Configuring Excluded Users

The **SSO Agent > Excluded Users** page of the Directory Connector Configuration Tool displays all the service users that are configured on the SonicWall security appliance. The users might be used by services on the end-user's computer. The SSO Agent ignores all events for user names that are in this list.



You can add users to, or remove users from the excluded users list.

To view and refresh the list of excluded users:

1. Launch the Directory Connector Configuration Tool and navigate to the **SSO Agent > Excluded Users** page.

   The list of excluded users is displayed, including any edits you have made.

2. Click the **Refresh** button at the bottom of the page to refresh the list.

To add a local user name to the list of excluded users:

1. At the bottom of the **SSO Agent > Excluded Users** page, type the user name into the **Add Local User** field.

   Wildcard characters are supported in the user name.

2. Click the **Add** button next to the field.

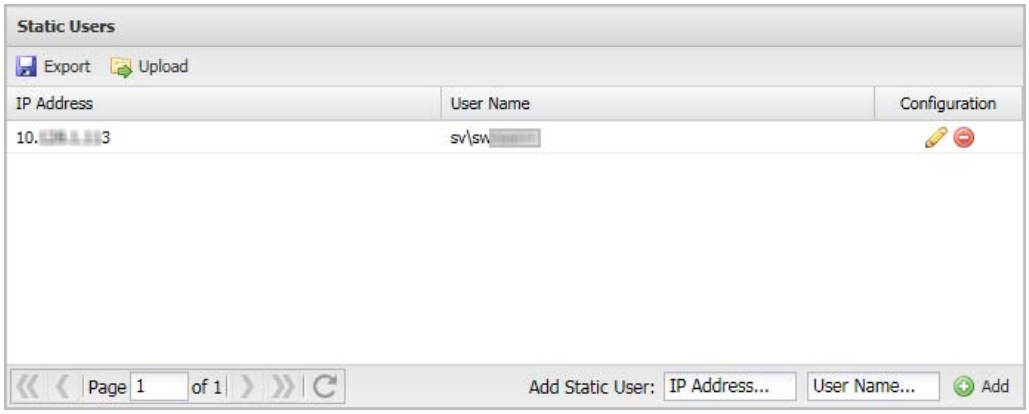
TIP: You can also add Windows service users from SonicOS/X (see the *SonicOS and SonicOSX Administration Guides* for details).

To remove a user name from the list of excluded users:

1. In the Directory Connector Configuration Tool, navigate to the **SSO Agent > Excluded Users** page.
2. Click the *Remove User* button in the **Configuration** column for the user name you want to remove.
3. Click **Yes** in the confirmation dialog.

Configuring Static Users

The **SSO Agent > Static Users** page of the Directory Connector Configuration Tool displays all the static users configured in the SSO Agent. You can manually add and remove a static user from this page. You can also import and export the whole user list.



To view and refresh the list of static users:

1. Launch the Directory Connector Configuration Tool and navigate to the **SSO Agent > Static Users** page.

   The list of static users is displayed, including any edits you have made.

2. On deployments with many static users, use the following **Page** functions at the bottom of the page to display additional users:

   - Enter the desired page number and press Enter.
   - Click the single arrow buttons to scroll forward or backward one page.
   - Click the double arrow buttons to jump to the beginning or end of the list.

3. Click the *Refresh* button (icon) next to the **Page** functions to refresh the list.

To add a user to the list of static users:

1. At the bottom of the **SSO Agent > Static Users** page, type the user's IP address and the user name into the **Add Static User** fields.

   Static users can include a domain name by using the format: `domain\username`. Directory Connector verifies the entry and pops up an error dialog if it is not valid.

2. Click the **Add** button next to the field.

   The page changes to display the new static user.

To edit a static user:

1. On the **SSO Agent > Static Users** page, click the *Edit Static User* icon in the **Configuration** column for the user you want to edt.
2. In the **Edit Static User** dialog, edit the **Ip Address** and/or the **User Name** field as needed.
3. Click **OK**.

To export the list of static users:

1 At the top of the **SSO Agent > Static Users** page, click the **Export** button.

2 In the **File Download** dialog, click **Open** to view the exported CSV file or click **Save** to save it to your computer.

On Windows machines, the user list is saved in:

```
C:\Program Files\SonicWall\SSOAgent\static.csv
```

To delete a static user:

1 On the **SSO Agent > Static Users** page, click the *Remove Static User* icon in the **Configuration** column for the user you want to delete.

2 Click **Yes** in the confirmation dialog.

To import a list of static users from a CSV file:

1 At the top of the **SSO Agent > Static Users** page, click the **Upload** button.

2 In the **Upload a file** dialog, click the **Browse** button to locate the file, then double-click it or click it once and then click **Open**.

3 Click **Submit**.

4 Click **OK** in the **Success** dialog.

The page changes to display the new static user.

Viewing the Logs

On Windows, the SSO Agent log files and crash dump files are placed in the following folders:

- `C:\ProgramData\SonicWall\SSOAgent\log`
- `C:\ProgramData\SonicWall` (for SSO Agent service crash dumps)

On Linux, the SSO Agent log files can be found in:

- `/opt/ssoagent/SSOAgent/log`

The SSO Agent keeps several logs at a time:

- `SSOAgent.log` - This is the main log file.
- `SSOAgentService.log` - This is the log file for the service process.
- `SSOPacket.log` - This is the packets log between the firewall and Agent.
- `Rpc.log` - This is the RPC log between the Config Tool and Agent service.
- `SecurityEvent.log` - This is the DC/Exchange security event log.
- `SessionTable.log` - This shows the results returned by the NetSessionEnum API.

You can view the log files using a text editor.

More log entries are created with higher logging levels. Debug is the highest level. In the case of troubleshooting, all log files should be sent for investigation by the Support team.

Option to Automatically Remove Old Logs

Starting in the Directory Connector / SSO 4.1.17 release, the `config.xml` file has an option called **MaxLogRetentionHours** that enables the periodic, automatic removal of old log files. By default, the option is set to 168 to remove log files after a period of 168 hours, which is one week. There is no maximum value for it and there is no recommended or best value, as it depends on the customer requirements. When the option is set to zero, automatic log removal is disabled. After setting **MaxLogRetentionHours** to a new value, you must restart the SSO Agent service to make it take effect.

This option prevents the accumulation of old log files, which can cause resource issues if never removed. In the current implementation, when one log file's size exceeds 50MB, the SSO Agent renames the log file by appending the time stamp, and creates a new log file to continue to write logs.

5

Adding Firewalls, Servers and Remote Agents

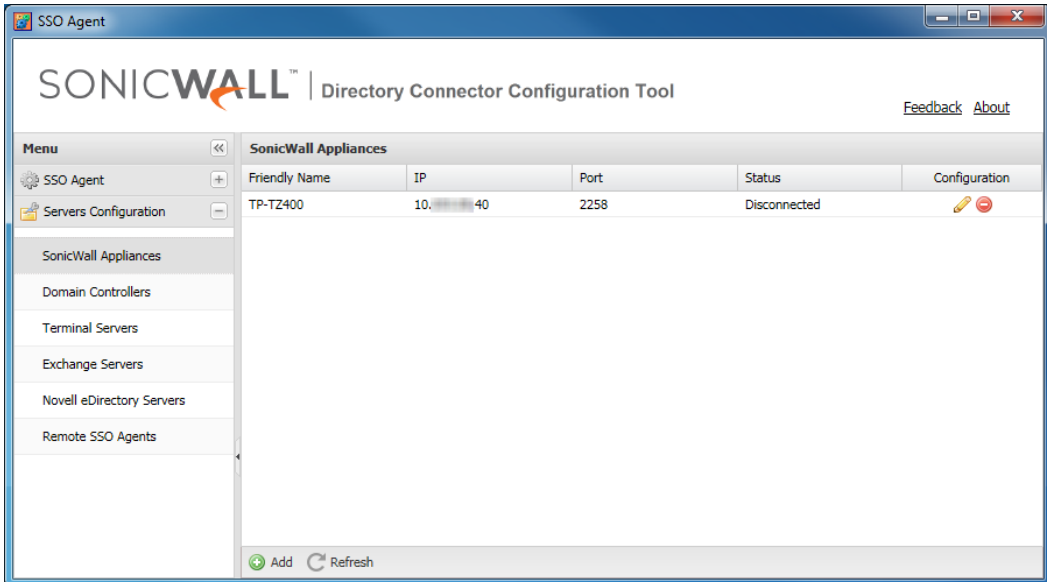
This section provides information about configuring systems, servers and Directory Connector to work together:

- How to use the Directory Connector Configuration Tool to configure systems and servers to work with the SSO Agent, including SonicWall firewalls, Domain Controllers, Terminal Servers, Exchange Servers, Novell eDirectory servers, and Remote SSO Agents.
- How to configure users, groups, and associated permissions settings on servers and client machines.

Topics

Adding SonicWall Appliances

To display all the configured SonicWall network security appliances, click on **SonicWall Appliances** in the left panel of the Directory Connector Configuration Tool.

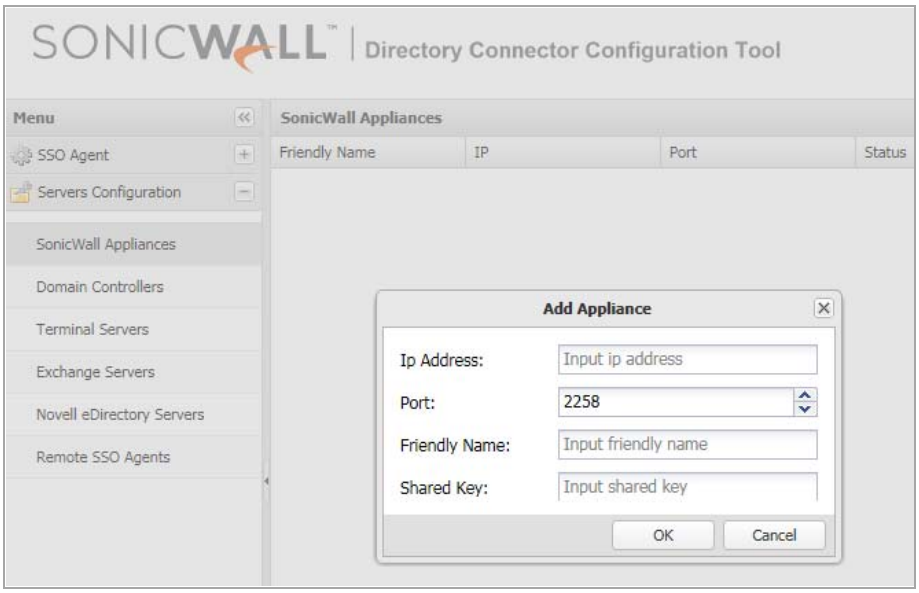


The Friendly Name, IP address, Port, and Status information for each appliance are displayed, along with Configuration buttons for editing or removing the appliance.

To add a SonicWall appliance in Directory Connector:

1 Launch the Directory Connector Configuration Tool either from the Start menu or by double-clicking the desktop shortcut.

2 Select **SonicWall Appliances** in the left pane and then click the **Add** button at the bottom of the right pane. The **Add Appliance** dialog displays.



3 In the **IP Address** field, type in the IP address of the firewall.

4 In the **Port** field, accept the default port of **2258** or use the up/down arrows to increment/decrement the port number or type in a custom port. The appliance sends the SSO protocol packets to the Agent on this port.

5 In the **Friendly Name** field, type in a descriptive name for this appliance. After adding the appliance, the friendly name will be displayed in the left pane as well.

6 In the **Shared Key** field, type in a hexadecimal (only 0-9, a-f, A-F) number of up to 16 characters (use an even number of characters) to use as the key for encrypting messages between the SonicWall appliance and the SSO Agent. You must also enter the same key when configuring the SSO Agent to communicate with the appliance.

7 Click **OK** to save the configuration.

NOTE: To modify the settings of an existing appliance, click on the Edit button in the **Configuration** column for that appliance.

Configuring Domain Controllers

The Domain Controller (DC) is a server that responds to security authentication requests (logging in, checking permissions, and so on) within the Windows domain. You can select **Domain Controllers** in the left pane of the Directory Connector Configuration Tool to display the **Host Address**, **Friendly Name**, **Domain Name**, **NETBIOS Name**, and **Status** of the known DCs, along with edit and delete buttons in the **Configuration** column.

Directory Connector provides the following functions for domain controllers:

- **Add**

  Select this option to manually add a domain controller to the SSO Agent configuration.

- **Auto Discovery**

  Select this option to have the SSO Agent use DNS queries to find DCs to which the Agent host machine belongs.

- **Config All**

  Select this option to configure the server monitoring method for all known DCs.

- **Refresh**

  Select this option to refresh the known domain controller information.

Topics:

The SSO Agent supports two methods to identify users who log on to a Windows domain:

- DC Security Log
- Server Session

Using Microsoft Windows, the DC Security Log contains login and logout activity records or other security-related events specified by the Domain Controller's audit policy.

By default, all of the DC Security Log options require a Domain Administrator account or a Local Administrator account on the Domain Controller to read the DC Security Log.

If an account with administrator privileges is not available, user identification through the DC Security Log can be configured for WMI with a non-administrator domain account. This account must have read access to the security log. For more information, refer to the following knowledge base article: https://www.sonicwall.com/en-us/support/knowledge-base/171004124849942.

Adding a Domain Controller

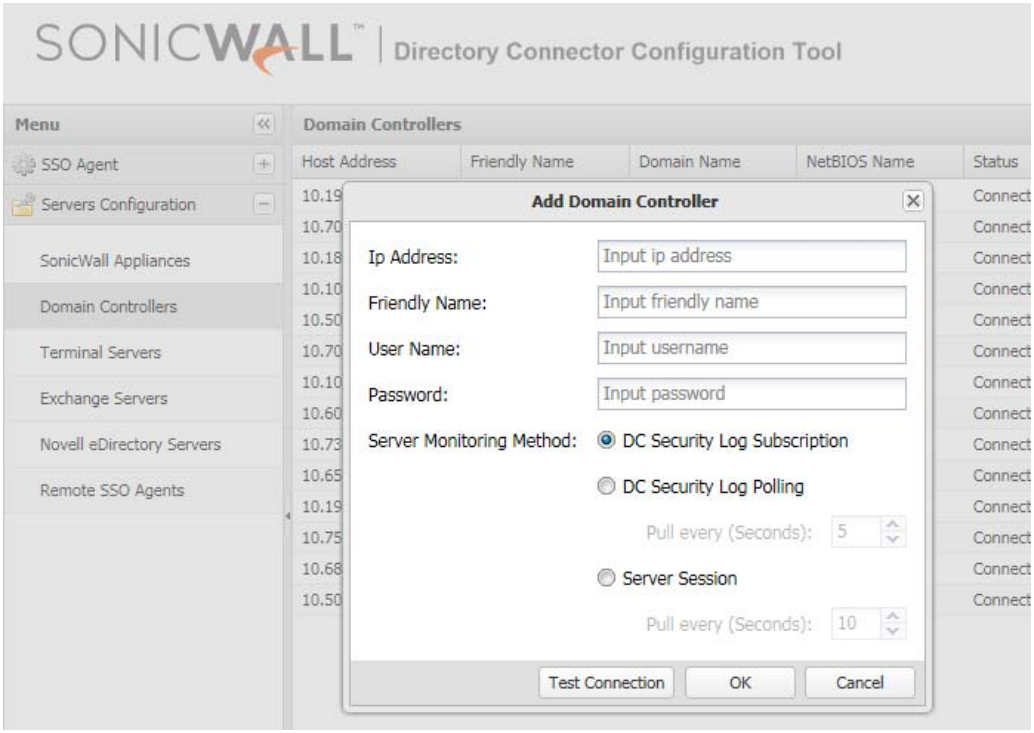
You can add domain controllers manually by entering a valid DC IP address and domain name into the Directory Connector Configuration Tool.

When adding a domain controller, you can specify the corresponding domainname\username and password. These credentials are independent of the Service Logon User name and do not have to be in the same domain. If this field is left empty, the service will use the Service Logon User name to query the DC log and probe clients.

To manually add a domain controller in Directory Connector:

1 Launch the Directory Connector Configuration Tool either from the Start menu or by double-clicking the desktop shortcut.

2 Select **Domain Controllers** in the left pane and then click the **Add** button at the bottom of the right pane. The **Add Domain Controller** dialog displays.



3 In the **Ip Address** field, type in the IP address of the domain controller to be added.

4 In the **Friendly Name** field, enter a descriptive name for the domain controller.

5 To access the domain controller using credentials that are different from the service logon credentials, enter the domain and user name in the form “domainname\username” into the **User Name** field, and enter the password into the **Password** field. These credentials will be used to query the DC log.

6 For **Server Monitoring Method**, select one of the following:

- **DC Security Log Subscription**

  You can select this method for getting DC event log updates if the domain controller and SSO Agent are installed on Windows machines that support the event subscription API. It is supported on Windows Server 2008 and higher.

- **DC Security Log Polling**

  This option causes the SSO Agent to request the event log information from the DC at the time interval indicated in the **Pull every** field. Accept the default of **5** seconds or type in the desired interval. The minimum is 5 seconds and the maximum is 300 seconds.

- **Server Session**

  This option causes the SSO Agent to request the server session information from the DC at the time interval indicated in the **Pull every** field. Accept the default of **10** seconds or type in the desired interval. The minimum is 5 seconds and the maximum is 300 seconds.

7 To test the connection to the domain controller using the configured IP address, click **Test Connection**.

If the IP address does not belong to a machine with a role of Domain Controller, the Configuration Tool displays an error message.

8 If no errors are displayed, click **OK**.

Using Auto Discovery

The SSO Agent can automatically discover all the domain controllers by using DNS queries to find DCs to which the Agent host machine belongs.

NOTE: DC Auto Discovery is not supported by Directory Connector on Linux.

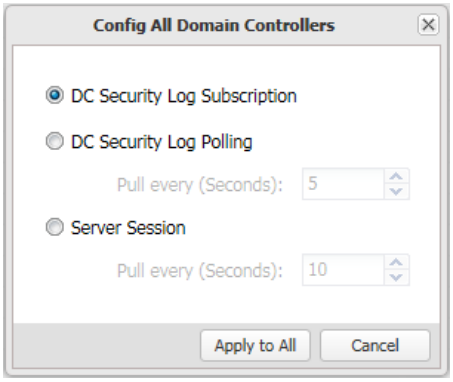
To initiate Auto Discovery:

1. In the Directory Connector Configuration Tool, select **Domain Controllers** in the left pane.
2. At the bottom of the right pane, click the **Auto Discovery** button. The right pane displays the discovered domain controllers.

Configuring All Domain Controllers

To configure the server monitoring method for all known domain controllers:

1. In the Directory Connector Configuration Tool, select **Domain Controllers** in the left pane.
2. At the bottom of the right pane, click the **Config All** button. The Config All Domain Controllers dialog is displayed.



3. Select one of the following:
   - **DC Security Log Subscription**

     You can select this method for getting DC event log updates if the domain controller and SSO Agent are installed on Windows machines that support the event subscription API. It is supported on Windows Server 2008 and higher.

     NOTE: DC Security Log Subscription is not supported by Directory Connector on Linux.

   - **DC Security Log Polling**

     This option causes the SSO Agent to request the event log information from the DC at the time interval indicated in the **Pull every** field. Accept the default of **5** seconds or type in the desired interval. The minimum is 5 seconds and the maximum is 300 seconds.

   - **Server Session**

     This option causes the SSO Agent to request the server session information from the DC at the time interval indicated in the **Pull every** field. Accept the default of **10** seconds or type in the desired interval. The minimum is 5 seconds and the maximum is 300 seconds.

NOTE: Server Session is not supported by Directory Connector on Linux.

4 Click **Apply to All**.

5 Click **Yes** in the confirmation dialog.

Refreshing the Domain Controller Display

To refresh the domain controller information:

1 In the Directory Connector Configuration Tool, select **Domain Controllers** in the left pane.

2 At the bottom of the right pane, click the **Refresh** button. The right pane displays the updated domain controller information.

Creating a Dedicated Domain User with Minimum Privileges for SSO Agent

The SSO Agent can identify users through NetAPI/WMI or DC/Exchange security log. NetAPI/WMI can run independently, however, DC/Exchange security log needs WMI support. If you choose DC/Exchange security log as the identification mechanism, then you must also enable WMI access in the DC server or Exchange server to allow the SSO Agent to get information from the DC or Exchange server using WMI.

This section describes how to add a domain user and configure settings for the minimum, necessary privileges.

Topics:

- Creating the Domain User for SSO Agent
- Adding DC/Exchange Security Log Support
- Adding WMI Support
- Adding NetAPI Support
- Configuring the SSO Agent

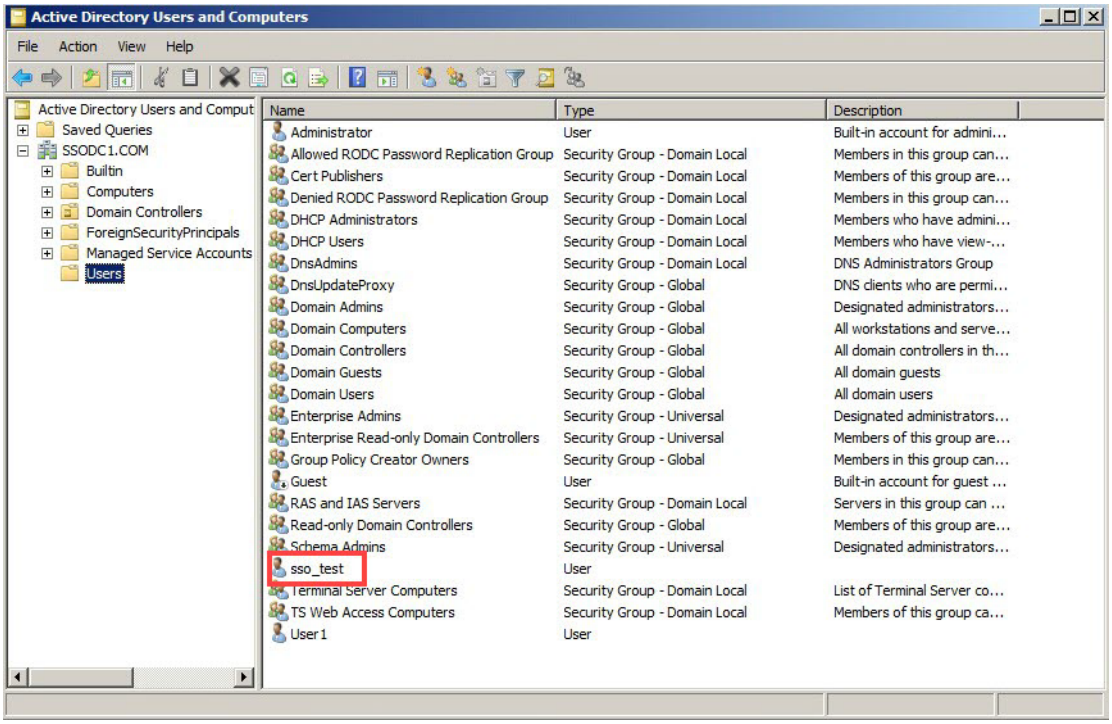
Creating the Domain User for SSO Agent

To create a domain user for SSO Agent:

1 In the DC server, open the **Active Directory Users and Computers** console.

2 Under the appropriate domain in the left pane, click **Users**.

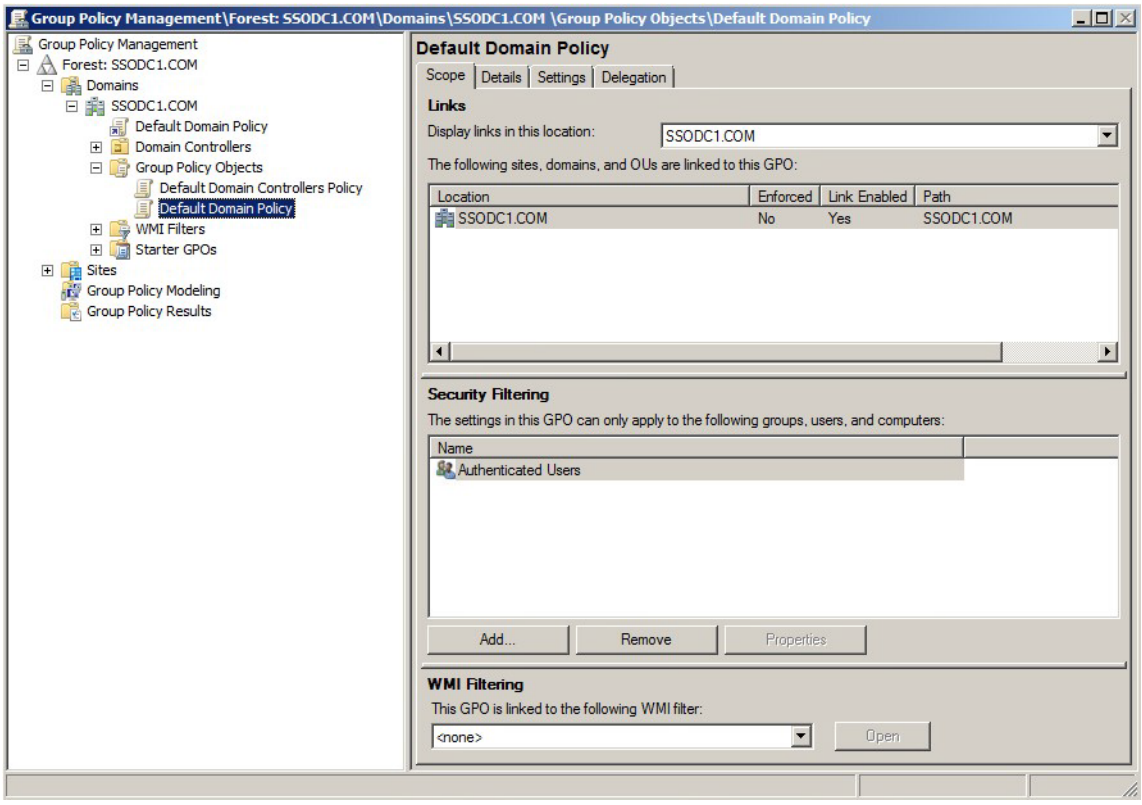
3 Add the new user. This example creates the user **sso_test** under the **SSODC1** domain.



4 Open the **Group Policy Management** console.

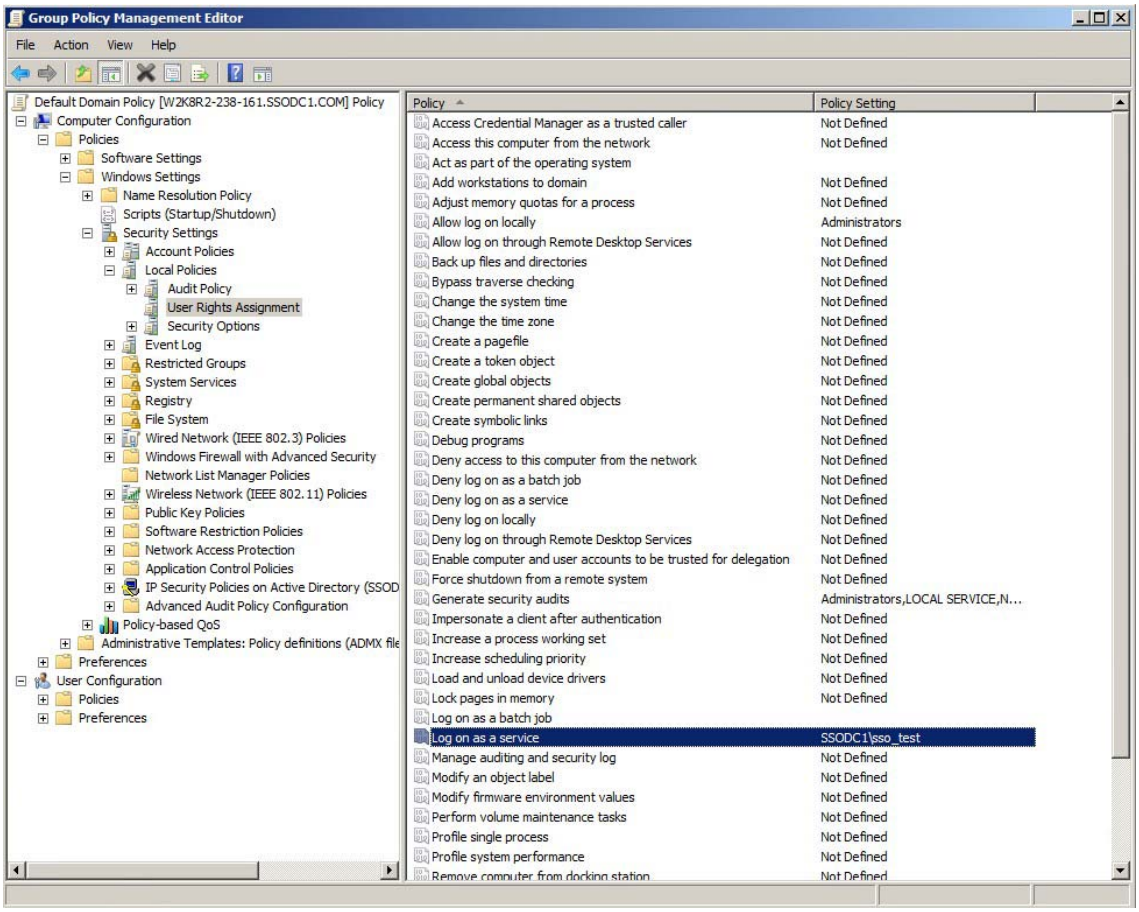
5 Browse to the following location: *Domain Name* > Domains > *Domain Name* > Group Policy Objects, where *Domain Name* is replaced with your domain.

6 Under **Group Policy Objects**, right-click on **Default Domain Policy**, and then select **Edit**.



7 In the **Group Policy Management Editor** left pane, navigate to **Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies** and select **User Rights Assignment**.

8 In the right pane, double-click **Log on as a service** and add your *Domain\Username* to it. In this example, we add **SSODC1\sso_test** to it.



Adding DC/Exchange Security Log Support

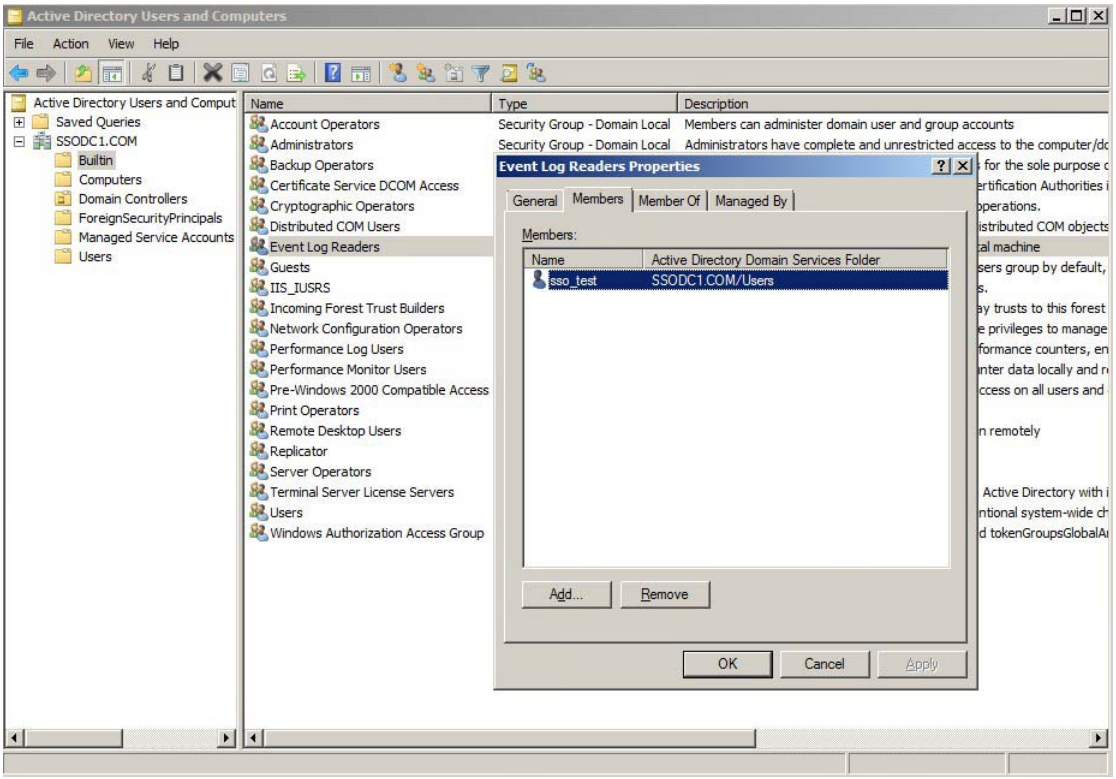
To give the user permission to read the Security Log on the DC or Exchange server:

1 In the DC server, open the **Active Directory Users and Computers** console.

2 Under the appropriate domain in the left pane, click **Builtin**.

3 In the right pane, double-click on **Event Log Readers** to open the **Event Log Readers Properties** dialog.

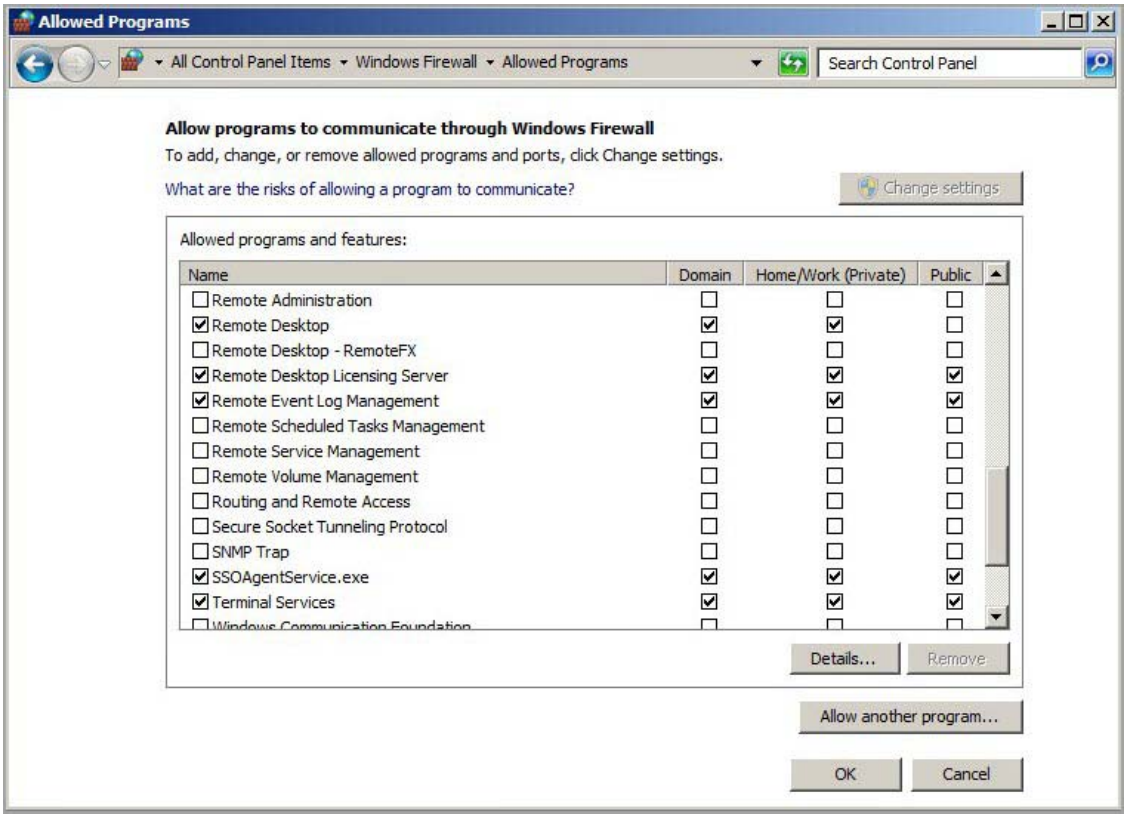
4 On the **Members** screen, add the user to the Event Log Readers group.



5 Click **OK**.

6 Open the Windows Control Panel and navigate to **All Control Panel Items > Windows Firewall > Allowed Programs**.

7 Select all the checkboxes in the **Remote Event Log Management** row (the checkboxes for **Domain**, **Home/Work (Private)**, and **Public**). This allows Remote Event Log Management traffic to pass through Windows Firewall.



8 Click **OK**.

Adding WMI Support

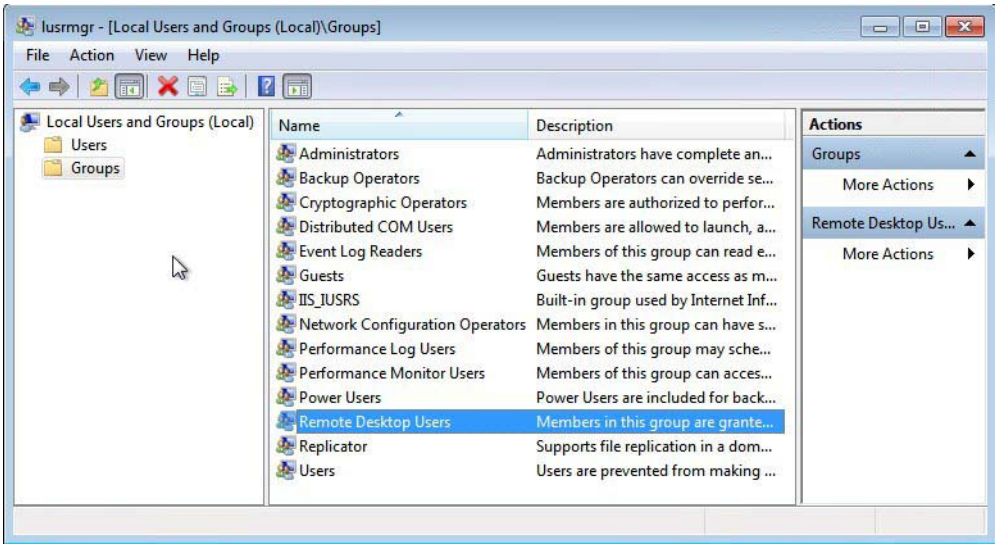
To allow the SSO Agent to query information through WMI from client machines, make the below changes in each client machine.

NOTE: To support reading the Security Log from a DC/Exchange server, also make the below changes on the DC/Exchange server, except for the lusrmgr.msc settings.

To allow SSO Agent to query information with this username using WMI from client machines:

1 On the Windows client machine, search for and open **lusrmgr.msc** in the **Start** menu.

2 Select **Groups** in the left pane.

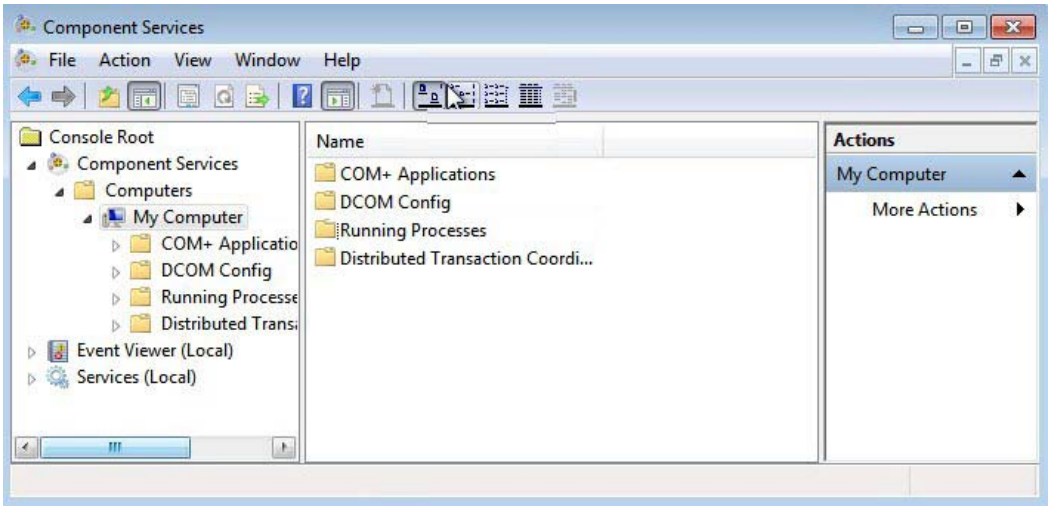


3 Double-click **Distributed COM Users** and add your *Domain\Username* to this group. In this example, we add **SSODC1\sso_test** to it.

4 Double-click **Remote Desktop Users** and add your *Domain\Username* to this group. In this example, we add **SSODC1\sso_test** to it.

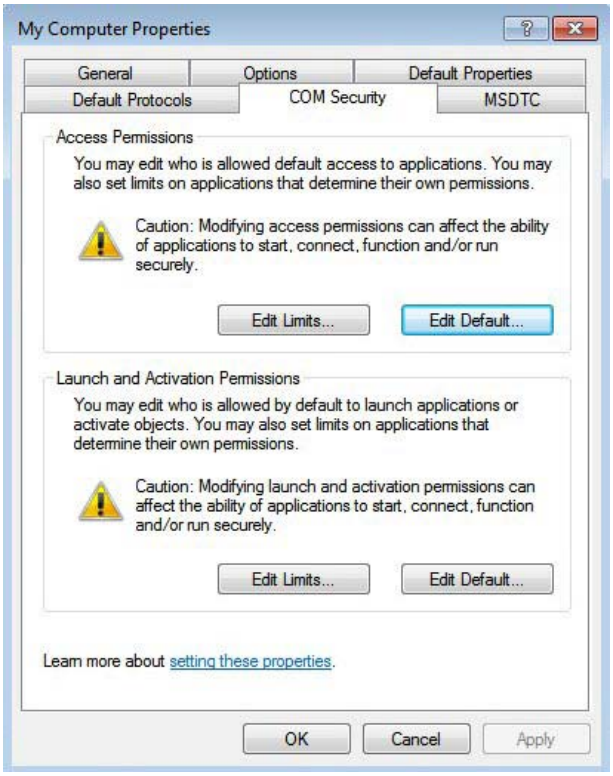
5 Search for and open **dcomcnfg** in the **Start** menu.

6 Navigate to **Component Services > Computers** in the left pane.



7 Right-click on **My Computer** and select **Properties** to launch the **My Computer Properties** dialog.

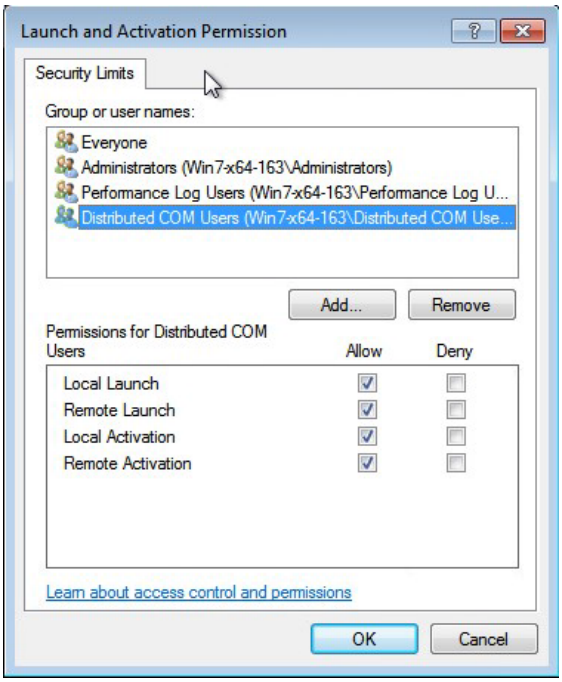
8 In the **My Computer Properties** dialog, select the **COM Security** tab.



9 Under **Launch and Activation Permissions**, click **Edit Limits**.

10 In the **Launch and Activation Permission** dialog, select **Distributed COM Users** in the **Group or user names** list.

11 Under **Permissions for Distributed COM Users**, select all checkboxes under **Allow** to allow all permissions.

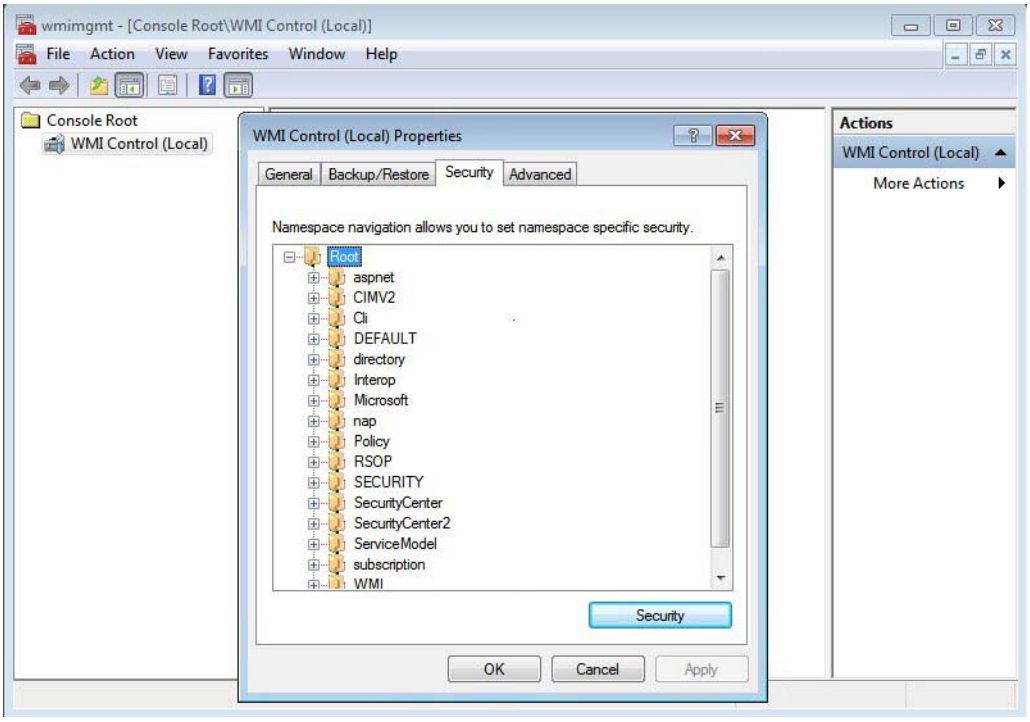


12 Click **OK** and then click **OK** in the **My Computer Properties** dialog.

13 Search for and open **wmimgmt.msc** in the **Start** menu.

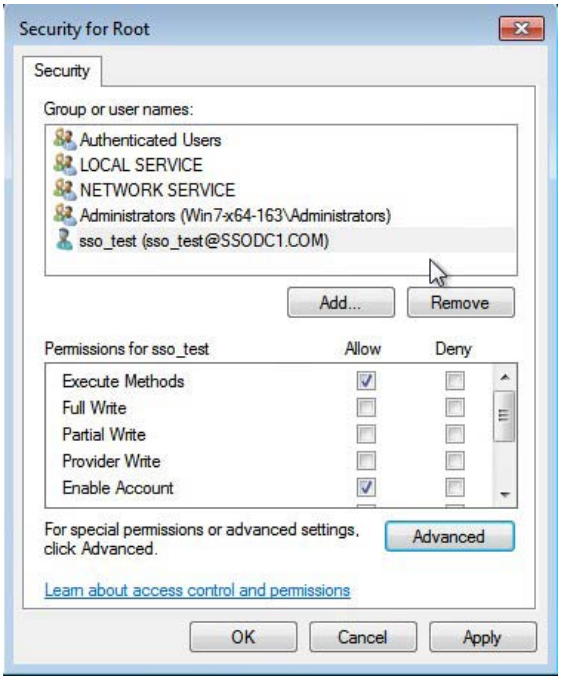
14 Right-click **WMI Control (Local)** and select **Properties**.

15 In the pop up dialog, select the **Security** tab and then select and expand the **Root** node.



16 Click the **Security** button.

17 In the **Security for Root** pop up dialog, add your *Domain\Username* under **Group or user names**. In this example, we add **SSODC1\sso_test** to the list.



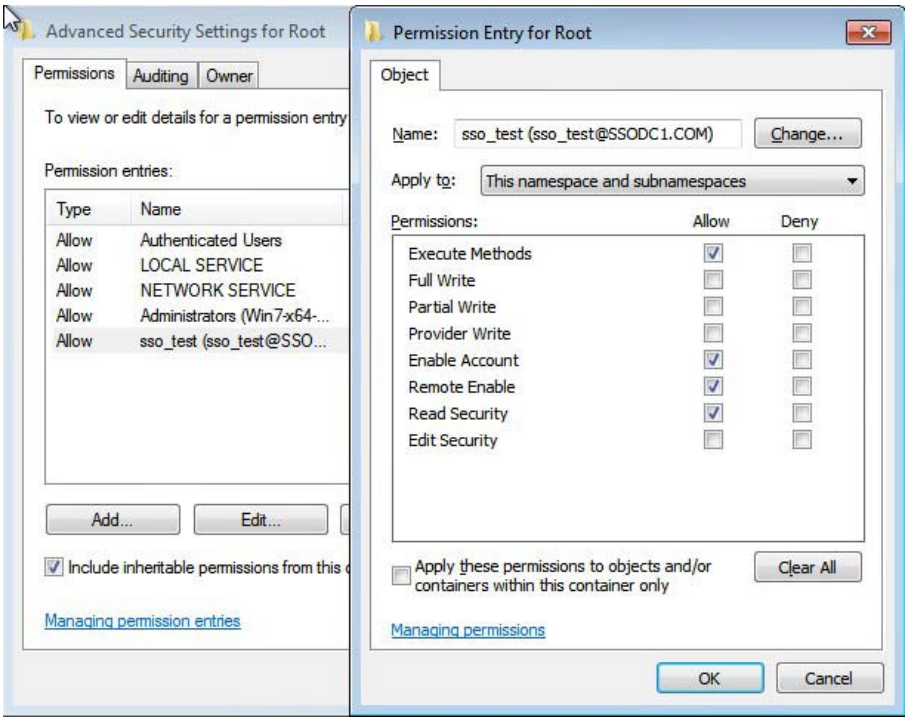
18 Select the entry that you just added (**sso_test** in this example) and then select the **Allow** checkboxes for the following settings under **Permissions for <*your username*>**:

- **Execute Methods**
- **Enable Account**
- **Remote Enable**
- **Read Security**

19 Click the **Advanced** button.

20 In the **Advanced Security Settings for Root** dialog, select the entry that you just added (**sso_test** in this example) and then click the **Edit** button to launch the **Permission Entry for Root** dialog.

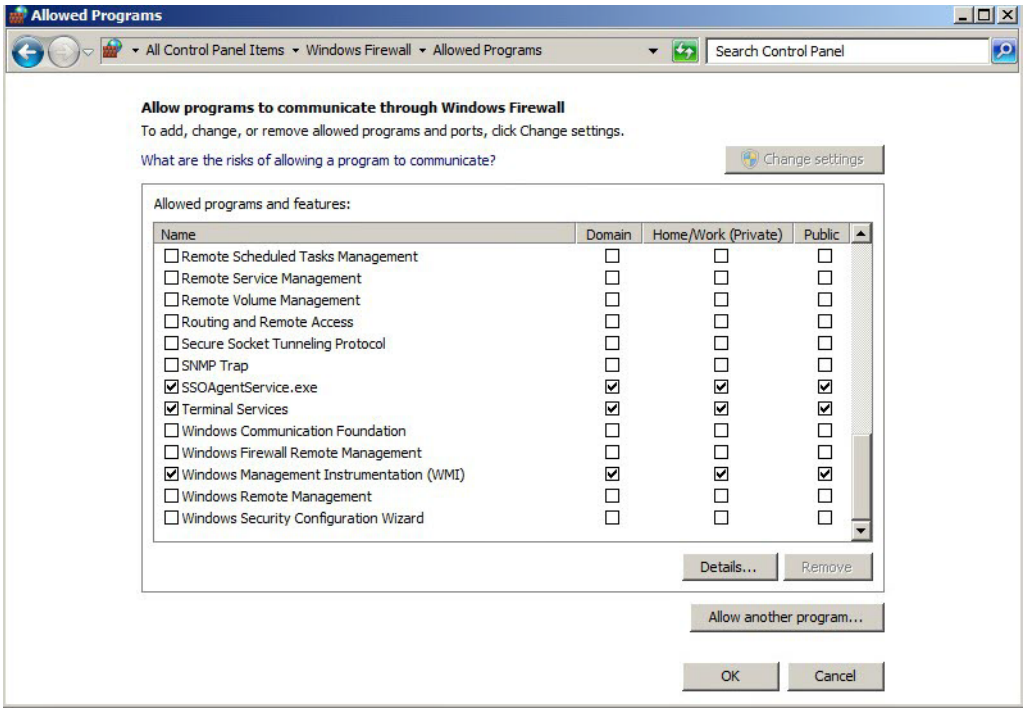
21 In the **Permission Entry for Root** dialog, select **This namespace and subnamespaces** from the **Apply to** drop-down list.



22 Click **OK** and then click **OK** in the parent dialogs.

23 Open the Windows Control Panel and navigate to **All Control Panel Items > Windows Firewall > Allowed Programs**.

24 Select all the checkboxes in the **Windows Management Instrumentation (WMI)** row (the checkboxes for **Domain**, **Home/Work (Private)**, and **Public**). This allows WMI traffic to pass through Windows Firewall.



Adding NetAPI Support

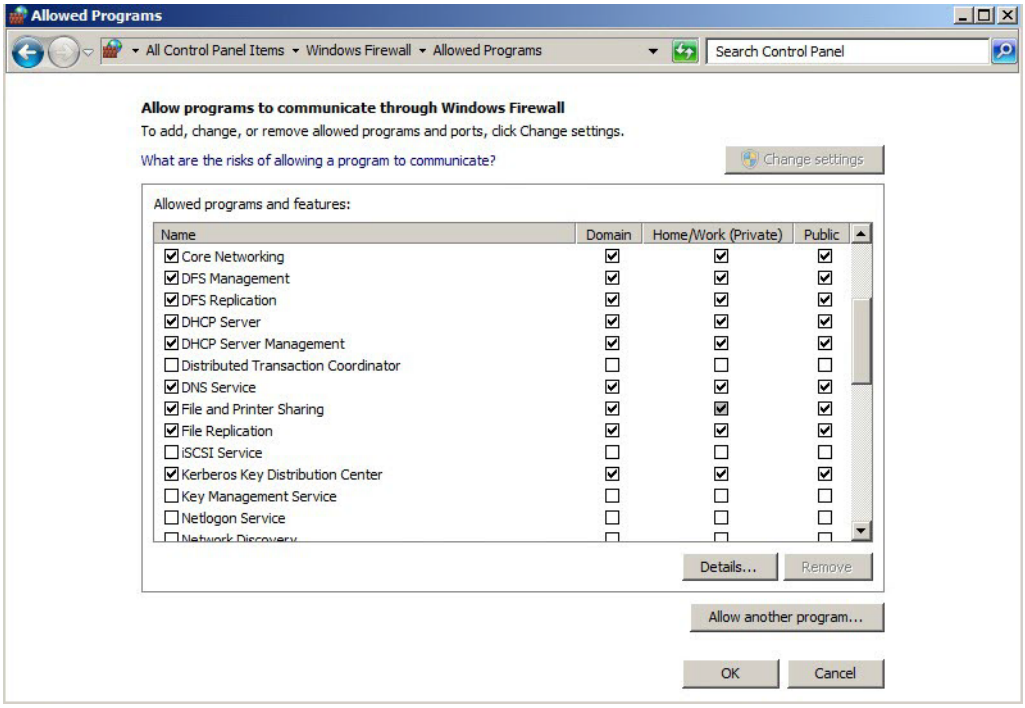
To support NetAPI, your *Domain\Username* needs to be added to the local Server Operator or Printer Operator group of each client machine, and if these two groups don't exist, your *Domain\Username* needs to be added to the Local Administrators group of each client machine. In addition, allow File and Printer Sharing traffic in Windows Firewall settings.

To allow SSO Agent to query information with this username using NetAPI from client machines:

1 Add your *Domain\Username* to the Server Operator, Printer Operator, or Local Administrators group on each client machine that will use NetAPI. In this example, **SSODC1\sso_test** needs to be added to the Server Operator, Printer Operator, or Local Administrators group.

2 Open **Windows Firewall > Allowed Programs** from the Control Panel and select all the checkboxes in the **File and Printer Sharing** row (the checkboxes for **Domain**, **Home/Work (Private)**, and **Public**).

This allows NetAPI traffic to pass through Windows Firewall.

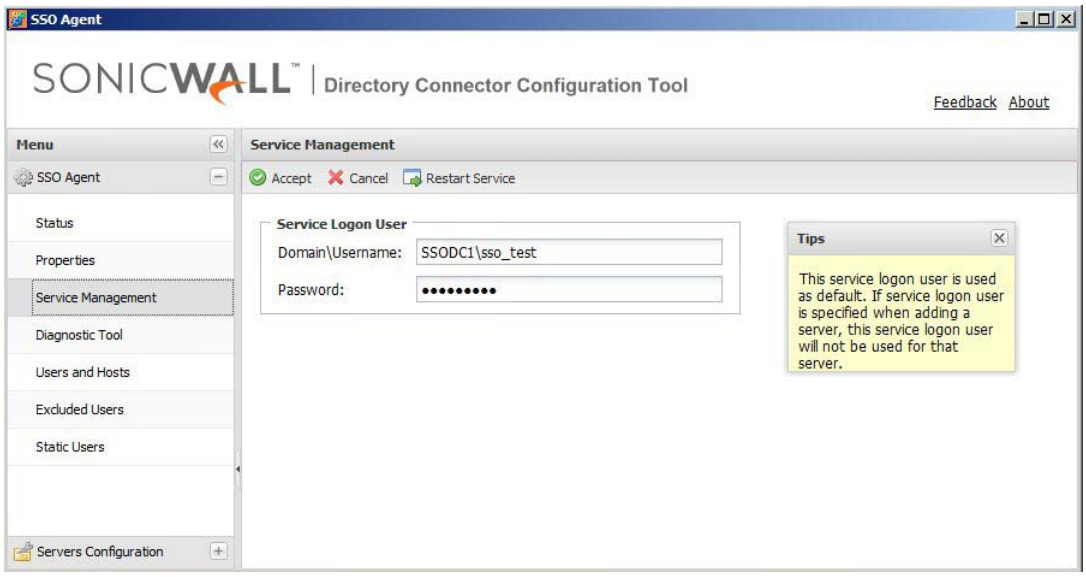


CAUTION: NetAPI has known security vulnerabilities on Windows and SonicWall does not recommend enabling it.

Configuring the SSO Agent

To configure the SSO Agent to use your minimum privilege account:

1. In the **Directory Connector Configuration Tool**, open the **Service Management** screen.
2. Add your *Domain\Username* in the **Domain\Username** field under **Service Logon User**. In this example, we add **SSODC1\sso_test**.



3 Enter the account password in the **Password** field.

> **CAUTION: For best security, the password should be a complex string of at least 20 characters using upper and lower case characters, numbers, and special characters.**

4 Restart the SSO Agent service. After configuring the **Service Logon User**, it is required to restart the SSO Agent service.

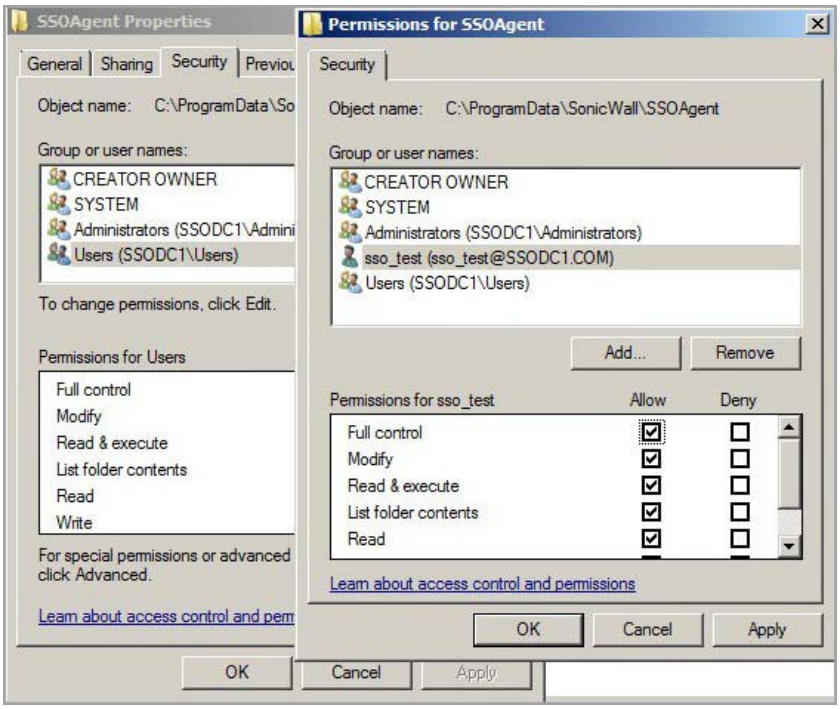
5 Navigate to the `C:\ProgramData\SonicWall` folder and right-click the `SSOAgent` folder, then select **Properties**.

6 In the **SSOAgent Properties** dialog, select the **Security** tab and then select **Users (*Domain*\Users)**.

7 Click **Edit**.

8 In the **Permissions for SSOAgent** dialog in the Group or user names section, add your minimum privileged *Username*. In this example, we add **sso_test**.

9 With your *Username* selected, select all the **Allow** checkboxes in the **Permissions for** *Username* section. This allows full control of the **C:\ProgramData\SonicWall\SSOAgent** folder.



> **NOTE:** If client machine is a server, querying users through WMI might fail.
>
> When a client machine cannot connect through WMI after applying the above settings, try restarting the client machine.

Setting Group Policy to Enable Audit Logon on Windows Server 2008

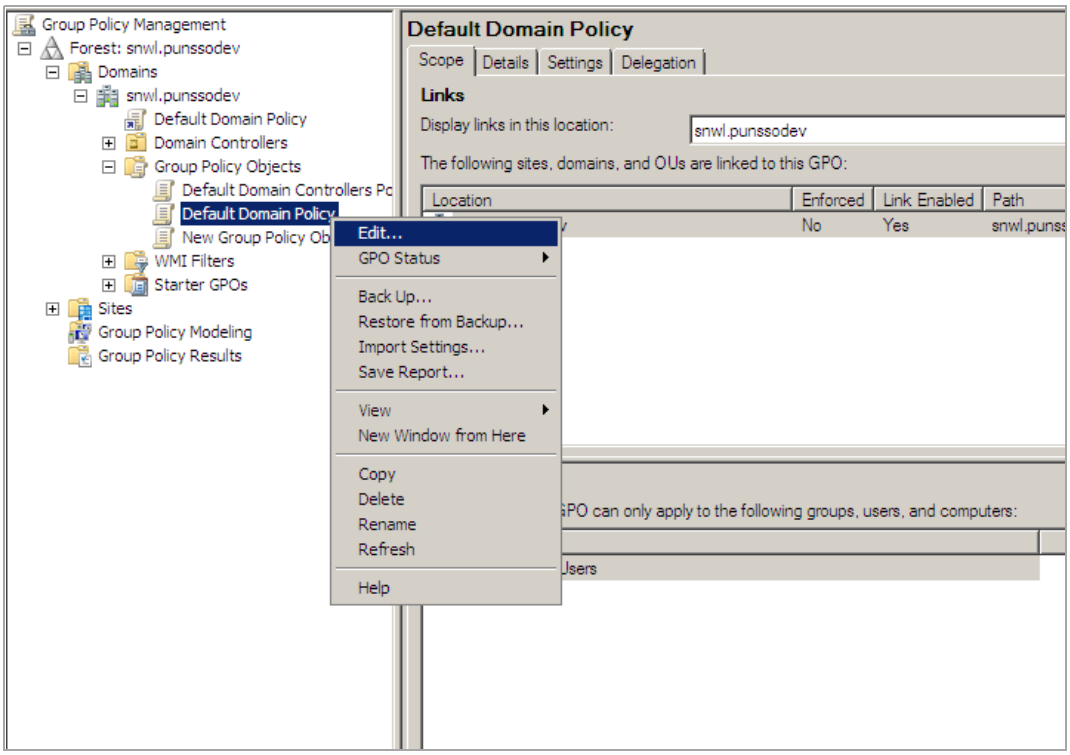
Audit Logon may need to be enabled on the Windows Server machine.

To enable Audit Logon on Windows Server 2008:

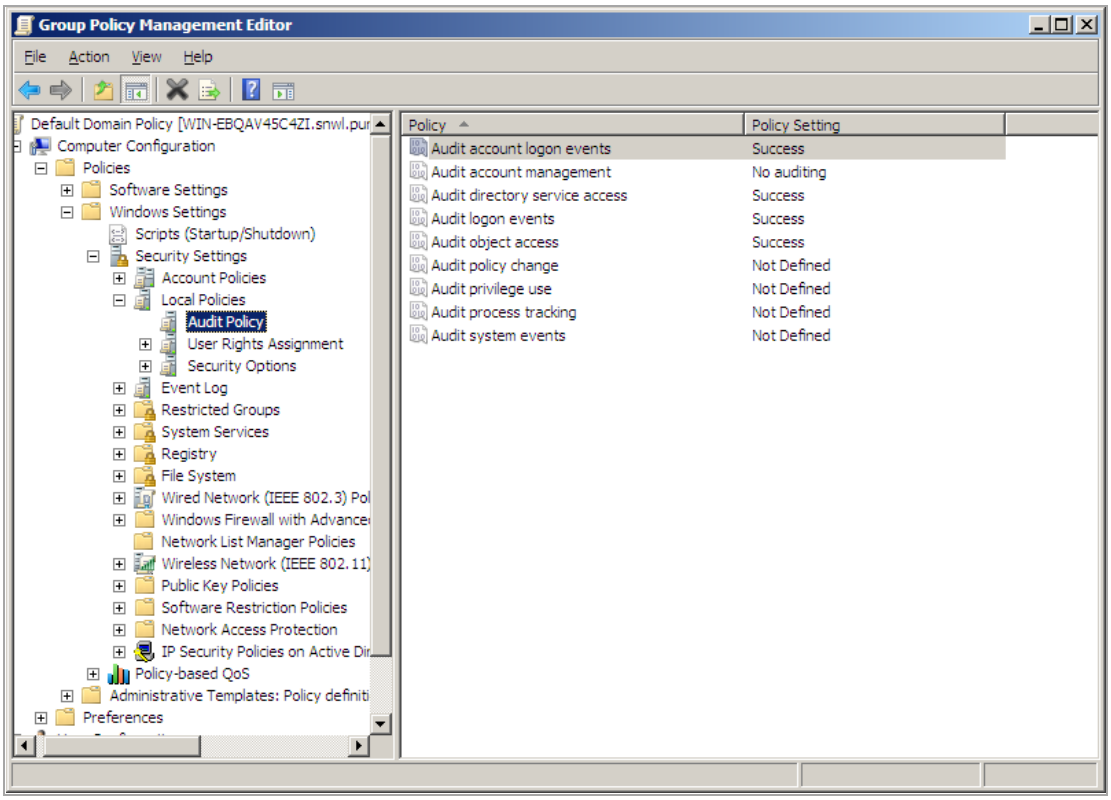
1 Start the Group Policy Management Console.

2 Browse to the following location: *Domain Name* > Domains > *Domain Name* > Group Policy Objects, where *Domain Name* is replaced with your domain.

3 Under **Group Policy Objects**, right-click on **Default Domain Policy**, and then select **Edit**.



The Group Policy Management Editor window displays.



4 Double-click on **Audit account logon events**, select **Success**, and then click **OK**.

5 Double-click on **Audit logon events**, select **Success**, and then click **OK**.

6 Double-click on **Audit Directory Service Access**, select **Success**, and then click **OK**.

7 Double-click on **Audit Object Access**, select **Success**, and then click **OK**.

8 Close the Group Policy window.

Setting Group Policy to Enable Audit Logon on Windows Server 2003

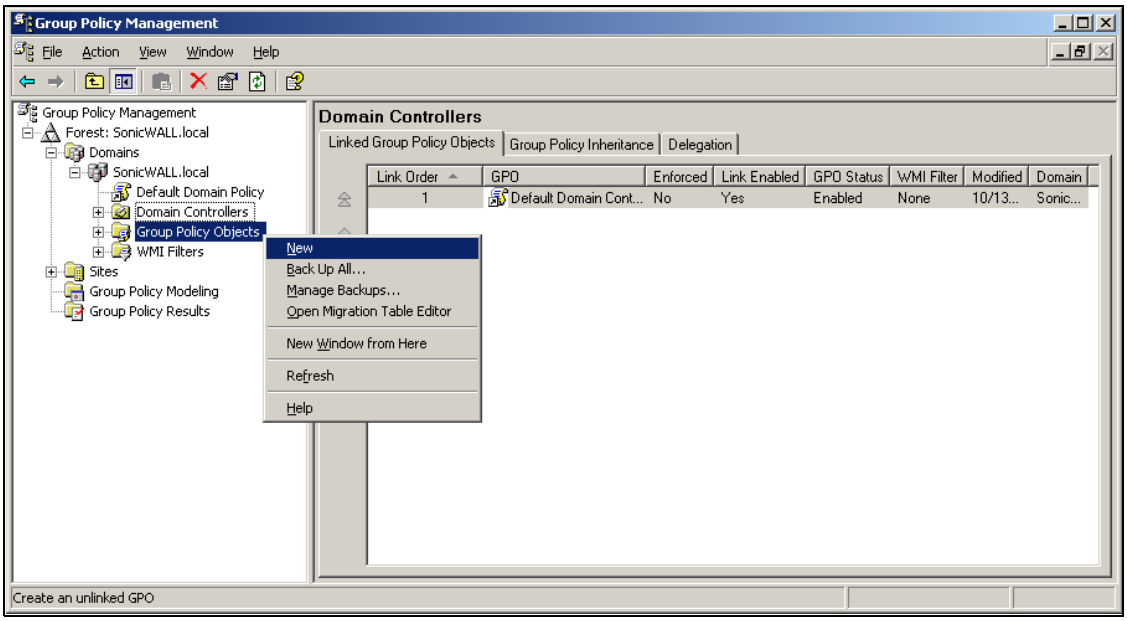
By default, Audit Logon is disabled on Windows Server 2003.

To enable Audit Logon on Windows Server 2003:

1 Start the Group Policy Management Console.

2 Browse to the following location: *Domain Name* > Domains > *Domain Name* > Group Policy Objects, where *Domain Name* is replaced with your domain.

3 Right-click on **Group Policy Objects**, and then select **New**.



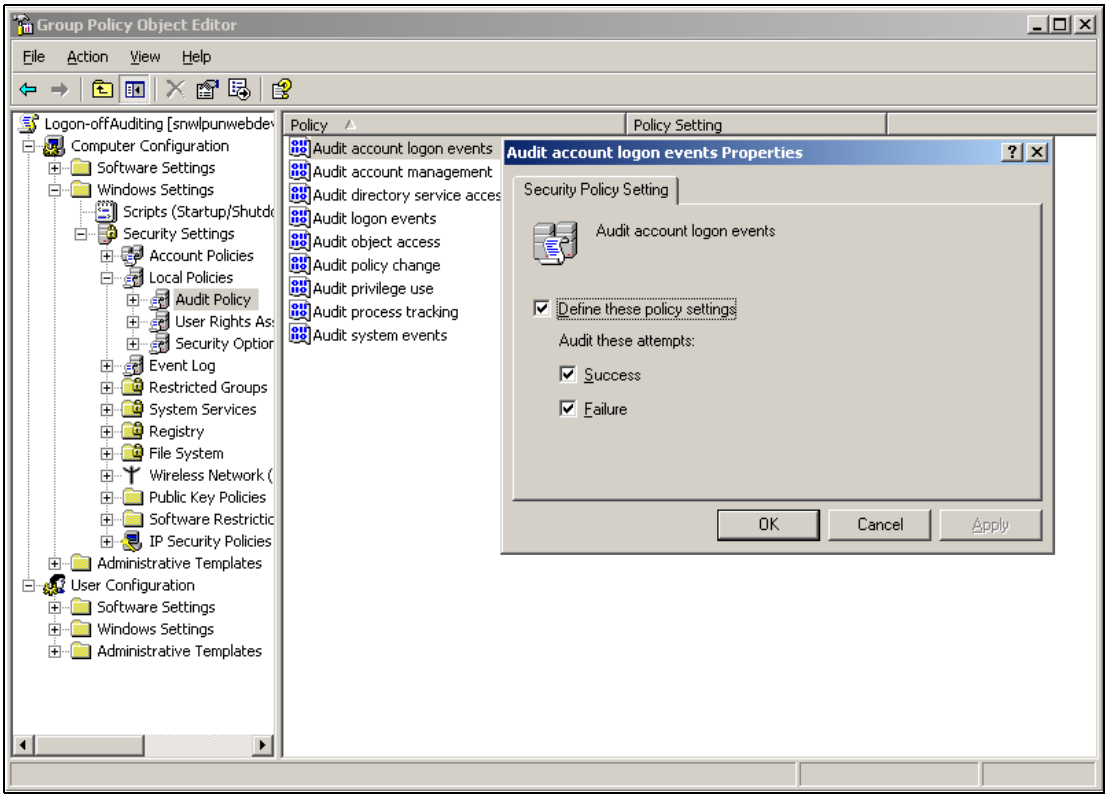
4 Enter a policy name, and then click **OK**.

5 Expand the **Group Policy Objects** folder and find your new policy.

6 Right-click on the policy, and then select **Edit**...

7 Browse to the following location: *`Policy Name`* `> Computer Configuration > Windows Settings > Security Settings > Local Policies > Audit Policy.`

8 Left-click on **Audit Policy**. The policy settings are displayed in the right pane.



9 Double-click on **Audit account logon events**, select **Success**, and then click **OK**.

10 Double-click on **Audit logon events**, select **Success**, and then click **OK**.

11 Double-click on **Audit Directory Service Access**, select **Success**, and then click **OK**.

12 Close the Group Policy window.

Configuring Terminal Servers

A terminal server uses Microsoft Windows Terminal Services / Remote Desktop Services (RDS) to provide separate desktop or application sessions to multiple logged in users. Terminal Server IP Virtualization makes it possible for the SSO Agent to uniquely identify each user on the terminal server, and is supported beginning in SonicWall Directory Connector with SSO 4.1. For more information, see About Terminal Servers on page 10.

NOTE: Terminal Servers are not supported by Directory Connector on Linux.

You can select **Terminal Servers** in the left pane of the Directory Connector Configuration Tool to display the **Host Address**, **Friendly Name**, and **Status** of the known terminal servers, along with edit and delete buttons in the **Configuration** column. Directory Connector provides the following functions for terminal servers:

- **Add**

  Select this option to add a terminal server to the SSO Agent configuration.

- **Config All**

  Select this option to configure the server monitoring method for all known terminal servers.

- **Refresh**

  Select this option to refresh the known terminal server information.

Topics:

Adding a Terminal Server

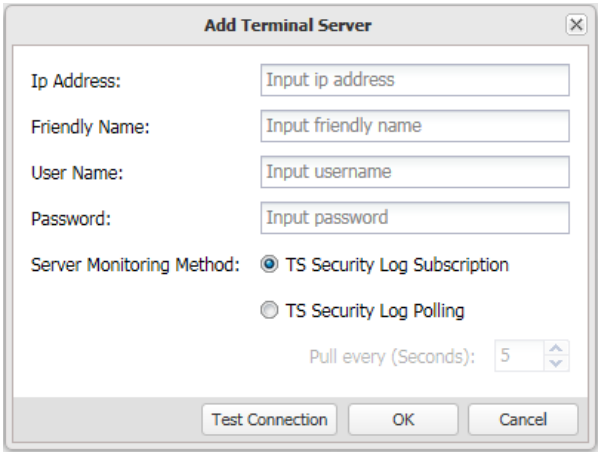
You can add terminal servers by entering a valid terminal server IP address and related information into the Directory Connector Configuration Tool.

When adding a terminal server, you can specify specific access credentials with the domainname\username and password. These credentials are independent of the Service Logon User name and do not have to be in the same domain. If this field is left empty, the service will use the Service Logon User name to access the terminal server.

To add a terminal server in Directory Connector:

1 Launch the Directory Connector Configuration Tool either from the Start menu or by double-clicking the desktop shortcut.

2 Select **Terminal Servers** in the left pane and then click the **Add** button at the bottom of the right pane. The **Add Terminal Server** dialog displays.



3 In the **Ip Address** field, type in the IP address of the terminal server to be added.

4 In the **Friendly Name** field, enter a descriptive name for the terminal server.

5 To access the terminal server using credentials that are different from the service logon credentials, enter the domain and user name in the form “domainname\username” into the **User Name** field, and enter the password into the **Password** field.

6 For **Server Monitoring Method**, select one of the following:

- **TS Security Log Subscription**

  You can select this method for getting terminal server event log updates if the terminal server and SSO Agent are installed on Windows machines that support the event subscription API. It is supported on Windows Server 2008 and higher.

- **TS Security Log Polling**

  This option causes the SSO Agent to request the event log information from the terminal server at the time interval indicated in the **Pull every** field. Accept the default of **5** seconds or type in the desired interval. The minimum is 5 seconds and the maximum is 300 seconds.

7 To test the connection to the terminal server using the configured IP address, click **Test Connection**.

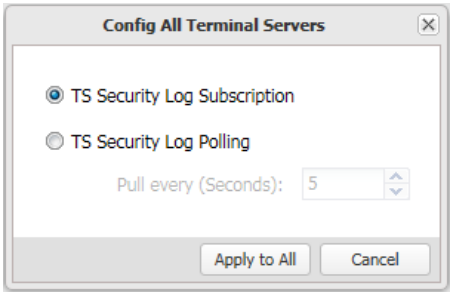
8 If no errors are displayed, click **OK**.

Configuring All Terminal Servers

To configure the server monitoring method for all known terminal servers:

1 In the Directory Connector Configuration Tool, select **Terminal Servers** in the left pane.

2 At the bottom of the right pane, click the **Config All** button. The Config All Terminal Servers dialog is displayed.



3 Select one of the following:

- **TS Security Log Subscription**

  You can select this method for getting terminal server event log updates if the terminal server and SSO Agent are installed on Windows machines that support the event subscription API. It is supported on Windows Server 2008 and higher.

- **TS Security Log Polling**

  This option causes the SSO Agent to request the event log information from the terminal server at the time interval indicated in the **Pull every** field. Accept the default of **5** seconds or type in the desired interval. The minimum is 5 seconds and the maximum is 300 seconds.

4 Click **Apply to All**.

5 Click **Yes** in the confirmation dialog.

Refreshing the Terminal Servers Display

To refresh the terminal server information:

1 In the Directory Connector Configuration Tool, select **Terminal Servers** in the left pane.

2 At the bottom of the right pane, click the **Refresh** button. The right pane displays the updated terminal server information.

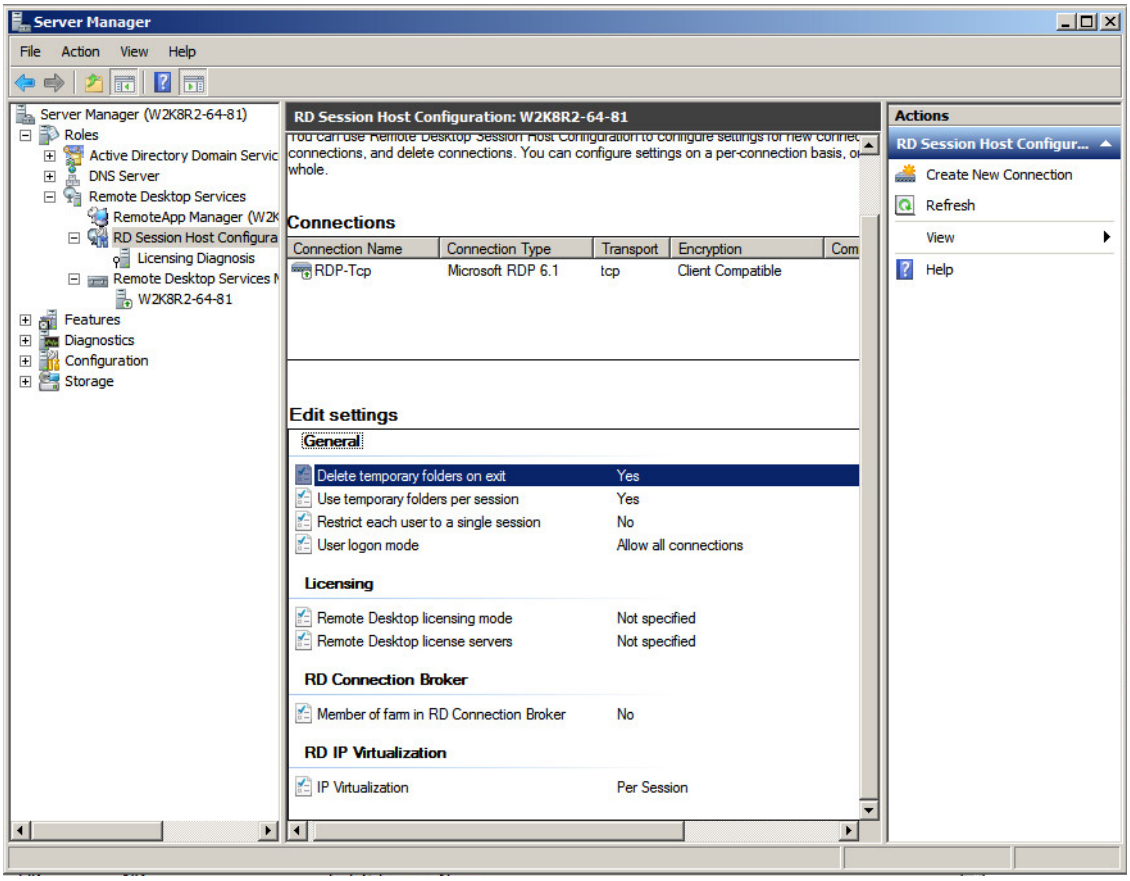
Enabling IP Virtualization in Windows Server 2008 R2

IP Virtualization must be enabled in Windows Server to properly identify users who are logged into a terminal server. Once a user logs into the terminal server with an RDP session, the Windows Server assigns a unique IP address to the session and logs an application event in the Windows event log. The SSO Agent reads the log remotely and notifies the firewall, allowing the user to be identified by SonicOS/X.

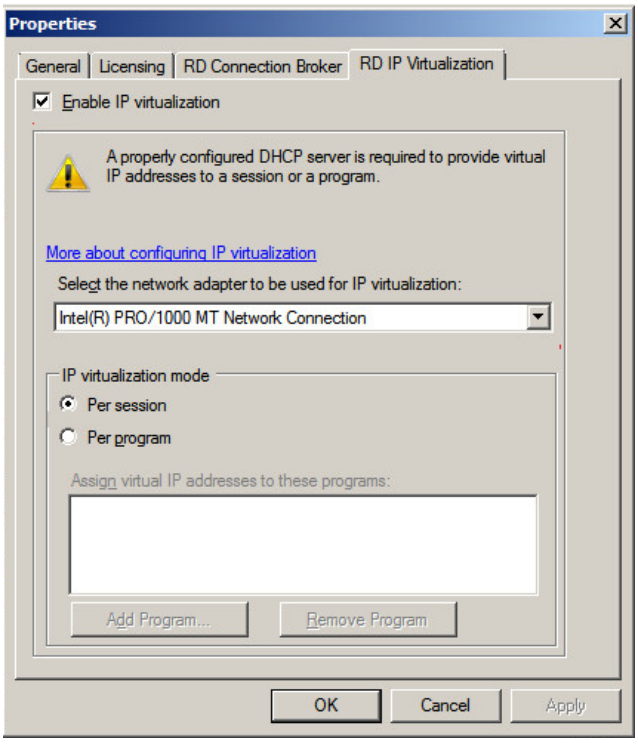
To enable IP Virtualization in Windows Server 2008 R2:

1 On the Terminal Server (on Windows Server 2008 R2), open the **Server Manager**.

2 Navigate to **Roles > Remote Desktop Services > RD Session Host Configuration**.



3 Double-click on **IP Virtualization** near the bottom to open the **Properties** window.



4 On the **RD IP Virtualization** tab, select the **Enable IP virtualization** checkbox.

5 Select the correct network adapter from the **Select the network adapter to be used for IP virtualization** drop-down list.

6 Under **IP virtualization mode**, select the **Per session** option.

7 Click **OK**.

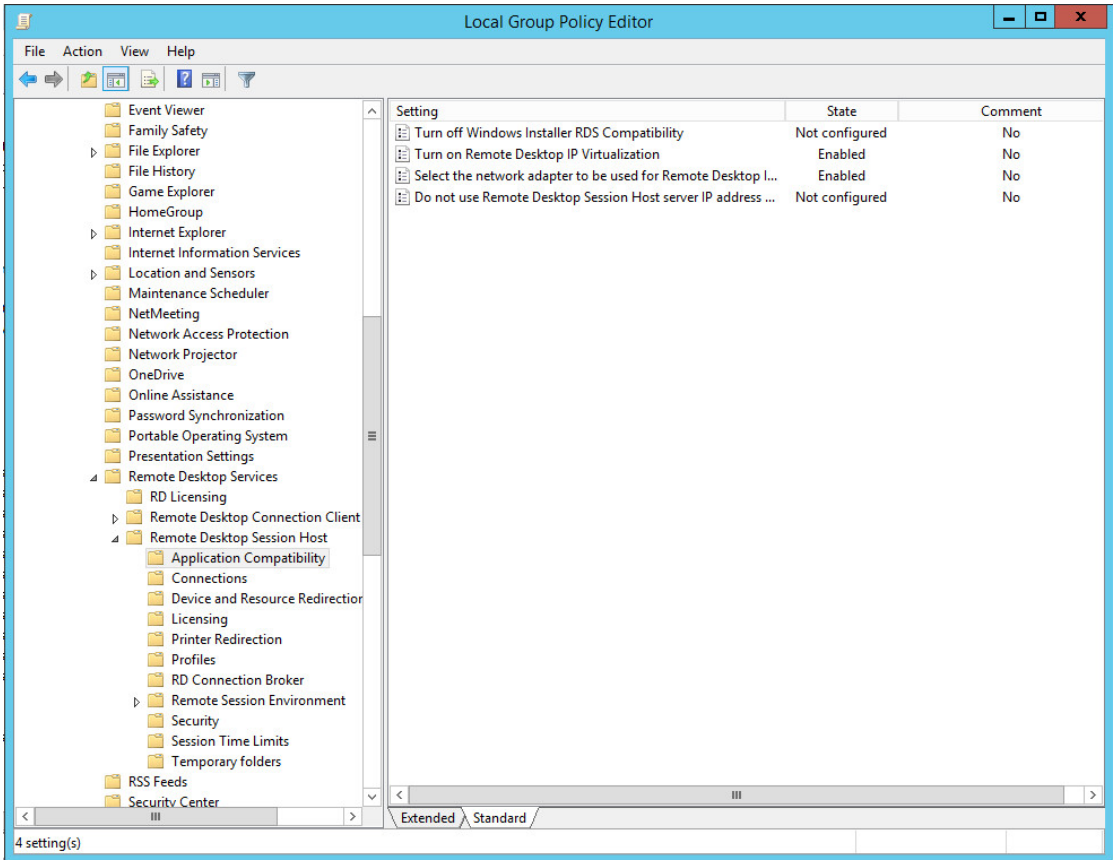
Enabling IP Virtualization in Windows Server 2012

The Remote Desktop Session Host Configuration MMC has been removed in Windows Server 2012. The way to enable RDS IP Virtualization is to edit group policy.

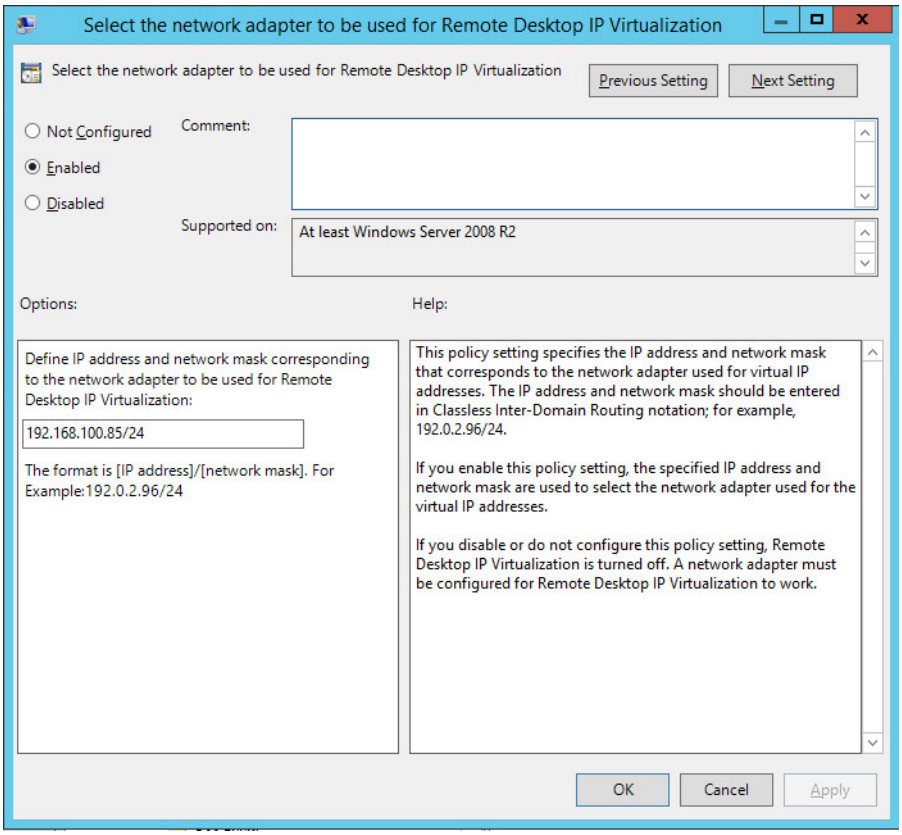
To enable IP Virtualization in Windows Server 2012:

1 On the Terminal Server (on Windows Server 2012), open the **Local Group Policy Editor**.

2 Navigate to **Computer Configuration > Administrative Templates > Windows Components > Remote Desktop Service > Application Compatibility**.



3 Double-click **Select the network adapter to be used for Remote Desktop IP Virtualization**. The dialog box opens.

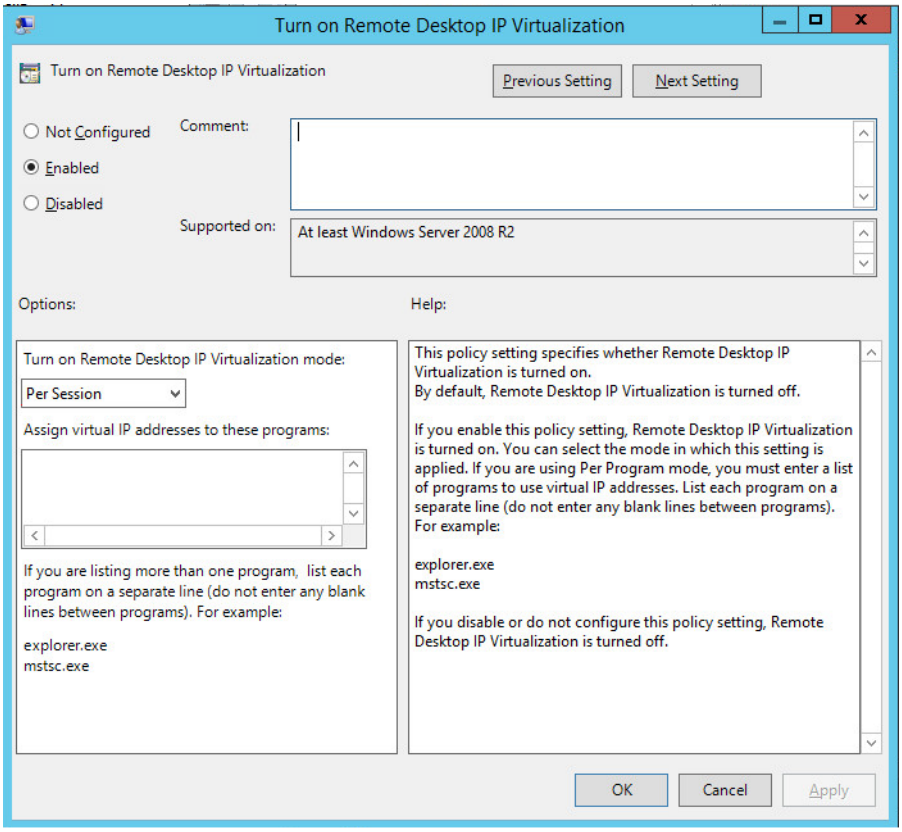


4 In the **Select the network adapter to be used for Remote Desktop IP Virtualization** dialog box, select **Enabled**.

5 Under **Options**, enter the IP address and network mask corresponding to the network adapter.

6 Click **OK** to accept the settings and return to the previous screen.

7 Double-click **Turn on Remote Desktop IP Virtualization**. The dialog box opens.



8 In the **Turn on Remote Desktop IP Virtualization** dialog box, select **Enabled**.

9 Under **Options**, select **Per Session** from the drop-down list for **Remote Desktop IP Virtualization mode**.

10 Click **OK**.

11 Continue as described in the following sections:

- Creating IP Address Pools in Window Server 2012 on page 70
- Verifying IP Virtualization in Window Server 2012 on page 73

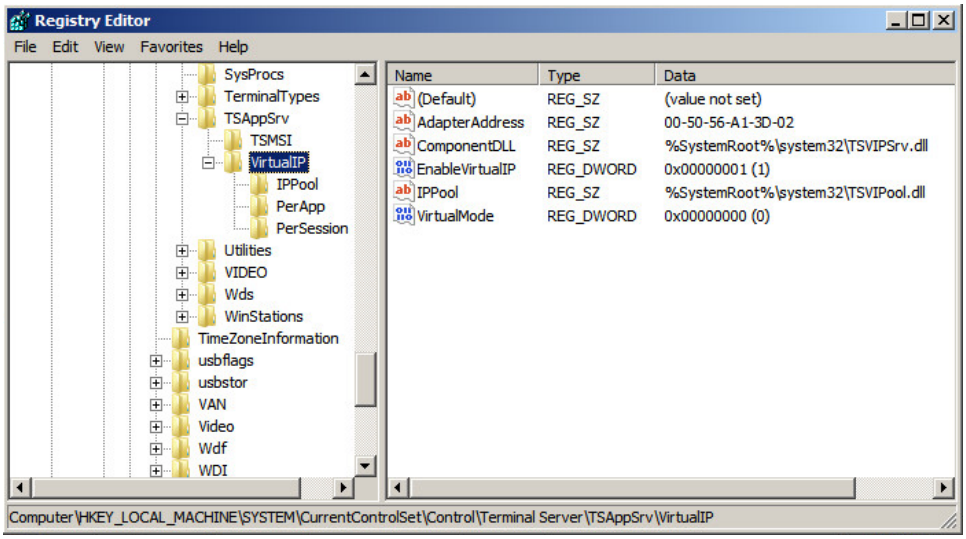
Creating IP Address Pools in Window Server 2012

Next for IP virtualization, you need to create an IP address pool. The IP pool can either be static or dynamic. For a static IP pool, you use *regedit*.

For a dynamic IP pool, you need to configure a DHCP server in your domain and ensure enough IP addresses. In this case, there is no need to create an IP pool for every Terminal Server.

To create a static IP address pool:

1 On the Terminal Server (Windows Server 2012), open **regedit.exe** and go to **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\TerminalServer\TSAPPSrv\VirtualIP**.



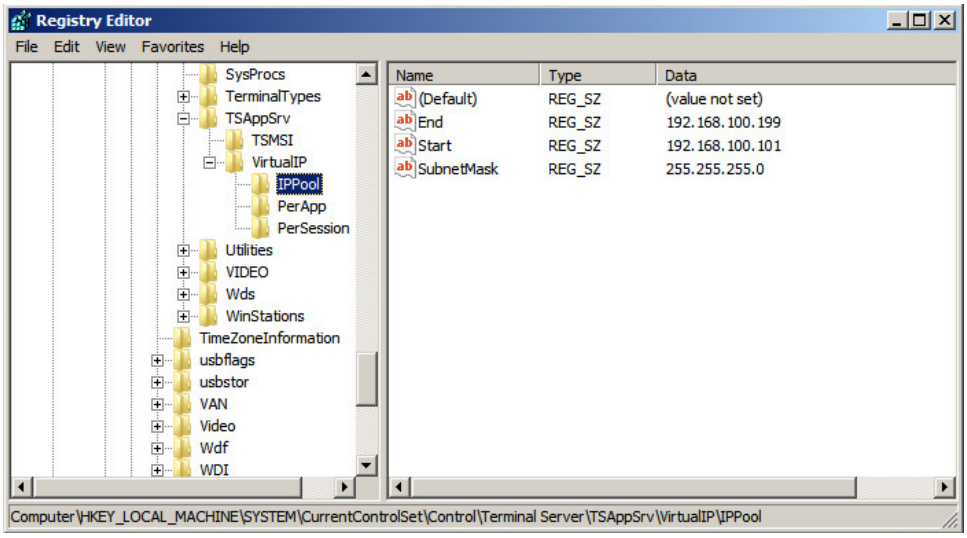
2 Add a string value: `"IPPool" = "%SystemRoot%\system32\TSVIPool.dll"`.

3 Add a new key, `IPPool`, and three string values:

`"Start" = IP range start`

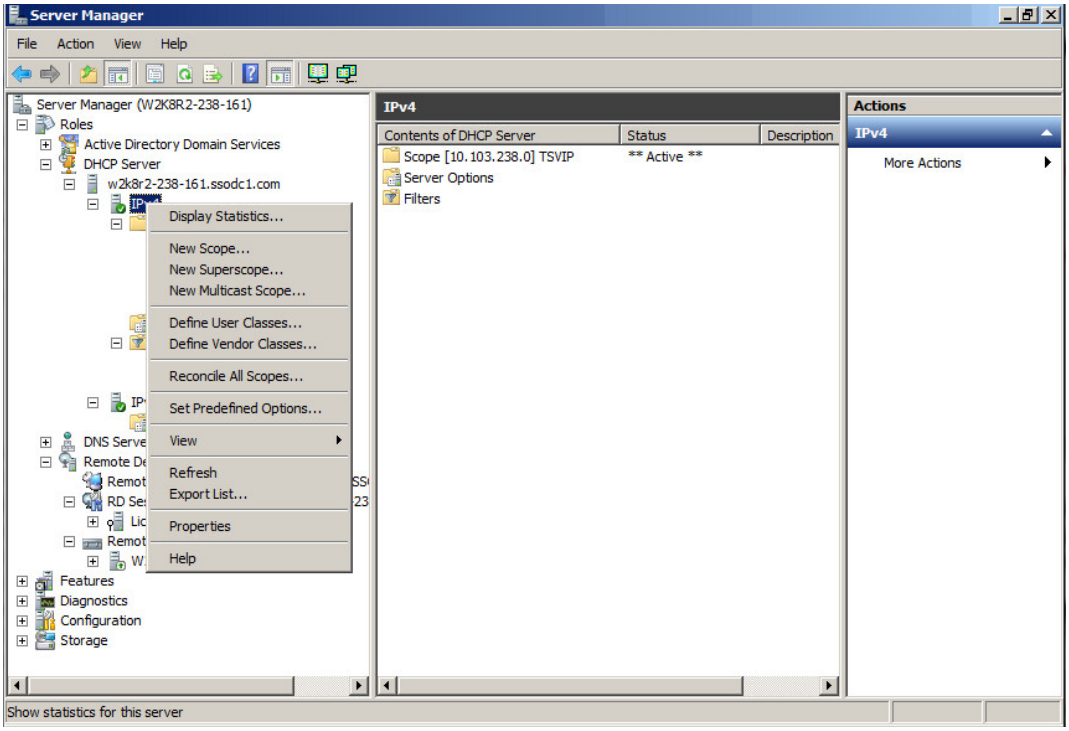
`"End" = IP range end`

`"SubnetMask" = IP subnet mask`



To create a dynamic IP address pool:

1 Open the **Server Manager** and go to **Roles > DHCP Server > *Domain Name* > IPv4**.



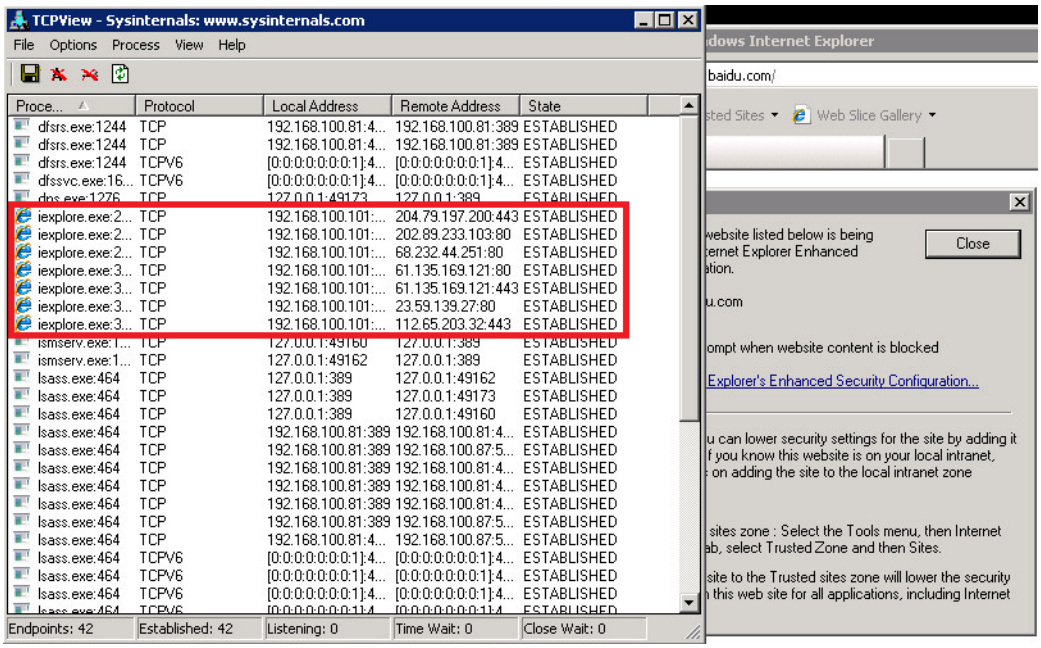
2 Right-click **IPv4** and select **New Scope** to create a scope for distributing enough IP addresses.

3 Use the wizard to set **scope name**, **IP address range**, **Exclusions**, **lease duration**, **default gateway**, **DNS servers** and **domain name**.

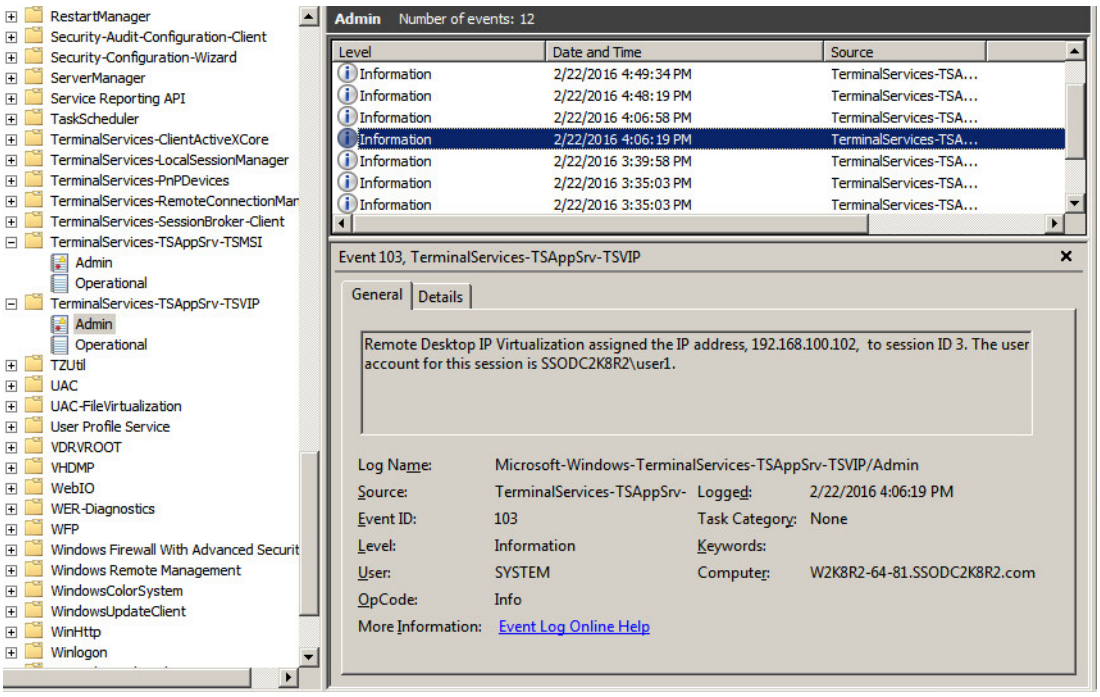
Verifying IP Virtualization in Window Server 2012

To verify that IP virtualization is working:

1 Do an RDP login from another computer to verify the IP virtualization is working. If it is working, you will see, for example, that all the TCP connections are from 192.168.100.101 instead of 192.168.100.81.



2 Check the logs on the Terminal Server at **Microsoft-Windows-TerminalServices-TSAppSrv-TSVIP/Admin**. Information is logged there when a user logs in or logs off. The SSO Agent can read events from this log and notify the firewall of the user IP address.



Configuring Exchange Server Settings

You can select **Exchange Servers** in the left pane of the Directory Connector Configuration Tool to display the **Friendly Name**, **IP** address, and **Status** of the known Exchange servers, along with edit and delete buttons in the **Configuration** column. Directory Connector provides the following functions for Exchange servers:

- **Add**

  Select this option to add an Exchange server to the SSO Agent configuration.

- **Config All**

  Select this option to configure the server monitoring method for all known Exchange servers.

- **Refresh**

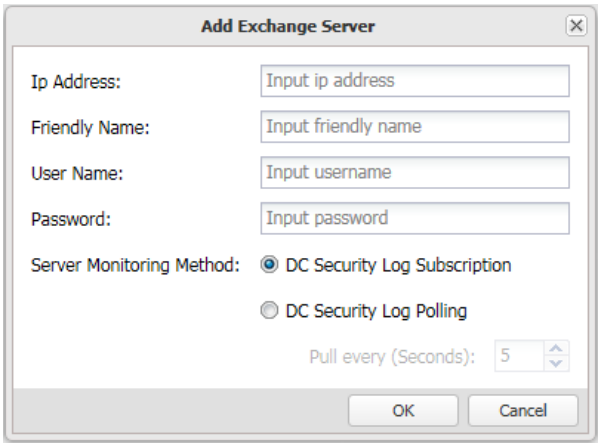
  Select this option to refresh the known Exchange server information.

For information about using an Exchange server to identify users, see About Exchange Servers on page 10.

To add an Exchange server for use by the SSO Agent:

1 Launch the Directory Connector Configuration Tool either from the Start menu or by double-clicking the desktop shortcut.

2 Select **Exchange Servers** in the left pane and then click the **Add** button at the bottom of the right pane. The **Add Exchange Server** dialog displays.



3 In the **Ip Address** field, type in the IP address of the Exchange server to be added.

4 In the **Friendly Name** field, enter a descriptive name for the Exchange server.

5 To access the Exchange server using credentials that are different from the service logon credentials, enter the domain and user name in the form “domainname\username” into the **User Name** field, and enter the password into the **Password** field.

6 For **Server Monitoring Method**, select one of the following:

7 For **Server Monitoring Method**, select one of the following methods for the SSO Agent to get the event logs from the server:

- **Use Event Subscription**

  This method causes the SSO Agent to request that the Exchange server automatically send any relevant events to the Agent as they occur.

- **Pull every <> seconds**

  This is the polling method. The SSO Agent requests information from the Exchange server at the configured interval.

  If **Pull every <> seconds** is selected, accept the default polling interval of **10** seconds or type in the desired interval in the provided field. The minimum is 1 second and the maximum is 60 seconds.

NOTE: You can configure the **Server Monitoring Method** for all known Exchange servers at the same time by selecting **Config All**.

8 Click **OK**.

Configuring Novell eDirectory Settings

You can select **Novell eDirectory Servers** in the left pane of the Directory Connector Configuration Tool to display the **Server Address**, **UserDN**, **BaseDN**, **Polling Interval**, and **Status** of the known eDirectory servers, along with edit and delete buttons in the **Configuration** column. Directory Connector provides the following functions for eDirectory servers:

- **Add**

  Select this option to manually add an eDirectory server to the SSO Agent configuration.

- **Refresh**

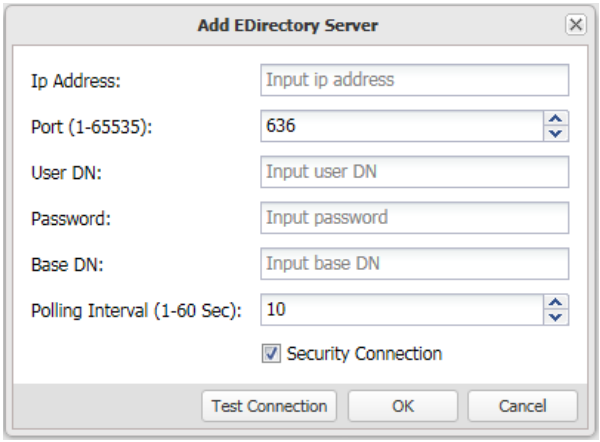
  Select this option to refresh the known eDirectory server information.

For information about using Novell eDirectory to identify users, see About Novell eDirectory on page 10.

To add a Novell eDirectory Server and configure eDirectory settings:

1 Launch the Directory Connector Configuration Tool either from the Start menu or by double-clicking the desktop shortcut.

2 Select **Novell eDirectory Servers** in the left pane and then click the **Add** button at the bottom of the right pane. The **Add EDirectory Server** dialog displays.



3 In the **Ip Address** field, type in the IP address of the Novell eDirectory server to be added.

4 In the **Port (1-65535)** field, type in the port for the service. The default port is:

- **636** if the **Security Connection** checkbox is selected.
- **389** if the **Security Connection** checkbox is not selected.

5 In the **User DN** field, type in the service user's domain name.

The **User DN** is case sensitive and should be entered in the following format:

`cn=xxx,o=xxx`

For example: `cn=admin, o=test`

6 In the **Password** field, type in the password for the service user.

7 In the **Base DN** field, type in the base domain name.

The **Base DN** is case sensitive and should be entered in the following format:

`o=xxx`

For example: `o=test`

8 In the **Polling Interval (1-60 Sec)** field, type in the number of seconds for the polling interval. The default value is **10** seconds, the minimum is 1 second, and the maximum is 60 seconds.

9 Click the **Test Connection** button to verify that the SSO Agent can connect with the eDirectory server.

10 Click **OK**.

Configuring Remote SSO Agents

A Single Sign-On deployment can contain up to eight SSO Agents on different servers. Each instance of the SSO Agent can exchange information with the other, remote Agents.

You can select **Remote SSO Agents** in the left pane of the Directory Connector Configuration Tool to display the **Friendly Name**, **IP** address, synchronization **Port**, and **Status** of the known remote SSO Agents, along with edit and delete buttons in the **Configuration** column. Directory Connector provides the following functions for remote SSO Agents:

- **Add**

  Select this option to add a remote SSO Agents to the SSO Agent configuration.

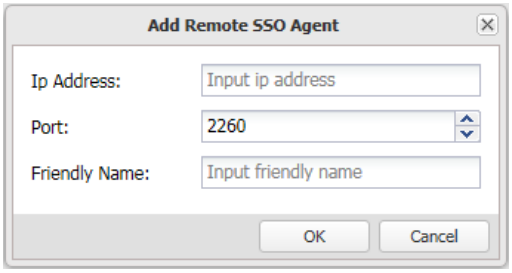
- **Refresh**

  Select this option to refresh the known remote SSO Agent information.

To configure remote SSO Agents in Directory Connector:

1 Launch the Directory Connector Configuration Tool either from the Start menu or by double-clicking the desktop shortcut.

2 Select **Remote SSO Agents** in the left pane and then click the **Add** button at the bottom of the right pane. The **Add Remote SSO Agent** dialog displays.



3 In the **Ip Address** field, type in the IP address of the remote SSO Agent to be added.

4 In the **Port** field, accept the default of **2260** or type in the custom synchronization port.

By default, the SSO Agent uses TCP port **2260** to receive the Agent synchronization data. When an SSO Agent starts up, it sends a TCP Reset notification to all the configured remote Agents. When a remote Agent receives this reset notification, it sends its user cache to the requesting Agent. Thereafter, the remote Agent sends any incremental changes.

5 In the **Friendly Name** field, type in a descriptive name for the remote SSO Agent.

6 Click **OK**.

Part 3

Appendices

- Licensing Information
- SonicWall Support

A

Licensing Information

Topics:

Open Source Code

SonicWall is able to provide a machine-readable copy of open source code with restrictive licenses such as GPL, LGPL, AGPL when applicable per license requirements. To obtain a complete machine-readable copy, send your written request, along with certified check or money order in the amount of US 25.00 payable to “SonicWall Inc.”, to:

General Public License Source Code Request
SonicWall Inc. Attn: Jennifer Anderson
1033 McCarthy Blvd
Milpitas, CA 95035

SonicWall End User Product Agreement

Revised 10 February 2017

PLEASE READ THIS AGREEMENT CAREFULLY BEFORE USING THIS PRODUCT. BY DOWNLOADING, INSTALLING OR USING THIS PRODUCT, YOU ACCEPT AND AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT. FOR DELIVERIES OUTSIDE THE UNITED STATES OF AMERICA, PLEASE GO TO HTTPS://WWW.SONICWALL.COM/LEGAL/EUPA.ASPX TO VIEW THE APPLICABLE VERSION OF THIS AGREEMENT FOR YOUR REGION. IF YOU DO NOT AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT OR THE APPLICABLE VERSION OF THIS AGREEMENT FOR YOUR REGION, DO NOT DOWNLOAD, INSTALL OR USE THIS PRODUCT.

This SonicWall End User Product Agreement (the "***Agreement***") is made between you, the Customer ("**Customer**" or "**You**") and the Provider, as defined below.

1.**Definitions**. Capitalized terms not defined in context shall have the meanings assigned to them below:

(a)"**Affiliate**" means any legal entity controlling, controlled by, or under common control with a party to this Agreement, for so long as such control relationship exists.

(b)"**Appliance**" means a computer hardware product upon which Software is pre-installed and delivered.

(c)"**Documentation**" means the user manuals and documentation that Provider makes available for the Products, and all copies of the foregoing.

(d) "**Maintenance Services**" means Provider's maintenance and support offering for the Products as identified in the Maintenance Services Section below.

(e)"**Partner**" means the reseller or distributor that is under contract with Provider or another Partner and is authorized via such contract to resell the Products and/or Maintenance Services.

(f)"**Provider**" means, (i) for the US, Europe, Middle East, Africa, Latin America, and Taiwan, SonicWall Inc., with its principal place of business located at 4 Polaris Way, Aliso Viejo, CA 92656 USA and (ii) for Asia (other than Taiwan) SonicWall International Ltd. City Gate Park Mahon, Cork, Ireland.

(g)"**Products**" means the Software and Appliance(s) provided to Customer under this Agreement.

(h)"**Software**" means the object code version of the software that is delivered on the Appliance and any other software that is later provided to Customer as well as any new versions and releases to such software that are made available to Customer pursuant to this Agreement, and all copies of the foregoing.

2.**Software License.**

(a)**General**. Subject to the terms of this Agreement, Provider grants to Customer, and Customer accepts from Provider, a non-exclusive, non-transferable (except as otherwise set forth herein) and non-sublicensable license to access and use the quantities of each item of Software purchased from Provider or a Partner within the parameters of the license type ("**License Type(s)**") described below in the quantities purchased ("License"). Except for MSP Licenses (as defined below), Customer shall only use the Software to support the internal business operations of itself and its worldwide Affiliates.

(b) **License Types.** The License Type for the Software initially delivered on the Appliance is "***per Appliance***". Software licensed per Appliance may be used only on the Appliance on which it is delivered, but without any other quantitative limitations. Software that is purchased on a subscription, or periodic basis is licensed by User or by Managed Node. A "**User**" is each person with a unique login identity to the Software. A "**Managed Node**" is any object managed by the Software including, but not limited to firewalls, devices, and other items sold by Provider.

(c)**Software as a Service.** When Customer purchases a right to access and use Software installed on equipment operated by Provider or its suppliers (the "***SaaS Software***"), (i) the License for such SaaS Software shall be granted for the duration of the term stated in the order (the "***SaaS Term***"), as such SaaS Term may be extended by automatic or agreed upon renewals, and (ii) the terms set forth in the SaaS Provisions Section of this Agreement shall apply to all access to and use of such Software. If any item of Software to be installed on Customer's equipment is provided in connection with SaaS Software, the License duration for such Software shall be for the corresponding SaaS Term, and Customer shall promptly install any updates to such Software as may be provided by Provider.

(d)**MSP License.**

"***Management Services***" include, without limitation, application, operating system, and database implementation, performance tuning, and maintenance services provided by Customer to its customers (each, a "***Client***") where Customer installs copies of the Software on its Clients' equipment or provides its Clients access to the Products. Customer shall be granted a License to use the Software and the associated Documentation to provide Management Services (the "***MSP License***"). Each MSP License is governed by the terms of this Agreement and any additional terms agreed to by the parties.

If the Product is to be used by Customer as a managed service provider, then Customer shall ensure that (i) Customer makes no representations or warranties related to the Products in excess of SonicWall's representations or warranties contained in this Agreement, (ii) each Client only uses the Products and Documentation as part of the Management Services provided to it by Customer, (iii) such use is subject to the restrictions and limitations contained in this Agreement, including, but not limited to those in the Export Section of this Agreement, and (iv) each Client cooperates with Provider during any compliance review that may be conducted by Provider or its designated agent. At the conclusion of any Management Services engagement with a Client, Customer shall promptly remove any Appliance and Software installed on its Client's computer equipment or require the Client to do the same. Customer agrees that it shall be jointly and severally liable to Provider for the acts and omissions of its Clients in connection with their use of the Software and Documentation and shall, at its expense, defend Provider against any action, suit, or claim brought against Provider by a Client in connection with or related to Customer's Management Services and pay any final judgments or settlements as well as Provider's expenses in connection with such action, suit, or claim.

(e)**Evaluation/Beta License.** If Software is obtained from Provider for evaluation purposes or in beta form, Customer shall be granted a License to use such Software and the associated Documentation solely for Customer's own non-production, internal evaluation purposes (an "***Evaluation License***"). Each Evaluation License shall be granted for an evaluation period of up to thirty (30) days beginning (i) five (5) days after the Appliance is shipped or (ii) from the date that access is granted to the beta Software or the SaaS Software, plus any extensions granted by Provider in writing (the "Evaluation Period"). There is no fee for an Evaluation License during the Evaluation Period, however, Customer is responsible for any applicable shipping charges or taxes which may be incurred, and any fees which may be associated with usage beyond the scope permitted herein. Beta Software licensed hereunder may include pre-release features and capabilities which may not be available in SonicWall's generally available commercial versions of the Software. SonicWall retains the right during the term of the Evaluation License to modify, revise, or remove SonicWall beta software from Customer's premises. Customer acknowledges that SonicWall owns all modifications, derivative works, changes, expansions or improvements to beta software, as well as all reports, testing data or results, feedback, benchmarking or other analysis completed in whole or in part in conjunction with usage of beta software. NOTWITHSTANDING ANYTHING OTHERWISE SET FORTH IN THIS AGREEMENT, CUSTOMER UNDERSTANDS AND AGREES THAT EVALUATION AND BETA SOFTWARE IS PROVIDED "AS IS", WHERE IS, WITH ALL FAULTS AND THAT SONICWALL DOES NOT PROVIDE A WARRANTY OR MAINTENANCE SERVICES FOR EVALUATION OR BETA LICENSES, AND SONICWALL BEARS NO LIABILITY FOR ANY DIRECT, INDIRECT, INCIDENTAL, PUNITIVE, SPECIAL OR CONSEQUENTIAL DAMAGES RESULTING FROM USE (OR ATTEMPTED USE) OF THE EVALUATION OR BETA SOFTWARE THROUGH AND AFTER THE EVALUATION PERIOD AND HAS NO DUTY TO PROVIDE SUPPORT TO CUSTOMER FOR SUCH SOFTWARE. BETA SOFTWARE MAY CONTAIN DEFECTS AND A PRIMARY PURPOSE OF LICENSING THE BETA SOFTWARE IS TO OBTAIN FEEDBACK ON THE BETA SOFTWARE'S PERFORMANCE AND THE IDENTIFICATION OF DEFECTS. CUSTOMER IS ADVISED TO SAFEGUARD IMPORTANT DATA, TO USE CAUTION AND NOT TO RELY IN ANY WAY ON THE CORRECT FUNCTIONING OR PERFORMANCE OF THE BETA SOFTWARE AND/OR ACCOMPANYING MATERIALS.

(f)**Use by Third Parties.** Customer may allow its services vendors and contractors (each, a "**Third Party User**") to access and use the Products and Documentation provided to Customer hereunder solely for purposes of providing services to Customer, provided that Customer ensures that (i) the Third Party User's access to or use of the Products and Documentation is subject to the restrictions and limitations contained in this Agreement, including, but not limited to those in the Export Section, (ii) the Third Party User cooperates with Provider during any compliance review that may be conducted by Provider or its designated agent, and (iii) the Third Party Users promptly removes any Software installed on its computer equipment upon the completion of the Third Party's need to access or use the Products as permitted by this Section. Customer agrees that it shall be liable to Provider for those acts and omissions of its Third Party Users which, if done or not done by Customer, would be a breach of this Agreement.

3. **Restrictions**. Customer may not reverse engineer, decompile, disassemble, or attempt to discover or modify in any way the underlying source code of the Software, or any part thereof unless and to the extent (a) such restrictions are prohibited by applicable law and (b) Customer has requested interoperability information in writing from Provider and Provider has not provided such information in a timely manner. In addition, Customer may not (i) modify, translate, localize, adapt, rent, lease, loan, create or prepare derivative works of, or create a patent based on the Products, Documentation or any part thereof, (ii) resell, sublicense or distribute the Products or Documentation, (iii) provide, make available to, or permit use of the Products, in whole or in part, by any third party (except as expressly set forth herein), (iv) use the Products or Documentation to create or enhance a competitive offering or for any other purpose which is competitive to Provider, (v) remove Software that was delivered on an Appliance from the Appliance on which it was delivered and load such Software onto a different appliance without Provider's prior written consent, or (vi) perform or fail to perform any other act which would result in a misappropriation or infringement of Provider's intellectual property rights in the Products or Documentation. Each permitted copy of the Software and Documentation made by Customer hereunder must contain all titles, trademarks, copyrights and restricted rights notices as in the original. Customer understands and agrees that the Products may work in conjunction with third party products and Customer agrees to be responsible for ensuring that it is properly licensed to use such third party products. Notwithstanding anything otherwise set forth in this Agreement, the terms and restrictions set forth herein shall not prevent or restrict Customer from exercising additional or different rights to any open source software that may be contained in or provided with the Products in accordance with the applicable open source software licenses which shall be either included with the Products or made available to Customer upon request. Customer may not use any license keys or other license access devices not provided by Provider, including but not limited to "pirate keys", to install or access the Software.

4.**Proprietary Rights.** Customer understands and agrees that (i) the Products are protected by copyright and other intellectual property laws and treaties, (ii) Provider, its Affiliates and/or its licensors own the copyright, and other intellectual property rights in the Products, (iii) the Software is licensed, and not sold, (iv) this Agreement does not grant Customer any rights to Provider's trademarks or service marks, and (v) Provider reserves any and all rights, implied or otherwise, which are not expressly granted to Customer in this Agreement.

5. **Title.** Provider, its Affiliates and/or its licensors own the title to all Software.

6. **Payment.** Customer agrees to pay to Provider (or, if applicable, the Partner) the fees specified in each order, including any applicable shipping fees. Customer will be invoiced promptly following delivery of the Products or prior to the commencement of any Renewal Maintenance Period and Customer shall make all payments due to Provider in full within thirty (30) days from the date of each invoice or such other period (if any) stated in an order. Provider reserves the right to charge Customer a late penalty of 1.5% per month (or the maximum rate permitted by law, whichever is the lesser) for any amounts payable to Provider by Customer that are not subject to a good faith dispute and that remain unpaid after the due date until such amount is paid.

7.**Taxes.** The fees stated in an order from Provider or a Partner may not include taxes. If Provider is required to pay sales, use, property, value-added or other taxes based on the Products or Maintenance Services provided under this Agreement or on Customer's use of Products or Maintenance Services, then such taxes shall be billed to and paid by Customer. This Section does not apply to taxes based on Provider's or a Partner's income.

8. **Termination.**

(a)This Agreement or the Licenses granted hereunder may be terminated (i) by mutual written agreement of Provider and Customer or (ii) by either party for a breach of this Agreement by the other party (or a Third Party User) that the breaching party fails to cure to the non-breaching party's reasonable satisfaction within thirty (30) days following its receipt of notice of the breach. Notwithstanding the foregoing, in the case of MSP Licenses, if Customer or its Client breaches this Agreement two (2) times in any twelve (12) consecutive month period, the breaching party shall not have a cure period for such breach and Provider may terminate this Agreement immediately upon providing written notice to the breaching party.

(b)Upon termination of this Agreement or expiration or termination of a License for any reason, all rights granted to Customer for the applicable Software shall immediately cease and Customer shall immediately: (i) cease using the applicable Software and Documentation, (ii) remove all copies, installations, and instances of the applicable Software from all Appliances, Customer computers and any other devices on which the Software was installed, and ensure that all applicable Third Party Users and Clients do the same, (iii) return the applicable Software to Provider together with all Documentation and other materials associated with the Software and all copies of any of the foregoing, or destroy such items, (iv) cease using the Maintenance Services associated with the applicable Software, (v) pay Provider or the applicable Partner all amounts due and payable up to the date of termination, and (vi) give Provider a written certification, within ten (10) days, that Customer, Third Party Users, and Clients, as applicable, have complied with all of the foregoing obligations.

(c)Any provision of this Agreement that requires or contemplates execution after (i) termination of this Agreement, (ii) a termination or expiration of a License, or (iii) the expiration of a SaaS Term, is enforceable against the other party and their respective successors and assignees notwithstanding such termination or expiration, including, without limitation, the Restrictions, Payment, Taxes, Termination, Survival, Warranty Disclaimer, Infringement Indemnity, Limitation of Liability, Confidential Information, Compliance Verification, and General Sections of this Agreement. Termination of this Agreement or a License shall be without prejudice to any other remedies that the terminating party or a Partner may have under law, subject to the limitations and exclusions set forth in this Agreement.

9. **Export.** Customer acknowledges that the Products and Maintenance Services are subject to the export control laws, rules, regulations, restrictions and national security controls of the United States and other applicable foreign agencies (the "Export Controls") and agrees to abide by the Export Controls. Customer hereby agrees to use the Products and Maintenance Services in accordance with the Export Controls, and shall not export, re-export, sell, lease or otherwise transfer the Products or any copy, portion or direct product of the foregoing in violation of the Export Controls. Customer is solely responsible for obtaining all necessary licenses or authorizations relating to the export, re-export, sale, lease or transfer of the Products and for ensuring compliance with the requirements of such licenses or authorizations. Customer hereby (i) represents that Customer, and if Customer is providing services under the MSP License herein each of its Clients, is not an entity or person to which shipment of Products, or provision of Maintenance Services, is prohibited by the Export Controls; and (ii) agrees that it shall not export, re-export or otherwise transfer the Products to (a) any country subject to a United States trade embargo, (b) a national or resident of any country subject to a United States trade embargo, (c) any person or entity to which shipment of Products is prohibited by the Export Controls, or (d) anyone who is engaged in activities related to the design, development, production, or use of nuclear materials, nuclear facilities, nuclear weapons, missiles or chemical or biological weapons. Customer shall, at its expense, defend Provider and its Affiliates from any third party claim or action arising out of any inaccurate representation made by Customer regarding the existence of an export license, Customer's failure to provide information to Provider to obtain an export license, or any allegation made against Provider due to Customer's violation or alleged violation of the Export Controls (an "Export Claim") and shall pay any judgments or settlements reached in connection with the Export Claim as well as Provider's costs of responding to the Export Claim.

10. **Maintenance Services.**

(a) **Description.** During any Maintenance Period, Provider shall:

(i)Make available to Customer new versions and releases of the Software, if and when Provider makes them generally available without charge as part of Maintenance Services.

(ii)Respond to communications from Customer that report Software failures not previously reported to Provider by Customer. Nothing in the foregoing shall operate to limit or restrict follow up communication by Customer regarding Software failures.

(iii)Respond to requests from Customer's technical coordinators for assistance with the operational/technical aspects of the Software unrelated to a Software failure. Provider shall have the right to limit such responses if Provider reasonably determines that the volume of such non-error related requests for assistance is excessive or overly repetitive in nature.

(iv)Provide access to Provider's software support web site at https://support.sonicwall.com (the "***Support Site***").

(v) For Customers that have purchased Maintenance Services continuously since the purchase of such License, provide the repair and return program described on the Support Site for the Appliance on which the Software is delivered.

Maintenance Services are available during regional business support hours ("Business Hours") as indicated on the Support Site, unless Customer has purchased 24x7 Support. The list of Software for which 24x7 Support is available and/or required is listed in the Global Support Guide on the Support Site.

The Maintenance Services for Software that Provider has obtained through an acquisition or merger may, for a period of time following the effective date of the acquisition or merger, be governed by terms other than those in this Section. The applicable different terms, if any, shall be stated on the Support Site.

(b)**Maintenance Period.** The first period for which Customer is entitled to receive Maintenance Services begins on the date of the registration of the Product at Provider's registration portal (the "Registration") and ends twelve (12) months thereafter (the "***Initial Maintenance Period***"). Following the Initial Maintenance Period, Maintenance Services for the Product(s) may then be renewed for additional terms of twelve (12) or more months (each, a "***Renewal Maintenance Period***") For purposes of this Agreement, the Initial Maintenance Period and each Renewal Maintenance Period shall be considered a "***Maintenance Period.***" For the avoidance of doubt, this Agreement shall apply to each Renewal Maintenance Period. Cancellation of Maintenance Services will not terminate Customer's rights to continue to otherwise use the Products. Maintenance fees shall be due in advance of each Renewal Maintenance Period and shall be subject to the payment requirements set forth in this Agreement. The procedure for reinstating Maintenance Services for the Products after it has lapsed is posted at https://support.sonicwall.com/essentials/support-guide. Maintenance Services are optional and only provided if purchased separately.

For SaaS Software, the Maintenance Period is equal to the duration of the applicable SaaS Term. For non-perpetual Licenses or for non-perpetual MSP Licenses, the Maintenance Period is equal to the duration of the License.

11. **Warranties and Remedies.**

(a)**Software Warranties.** Provider warrants that, during the applicable Warranty Period (as defined in subsection (c) below),

(i) the operation of the Software, as provided by Provider, will substantially conform to its Documentation (the "***Operational Warranty***");

(ii) the Software, as provided by Provider, will not contain any viruses, worms, Trojan Horses, or other malicious or destructive code designed by Provider to allow unauthorized intrusion upon, disabling of, or erasure of the Software, except that the Software may contain a key limiting its use to the scope of the License granted, and license keys issued by Provider for temporary use are time-sensitive (the "***Virus Warranty***");

(iii)it will make commercially reasonable efforts to make the SaaS Software available twenty-four hours a day, seven days a week except for scheduled maintenance, the installation of updates, those factors that are beyond the reasonable control of Provider, Customer's failure to meet any minimum system requirements communicated to Customer by Provider, and any breach of this Agreement by Customer that impacts the availability of the SaaS Software (the "***SaaS Availability Warranty***").

(b)**Appliance Warranties.** Provider warrants that, during the applicable Warranty Period, the Appliance will operate in a manner which allows the SNWL Software, respectively, to be used in substantial conformance with the Documentation (the ""***Appliance Warranty***",).

(c)**Warranty Periods.** The "***Warranty Period***" for each of the above warranties (except for E-class appliances which do not include a Software warranty, shall be as follows: (i) for the Operational Warranty as it applies to Software and the Virus Warranty, ninety (90) days following the initial Registration of the Software; (ii) for the Operational Warranty as it applies to SaaS Software and the SaaS Availability Warranty, the duration of the SaaS Term; and (iv) for the Appliance Warranty, one (1) year following the date the Appliance is registered with Provider.

(d)**Remedies.** Any breach of the foregoing warranties must be reported by Customer to Provider during the applicable Warranty Period. Customer's sole and exclusive remedy and Provider's sole obligation for any such breach shall be as follows:

(i)For a breach of the *Operational Warranty* that impacts the use of Software, Provider shall correct or provide a workaround for reproducible errors in the Software that caused the breach within a reasonable time considering the severity of the error and its effect on Customer or, at Provider's option, refund the license fees paid for the nonconforming Software upon return of such Software to Provider and termination of the related License(s) hereunder.

(ii)For a breach of the *Operational Warranty* that impacts the use of SaaS Software, Provider shall correct or provide a workaround for reproducible errors in the Software that caused the breach and provide a credit or refund of the fees allocable to the period during which the Software was not operating in substantial conformance with the applicable Documentation.

(iii)For a breach of the *Virus Warranty*, Provider shall replace the Software with a copy that is in conformance with the Virus Warranty.

(v)For a breach of the *SaaS Availability Warranty*, Provider shall provide a credit or refund of the fees allocable to the period during which the SaaS Software was not available for use.

(e)**Warranty Exclusions.** The warranties set forth in this Section shall not apply to any non-conformance (i) that Provider cannot recreate after exercising commercially reasonable efforts to attempt to do so; (ii) caused by misuse of the applicable Product or by using the Product in a manner that is inconsistent with this Agreement or the Documentation; or (iii) arising from the modification of the Product by anyone other than Provider.

(f)**Third Party Products.** Certain Software may contain features designed to interoperate with third-party products. If the third-party product is no longer made available by the applicable provider, Provider may discontinue the related product feature. Provider shall notify Customer of any such discontinuation, however Customer will not be entitled to any refund, credit or other compensation as a result of the discontinuation.

(g)**Warranty Disclaimer.** THE EXPRESS WARRANTIES AND REMEDIES SET FORTH IN THIS SECTION ARE THE ONLY WARRANTIES AND REMEDIES PROVIDED BY PROVIDER HEREUNDER. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, ALL OTHER WARRANTIES OR REMEDIES ARE EXCLUDED, WHETHER EXPRESS OR IMPLIED, ORAL OR WRITTEN, INCLUDING ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR ANY PARTICULAR PURPOSE, NON-INFRINGEMENT, SATISFACTORY QUALITY, AND ANY WARRANTIES ARISING FROM USAGE OF TRADE OR COURSE OF DEALING OR PERFORMANCE. PROVIDER DOES NOT WARRANT UNINTERRUPTED OR ERROR-FREE OPERATION OF THE PRODUCTS.

(h)**High-Risk Disclaimer.** CUSTOMER UNDERSTANDS AND AGREES THAT THE PRODUCTS ARE NOT FAULT-TOLERANT AND ARE NOT DESIGNED OR INTENDED FOR USE IN ANY HIGH-RISK OR HAZARDOUS ENVIRONMENT, INCLUDING WITHOUT LIMITATION, THE OPERATION OF NUCLEAR FACILITIES, AIRCRAFT NAVIGATION, AIR TRAFFIC CONTROL, LIFE SUPPORT MACHINES, WEAPONS SYSTEMS, OR ANY OTHER APPLICATION WHERE THE FAILURE OR MALFUNCTION OF ANY PRODUCT CAN REASONABLY BE EXPECTED TO RESULT IN DEATH, PERSONAL INJURY, SEVERE PROPERTY DAMAGE OR SEVERE ENVIRONMENTAL HARM (A "***HIGH RISK ENVIRONMENT***"). ACCORDINGLY, (I) CUSTOMER SHOULD NOT USE THE PRODUCTS IN A HIGH RISK ENVIRONMENT, (II) ANY USE OF THE PRODUCTS BY CUSTOMER IN A HIGH RISK ENVIRONMENT IS AT CUSTOMER'S OWN RISK, (III) PROVIDER, ITS AFFILIATES AND SUPPLIERS SHALL NOT BE LIABLE TO CUSTOMER IN ANY WAY FOR USE OF THE PRODUCTS IN A HIGH RISK ENVIRONMENT, AND (IV) PROVIDER MAKES NO WARRANTIES OR ASSURANCES, EXPRESS OR IMPLIED, REGARDING USE OF THE PRODUCTS IN A HIGH RISK ENVIRONMENT.

12.**Infringement Indemnity.** Provider shall indemnify Customer from and against any claim, suit, action, or proceeding brought against Customer by a third party to the extent it is based on an allegation that the Software directly infringes any patent, copyright, trademark, or other proprietary right enforceable in the country in which Provider has authorized Customer to use the Software, including, but not limited to the country to which the Software is delivered to Customer, or misappropriates a trade secret in such country (a "***Claim***"). Indemnification for a Claim shall consist of the following: Provider shall (a) defend or settle the Claim at its own expense, (b) pay any judgments finally awarded against Customer under a Claim or any amounts assessed against Customer in any settlements of a Claim, and (c) reimburse Customer for the reasonable administrative costs or expenses, including without limitation reasonable attorneys' fees, it necessarily incurs in responding to the Claim. Provider's obligations under this *Infringement Indemnity* Section are conditioned upon Customer (i) giving prompt written notice of the Claim to Provider, (ii) permitting Provider to retain sole control of the investigation, defense or settlement of the Claim, and (iii) providing Provider with cooperation and assistance as Provider may reasonably request in connection with the Claim. Provider shall have no obligation hereunder to defend Customer against any Claim (a) resulting from use of the Software other than as authorized by this Agreement, (b) resulting from a modification of the Software other than by Provider, (c) based on Customer's use of any release of the Software after Provider recommends discontinuation because of possible or actual infringement and has provided a non-infringing version at no charge, or (d) to the extent the Claim arises from or is based on the use of the Software with other products, services, or data not supplied by Provider if the infringement would not have occurred but for such use. If, as a result of a Claim or an injunction, Customer must stop using any Software ("***Infringing Software***"), Provider shall at its expense and option either (1) obtain for Customer the right to continue using the Infringing Software, (2) replace the Infringing Software with a functionally equivalent non-infringing product, (3) modify the Infringing Software so that it is non-infringing, or (4) terminate the License for the Infringing Software and (A) for non-SaaS Software, accept the return of the Infringing Software and refund the license fee paid for the Infringing Software, pro-rated over a sixty (60) month period from the date of initial delivery of such Software, or (B) for SaaS Software, discontinue Customer's right to access and use the Infringing Software and refund the unused pro-rated portion of any license fees pre-paid by Customer for such Software. This Section states Provider's entire liability and its sole and exclusive indemnification obligations with respect to a Claim and Infringing Software.

13.**Limitation of Liability**. EXCEPT FOR (A) ANY BREACH OF THE *RESTRICTIONS* OR *CONFIDENTIAL INFORMATION* SECTIONS OF THIS AGREEMENT, (B) AMOUNTS CONTAINED IN JUDGMENTS OR SETTLEMENTS WHICH PROVIDER OR CUSTOMER IS LIABLE TO PAY TO A THIRD PARTY UNDER THE *INFRINGEMENT INDEMNITY* SECTION OF THIS AGREEMENT AND CUSTOMER IS LIABLE TO PAY ON BEHALF OF OR TO PROVIDER UNDER THE *CONDUCT*, *EXPORT*, *MSP LICENSE*, AND *USE BY THIRD PARTIES SECTIONS* OF THIS AGREEMENT, OR (C) ANY LIABILITY TO THE EXTENT LIABILITY MAY NOT BE EXCLUDED OR LIMITED AS A MATTER OF APPLICABLE LAW, IN NO EVENT SHALL CUSTOMER OR ITS AFFILIATES, OR PROVIDER, ITS AFFILIATES OR SUPPLIERS BE LIABLE FOR (X) ANY INDIRECT, INCIDENTAL, SPECIAL OR CONSEQUENTIAL LOSS OR DAMAGE OF ANY KIND OR (Y) LOSS OF REVENUE, LOSS OF ACTUAL OR ANTICIPATED PROFITS, LOSS OF BUSINESS, LOSS OF CONTRACTS, LOSS OF GOODWILL OR REPUTATION, LOSS OF ANTICIPATED SAVINGS, LOSS OF, DAMAGE TO OR CORRUPTION OF DATA, HOWSOEVER ARISING, WHETHER SUCH LOSS OR DAMAGE WAS FORESEEABLE OR IN THE CONTEMPLATION OF THE PARTIES AND WHETHER ARISING IN OR FOR BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), BREACH OF STATUTORY DUTY, OR OTHERWISE.

EXCEPT FOR (A) ANY BREACH OF THE *SOFTWARE LICENSE*, *RESTRICTIONS*, OR CONFIDENTIAL INFORMATION SECTIONS OF THIS AGREEMENT, OR ANY OTHER VIOLATION OF THE OTHER PARTY'S INTELLECTUAL PROPERTY RIGHTS; (B) PROVIDER'S EXPRESS OBLIGATIONS UNDER THE *INFRINGEMENT INDEMNITY* SECTION OF THIS AGREEMENT AND CUSTOMER'S EXPRESS OBLIGATIONS UNDER THE *CONDUCT*, *EXPORT*, *MSP LICENSE*, AND *USE BY THIRD PARTIES* SECTIONS OF THIS AGREEMENT, (C) PROVIDER'S COSTS OF COLLECTING DELINQUENT AMOUNTS WHICH ARE NOT THE SUBJECT OF A GOOD FAITH DISPUTE; (D) A PREVAILING PARTY'S LEGAL FEES PURSUANT TO THE *LEGAL FEES* SECTION OF THIS AGREEMENT; OR (E) ANY LIABILITY TO THE EXTENT LIABILITY MAY NOT BE EXCLUDED OR LIMITED AS A MATTER OF APPLICABLE LAW, THE MAXIMUM AGGREGATE AND CUMULATIVE LIABILITY OF CUSTOMER AND ITS AFFILIATES, AND PROVIDER, ITS AFFILIATES AND SUPPLIERS, FOR DAMAGES UNDER THIS AGREEMENT, WHETHER ARISING IN OR FOR BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), BREACH OF STATUTORY DUTY, OR OTHERWISE, SHALL BE AN AMOUNT EQUAL TO (Y) THE GREATER OF THE FEES PAID AND/OR OWED (AS APPLICABLE) BY CUSTOMER OR ITS AFFILIATES FOR THE PRODUCTS THAT ARE THE SUBJECT OF THE BREACH OR FIVE HUNDRED DOLLARS ($500.00),EXCEPT FOR (Z) MAINTENANCE SERVICES OR A PRODUCT SUBJECT TO RECURRING FEES, FOR WHICH THE MAXIMUM AGGREGATE AND CUMULATIVE LIABILITY SHALL BE THE GREATER OF THE AMOUNT PAID AND/OR OWED (AS APPLICABLE) FOR SUCH MAINTENANCE SERVICE OR PRODUCT DURING THE TWELVE (12) MONTHS PRECEDING THE BREACH OR FIVE HUNDRED DOLLARS ($500.00). THE PARTIES AGREE THAT THESE LIMITATIONS OF LIABILITY ARE AGREED ALLOCATIONS OF RISK CONSTITUTING IN PART THE CONSIDERATION FOR PROVIDER PROVIDING PRODUCTS AND SERVICES TO CUSTOMER, AND SUCH LIMITATIONS WILL APPLY NOTWITHSTANDING THE FAILURE OF THE ESSENTIAL PURPOSE OF ANY LIMITED REMEDY AND EVEN IF A PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH LIABILITIES OR FAILURES.

Provider's Affiliates and suppliers and Customer's Affiliates shall be beneficiaries of this Limitation of Liability Section and Customer's Clients and Third Party Users are entitled to the rights granted under the MSP License and Use by Third Parties Sections of this Agreement; otherwise, no third party beneficiaries exist under this Agreement. Provider expressly excludes any and all liability to Third Party Users, Clients and to any other third party.

14.**Confidential Information.**

(a)**Definition.** "***Confidential Information***" means information or materials disclosed by one party (the "***Disclosing Party***") to the other party (the "***Receiving Party***") that are not generally available to the public and which, due to their character and nature, a reasonable person under like circumstances would treat as confidential, including, without limitation, financial, marketing, and pricing information, trade secrets, know-how, proprietary tools, knowledge and methodologies, the Software (in source code and/or object code form), information or benchmark test results regarding the functionality and performance of the Software, any Software license keys provided to Customer, and the terms and conditions of this Agreement.

Confidential Information shall not include information or materials that (i) are generally known to the public, other than as a result of an unpermitted disclosure by the Receiving Party after the date that Customer accepts the Agreement (the "***Effective Date***"); (ii) were known to the Receiving Party without an obligation of confidentiality prior to receipt from the Disclosing Party; (iii) the Receiving Party lawfully received from a third party without that third party's breach of agreement or obligation of trust; (iv) are protected by Provider in accordance with its obligations under the Protected Data Section below, or (v) are or were independently developed by the Receiving Party without access to or use of the Disclosing Party's Confidential Information.

(b)**Obligations.** The Receiving Party shall (i) not disclose the Disclosing Party's Confidential Information to any third party, except as permitted in subsection (c) below and (ii) protect the Disclosing Party's Confidential Information from unauthorized use or disclosure by exercising at least the same degree of care it uses to protect its own similar information, but in no event less than a reasonable degree of care. The Receiving Party shall promptly notify the Disclosing Party of any known unauthorized use or disclosure of the Disclosing Party's Confidential Information and will cooperate with the Disclosing Party in any litigation brought by the Disclosing Party against third parties to protect its proprietary rights. For the avoidance of doubt, this Section shall apply to all disclosures of the parties' Confidential Information as of the Effective Date, whether or not specifically arising from a party's performance under this Agreement.

(c)**Permitted Disclosures.** Notwithstanding the foregoing, the Receiving Party may disclose the Disclosing Party's Confidential Information without the Disclosing Party's prior written consent to any of its Affiliates, directors, officers, employees, consultants, contractors or representatives (collectively, the "***Representatives***"), but only to those Representatives that (i) have a "need to know" in order to carry out the purposes of this Agreement or to provide professional advice in connection with this Agreement, (ii) are legally bound to the Receiving Party to protect information such as the Confidential Information under terms at least as restrictive as those provided herein, and (iii) have been informed by the Receiving Party of the confidential nature of the Confidential Information and the requirements regarding restrictions on disclosure and use as set forth in this Section. The Receiving Party shall be liable to the Disclosing Party for the acts or omissions of any Representatives to which it discloses Confidential Information which, if done by the Receiving Party, would be a breach of this Agreement.

Additionally, it shall not be a breach of this Section for the Receiving Party to disclose the Disclosing Party's Confidential Information as may be required by operation of law or legal process, provided that the Receiving Party provides prior notice of such disclosure to the Disclosing Party unless expressly prohibited from doing so by a court, arbitration panel or other legal authority of competent jurisdiction.

15.**Protected Data.** For purposes of this Section, "***Protected Data***" means any information or data that is provided by Customer to Provider during this Agreement that alone or together with any other information relates to an identified or identifiable natural person or data considered to be personal data as defined under Privacy Laws, and "***Privacy Laws***" means any applicable law, statute, directive or regulation regarding privacy, data protection, information security obligations and/or the processing of Protected Data.

Except as permitted herein or to the extent required by Privacy Laws or legal process, Provider shall implement reasonable technical and organizational measures to prevent unauthorized disclosure of or access to Protected Data by third parties, and shall only store and process Protected Data as may be required to fulfill its obligations under this Agreement. If Provider complies with Customer's written instructions with respect to the Protected Data, Provider shall have no liability to Customer for any breach of this Section resulting from such compliance. Provider shall promptly notify Customer of any disclosure of or access to the Protected Data by a third party in breach of this Section and shall cooperate with Customer to reasonably remediate the effects of such disclosure or access. Provider further affirms to Customer that it has adequate agreements in place incorporating the EU standard contractual clauses for the transfer of Protected Data from the European Union ("EU") to a country outside the EU.

Customer hereby (i) represents that it has the right to send the Protected Data to Provider, (ii) consents for Provider to store and use the Protected Data worldwide for the sole purpose of performing its obligations under this Agreement, (iii) agrees that the Protected Data may be accessed and used by Provider and its Representatives worldwide as may be needed to support Provider's standard business operations, and (iv) agrees that Protected Data consisting of Customer contact information (e.g., email addresses, names) provided as part of Maintenance Services may be sent to Provider's third party service providers as part of Provider's services improvement processes.

16.**Compliance Verification.** Customer agrees to maintain and use systems and procedures to accurately track, document, and report its installations, acquisitions and usage of the Software. Such systems and procedures shall be sufficient to determine if Customer's deployment of the Software or, if applicable, use of the SaaS Software is within the quantities, terms, and maintenance releases to which it is entitled. Provider or its designated auditing agent shall have the right to audit Customer's deployment of the Software or, if applicable, use of the SaaS Software for compliance with the terms and conditions of this Agreement. Any such audits shall be scheduled at least ten (10) days in advance and shall be conducted during normal business hours at Customer's facilities. Customer shall provide its full cooperation and assistance with such audit and provide access to the applicable records and computers. Without limiting the generality of the foregoing, as part of the audit, Provider may request, and Customer agrees to provide, a written report, signed by an authorized representative, listing Customer's then current deployment of the Software and/or the number of individuals that have accessed and used SaaS Software. If Customer's deployment of the Software or, if applicable, use of the SaaS Software is found to be greater than its purchased entitlement to such Software, Customer will be invoiced for the over-deployed quantities at Provider's then current list price plus the applicable Maintenance Services and applicable over-deployment fees. All such amounts shall be payable in accordance with this Agreement. Additionally, if the unpaid fees exceed five percent (5%) of the fees paid for the applicable Software, then Customer shall also pay Provider's reasonable costs of conducting the audit. The requirements of this Section shall survive for two (2) years following the termination of the last License governed by this Agreement.

17.**SaaS Provisions.**

(a)**Data.** Customer may store data on the systems to which it is provided access in connection with its use of the SaaS Software (the "***SaaS Environment***"). Provider may periodically make back-up copies of Customer data, however, such back-ups are not intended to replace Customer's obligation to maintain regular data backups or redundant data archives. Customer is solely responsible for collecting, inputting and updating all Customer data stored in the SaaS Environment, and for ensuring that it does not (i) knowingly create and store data that actually or potentially infringes or misappropriates the copyright, trade secret, trademark or other intellectual property right of any third party, or (ii) use the SaaS Environment for purposes that would reasonably be seen as obscene, defamatory, harassing, offensive or malicious. Provider shall have the right to delete all Customer data stored in connection with the use of the SaaS Software thirty (30) days following any termination of this Agreement or any License to SaaS Software granted hereunder.

Customer represents and warrants that it has obtained all rights, permissions and consents necessary to use and transfer all Customer and/or third party data within and outside of the country in which Customer or the applicable Customer Affiliate is located (including providing adequate disclosures and obtaining legally sufficient consents from Customer's employees, customers, agents, and contractors). If Customer transmits data to a third-party website or other provider that is linked to or made accessible by the SaaS Software, Customer will be deemed to have given its consent to Provider enabling such transmission and Provider shall have no liability to Customer in connection with any claims by a third party in connection with such transmission.

(b)**Conduct.** In connection with the use of SaaS Software, Customer may not (i) attempt to use or gain unauthorized access to Provider's or to any third-party's networks or equipment; (ii) permit other individuals or entities to copy the SaaS Software; (iii) provide unauthorized access to or use of any SaaS Software or the associated access credentials; (iv) attempt to probe, scan or test the vulnerability of the SaaS Software, the SaaS Environment, or a system, account or network of Provider or any of Provider's customers or suppliers; (v) interfere or attempt to interfere with service to any user, host or network; (vi) engage in fraudulent, offensive or illegal activity of any nature or intentionally engage in any activity that infringes the intellectual property rights or privacy rights of any individual or third party; (vii) transmit unsolicited bulk or commercial messages; (viii) intentionally distribute worms, Trojan horses, viruses, corrupted files or any similar items; (ix) restrict, inhibit, or otherwise interfere with the ability of any other person, regardless of intent, purpose or knowledge, to use or enjoy the SaaS Software (except for tools with safety and security functions); or (x) restrict, inhibit, interfere with or otherwise disrupt or cause a performance degradation to any Provider (or Provider supplier) facilities used to provide the SaaS Environment. Customer shall

cooperate with Provider's reasonable investigation of SaaS Environment outages, security issues, and any suspected breach of this Section, and shall, at its expense, defend Provider and its Affiliates from any claim, suit, or action by a third party (a "***Third Party Claim***") alleging harm to such third party caused by Customer's breach of any of the provisions of this Section. Additionally, Customer shall pay any judgments or settlements reached in connection with the Third Party Claim as well as Provider's costs of responding to the Third Party Claim.

(c)**Suspension.** Provider may suspend Customer's use of SaaS Software (a) if so required by law enforcement or legal process, (b) in the event of an imminent security risk to Provider or its customers, or (c) if continued use would subject Provider to material liability. Provider shall make commercially reasonable efforts under the circumstances to provide prior notice to Customer of any such suspension.

18.**General.**

(a)**Governing Law and Venue.** This Agreement shall be governed by and construed in accordance with the laws of the State of California, without giving effect to any conflict of laws principles that would require the application of laws of a different state. Any action seeking enforcement of this Agreement or any provision hereof shall be brought exclusively in the state or federal courts located in the Santa Clara County, California. Each party hereby agrees to submit to the jurisdiction of such courts. The parties agree that neither the United Nations Convention on Contracts for the International Sale of Goods, nor the Uniform Computer Information Transaction Act (UCITA) shall apply to this Agreement, regardless of the states in which the parties do business or are incorporated.

(b)**Assignment.** Except as otherwise set forth herein, Customer shall not, in whole or part, assign or transfer any part of this Agreement, the Licenses granted under this Agreement or any other rights, interest or obligations hereunder, whether voluntarily, by contract, by operation of law or by merger (whether that party is the surviving or disappearing entity), stock or asset sale, consolidation, dissolution, through government action or order, or otherwise without the prior written consent of Provider. Any attempted transfer or assignment by Customer that is not permitted by this Agreement shall be null and void.

(c)**Severability.** If any provision of this Agreement shall be held by a court of competent jurisdiction to be contrary to law, such provision will be enforced to the maximum extent permissible by law to effect the intent of the parties and the remaining provisions of this Agreement will remain in full force and effect. Notwithstanding the foregoing, the terms of this Agreement that limit, disclaim, or exclude warranties, remedies or damages are intended by the parties to be independent and remain in effect despite the failure or unenforceability of an agreed remedy. The parties have relied on the limitations and exclusions set forth in this Agreement in determining whether to enter into it.

(d)**Use by U.S. Government.** The Software is a "commercial item" under FAR 12.201. Consistent with FAR section 12.212 and DFARS section 227.7202, any use, modification, reproduction, release, performance, display, disclosure or distribution of the Software or Documentation by the U.S. government is prohibited except as expressly permitted by the terms of this Agreement. In addition, when Customer is a U.S. government entity, the language in Subsection (ii) of the *Infringement Indemnity* Section of this Agreement and the *Injunctive Relief* Section of this Agreement shall not be applicable.

(e)**Notices.** All notices provided hereunder shall be in writing and may be delivered by email, in the case of Provider to *legal@sonicwall.com* and in the case of Customer to the email address Provider has on file for Customer. All notices, requests, demands or communications shall be deemed effective upon delivery in accordance with this paragraph.

(f)**Disclosure of Customer Status.** Provider may include Customer in its listing of customers and, upon written consent by Customer, announce Customer's selection of Provider in its marketing communications.

(g)**Waiver.** Performance of any obligation required by a party hereunder may be waived only by a written waiver signed by an authorized representative of the other party, which waiver shall be effective only with respect to the specific obligation described therein. Any waiver or failure to enforce any provision of this Agreement on one occasion will not be deemed a waiver of any other provision or of such provision on any other occasion.

(h)**Injunctive Relief.** Each party acknowledges and agrees that in the event of a material breach of this Agreement, including but not limited to a breach of the *Software License*, *Restrictions* or *Confidential Information* Sections of this Agreement, the non-breaching party shall be entitled to seek immediate injunctive relief, without limiting its other rights and remedies.

(i**)Force Majeure.** Each party will be excused from performance for any period during which, and to the extent that, it is prevented from performing any obligation or service as a result of causes beyond its reasonable control, and without its fault or negligence, including without limitation, acts of God, strikes, lockouts, riots, acts of war, epidemics, communication line failures, and power failures. For added certainty, this Section shall not operate to change, delete, or modify any of the parties' obligations under this Agreement (e.g., payment), but rather only to excuse a delay in the performance of such obligations.

(j)**Equal Opportunity.** Provider is a federal contractor and Affirmative Action employer (M/F/D/V) as required by the Equal Opportunity clause C.F.R. § 60-741.5(a).

(k)**Headings**. Headings in this Agreement are for convenience only and do not affect the meaning or interpretation of this Agreement. This Agreement will not be construed either in favor of or against one party or the other, but rather in accordance with its fair meaning. When the term "including" is used in this Agreement it will be construed in each case to mean "including, but not limited to."

(l) **Legal Fees.** If any legal action is brought to enforce any rights or obligations under this Agreement, the prevailing party shall be entitled to recover its reasonable attorneys' fees, court costs and other collection expenses, in addition to any other relief it may be awarded.

(m)**Entire Agreement.** This Agreement is intended by the parties as a final expression of their agreement with respect to the subject matter thereof and may not be contradicted by evidence of any prior or contemporaneous agreement unless such agreement is signed by both parties. In the absence of such an agreement, this Agreement shall constitute the complete and exclusive statement of the terms and conditions and no extrinsic evidence whatsoever may be introduced in any proceeding that may involve the Agreement. Each party acknowledges that in entering into the Agreement it has not relied on, and shall have no right or remedy in respect of, any statement, representation, assurance or warranty (whether made negligently or innocently) other than as expressly set out in the Agreement. In those jurisdictions where an original (non-faxed, non-electronic, or non-scanned) copy of an agreement or an original (non-electronic) signature on agreements such as this Agreement is required by law or regulation, the parties hereby agree that, notwithstanding any such law or regulation, a faxed, electronic, or scanned copy of and a certified electronic signature on this Agreement shall be sufficient to create an enforceable and valid agreement. This Agreement, may only be modified or amended t by a writing executed by a duly authorized representative of each party. No other act, document, usage or custom shall be deemed to amend or modify this Agreement.

B

SonicWall Support

Technical support is available to customers who have purchased SonicWall products with a valid maintenance contract.

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://www.sonicwall.com/support.

The Support Portal enables you to:

- View knowledge base articles and technical documentation
- View and participate in the Community forum discussions at https://community.sonicwall.com/technology-and-support.
- View video tutorials
- Access MySonicWall
- Learn about SonicWall professional services
- Review SonicWall Support services and warranty information
- Register for training and certification
- Request technical support or customer service

To contact SonicWall Support, visit https://www.sonicwall.com/support/contact-support.

About This Document

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.

Directory Connector Administration Guide
Updated - December 2020
Software Version - 4.1
232-004068-00 Rev C