Dell SonicWALL™ Directory Services Connector 3.7

Administration Guide

If you have any questions regarding your potential use of this material, contact:

Dell Inc.
Attn: LEGAL Dept
5 Polaris Way
Aliso Viejo, CA 92656

Refer to our website (software.dell.com) for regional and international office information.

Patents

This product is protected by multiple U.S. Patents. For more information, go to http://software.dell.com/legal/patents.aspx.

Trademarks

Dell, the Dell logo, and SonicWALL are trademarks of Dell, Inc. Windows® and Active Directory® are trademarks of Microsoft. Novell eDirectory is a trademark of Novell, Inc. Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and names or their products. Dell disclaims any proprietary interest in the marks and names of others.

Legend

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

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

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

Directory Services Connector Administration Guide
Updated - March 2015
Software Version - 3.7
232-002804-00 Rev A

Contents

1

About this guide

Introduction

Welcome to the *Dell SonicWALL™ Directory Services Connector Administration Guide*. It provides information on installing and configuring the Dell SonicWALL Single Sign-On agent and other elements of Directory Services Connector (DSC).

Always check https://support.software.dell.com for the latest version of this guide as well as other Dell SonicWALL products and services documentation.

Organization of this guide

The *Dell SonicWALL Directory Services Connector Administration Guide* is structured into the following parts:

Chapter 1 About this guide

This chapter provides helpful information for using this guide. It includes conventions used in this guide, information on how to obtain additional product information, and a summary of the chapters in the guide.

Chapter 2 Directory Services Connector overview

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

Chapter 3 Installing Directory Services Connector

This chapter provides installation procedures for Directory Services Connector and the Single Sign-On (SSO) Agent. It includes procedures for installations that use either Active Directory or NovelIl eDirectory.

Chapter 4 Using and configuring Directory Services Connector

This chapter explains the options in the DSC Configuration Tool and provides configuration procedures for the Single Sign-On (SSO) Agent.

2

Directory Services Connector overview

This chapter provides an overview of the Dell SonicWALL Directory Services Connector (DSC). It includes an introduction to DSC and the SSO Agent, along with the supported user identification methods and platform compatibilities.

Topics:

About Single Sign-On

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

SSO is configured in the **Users > Settings** page of the SonicOS 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.

About Directory Services Connector

Dell SonicWALL Directory Services Connector includes the Dell SonicWALL Single Sign-On Agent (SSO Agent) as well as certain configuration functions. The SSO Agent provides centralized user-identification to Dell SonicWALL network security appliances, interacting with the SonicOS Single Sign-On feature.

Directory Services Connector provides integration with both Active Directory and Novell eDirectory. Specifically, these are supported as follows:

1 Dell SonicWALL SuperMassive series, E-Class NSA series, NSA series, and TZ series appliances (TZ 100 and newer) to achieve transparent, automated Single Sign-On integration with both Active Directory and Novell eDirectory.

2 SonicWALL PRO and TZ 190/180 series appliances to achieve Single Sign-On integration with Active Directory.

The Dell SonicWALL appliance 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.

NOTE: It is normal for the system running Dell SonicWALL Directory Services Connector to have high CPU activity for the first few hours after installation, while the software creates a database of the user network.

Dell SonicWALL Directory Services Connector runs as a 32-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 query source.

Upon identifying a logged in user or finding updated user information, the SSO Agent sends login notifications to the appliance in the following cases:

- If the query source is set to DC security log, the agent sends a notification with the User IP Address, User Name and Login Session ID, User ID Mechanisms, domain controller IP Address, and Login Time.
- If using NETAPI or WMI, the agent sends a login notification only if an `In_Progress` status was previously sent for the same IP address. The agent does not send a notification for an updated user, but only updates its internal cache with the updated user information, if caching is enabled. When the appliance sends a multi-user request to the SSO Agent and includes an Operation Timeout value, the agent divides the time by the number of IP addresses present in the request. If the query times out, it is aborted and an Operation_Time_Out status is included in the agent's reply to the appliance.

The Dell SonicWALL SSO Agent is not supported in a Citrix or Terminal Services Environment. In these environments, you can use the Dell SonicWALL Terminal Services Agent (TSA) to communicate with Dell SonicWALL SSO. The TSA is not included as part of this release. For more information about the TSA, see the latest *Terminal Services Agent Release Notes*, the latest *SonicOS Administration Guide* and the *SonicOS Enhanced Single Sign-On Feature Module*, available on https://support.software.dell.com.

About Agent-to-Agent communication

When multiple SSO Agents are configured in Directory Services Connector, these Agents can communicate with each other to share information. This allows a global user database to be shared among all SSO Agents. This feature is also called *Agent Synchronization*.

The **Allow Agent synchronization** option is available when a DC Security Log method is selected for Query Source.

The benefits of Agent-to-Agent communication include:

- Shared User-detection Times — User detection information is shared among more than one Domain Controller (DC). For example, when agent1 fetches logs from DC1 and DC2, and agent2 fetches logs from DC3 and DC4, both agents can update each other when new users have been added. Even when user1 is logged on to DC3 or DC4, the Dell SonicWALL network security appliance is able to retrieve information from agent1. Both agents share user-identification times along with each add/update notification, which helps to identify recently logged-in users.
- Decreased Redundancy — When Query Source is set to DC Security Log and no fallback query method is configured, new and identified users logging in to that DC could be missed if that agent were to fail. Agent-to-Agent communication takes over for the failed agent, preserving currently-identified users and logs. It then begins fetching logs from the DC on the failed agent's behalf; ensuring that agents are always correctly reporting usernames.
- Smart NetAPI/WMI Scanners — When one agent is overloaded with requests while other agents are comparatively free, polling requests can be transferred to one of the free agents.

- Non-matching Query Sources — Agent synchronization can be used between agents which are using different Query Source methods.

About the SSO Agent cache

By default, the SSO Agent caches user information for 60 seconds, with a range of 30–600 seconds.

The cache settings can be overridden from the Windows Registry. To disable caching (cache refresh time = 0), edit the Registry and set the REFRESHTIME value to 0. If the cache refresh rate is set to zero seconds, user information is fetched from the workstation for every request from the Dell SonicWALL appliance.

The appliance default is to time out after 10 seconds and to retry up to six times, so the agent receives multiple requests from it if a NetAPI request is slow to complete. The agent does not initiate a new NetAPI request if the previous one is still going, but there might be situations where using the cache can help and having it disabled could be a small disadvantage:

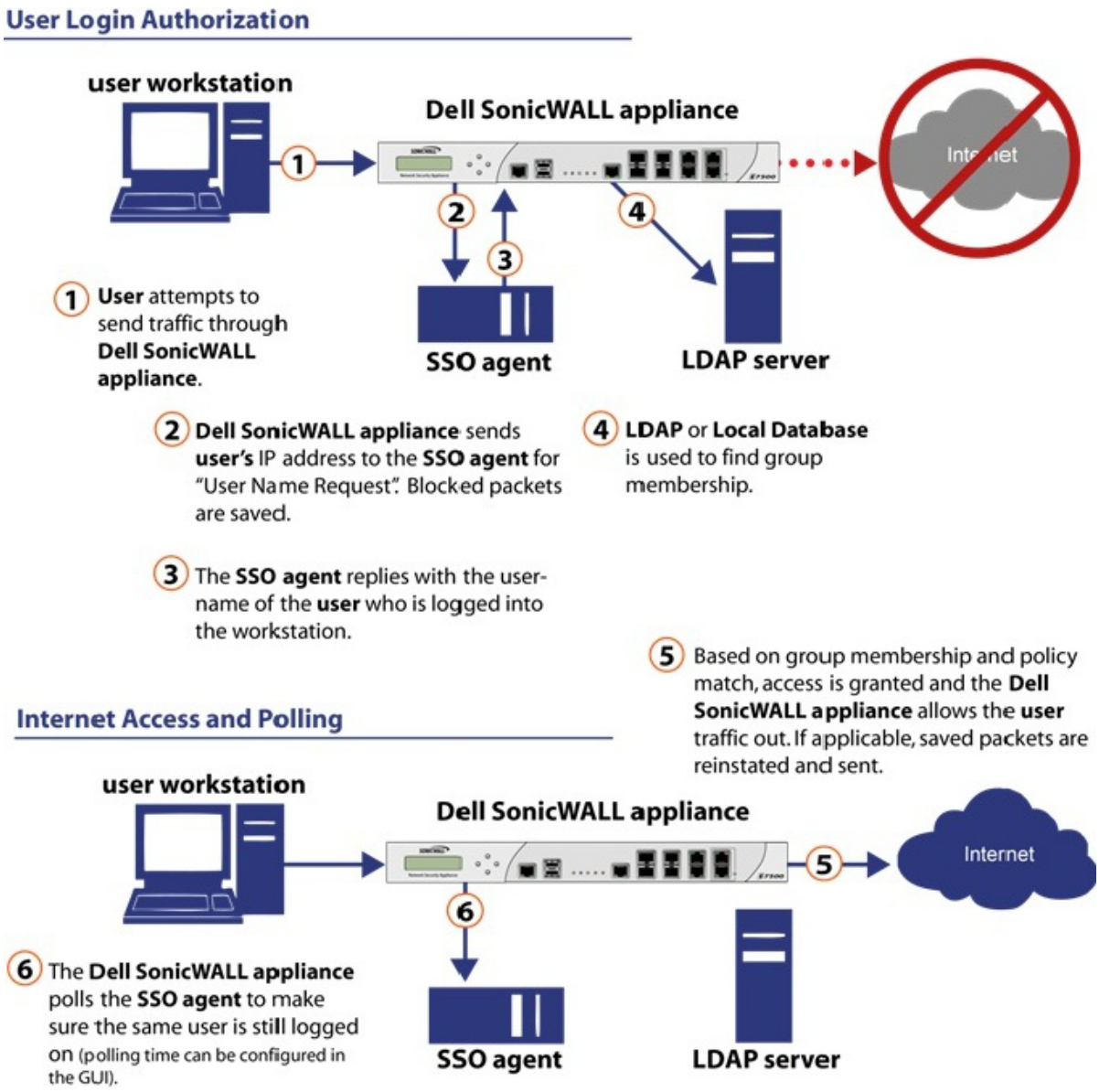
- If a NetAPI request happens to take a multiple of 10 seconds, then the agent's reply could cross over with a request retry from the appliance. This would cause the agent to initiate another NetAPI request where, if using a non-zero refresh rate for the cache, it would simply repeat the last reply from its cache.
- If a reply from the agent is somehow lost, the appliance would re-send it after 10 seconds and the agent would make another NetAPI request where otherwise it would reply from its cache.

When using the SSO Agent cache, be sure to consider the following:

- No caching (refresh time set to zero) in the agent gives faster detection of changes in user information, but using the cache avoids possible unnecessary extra NetAPI/WMI requests when problems occur.
- If significant numbers of NetAPI/WMI errors are being shown in the statistics, then setting the cache refresh time to about 60 seconds might help to reduce them.
- The agent's cache refresh time should never be set greater than the user polling period set on the appliance.

About Single Sign-On with Active Directory or LDAP

While most users are found through the Active Directory/Exchange Server/eDirectory method, the following image represents an alternative method of locating users.



The Dell SonicWALL SSO Agent identifies users by IP address using a protocol compatible with Active Directory and automatically determines when a user has logged out to prevent unauthorized access. Based on data from the SSO Agent, the Dell 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 Firewall to control what they are allowed to access.

User names learned through SSO are reported in the Dell 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 who are not logged into the domain, an Authentication required screen displays, indicating that a manual login is required for further authentication. Users who are identified, but lack the group memberships required by the configured policy rules, are redirected to an Access Barred page.

To use Dell SonicWALL SSO, it is required that the SSO Agent be installed on a server that can communicate with the Active Directory server and with clients and the Dell SonicWALL security appliance directly using the IP address or using a path, such as VPN.

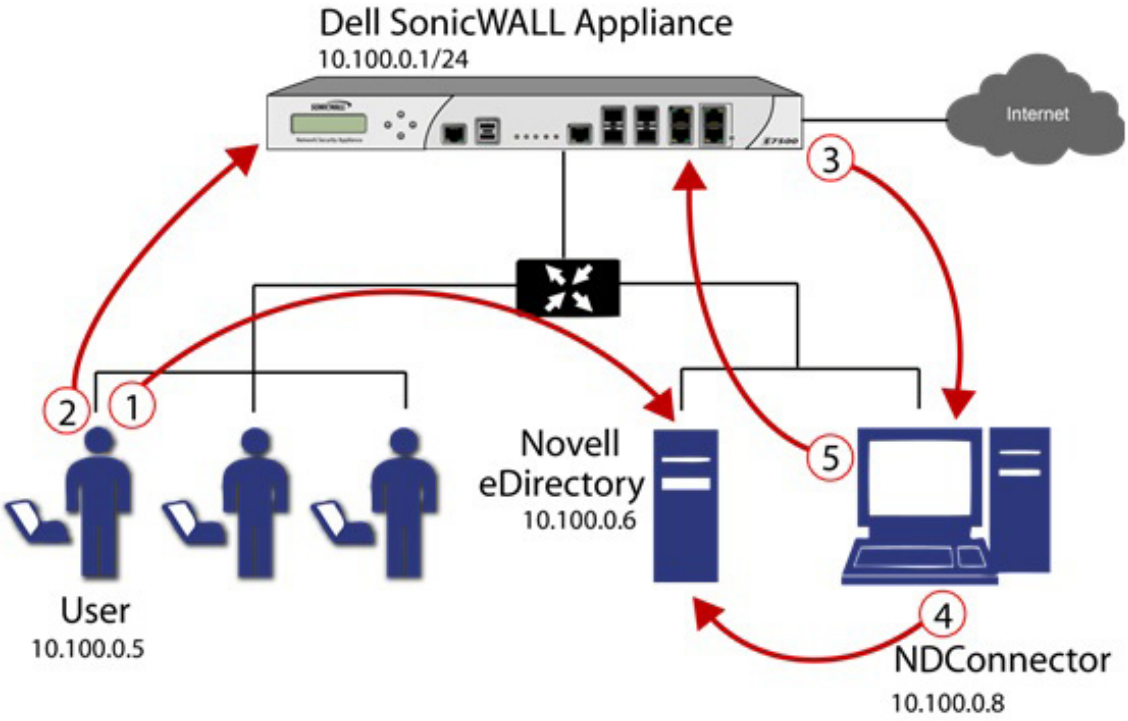
The following requirements must be met in order to run the SSO Agent:

- 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 4.0 or above
- NETAPI or WMI (unless using DC Windows security log as the query source)
- The SSO Agent must run under Domain Admin privileges.

About Single Sign-On with 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 are 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 as follows:

1 The user logs in to 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 Dell SonicWALL network security appliance detects the request.

3 The Dell SonicWALL appliance queries the SSO Agent.

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

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

About user identification methods

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

- About client probing with NETAPI or WMI on page 11
- About DC security logs on page 11
- About using Samba on Linux/UNIX clients on page 13
- About NetBIOS mapping support on page 12

About client probing with NETAPI or WMI

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 logons. 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.

Windows Firewall might block both methods by default.

To enable WMI methods in the Windows Firewall, you can select Windows Management Instrumentation in **Control Panel > All Control Panel Items > Windows Firewall > Allowed Programs**.

To enable the NetAPI method in Windows Firewall, you can select **File** and **Printer Sharing.**

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 Services Connector, the SSO Agent repeatedly probes 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.

About DC security logs

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. In Microsoft Windows, the DC 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.

Using DC Security Log as the query source method, the SSO Agent can identify users who log on to the Windows domain. The SSO Agent sends a login notification to the appliance as soon as it detects a user login. The SSO Agent also monitors event messages with specific Event IDs and notifies SonicOS with the user’s information and logoff status.

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 *Configuring a Non-Admin Domain Account for SSO Agent to Read Domain Security Logs* configuration guide, available at https://support.software.dell.com.

About LogWatcher

The **Add LogWatcher Support** option is available when a DC Security Log method is selected for Query Source.

LogWatcher is a Windows service that runs on each Domain Controller. Its fetches the security event log, parses the log events, and sends user logon/logoff information to the SSO Agent and/or the Dell SonicWALL network security appliance. LogWatcher is most suitable in a distributed DC environment where the DC logs are replicated across multiple Domain Controllers.

LogWatcher Requirements

1. The Domain Controller must be running Windows Server 2003 or higher.
2. Microsoft Visual C++ 2010 Redistributable Package (x86) (for Windows Server 2008 and above) or Microsoft Visual C++ 2008 Redistributable Package (x86) (for Windows Server 2003) must be installed on the Domain Controller.
    - Microsoft Visual C++ 2010 Redistributable Package (x86) (for Windows Server 2008 and above): http://www.microsoft.com/en-us/download/details.aspx?id=8328
    - Microsoft Visual C++ 2008 Redistributable Package (x86) (for Windows Server 2003): http://www.microsoft.com/en-us/download/details.aspx?id=29
3. The Domain Controller must have Microsoft Core XML Services (MSXML) 6.0 (also known as Microsoft MSXML Parser 6.0) installed:| http://www.microsoft.com/en-us/download/details.aspx?id=3988
4. The Domain Controller must have audit logon enabled.
5. The LogWatcher Service only works with SSO Agent 3.6.02 and higher.
6. The SSO Agent must be configured for LogWatcher support.

About enabling audit logs in DC policy

The Domain Controller must have audit logon enabled for LogWatcher to work. Audit logon is disabled by default in Windows Server. Steps to enable audit logon are provided in the following sections:

- Setting a group policy to enable audit logon on Windows Server 2003 on page 44
- Setting a group policy to enable audit logon on Windows Server 2008 on page 46

About NetBIOS mapping support

The **Add NetBIOS mapping support** option is available when a DC Security Log method is selected for Query Source.

Windows Server 2000 and higher provide 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 operating systems. 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.

You can enable or disable the NetBIOS feature from the DSC Configuration Tool. By default the NetBIOS feature is disabled.

About using Samba on Linux/UNIX clients

Samba 3.0 or newer can be installed on Linux/UNIX clients for use with Dell SonicWALL SSO. 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 smb client utility). A user working on a Linux PC with Samba in a Windows domain can be identified through the 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, available at: https://support.software.dell.com.

Without Samba, Linux PCs do not support the Windows networking requests that are used by the Dell SonicWALL SSO Agent, and therefore, do 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. Without Samba, the DC security log method works for using Single Sign-On with Linux clients.

Platform compatibility

To use Dell SonicWALL Single Sign-On, it is required that the SSO Agent is installed on a server that can communicate with the Active Directory or eDirectory server and with clients and the Dell 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 2.0 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

Dell SonicWALL Directory Services Connector and the SSO Agent run as a 32-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.

See the following sections:

- SonicWALL appliance/firmware compatibility on page 14
- Virtual environment compatibility on page 14
- eDirectory server compatibility on page 14
- Domain controller server compatibility on page 15
- SSO Agent platform compatibility on page 15
- Client compatibility on page 16
- Citrix or terminal services compatibility on page 16

SonicWALL appliance/firmware compatibility

SonicWALL Directory Services Connector is a supported release for use with the following SonicWALL platforms:

- SuperMassive 9200 / 9400 / 9600 running SonicOS 6.1 and above
- SuperMassive E10200 / E10400 / E10800 running SonicOS 6.0.x
- 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
- 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 1ms.

Virtual environment compatibility

Recommended Virtual Environments for Directory Services Connector include:

- VMware ESX 5.5
- VMware ESX 5.1
- VMware ESX 4.x
- Microsoft Hyper-V 2012 R2
- Microsoft Hyper-V 2008 R2

Virtual Machine host configuration requirements:

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

eDirectory server compatibility

SonicWALL Directory Services Connector is supported for use with the following eDirectory Servers

- Novell eDirectory 8.8.5
- Novell eDirectory 8.8.7

Domain controller server compatibility

SonicWALL Directory Services Connector is supported for use with domain controllers running the following operating systems:

- Windows Server 2012 — 64-bit
- Windows Server 2012 R2 — 64-bit
- Windows Server 2012 R2 — 64-bit
- Windows Server 2012 — 32/64-bit
- Windows Server 2012 R2 — 32/64-bit

NOTE: 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.

SSO Agent platform compatibility

SonicWALL Directory Services Connector and SSO Agent are supported for installation on 32-bit and 64-bit Windows systems running the following operating systems:

- Windows Server 2012 — 64-bit
- Windows Server 2012 R2 — 64-bit
- Windows Server 2012 R2 — 64-bit
- Windows Server 2012 — 32/64-bit
- Windows Server 2012 R2 — 32/64-bit
- Windows 8 — 32/64-bit
- Windows 7 — 32/64-bit
- Windows Vista — 32/64-bit
- Windows XP — 32/64-bit

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

- .NET Framework 2.0 and above

The following Microsoft Windows operating systems are not supported as servers:

- Windows 2000 – All versions

NOTE: Windows Server 2008 and higher or Windows 7 and higher are recommended.

Limitations:

The following limitations exist in Windows operating systems prior to Windows Server 2008 or Windows 7:

- Certain Windows API elements are not supported, including the Event Subscription API for communicating with the domain controller. This requires Directory Services Connector to use the WMI event subscription mechanism on older Windows versions, which is much slower than an event subscription.
- The SMB2 protocol is not supported on older Windows versions.
- Single Sign-On related functions could operate at approximately half the performance on older Windows versions.

Client compatibility

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

- Windows 8 — 32/64-bit
- Windows 7 — 32/64-bit
- Windows Vista — 32/64-bit
- Windows XP — 32/64-bit

Citrix or terminal services compatibility

The Dell SonicWALL SSO Agent is not supported in a Citrix or Terminal Services Environment.

In these environments, you can use the Dell SonicWALL Terminal Services Agent (TSA) to communicate with the SonicOS Single Sign-On feature.

The TSA is not included as part of Dell SonicWALL Directory Services Connector. For more information about the TSA, see the latest *Terminal Services Agent Release Notes* and the latest *SonicOS Administration Guide*, available at: https://support.software.dell.com/.

3

Installing Directory Services Connector

Topics:

Installing DSC with Active Directory

When using Single Sign-On with Windows, install Directory Services Connector and the SSO Agent on a host on your network that has access to the Active Directory server and all client workstations.

NOTE: The default user cache time (refresh time) is set to “0” seconds, which means the information about identified users is not cached on the agent.

To install Directory Services Connector for use with Active Directory:

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

- SonicWALL Directory Connector (32-bit) 3.7.*xx*.exe
- SonicWALL Directory Connector (64-bit) 3.7.*xx*.exe

You can find these installers on http://www.mysonicwall.com under Directory Services Connector.

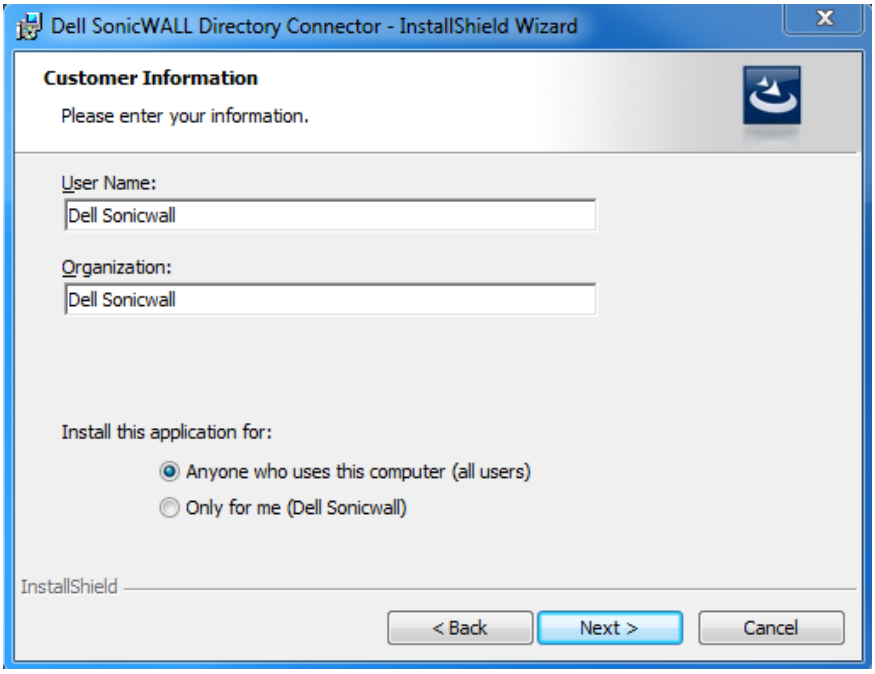
2 Double-click the installer to begin installation.

3 If prompted, install the Microsoft .NET framework.

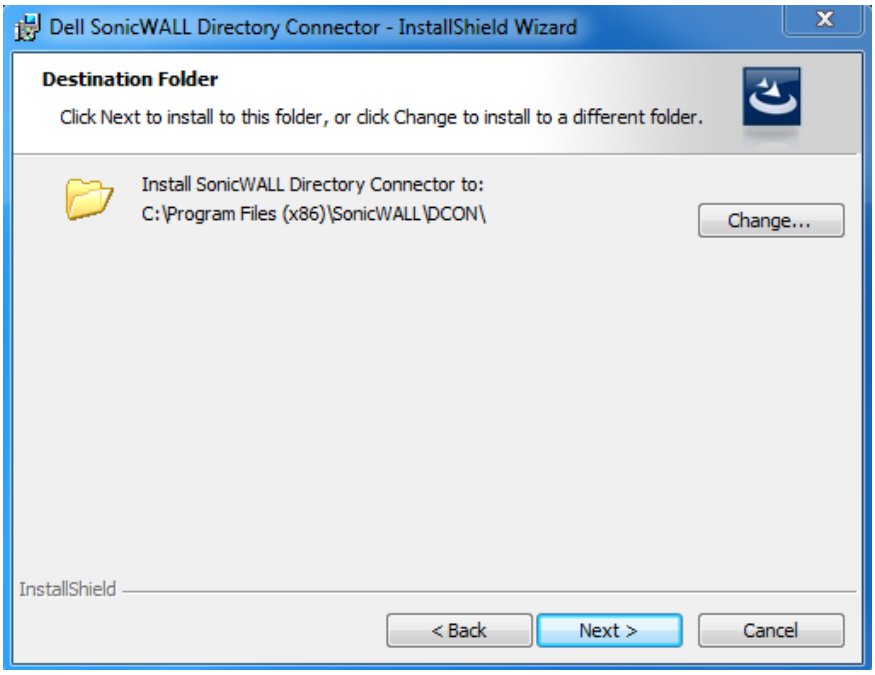
4 In the Welcome screen, click **Next** to continue the installation.

5 In the License Agreement screen, accept the terms of the license agreement, and then click **Next**.

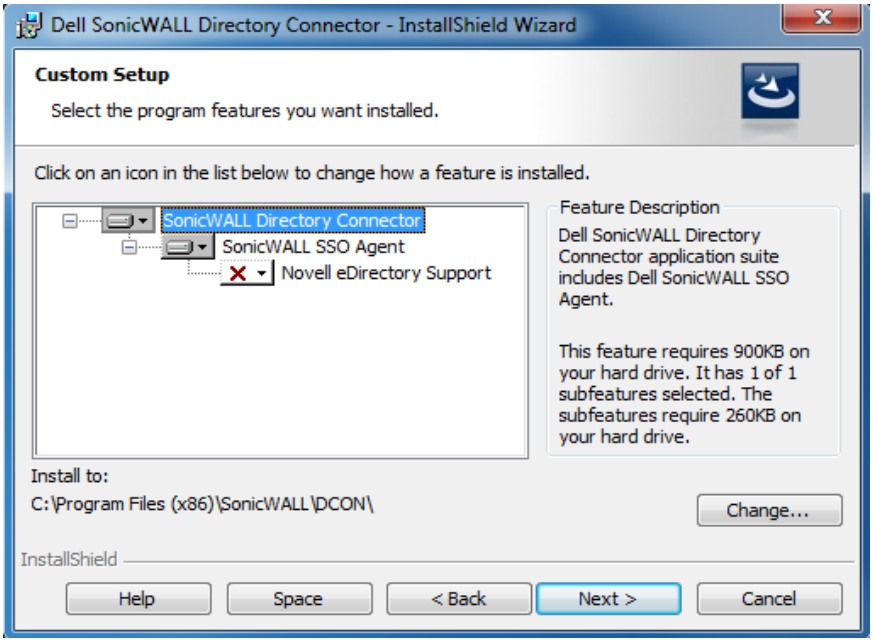
6 In the Customer Information screen, enter your username and the name of the company that owns the workstation where you are installing the Directory Connector, select the application use privileges, and then click **Next**.



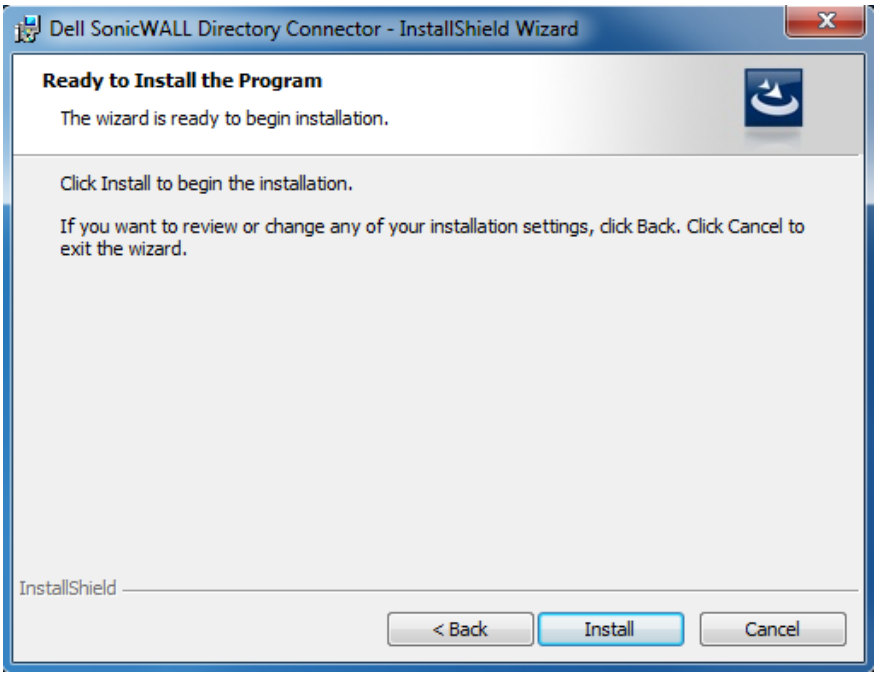
7 Select the destination folder. To use the default folder, *C:\Program Files\SonicWALL\DCON*, click **Next**. To specify a custom location, click **Change**, select the folder, and click **Next**.



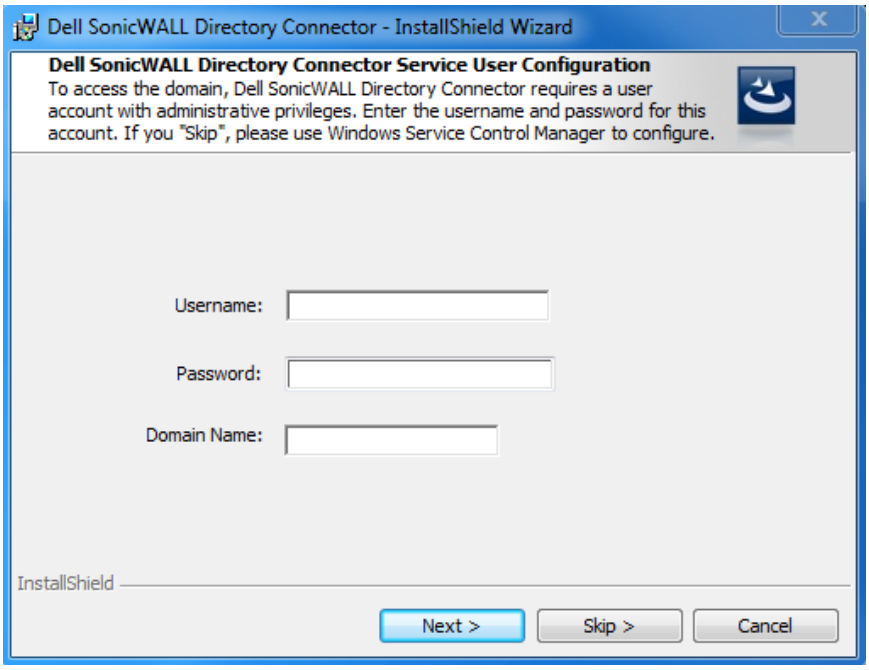
8 On the Custom Setup page, the installation icon is displayed by default next to the SonicWALL SSO Agent feature. Click **Next**.



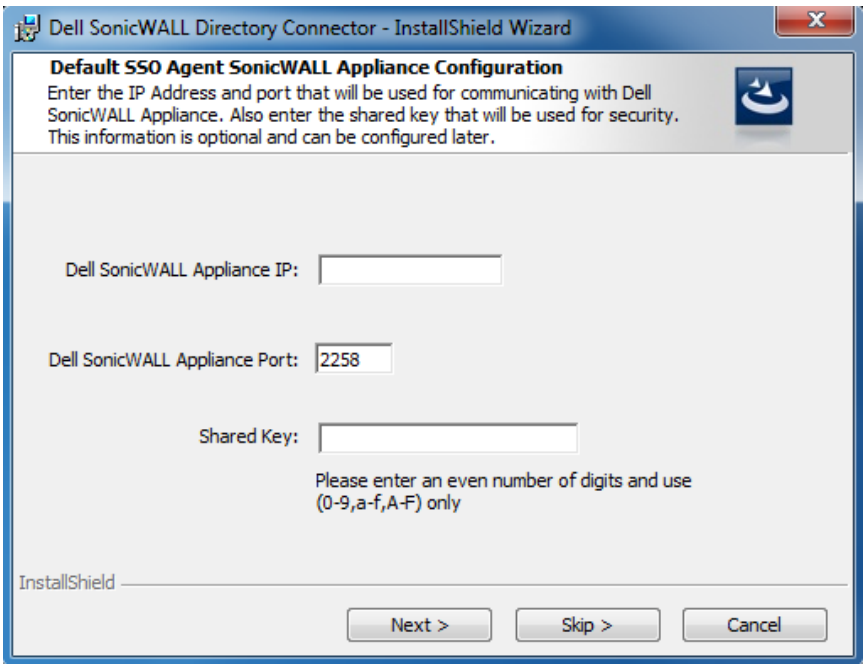
9 In the next screen, click **Install** to install Directory Connector.



10 To configure a common service account that the SSO Agent uses to log into a specified Windows domain, enter the username of an account with administrative privileges in the **Username** field, the password for the account in the **Password** field, and the domain name of the account in the **Domain Name** field. Click **Next**.



11 Enter the IP address of your SonicWALL security appliance in the **SonicWALL Appliance IP** field. Type the port number for the same appliance in the **Dell SonicWALL Appliance Port** field. Enter a shared key (a hexadecimal number from 1 to 16 digits in length) in the **Shared Key** field, using an even number of digits. Click **Next** to continue.



12 Wait for the installation to complete. The status bar displays while Directory Services Connector installs.

13 When installation is complete, optionally select **Launch SonicWALL Directory Connector** to launch the Dell SonicWALL Directory Services Connector Configuration tool, and then click **Finish**.

Installing DSC with Novell eDirectory

To use Single Sign-On with Novell eDirectory, install Directory Services Connector and the SSO Agent on a host on your network that has access to the Novell eDirectory server and all client workstations. It does not need to run on a machine with a Novell client installed.

To install Directory Services Connector for use with Novell eDirectory Support:

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

- SonicWALL Directory Connector (32-bit) 3.7.*xx*.exe
- SonicWALL Directory Connector (64-bit) 3.7.*xx*.exe

You can find these installers on http://www.mysonicwall.com under Directory Services Connector.

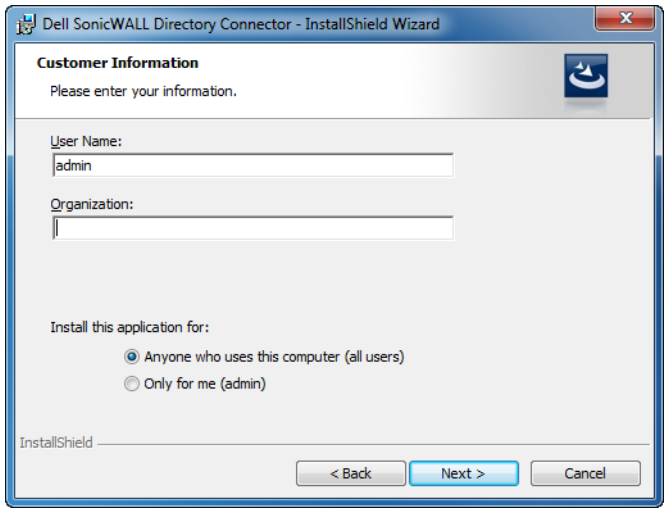
2 Double-click the installer to begin installation.

3 If prompted, install the Microsoft .NET framework.

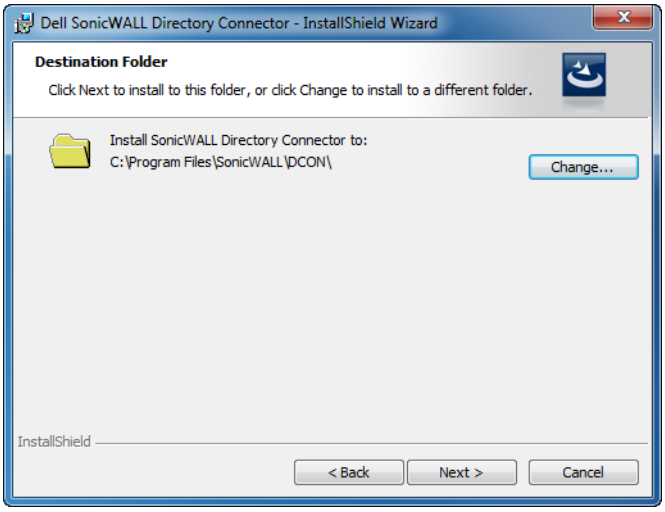
4 In the Welcome screen, click **Next** to continue the installation.

5 In the License Agreement screen, accept the terms of the license agreement, and then click **Next**.

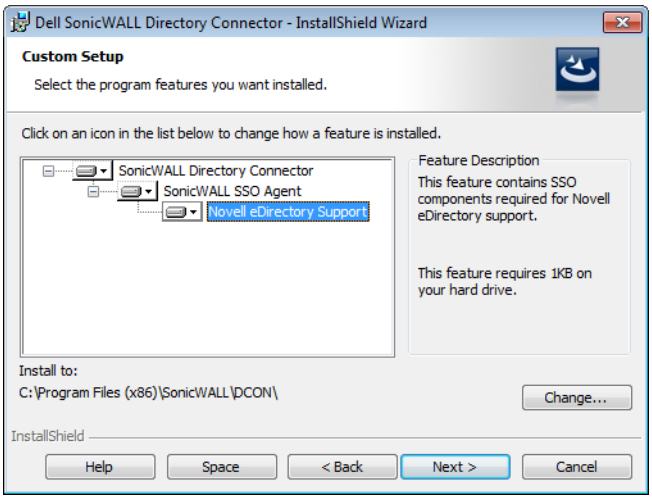
6 In the Customer Information screen, enter your username and the name of the company that owns the workstation where you are installing the SSO Agent, select the application use privileges, and then click **Next**.



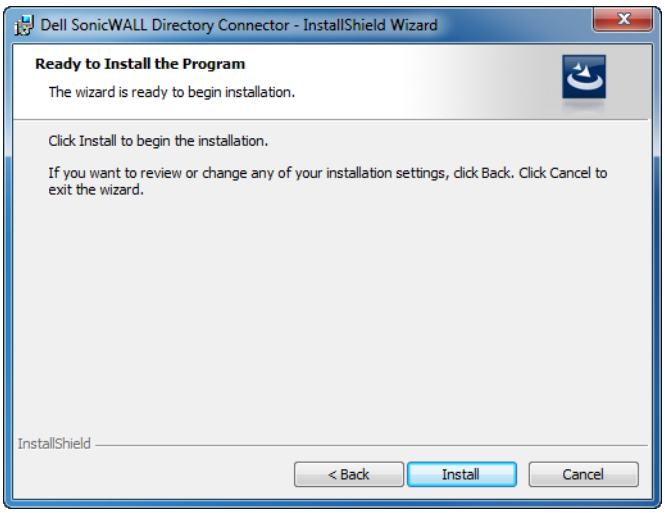
7 Select the destination folder. To use the default folder, *C:\Program Files\SonicWALL\DCON*, click **Next**. To specify a custom location, click **Change**, select the folder, and click **Next**.



8 On the Custom Setup page, select the **Novell eDirectory Support** feature for installation. Click **Next**.



9 In the Ready to Install the Program screen, click **Install**.



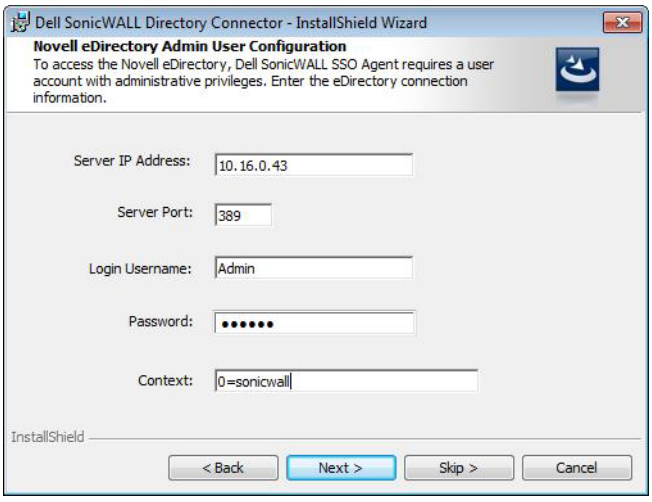
10 In the Default SSO Agent SonicWALL Appliance Configuration screen, enter the Dell SonicWALL appliance information and then click **Next**:

- **SonicWALL Appliance IP** — Type in the Dell SonicWALL appliance IP address.
- **SonicWALL Appliance Port** — Type in the port used by the SSO Agent to communicate with the Dell SonicWALL appliance. The default port is 2258.
- **Shared Key** — Type in a hexadecimal number of up to 16 characters (use an even number of characters) to use as the key for encrypting messages between the SSO Agent and the Dell SonicWALL appliance. You must also enter the same key when configuring the appliance to use Dell SonicWALL SSO.

11 In the Novell eDirectory Admin User Configuration screen, enter the information for the Novell eDirectory server, and then click **Next**:

- **Server IP Address** — eDirectory Server IP Address
- **Server Port** — eDirectory Server Port (389 by default)
- **Login Username** — Login username for the administrator account to access the eDirectory server
- **Password** — Password for the administrator account to access the eDirectory server
- **Context** — eDirectory context in which the administrator account for the eDirectory server resides

These same settings can be modified after installation by right-clicking on **eDirectory** in the Directory Connector Configuration Tool.



12 When the installation is complete, optionally select **Launch SonicWALL Directory Connector** to launch the Dell SonicWALL Directory Services Connector, and then click **Finish**.

For more information about configuring and using Dell SonicWALL SSO with Novell eDirectory support, see the *SonicOS Single sign-on Feature Module* and the latest *SonicOS Administration Guide*, available on https://support.software.dell.com/release-notes-product-select.

4

Using and configuring Directory Services Connector

Topics:

Using the DSC Configuration Tool menus

The Directory Services Connector Configuration Tool provides several menus at the top of the screen for configuring settings and viewing information.

Using the File menu

The File menu in the Directory Connector Configuration Tool provides the Exit option.

1 Click **File > Exit** to close the Directory Connector Configuration Tool.

Using the View menu

The View menu in the Directory Connector Configuration Tool provides options for displaying or hiding the toolbar and status bar.

1 Click **View > ToolBar** to toggle the toolbar display. If it is currently hidden, it will be displayed. If currently displayed, it will be hidden.

2 Click **View > StatusBar** to toggle the status bar display. If it is currently hidden, it will be displayed. If currently displayed, it will be hidden.

The toolbar provides icon buttons near the top of the screen for the following:

- Adding servers to the SSO Agent configuration
- Removing servers from the SSO Agent configuration
- Starting the Windows service
- Stopping the Windows service
- Refreshing the items displayed in the Configuration Tool
- Viewing the SSO Agent properties
- Accessing the diagnostics tool

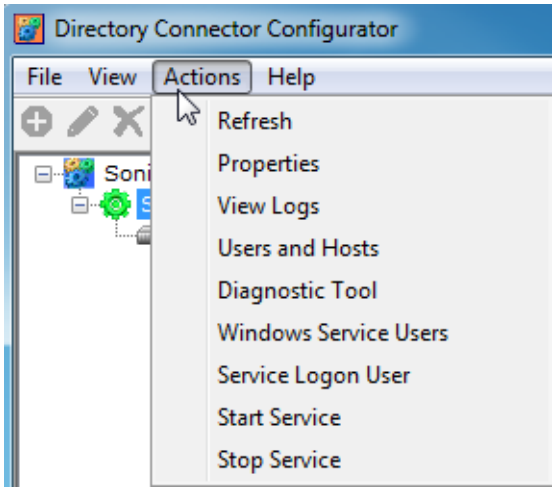
Each button is only active when a relevant item is selected in the left panel. Not all buttons are active at the same time.

The status bar displays the current SSO Agent status along the bottom of the screen. The installed version of the SSO Agent is also displayed there.

Using the Actions menu

With SonicWALL SSO Agent selected in the Directory Connector Configuration Tool, the Actions menu provides options for editing the SSO Agent configuration settings, viewing the log entries, viewing users and hosts, using the diagnostic tool, and refreshing the display. It also provides options for managing the SSO Agent Windows service.

Figure 1. Actions menu with SonicWALL SSO Agent selected



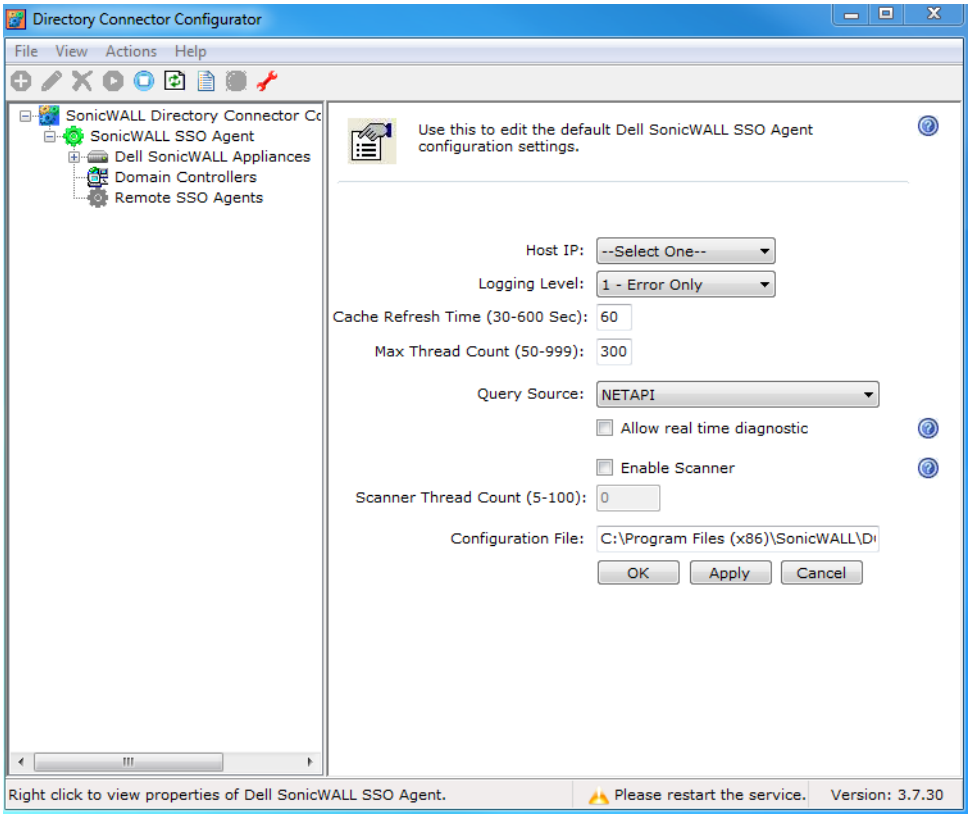
All of the **Actions** menu options are also available on the right-click menu for the SonicWALL SSO Agent from within the Configuration Tool. See the following:

- Configuring SSO Agent settings on Actions > Properties on page 27
- Viewing logs on page 28
- Displaying Users and Hosts statistics on page 29
- Using the Diagnostic Tool on page 30
- Using the Windows Service Users page on page 31
- Using the Service Logon User page on page 31
- Starting and stopping the Windows service on page 31

Configuring SSO Agent settings on Actions > Properties

The Actions > Properties page provides a number of configuration settings for the SSO Agent.

Figure 2. Actions > Properties page



To configure the SSO Agent settings:

1. In the DSC Configuration Tool, select **SonicWALL SSO Agent** in the left pane and then navigate to the **Actions > Properties** page.
2. For **Host IP**, type in the IP address of the machine with the SSO Agent installed.
3. For **Logging Level**, select one of the following from the drop-down list:
   - **0** - No logging
   - **1** - Errors will be logged
   - **2** - Debug messages and errors will be logged
   - **3** - Diagnostic messages, debug messages, and errors will be logged
4. For **Cache Refresh Time**, enter the number of seconds that items should remain in the SSO Agent cache. The default is 60 seconds, the range is 30-600 seconds. For more information, see About the SSO Agent cache on page 8 and Using the SSO Agent cache on page 36.
5. For **Max Thread Count**, enter the maximum number of threads that the SSO Agent can use at one time. The default is 300, the range is 50-999.
6. For **Query Source**, select the desired method for the SSO Agent to identify the user. Select one of the following from the drop-down list:
   - **NETAPI** - Use NETAPI to identify the user (default)
   - **WMI** - Use WMI to identify the user

For more information about using NETAPI or WMI, see:

- About client probing with NETAPI or WMI on page 11
- Configuring NETAPI and WMI methods on page 37
- Using the NETAPI/WMI scanner on page 38

- **DC Security Log + WMI** - Use Domain Controller security logs to identify the user and use WMI as a fallback method
- **DC Security Log + NETAPI** - Use Domain Controller security logs to identify the user and use NETAPI as a fallback method
- **DC Security Log** - Use Domain Controller security logs to identify the user
- **DC Security Log + NetAPI + WMI** - Use Domain Controller security logs to identify the user and use NETAPI and WMI as fallback methods

  For more information about using DC Security Log, see:

  - About DC security logs on page 11
  - Configuring the DC security log method on page 40

7 Select the **Allow real time diagnostic** checkbox to make the SSO Agent service send diagnostic messages in real time. This option is available with all **Query Source** methods.

8 Depending on the selected Query Source method, additional options are displayed.

See Configuring NETAPI and WMI methods on page 37 or Configuring the DC security log method on page 40 for information about these options.

9 For **Configuration File**, if not using the default file or path, enter the custom path and name of the configuration file. The default is:
`C:\Program Files (x86)\SonicWALL\DCON\SSO\CIAConfig.xml`.

10 Click **Apply** to restart the service with the new settings and stay on the page.

11 Click **OK** to restart the service with the new settings and close the page.

Viewing logs

To view the SSO Agent log messages:

1 In the DSC Configuration Tool, select **SonicWALL SSO Agent** in the left pane and then navigate to the **Actions > View Logs** page.

The log viewer page is displayed. Log entries from the last 10 minutes are shown. For entries older than this, you can check Applicaton Logs from the Windows Event Viewer.

You can control the type of log messages displayed by setting the **Logging Level** in the **Actions > Properties** page.

2 To refresh the page, click **Refresh**.

3 To export the log entries as a CSV file, click **Export**.

4 To close the window, click **Close**.

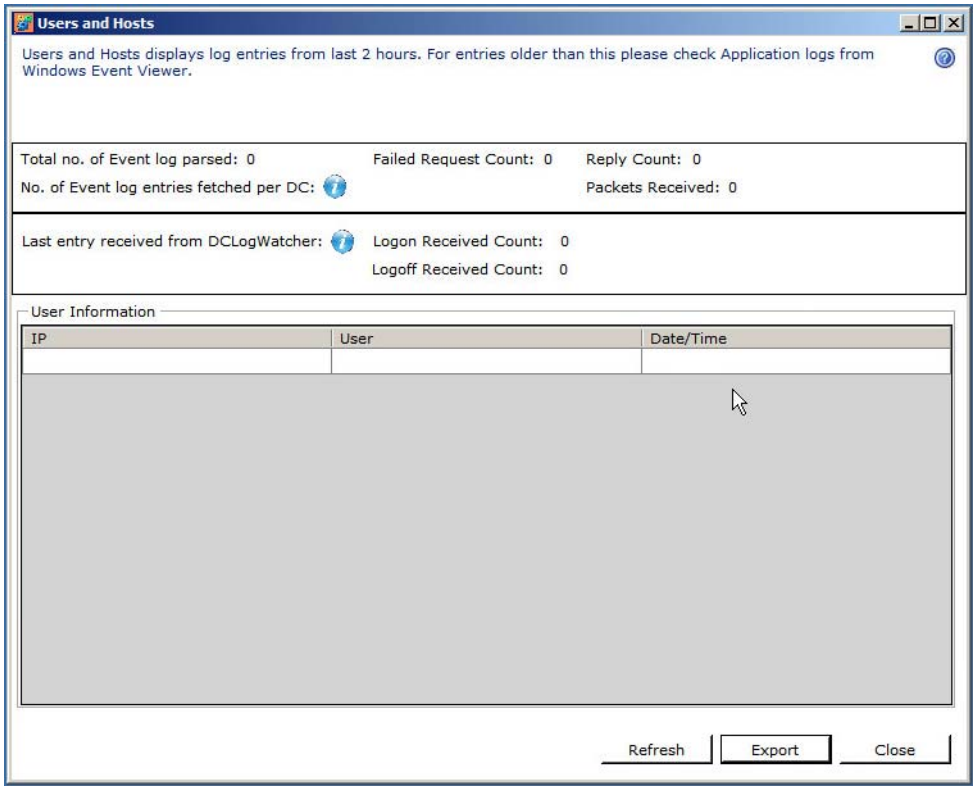
Displaying Users and Hosts statistics

The Users and Hosts page of the DSC Configuration Tool displays the IP address of the user, the user name, and the date/time of the login/logoff event. It also shows the number of requests received from the appliance and the number of replies sent back to it. For DC security log, the page displays the number of event log entries parsed and the number of event log entries fetched from each domain controller.

Viewing LogWatcher Information in Users and Hosts Page

The Users and Hosts page shows the list of DC LogWatcher(s) that are communicating with DSC, and the time of the last packet received from each DC LogWatcher. It also displays the total number of logon and logoff packets received from DC LogWatcher(s).

Figure 3. Actions > Users and Hosts page



To use the Users and Hosts page:

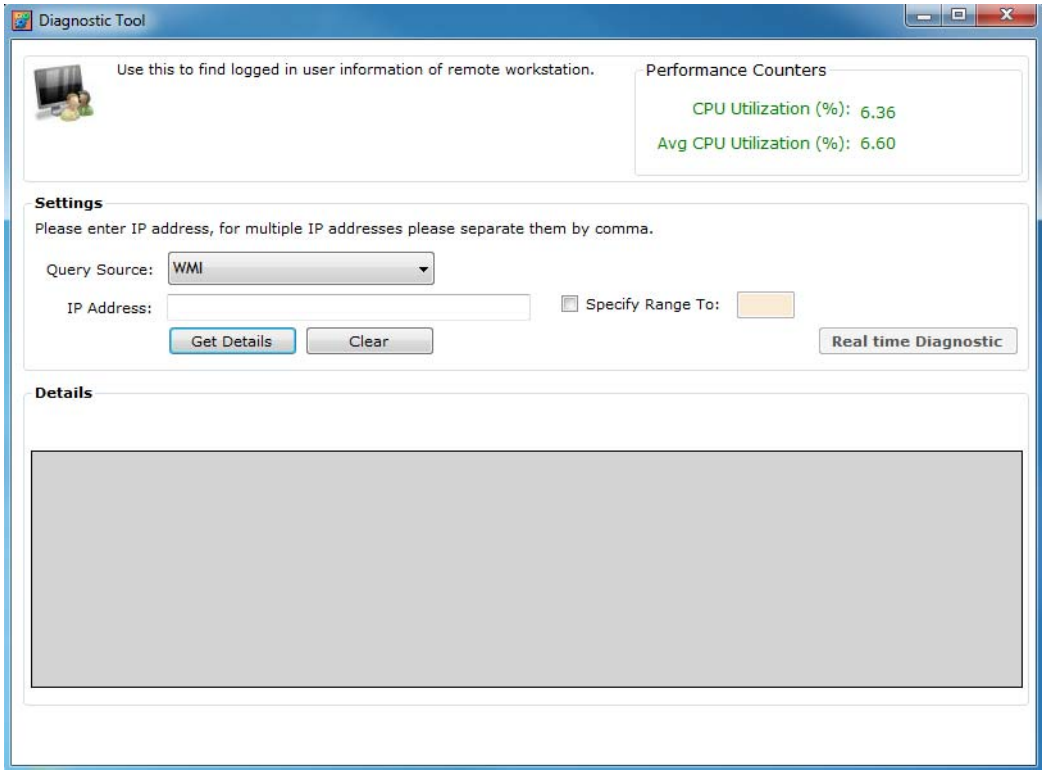
1. In the DSC Configuration Tool, select **SonicWALL SSO Agent** in the left pane and then navigate to the **Actions > Users and Hosts** page.
2. To refresh the page, click **Refresh**.
3. To export the entries as a CSV file, click **Export**.
4. To close the window, click **Close**.

Using the Diagnostic Tool

The Action > Diagnostics Tool page of the DSC Configuration Tool provides a way to find logged in user information for remote workstations. You can manually identify IP addresses by entering multiple IP addresses separated by commas or an IP address range. The results can be exported to a CSV file.

The Diagnostic Tool indicates current and average CPU utilization by the SSO Agent. You can also get real-time diagnostic information on this page.

Figure 4. Actions > Diagnostic Tool page



To display and use the Diagnostic Tool:

1. In the DSC Configuration Tool, select **SonicWALL SSO Agent** in the left pane and then navigate to the **Actions > Diagnostic Tool** page.

   The Diagnostic Tool page is displayed.

2. Select one of the following from the **Query Source** drop-down list.
   - **WMI**
   - **NETAPI**
   - **NETAPI - Workstation Info**
   - **DC Security Logs - All Users**
3. In the IP Address field, type in the IP address of the SSO Agent.
4. Optionally select the **Specify Range To** checkbox and fill in the field.
5. Click **Real time Diagnostic** to get real-time diagnostic messages.
6. Click **Get Details**. The information is displayed in the **Details** field.
7. Click **Clear** to clear the **Details** field.
8. Click **Export to CSV** to save the details to a CSV file on your computer.

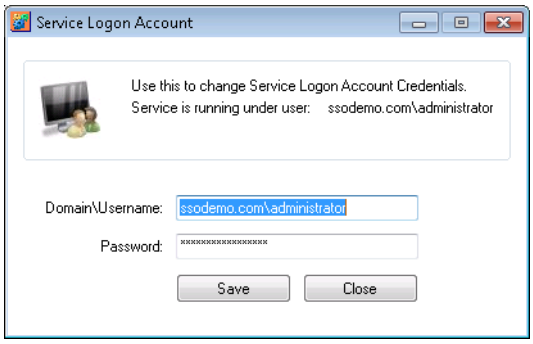
Using the Windows Service Users page

The **Action > Windows Service Users** page displays all the service users configured by the administrator. The users might be used by services on the end-user's computer. The SSO Agent ignores all events whose user names are in this list.

Using the Service Logon User page

The **Action > Service Logon User** page displays the current service logon user and allows you to configure it. The WMI, NetAPI, and DC security log methods require domain administrator privileges. The service should be run with a domain administrator account. You can set up an account name and password on this page.

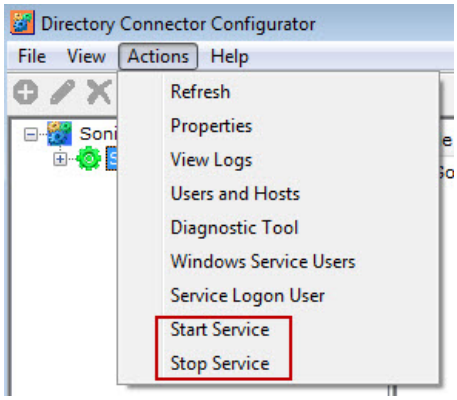
Figure 5. Actions > Service Logon User page



Starting and stopping the Windows service

The **Action > Start Service** and **Action > Stop Service** pages provide a way to start and stop the Windows service for the SSO Agent.

Figure 6. Actions pages for starting/stopping Windows service



Using the Load Test file

The Load Test feature allows you to preload a static set of IP-to-username mappings and static user configuration in a user-defined test file.

The tester can create a file named static.csv in the program installation directory, which by default is *C:\Program Files\Dell SonicWALL\SSOAgent*. The following is an example of a static.csv:

```
10.0.0.0,user0
10.0.0.1,user1
10.0.0.2,domain\user2
...
```

If this file exists, the SSO Agent loads it at the service start time and checks and reloads this file every 60 seconds.

You can view the test users and IP addresses in the **Action > Users and Hosts** screen of the DSC Configuration Tool, in the User Information list.

Using the Help Menu

The **Help** menu in the Directory Connector Configuration Tool has two options:

- Send Feedback

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

- About

  Select **About** to display a popup window with the installed version number of Directory Services Connector and the SSO Agent.

Adding Dell SonicWALL appliances

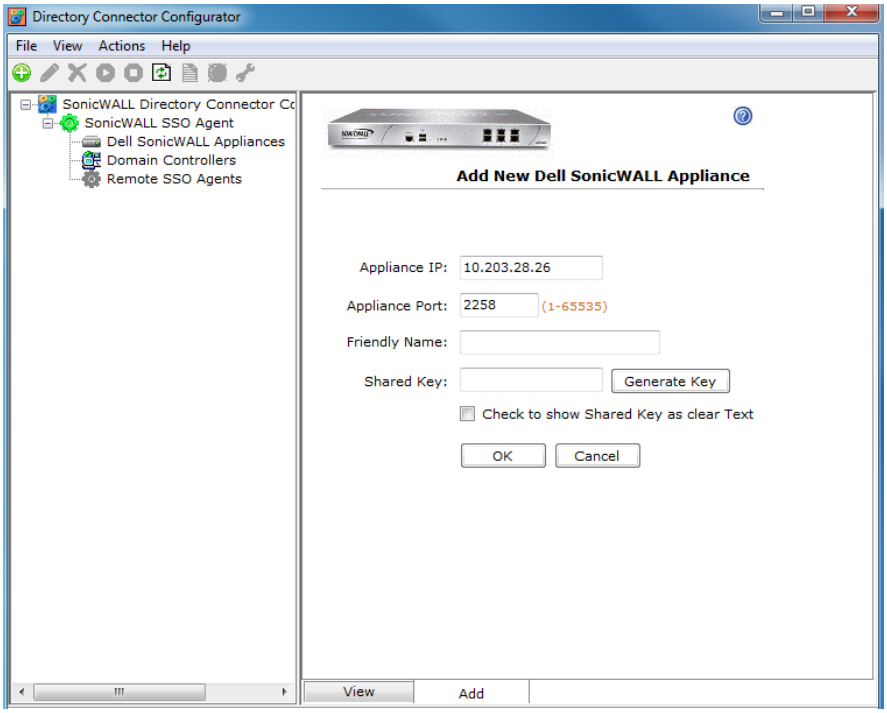
Dell SonicWALL network security appliances provide Single Sign-On functionality using the SSO Agent to identify user activity based on the workstation IP address.

To add a Dell SonicWALL network security appliance in Directory Services Connector:

1 Launch the Configuration Tool.

2 Expand **SonicWALL Directory Connector** and **SonicWALL SSO Agent** in the left column by clicking the **+** buttons.

3 Right-click **Dell SonicWALL Appliances** and select **Add**.



4 For **Appliance IP**, type in the IP address of the appliance.

5 For **Appliance Port**, type in the port on which the SSO Agent will communicate with the appliance. The default is 2258.

6 For **Friendly Name**, enter a descriptive name for the appliance.

7 For **Shared Key**, do one of the following:

- Type in the key (password) to use.
- Click **Generate Key** to automatically create a key.

> **IMPORTANT:** You must enter the same Shared Key in SonicOS when configuring the appliance for Single Sign-On.

8 Optionally select the **Check to show Shared Key as clear Text** checkbox. The key is displayed in readable text in the above field.

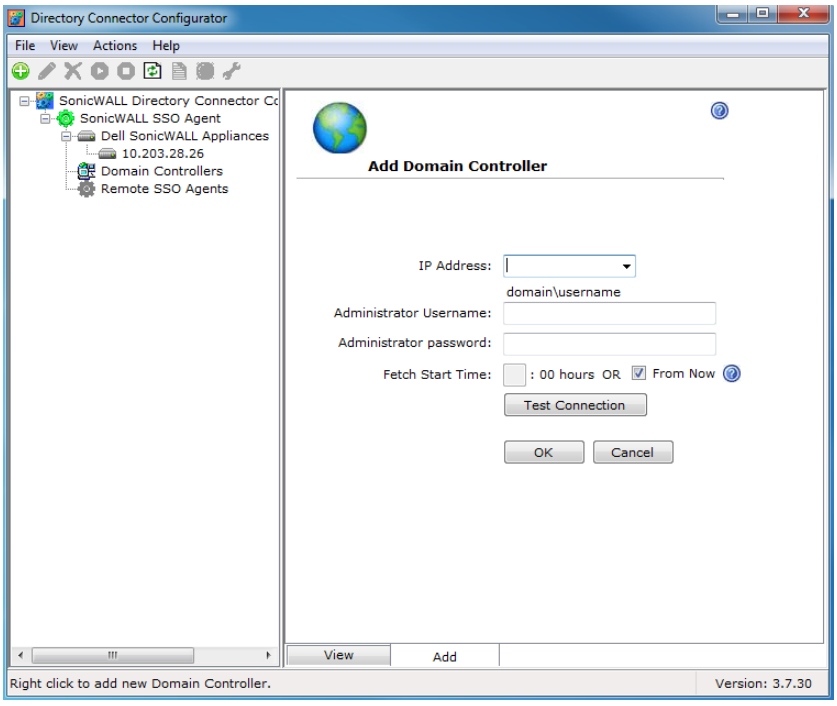
9 Click **OK**.

Adding domain controllers

Only machines configured with a domain controller role can be set as the domain controller in the Directory Connector Configuration Tool.

1 In the Directory Connector Configuration Tool, right-click **Domain Controllers** in the left pane.

2 Select **Add**.



3 In the right pane, type the domain controller IP address in the **IP Address** field.

4 In the **Administrator Username** field, enter the domain administrator user name.

5 In the **Administrator password** field, enter the domain administrator password.

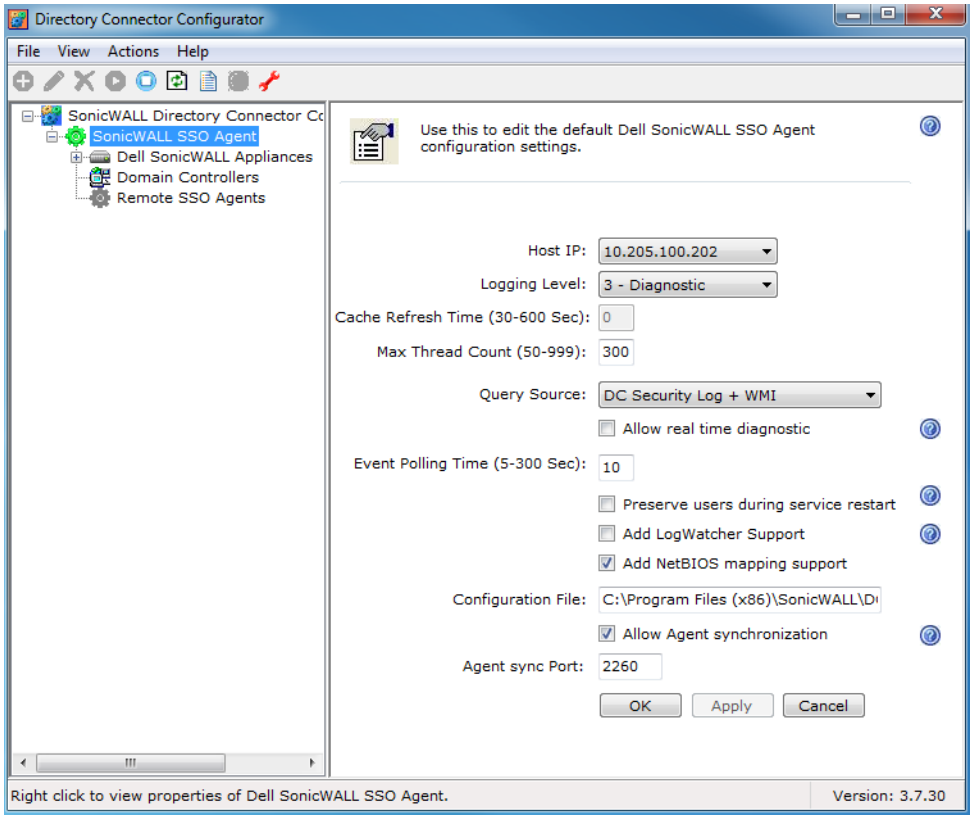
6 The **Fetch Start Time** is the start time from which the agent starts fetching all event logs from the DC during the service start up. It fetches all logs for a specified time until the service start time.

7 Click **Test Connection** to check the connectivity to the domain controller.

8 Click **OK**.

Configuring remote SSO Agents

To enable the agent synchronization (Agent-to-Agent communication), go to the **SonicWALL SSO Agent > Properties** page (Actions > Properties) in the Configuration tool.

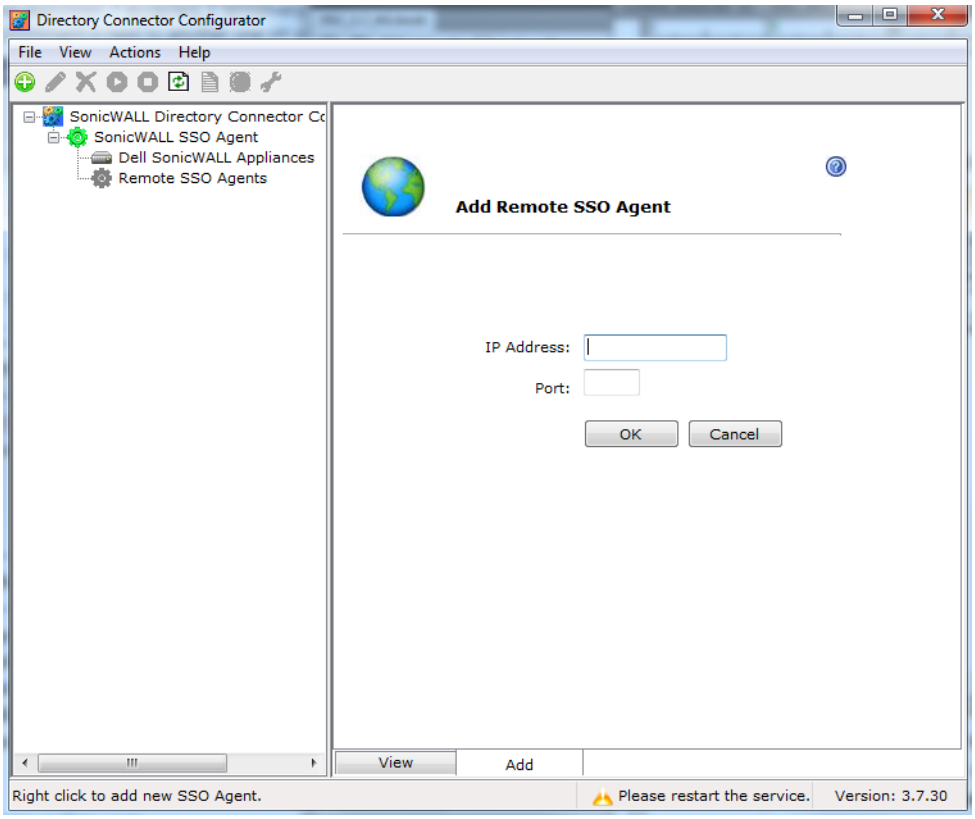


To configure remote SSO Agents in Directory Services Connector:

1 Launch the Dell SonicWALL Directory Services Connector Configuration Tool.

2 Expand **SonicWALL Directory Connector** and **SonicWALL SSO Agent** in the left column by clicking the **+** buttons.

3 Right-click **Remote SSO Agents** and select **Add**.



4 In the **Agent IP** field, type in the IP address of the remote SSO Agent.

5 In the **Sync Port** field, accept the default of 2260 or type in the custom sync port.

By default, the SSO Agent uses TCP port 2260 to receive the agent synchronization data.

6 Click **OK**.

Configuring Agent-to-Agent communication

Dell SonicWALL Directory Services Connector SSO Agents can communicate and share information (such as global user-databases) between agents.

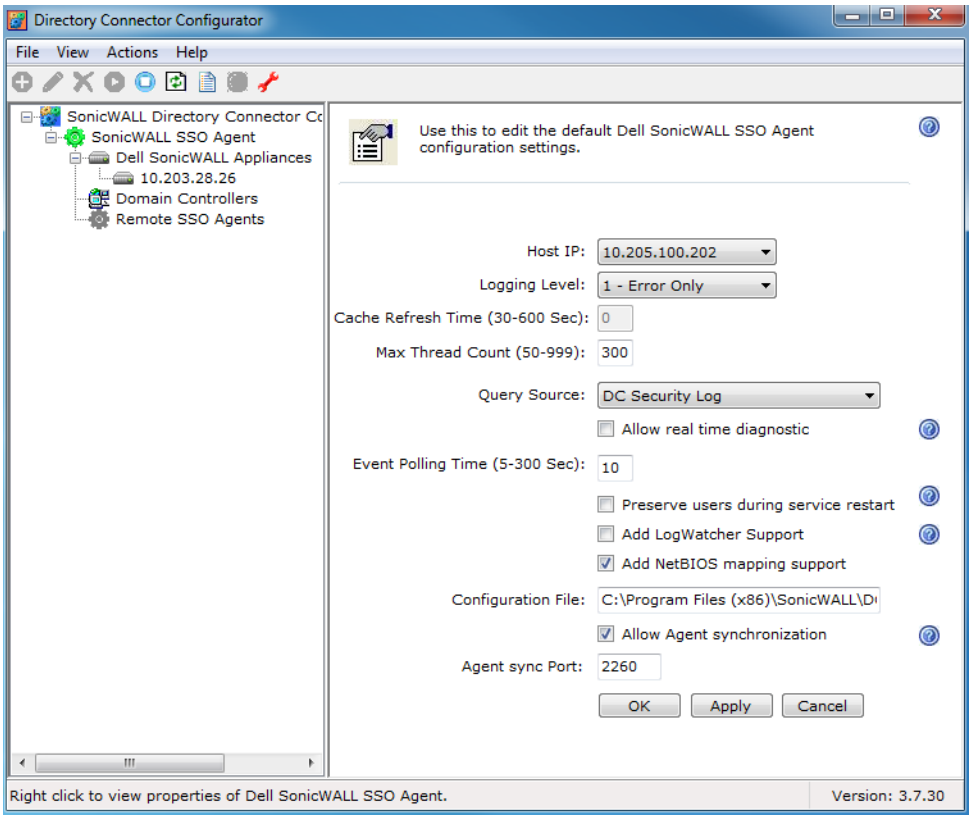
Also known as Agent Synchronization, this feature is available when Query Source is set to DC Security Log with or without NetAPI/WMI, and when Enable Scanner is selected when Query Source is set to either NETAPI or WMI. Agent synchronization can be used between agents which are using different Query Source methods.

To enable Agent Synchronization (Agent-to-Agent Communication):

1 In the Directory Connector Configuration Tool, right-click **SonicWALL SSO Agent** in the left pane.

2 Select **Properties**.

The agent configuration settings screen appears.



3 Select the **Allow Agent synchronization** checkbox and enter 2260 (the default port for Agent-to-Agent Communication) in the **Agent sync Port** field.

> **NOTE:** This option is only available when Query Source is set to DC Security Log with or without NetAPI and/or WMI, and when Enable Scanner is selected when Query Source is set to either NETAPI or WMI. Agent synchronization can be used between agents which are using different Query Source methods.

4 Click **OK**.

Using the SSO Agent cache

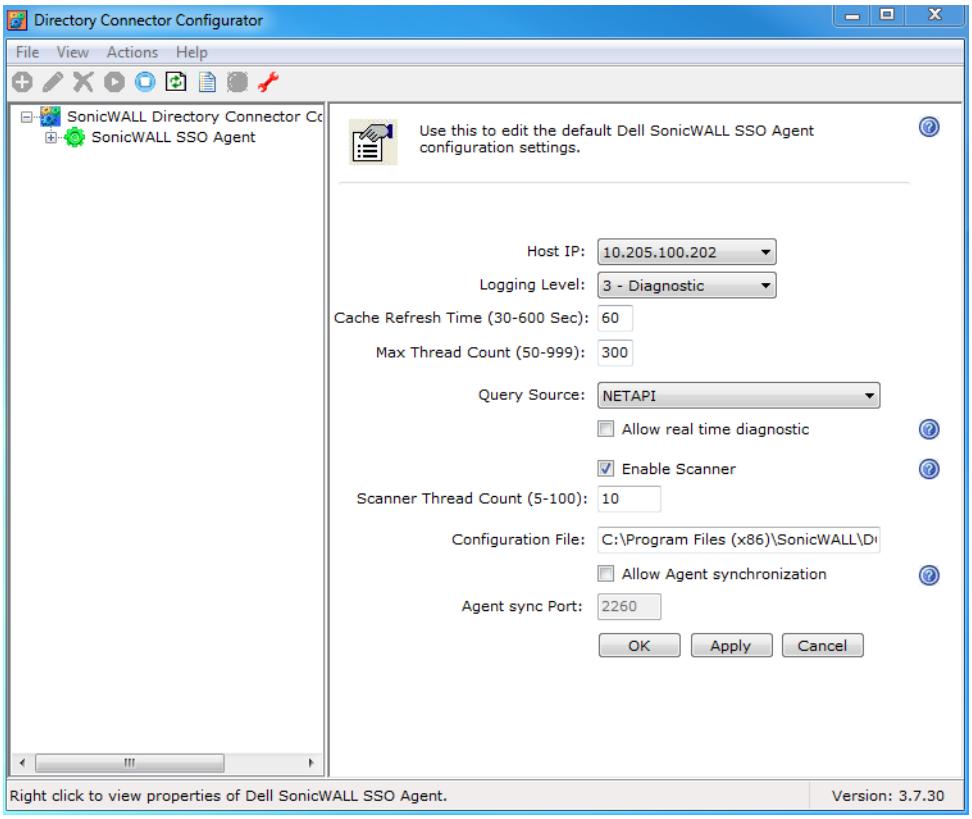
The SSO Agent can cache user information. By default, the cache refresh rate is set to 60 seconds, with a range of 30–600 seconds.

The cache settings can be overridden from the Windows Registry. To disable caching (cache refresh time = 0), edit the Registry and set the REFRESHTIME value to 0. If the cache refresh rate is set to zero seconds, user information is fetched from the workstation for every request from the Dell SonicWALL appliance.

See About the SSO Agent cache on page 8 for more information on when the cache can be helpful.

To change the cache refresh time in the SSO Agent:

1 In the DSC Configuration Tool, right-click the **SonicWALL SSO Agent** in the left pane and select **Properties**.



2 In the right pane, enter the desired number of seconds in the **Cache Refresh Time** field. The default is 60 seconds, with a range of 30–600 seconds.

NOTE: See About the SSO Agent cache on page 8 for information about appropriate values for the cache refresh time.

3 Click **OK**.

Configuring NETAPI and WMI methods

As a query source, the SSO Agent can use either the NETAPI or WMI protocol to communicate with workstations. You can select the desired protocol as the Query Source option in the Directory Connector Configuration Tool. NETAPI and WMI provide information about users that are logged into a workstation, including domain users, local users, and Windows services.

NETAPI provides faster, though possibly slightly less accurate, performance. WMI provides slower, though possibly more 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 on to the same computer, then at that point the previous user is logged out from the Dell SonicWALL appliance.

To configure the NETAPI or WMI method in Directory Services Connector:

1 In the Directory Connector Configuration Tool, right-click **SonicWALL SSO Agent** in the left panel.

2 Select **Properties**.

3 For the options above **Query Source**, see Configuring SSO Agent settings on Actions > Properties on page 27.

4 For **Query Source**, select either **NETAPI** or **WMI** from the drop-down list.

5 Select the **Allow real time diagnostic** checkbox to make the SSO Agent service send diagnostic messages in real time.

6 Select the **Enable Scanner** checkbox to enable a NETAPI/WMI scanner that will keep track of logged in users from remote clients.

For information about the scanner, see Using the NETAPI/WMI scanner on page 38.

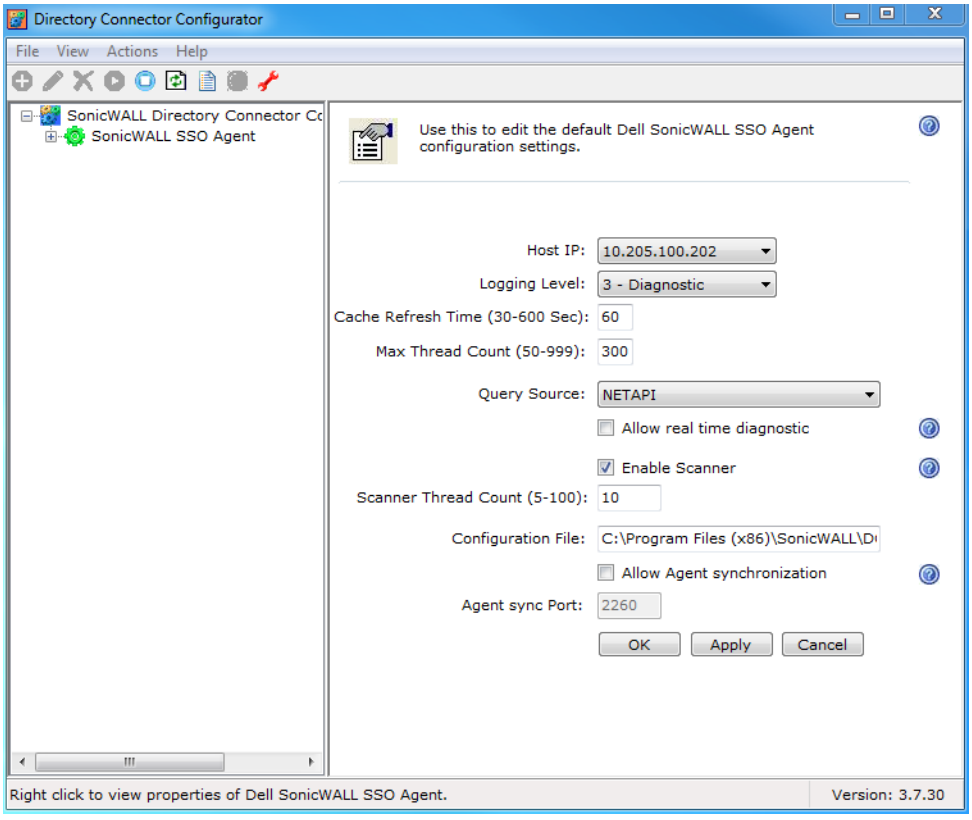
7 For **Scanner Thread Count**, enter the maximum number of threads that the scanner can use at one time. The default is 10 and the range is 5-100.

8 Click **Apply** to restart the service with the new settings and stay on the page.

9 Click **OK** to restart the service with the new settings and close the page.

Using the NETAPI/WMI scanner

The SSO Agent Properties (Actions > Properties) page in the DSC Configuration Tool provides the **Enable Scanner** option to enable the NETAPI/WMI background scanner. The scanner works with either NETAPI or WMI as the query source, and keeps track of logged in users from remote clients. Right-click the SSO Agent or use the Actions menu to go to the Properties page and set this option.



Upon a user information request for any IP address from the appliance, if caching is enabled, 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 address to its scanner queue for further processing.

Depending on the firmware version running on the appliance, the SSO Agent does one of the following when the entry is not present in its cache:

- Replies back to the appliance with an In_Progress status
- Does not send a reply back to the appliance

The SSO Agent initially starts a configurable number of threads (scanner thread count). 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.

Upon identifying the user through either NETAPI or WMI, the agent sends a log in notification with the user name if an In_Progress status was previously sent for the same IP address. If no reply was previously sent, the user information is simply cached.

When the scanner is enabled and the SSO Agent detects a user change on a client machine, it sends the logoff or update notification to the firewall.

Bad IP address handling by scanner

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.

Priority queues in the scanner

With Agent-to-Agent communication, smart NETAPI/WMI scanners allow the transfer of polling requests between SSO Agents. When one agent is overloaded with requests, a comparatively free agent can handle the requests.

The scanner differentiates IP addresses into three queues, each with a specified priority:

- New IP request (High Priority)
- Succeeded IP (Mid Priority)
- Bad IP (Low Priority)

Any IP address for which the agent already sent an In Progress status is treated as High Priority.

For any IP address present in either the Mid Priority queue or Bad IP queue, if the difference between the current time and the time of the last request is greater than session time, the agent drops that IP address and moves on to process another address in the queue.

The number of processing threads allocated for the scanner is divided into three categories:

- High — 70 percent of threads
- Mid — 20 percent of threads
- Low — 10 percent of threads

This thread allocation is dynamic and depends on the frequency of requests for identifying new IP addresses from the appliance. This dynamic thread allocation ensures that no thread is idle or wasted in any scenario.

To ensure that the agent does not process any IP addresses that have 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."

Non-responsive workstation handling

The handling of non-responsive workstations to queries from WMI and NETAPI is optimized in Dell SonicWALL Directory Services Connector. 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.

Configuring the DC security log method

See the following sections:

Using DC Security Log

Dell SonicWALL Directory Services Connector provides an option for the SSO Agent to identify logged in user information from the domain controller's Windows security log (DC security log or WSL). When using DC security log method as the query source, Directory Services Connector fetches security logs from the configured domain controller. The SSO Agent sends a login notification to the appliance as soon as it detects a user login.

The DC Security Log method works in a fully trusted domain environment where all users are domain users using domain accounts to access Windows or Linux workstations.

The DC Security Log method can optionally be used with either NETAPI or WMI as a fall back to support user identification from non-domain Windows PCs or domain PCs using local accounts. Altogether, there are four query source options involving the DC security log:

- **DC Security Log** — Users are identified from the domain controller's Windows security log; use this option if all users log in to the domain.
- **DC Security Log + NETAPI** — In addition to using the DC security log, this option provides a fall back to using NETAPI to identify users. In case the SSO Agent fails to identify users from the domain controller, it uses traditional NETAPI queries to the user's workstation to fetch user information.
- **DC Security Log + WMI** — In addition to using the DC security log, this option provides a fall back to using WMI to identify users. In case the SSO Agent fails to identify users from the domain controller, it uses traditional WMI queries to the user's workstation to fetch user information.
- **DC Security Log + NETAPI + WMI**— In addition to using the DC security log, this option provides a fall back to using NETAPI or WMI to identify users.

To use DC security log method in Dell SonicWALL Directory Services Connector, ensure that the agent machine has the following minimum requirements:

- Multi-Core processors: two or more, or a dual CPU
- Speed: 2GHz+
- RAM: 2GB, minimum

NOTE: For single core processors, CPU spikes might reach up to 100 percent periodically while using the DC Security Log method in Dell SonicWALL Directory Services Connector. To avoid this, optimization is provided for reading security logs. Also an option is available to read the security logs in current time, minimizing the initial log processing time.

By default, all of the DC Security Log options require a domain administrator account or local administrator account on the domain controller to read the DC security log. The account information is entered during the configuration, described in the following paragraphs. If an account with administrator privileges is not available, user identification through the domain controller security log can be configured for WMI with a non-administrator domain account.

User identification through the domain controller security log can also be configured by using WMI with a non-administrator domain account. Although this option does not require use of the administrator domain account, it still requires read access to the security log, which can be accomplished by configuring a non-admin account. For more information, refer to the *Configuring a Non-Admin Domain Account for SSO Agent to Read Domain Security Logs* configuration guide, available at:

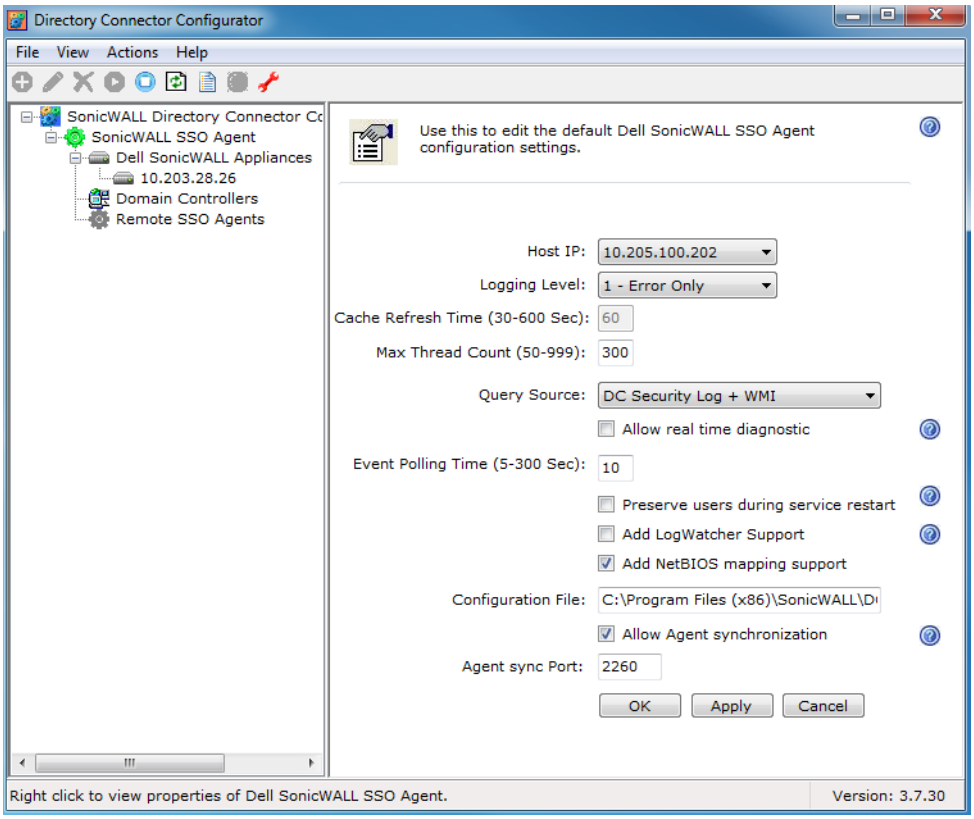
https://support.software.dell.com/kb/sw9764

Windows Server uses the DC security log to record logon/logoff events and/or other security-related events specified by the system's audit policy. If the audit policy is set to record log ins, a successful domain log in records the user's user name and computer name in the security log. On Windows Server 2003 and above, the computer's IP address is also logged.

To configure the DC Security Log method in Directory Services Connector:

1 In the Directory Connector Configuration Tool, right-click **SonicWALL SSO Agent** in the left panel.

2 Select **Properties**.



3 For the options above **Query Source**, see Configuring SSO Agent settings on Actions > Properties on page 27.

4 For **Query Source**, select one of the **DC Security Log** options from the drop-down list.

5 Select the **Allow real time diagnostic** checkbox to make the SSO Agent service send diagnostic messages in real time.

6 For **Event Polling Time**, enter the number of seconds to use for the polling interval.

The Event Polling Time option is visible only if one of the DC Security Log options is selected in the query source field. The SSO Agent fetches event logs from the domain controller on a regular time interval to

discover updated user information. The Event Polling Time option provides a way to specify this interval. The minimum is five seconds, and the maximum is 300 seconds, with a default of 10 seconds.

7 Select the **Preserve users during service restart** checkbox to save user information across a service restart.

After restarting the SSO Agent service, the user information is restored. Because the SSO Agent must be restarted for Properties changes to take effect, this allows the agent to maintain current user information across these restarts. When a backup is older than 15 minutes, the information is not restored to avoid restoring outdated information.

If this option is unchecked when using DC security log, the user information is not saved during a service restart. When the next user information request comes in for a previously logged in user, the DC logs are checked, but there is no new logon event and so the user is not identified. If Query Source is set to DC security log only, the SSO Agent sends no user information to the appliance. If Query Source is set to DC security log with NETAPI or WMI, the agent does a NETAPI or WMI query to the user PC to identify the user.

8 Optionally select the **Add LogWatcher Support** checkbox. For information about LogWatcher, see About LogWatcher on page 12 and Installing and configuring LogWatcher on page 42.

- Enter the **LogWatcher Port** number (default is 2259).
- Enter the **LogWatcher Shared Key**.

NOTE: The SSO port number and shared key in the DCConfig.xml file on the Domain Controller must be the same as the LogWatcher Port number and LogWatcher Shared Key.

9 Optionally select the **Add NetBIOS mapping support** checkbox.

For information about the NetBIOS option, see About NetBIOS mapping support on page 12.

10 If multiple SSO Agents exist, select the **Allow Agent synchronization** checkbox to allow Agent-to-Agent communication. For information about Agent synchronization, see About Agent-to-Agent communication on page 7 and Configuring Agent-to-Agent communication on page 35.

11 For **Agent sync Port**, if **Allow Agent synchronization** is enabled, enter the port number of the synchronization port that the SSO Agents should use. The default is 2260.

12 Click **Apply** to restart the service with the new settings and stay on the page.

13 Click **OK** to restart the service with the new settings and close the page.

14 If a domain controller is not already added, configure the domain controller information in the Configuration Tool. See Adding domain controllers on page 33.

Installing and configuring LogWatcher

The **Add LogWatcher Support** option is available when a DC Security Log method is selected for Query Source.

The LogWatcher installer is available on MySonicWALL with the SSO group in the Download Center. The installation setup program checks for pre-requisites during the installation process. LogWatcher can be installed on all Domain Controllers.

After installation, LogWatcher needs to be configured to communicate with the SSO Agent and Directory Services Connector. The administrator must open the install folder and change the DCConfig.xml as described below. A readme.txt file is launched at the end of the installation which describes this procedure.

Logon Audit must be enabled on the domain controller.

Configuring LogWatcher on the Domain Controller

The DCConfig.xml file is used for configuration. The following XML snippet shows how the data is stored in the DCConfig.xml file:

```
<SONICWALL_LOG_WATCHER>
    <AGENTS>
        <AGENT>
            <IP_ADDRESS>10.50.173.252</IP_ADDRESS>
            <PORT_NO>2259</PORT_NO>
        </AGENT>
    </AGENTS>
    <SEC_KEY>abc123</SEC_KEY>
    <IGNORE_TIME>10</IGNORE_TIME>
    <LOG_LEVEL>0</LOG_LEVEL >
    <LW_PORT_NO>2259</LW_PORT_NO>
    <DC_IP>10.50.173.54</DC_IP>
</SONICWALL_LOG_WATCHER>
```

The above data fields are defined as follows:

Table 1. LogWatcher data fields

IP_ADDRESS	IP address of the SSO Agent
PORT_NO	Port number of the SSO Agent for receiving the UDP packet
SEC_KEY	Secret Key for encrypting the packet data
IGNORE_TIME (in seconds)	Used to avoid successive user logon/logoff; default value is 10 seconds
LOG_LEVEL	Can have any of three values: • 0 (NOLOGS) - Do not log any messages • 1 (ERRORSONLY) - Log only Error messages • 2 (DIAGNOSTIC) - Log all messages
LW_PORT_NO	LogWatcher port for sending the UDP packet
DC_IP	IP address of the Domain Controller

Configuring/Enabling LogWatcher in Directory Services Connector

To configure LogWatcher in Directory Services Connector, perform the following steps:

1. In the DSC Configuration Tool, right-click the **SSO Agent** or use the **Actions** menu to open the **Properties** page of the SSO Agent.
2. Select **DC Security Log** in the **Query Source** drop-down list.
3. Select the **Add LogWatcher Support** checkbox.
4. Enter the **LogWatcher Port** number (default is 2259).
5. Enter the **LogWatcher Shared Key**.

> **NOTE:** The SSO port number and shared key in the DCConfig.xml file on the Domain Controller must be the same as the LogWatcher Port number and LogWatcher Shared Key.

Setting a group policy to enable audit logon on Windows Server 2003

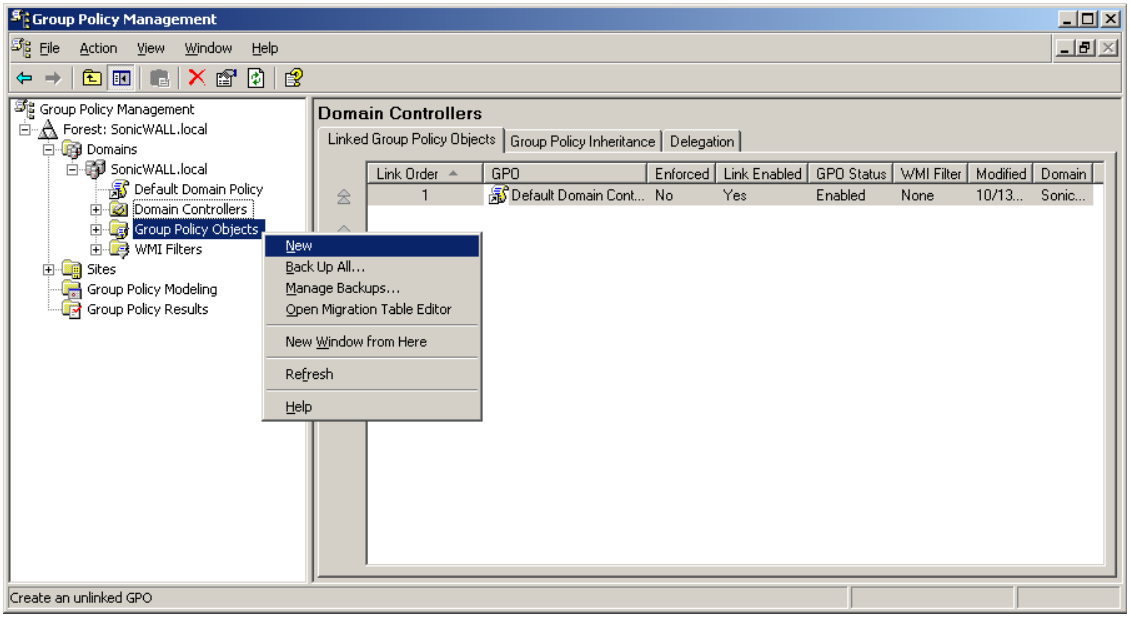
By default the audit logon is disabled on Windows server 2003.

To enable audit logon, complete the following steps:

1 Start the Group Policy Management Console.

2 Browse to the following location - Forest: **Domain Name > Domains > Domain Name > Group Policy Objects**, replacing “Domain Name” with your domain.

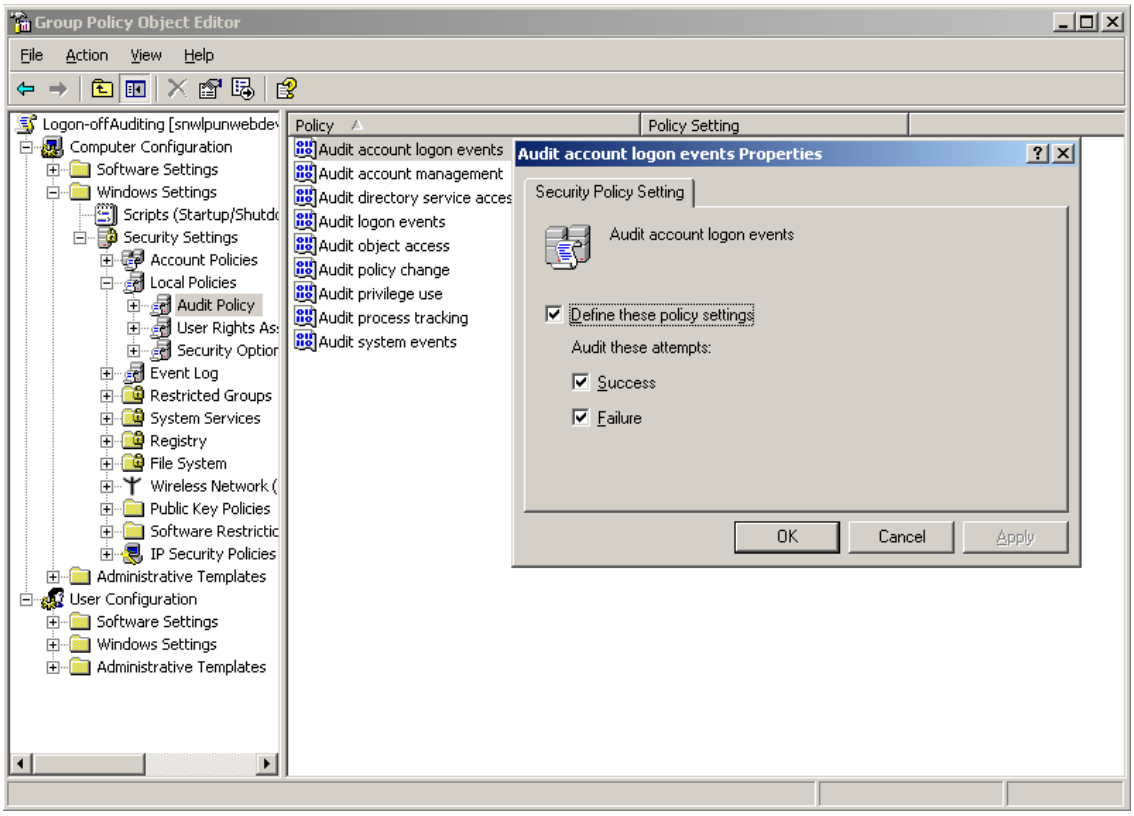
3 Right-click on **Group Policy Objects** and select **New**.



4 Give your policy a name and click **OK**.

5 Expand the Group Policy Objects folder and find your new policy. Right-click on the policy and select **Edit**...

6 Browse to the following location: *Policy Name* **> Computer Configuration > Windows Settings > Security Settings > Local Policies > Audit Policy**. Left-click on **Audit Policy**. The policy settings are displayed in the right window.



7 Double-click **Audit account logon events** and select **Success**.

8 Click **OK**.

9 Double-click “Audit logon events” and select **Success**.

10 Click **OK**.

11 Double-click “Audit Directory Service Access” and select **Success**.

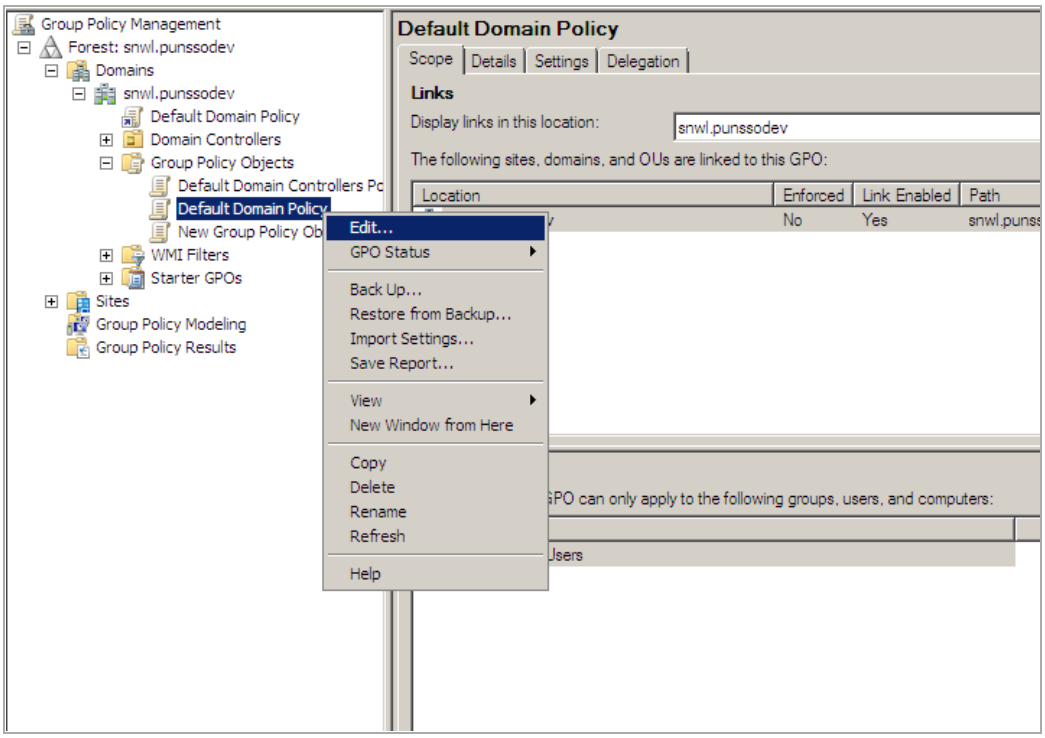
12 Click **OK**.

13 Close the Group Policy Window.

Setting a group policy to enable audit logon on Windows Server 2008

Refer to the following screen to edit the Default Domain Policy.

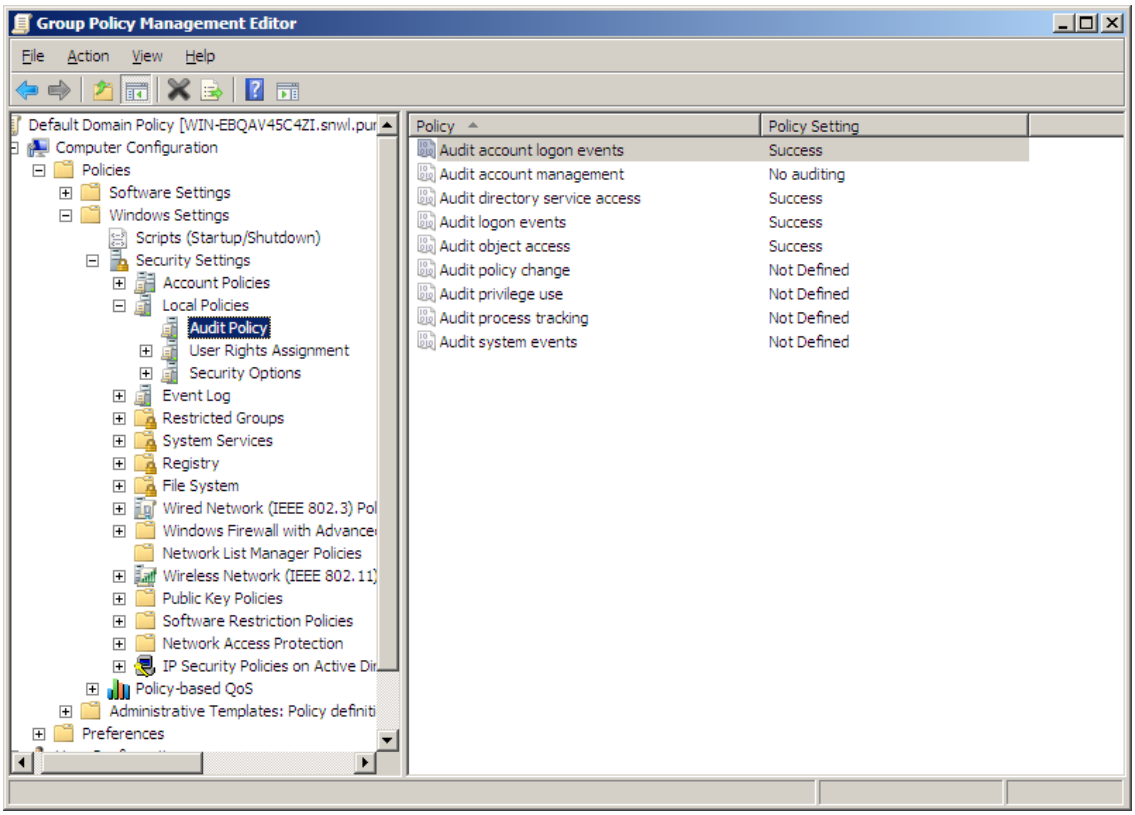
Figure 7. Default domain policy, Windows Server 2008



To finish the Audit Policy, complete the following steps for the screen that follows:

1. Double-click **Audit account logon events** and select **Success**.
2. Click **OK**.
3. Double-click **Audit logon events** and select **Success**.
4. Click **OK**.
5. Double-click **Audit Directory Service Access** and select **Success**.
6. Click **OK**.

7 Double-click **Audit Object access** and select **Success**. Click **OK**.



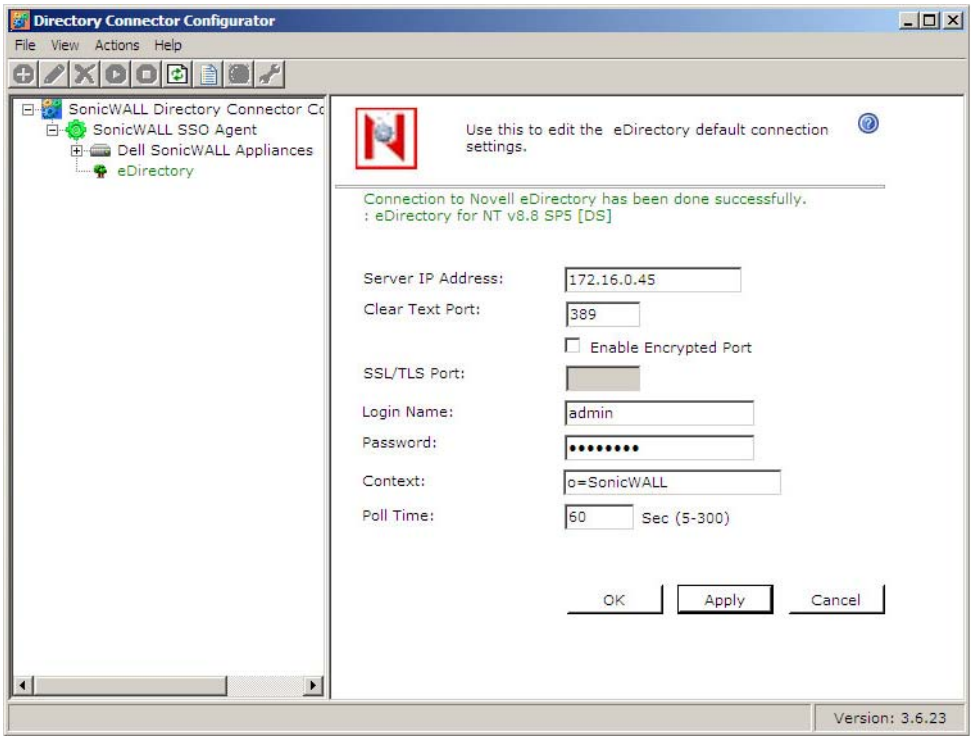
Enabling LDAP over TLS with Novell eDirectory

The SSO Agent supports Novell eDirectory connections secured by Transport Layer Security (TLS). TLS provides secure encryption of communications and verifies the server certificate. The software on your LDAP server must support TLS.

To enable Novell eDirectory connections using LDAP over TLS, complete the following steps:

1 In the Directory Connector Configuration Tool, right-click **eDirectory** in the left pane and select **Properties**.

2 In the right pane, select **Enable Encrypted Port**.



3 Type the port number into the **SSL/TLS Port** field. This can be port 636 or another configured port.

4 Click **OK**.

About Dell

Dell listens to customers and delivers worldwide innovative technology, business solutions and services they trust and value. For more information, visit www.software.dell.com.

Contacting Dell

Technical support:
Online support

Product questions and sales:
(800) 306-9329

Email:
info@software.dell.com

Technical support resources

Technical support is available to customers who have purchased Dell software with a valid maintenance contract and to customers who have trial versions.

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

The site enables you to:

- Create, update, and manage Service Requests (cases)
- View Knowledge Base articles
- Obtain product notifications
- Download software. For trial software, go to Trial Downloads.
- View how-to videos
- Engage in community discussions
- Chat with a support engineer