Release Notes

Directory Connector

SonicWALL Directory Services Connector 3.4.51

Contents

Platform Compatibility

SonicWALL Appliance / Firmware Compatibility

SonicWALL Directory Services Connector version 3.4.51 software is a supported release for use with the following SonicWALL platforms:

- NSA E-Class E5500 / E6500 / E7500 running SonicOS Enhanced 5.0 and above
- NSA 240 / 2400 / 3500 / 4500 / 5000 running SonicOS Enhanced 5.0 and above
- TZ 210 / 210W / 200 / 200W / 100 / 100W running SonicOS Enhanced 5.0 and above
- TZ 190 / 190W / 180 / 180W running SonicOS Enhanced 4.0 and above
- PRO 2040 / 3060 / 4060 / 4100 / 5060 running SonicOS Enhanced 4.0 and above

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

Note: When configuring Active-Active on a SonicWALL SuperMassive E10000 Series appliance, SonicWALL Directory Services Connector version 3.4.51 or newer software is required.

Server Compatibility

SonicWALL Directory Services Connector version 3.4.51 software is supported for installation on servers running the following operating systems:

- Windows 32-bit:
  - Windows Server 2008
  - Windows Server 2003
- Windows 64-bit:
  - Windows Server 2008
  - Windows Server 2003

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
- .Net Framework 3.0
- .Net Framework 3.5

The following Microsoft Windows operating systems and service packs are **not** supported as servers for this version of SonicWALL Directory Connector:

- Windows 7 – All versions
- Windows Vista – All versions
- Windows XP – All versions
- Windows 2000 – All versions

Client Compatibility

The following client operating systems are supported by SonicWALL Directory Services Connector 3.4.51 software:

- Windows 7
- Windows Vista
- Windows XP
- Windows 2000 Professional
- Mac OS X 10.6.0
- Linux/Unix machines running Samba 3.0 or newer

  For information about Samba support, see the *Using Single Sign-On with Samba* Tech Note, available on: http://www.sonicwall.com/us/Support.html

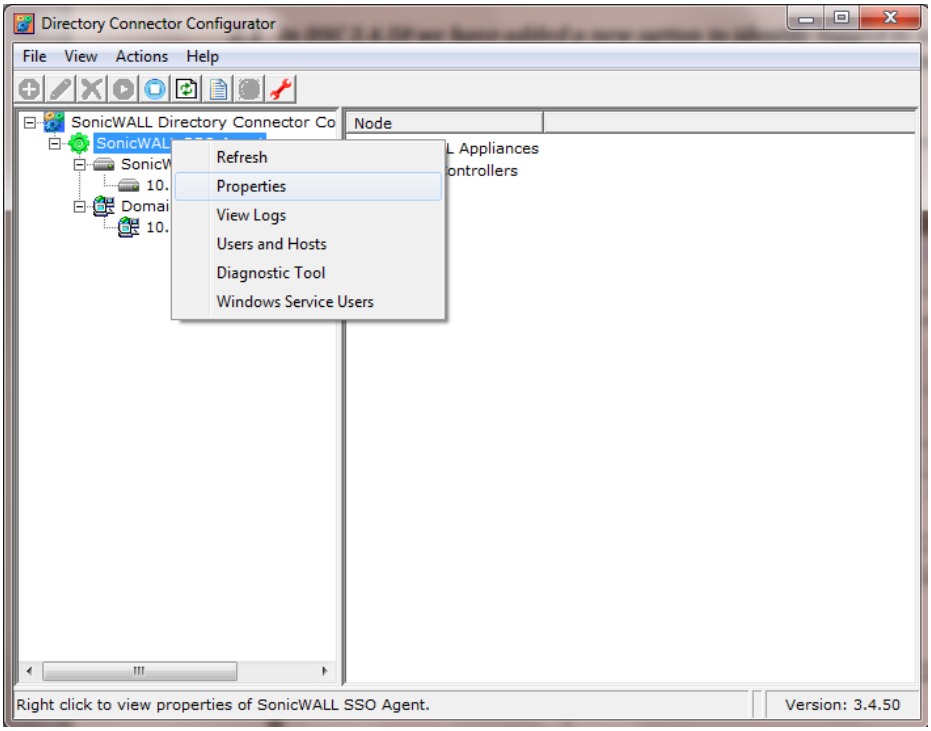
New Features in DSC 3.4.51

SonicWALL Directory Services Connector 3.4.51 provides a new version of the Directory Connector Configurator with the following new features:

Identify Users with DC Windows Security Log

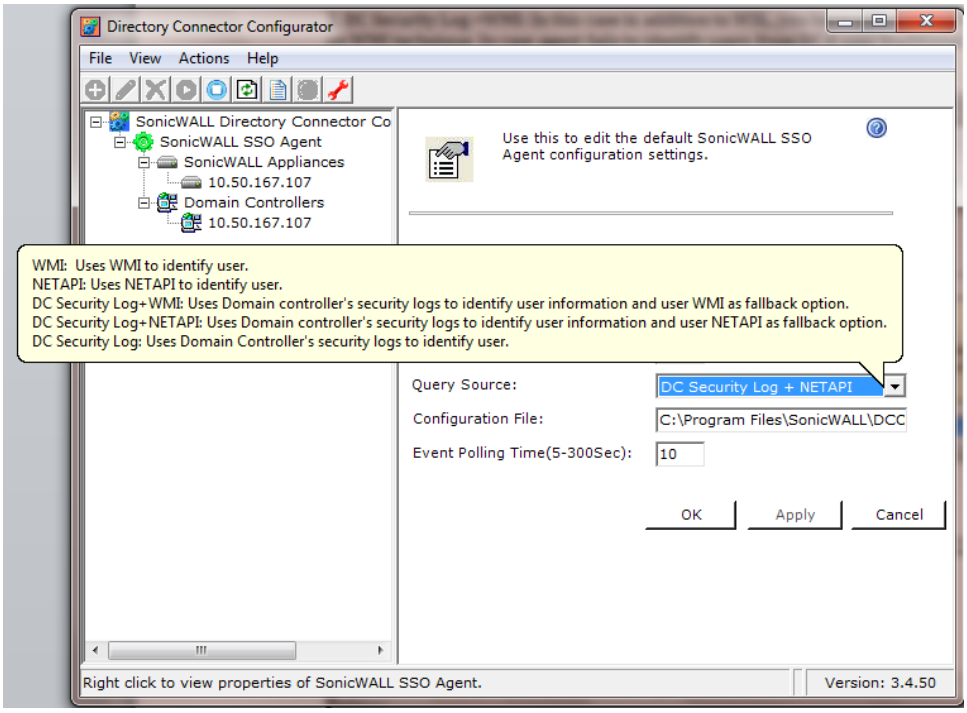
A new option to identify logged in user information from the Domain Controller's Windows Security Log (WSL). It uses SSO UDP Protocol version 4.0. To use this option,

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



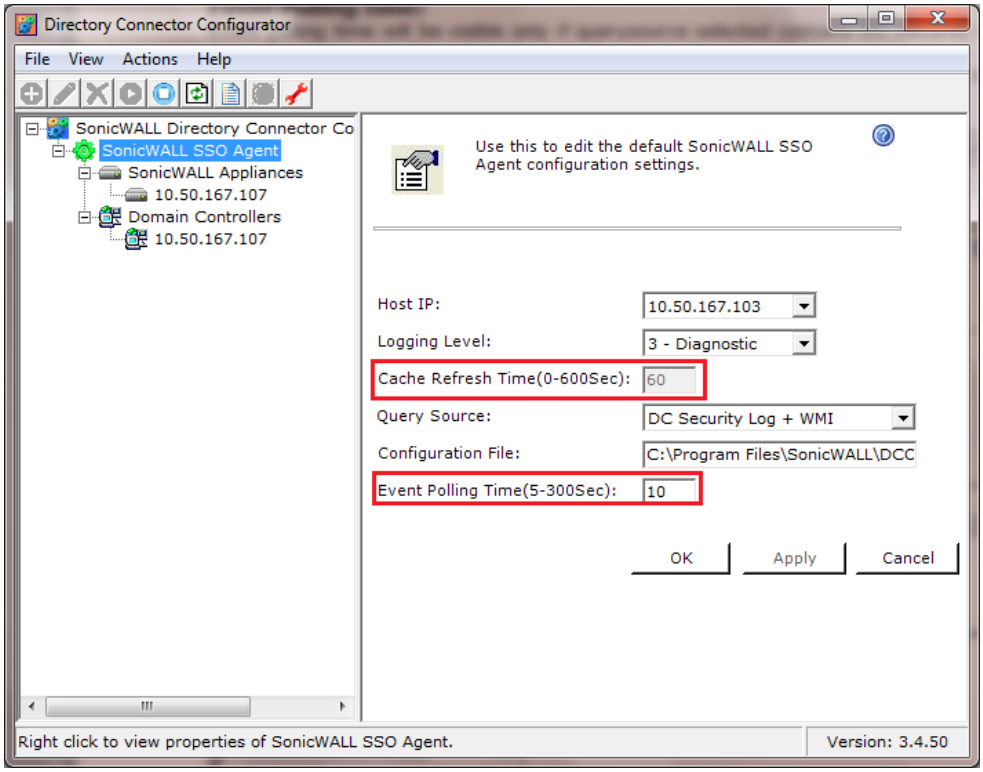
3. In the right pane in the **Query Source** field, select one of the following three new options:
   - **DC Security Log** – User will be identified from the Domain Controller's Windows Security Log; use this option if all users log into the domain.
   - **DC Security Log + NETAPI** – In addition to WSL, 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 WSL, 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.



Event Polling Time

The new **Event Polling Time** option is visible only if one of the **DC Security Log** options are 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 5 seconds, and the maximum is 300 seconds, with a default of 10 seconds.



Configure Domain Controller Information

When using the DC WSL and Event Polling Time options, you must configure Domain Controller information in the Directory Connector Configurator, including the IP address, admin user account, and password.

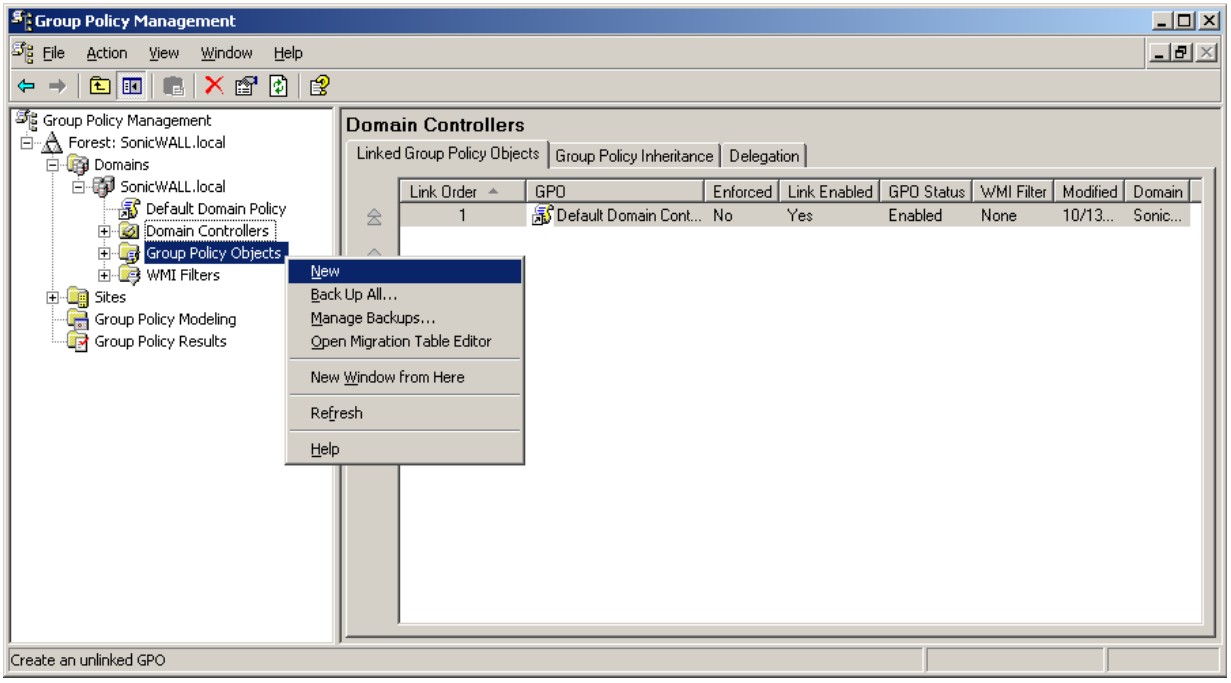
To configure the Domain Controller information:

1. In the Directory Connector Configuration Tool, right-click **Domain Controller** in the left pane.
2. Select **Add**.
3. In the right pane on the **Edit** tab, type the DC IP address into the **IP Address** field.
4. In the **Administrator User** field, enter the domain and admin user name separated by a backslash, such as “snwl\administrator”.
5. In the **Administrator Password** field, type in the password for the admin user.
6. In the **Initial Fetch Time** field, select the time of day for the SSO Agent to begin service startup and fetch event logs from the Domain Controller for the first time. All event logs are fetched before the SSO Agent service is started.
7. To test the connection to the Domain Controller using the IP address and user credentials, click **Test Connection**.
8. Click **OK**.
9. Repeat this procedure to add another Domain Controller.

Setting Group Policy to Enable Logon Audit on Windows Server 2003

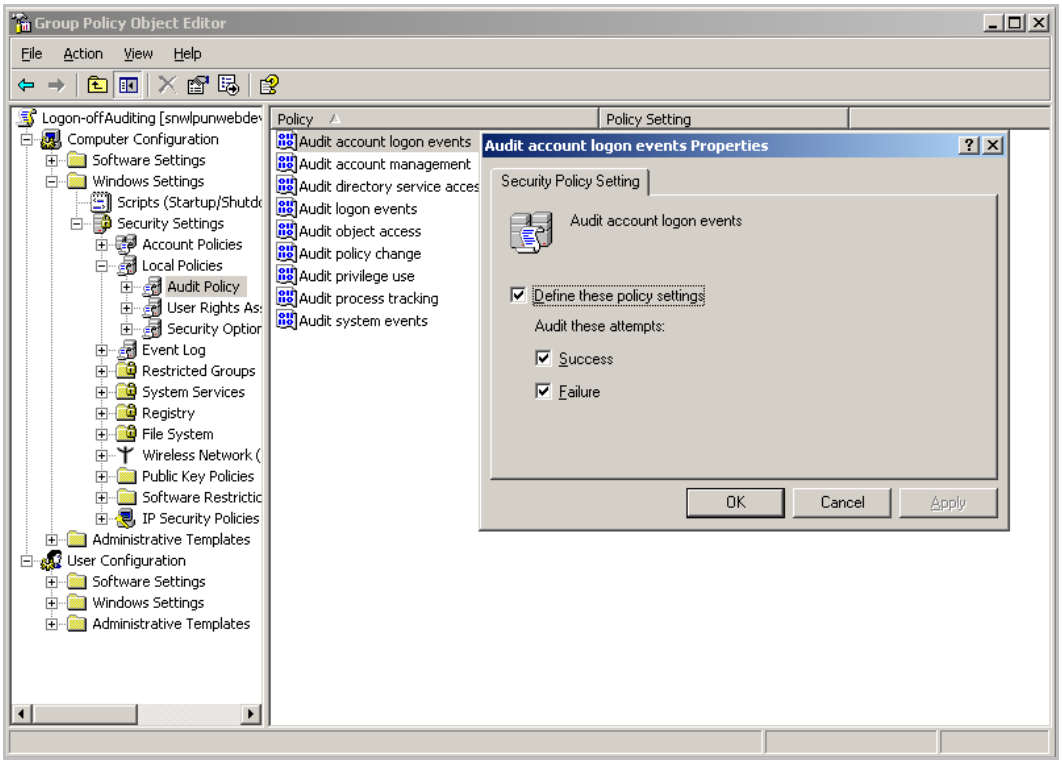
By default the audit logon is disabled on Windows Server 2003. To enable logon audit, perform the following steps:

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 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**.

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

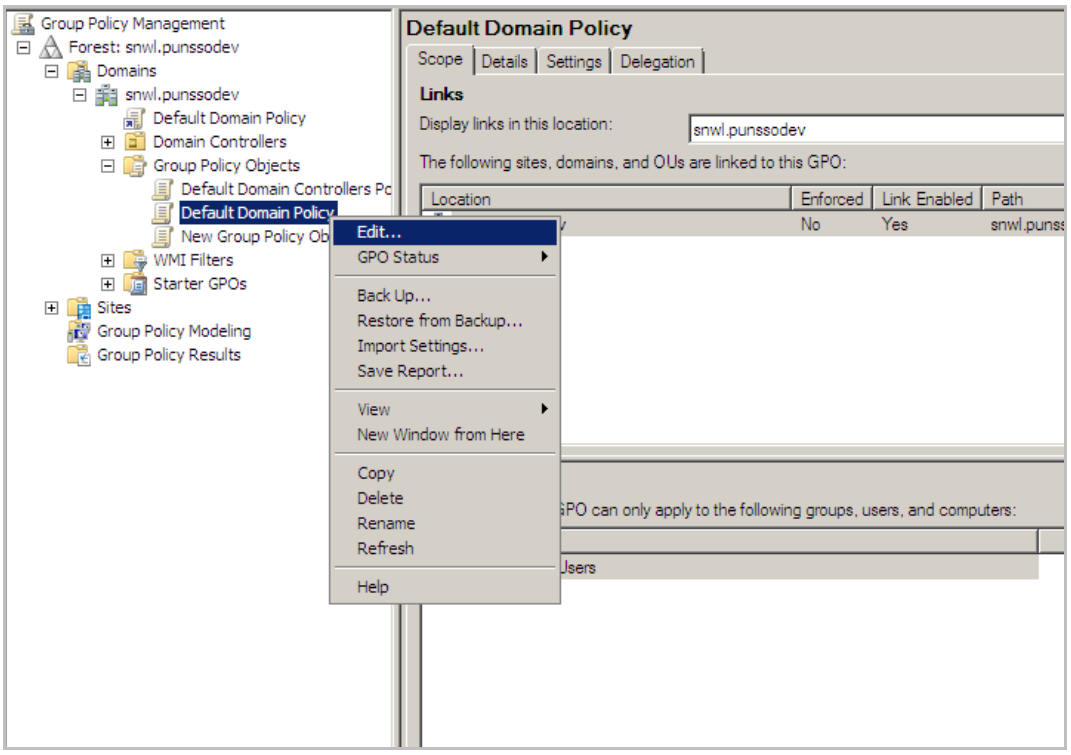


8. Double-click on **Audit account logon events** and select **Success**. Click **OK**.
9. Double-click on **Audit logon events** and select **Success**. Click **OK**.
10. Double-click on **Audit Directory Service Access** and select **Success**. Click **OK**.
11. Close the Group Policy window.

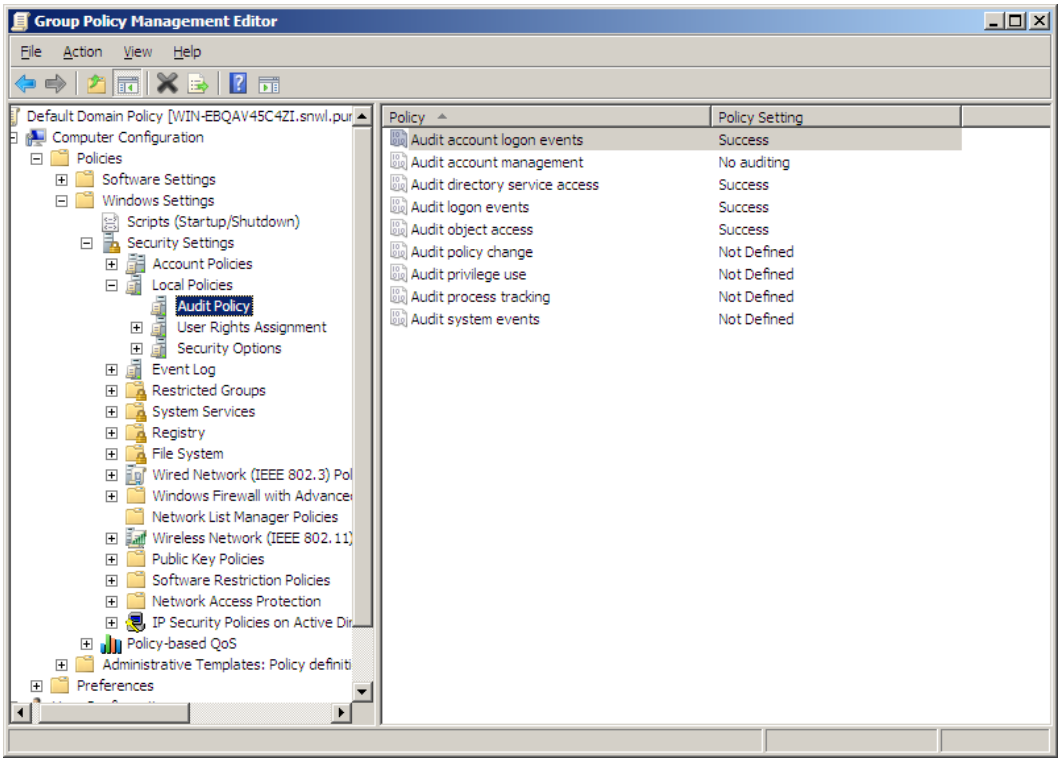
Setting Group Policy to Enable Logon Audit on Windows Server 2008

To enable logon audit on Windows Server 2008, perform the following steps:

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 select **Edit**.



The Group Policy Management Editor window is displayed.



4. Double-click on **Audit account logon events** and select **Success**. Click **OK**.
5. Double-click on **Audit logon events** and select **Success**. Click **OK**.
6. Double-click on **Audit Directory Service Access** and select **Success**. Click **OK**.
7. Double-click on **Audit Object Access** and select **Success**. Click **OK**.
8. Close the Group Policy window.

Known Issues

This section contains a list of known issues in the SonicWALL Directory Services Connector 3.4.51 release.

Configuration Tool

Symptom	Condition / Workaround	Issue
The Agent does not detect that a domain user has logged off. No log event is provided.	Occurs when using Windows Server 2003 32-bit and 64-bit OS. The Agent cannot detect when a domain user has logged off. If another user logs into the PC locally without logging into the domain, the Agent will continue reporting that the first user is still logged in. The second user would get any access rights that were set for the first user on the appliance.	104201

Resolved Issues

This section contains a list of resolved issues in the SonicWALL Directory Services Connector 3.4.51 release.

Single Sign On

Symptom	Condition / Workaround	Issue
Logged in users are not detected correctly by the Single Sign On (SSO) agent.	Occurs when using NetAPI with a Windows 7 operating system.	106569

Overview of SonicWALL Directory Services Connector

SonicWALL Directory Services Connector 3.4.51 allows SonicWALL NSA and TZ 210/200/100 series appliances to achieve transparent, automated Single-Sign-On (SSO) integration with both Active Directory and Novell eDirectory, and allows SonicWALL PRO and TZ 190/180 series appliances to achieve Single-Sign-On (SSO) integration with Active Directory.

Note: SonicWALL Directory Services Connector 3.3.3 and newer includes only the Single Sign-On Agent (SSO Agent) with support for Novell eDirectory and other enhancements.

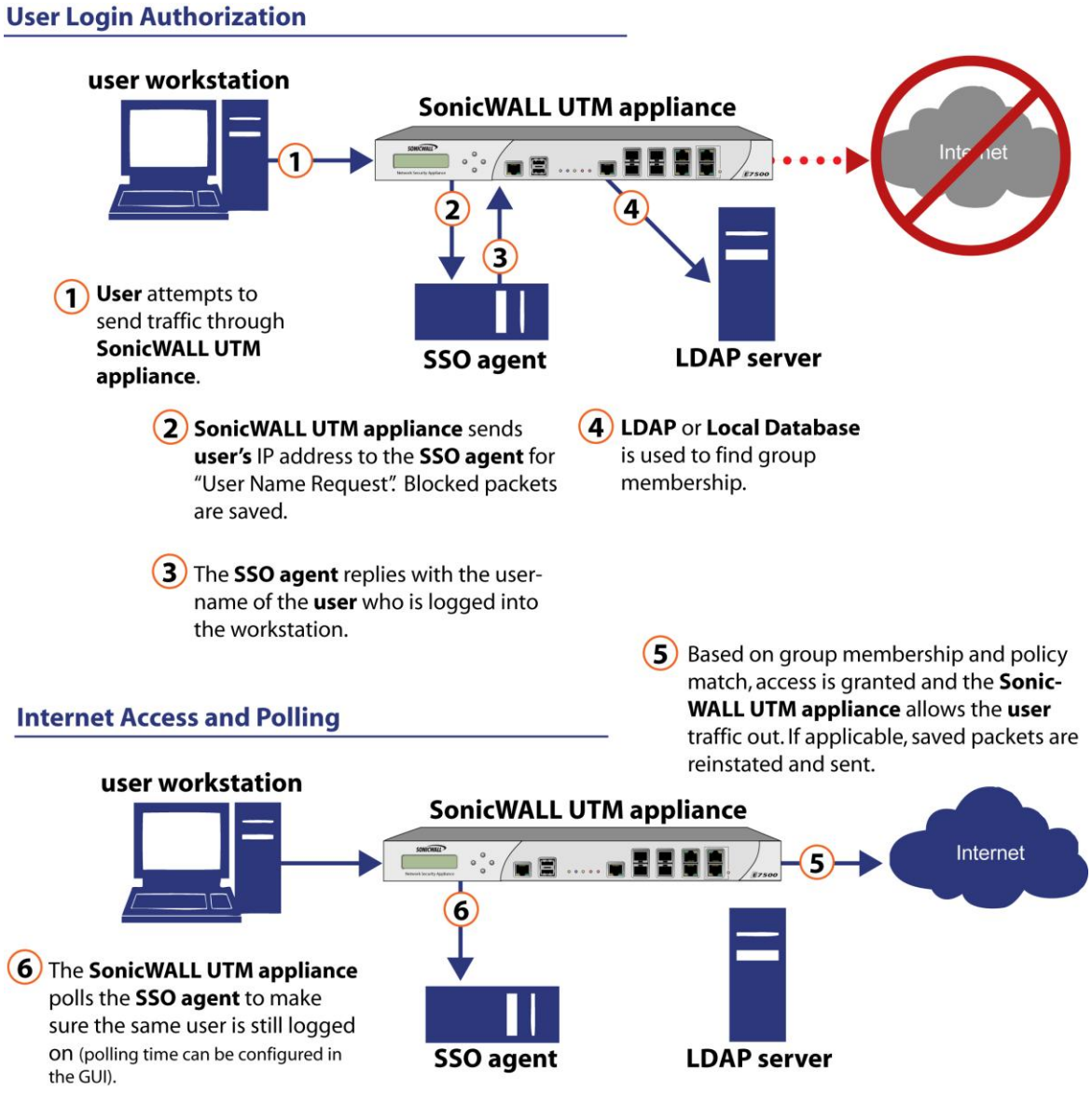
With Directory Services Connector 3.3.3 and newer, the SonicWALL appliance can use Active Directory or Novell eDirectory to authenticate users and determine the filtering policies to assign to each user or user group. The SonicWALL SSO Agent identifies users by IP address and automatically determines when a user has logged out to prevent unauthorized access.

The SonicWALL SSO Agent is not supported in a Citrix or Terminal Services Environment. In these environments, you can use the SonicWALL Terminal Services Agent (TSA) to communicate with SonicWALL SSO. The TSA is not included as part of this release. For more information about the TSA, see the *SonicOS Enhanced 5.6 Administrator's Guide* (or newer) and the *SonicOS Enhanced 5.6 Single Sign-On Feature Module*, available on http://www.sonicwall.com/us/Support.html.

About SonicWALL SSO 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 management interface. SSO is separate from the authentication method for login settings, which can be used at the same time for authentication of VPN/L2TP client users or administrative users.

SonicWALL Single Sign-On Solution Architecture with Active Directory or LDAP



When installed without the Novell eDirectory Support option, 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 SonicWALL 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 Firewall to control what they are allowed to access.

User names learned via 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, will not be authenticated. For users that are not logged into the domain, an Authentication Required screen will display, indicating that a manual login is required for further authentication.

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

To use SonicWALL SSO, it is required that the SonicWALL SSO Agent be installed on a server that can communicate with the Active Directory 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 SonicWALL 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
- The SSO Agent must run under Domain Admin privileges

About the SSO Agent Cache

In DSC 3.3.3 and newer, the SSO Agent does not cache any user information. Previously, the cache was used with a refresh rate of 60 seconds. The refresh rate is now set to zero seconds, which means no caching on the Agent side. User information will be fetched from the workstation for every request from the SonicWALL appliance.

The appliance default is to time out after 10 seconds and to retry up to 6 times, so the Agent will receive multiple requests from it if a NetAPI request is slow to complete. The agent will not initiate a new NetAPI request if the previous one is still going, but there may 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 somehow got lost. The appliance would re-send 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.
- The cache is disabled by default, which is a good setting for a network in which the NetAPI/WMI requests work well and give few errors.
- If significant numbers of NetAPI/WMI errors are being shown in the statistics, then setting the cache refresh time to about 60 seconds may help to reduce them.
- The Agent's cache refresh time should never be set greater than the user polling period set on the appliance.

Samba

Samba 3.0 or newer is required on Linux/Unix clients for use with SonicWALL SSO. Samba is a software package used on Linux/Unix machines to give them access to resources in a Windows domain (via Samba's **smbclient** utility). A user working on a Linux PC with Samba in a Windows domain can be identified via 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 on: http://www.sonicwall.com/us/Support.html

Without Samba, Linux PCs do not support the Windows networking requests that are used by the SonicWALL SSO Agent, and hence do not work with SonicWALL SSO. Linux users can still get access, but will need to log in to do so. They can be redirected to the login prompt if policy rules are set to require authentication.

Installing the SonicWALL SSO Agent

When using SSO with Windows, install the SonicWALL SSO Agent on a host on your network that has access to the Active Directory server and all client workstations.

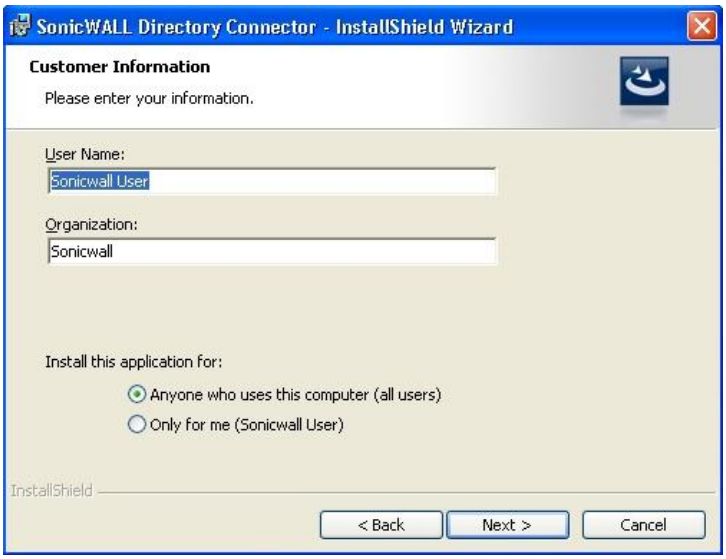
When using SSO with Novell eDirectory Support, install the SonicWALL SSO Agent on a host on your network that has access to the Novell eDirectory server. See the following section for more information about using SSO with Novell eDirectory Support: About Novell eDirectory Support and the SonicWALL SSO Agent

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.

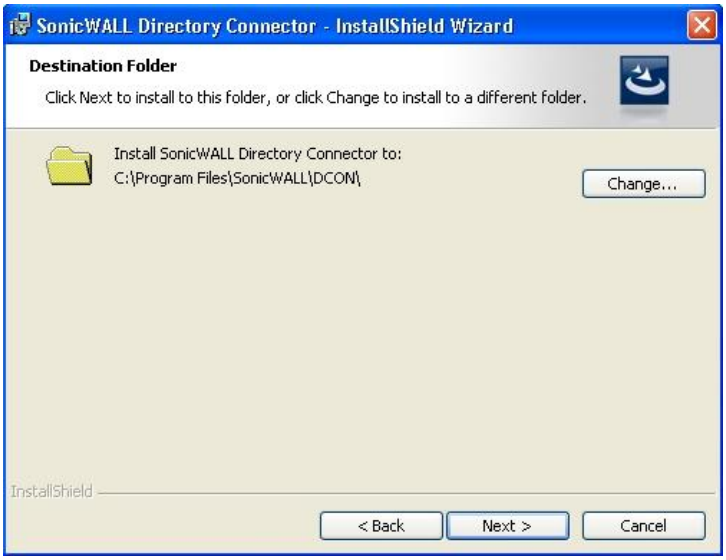
To install the SonicWALL SSO Agent, perform the following steps:

1. Download one of the following installation programs, depending on your computer:
   - **SonicWALL Directory Connector (32-bit) 3.4.51.exe**
   - **SonicWALL Directory Connector (64-bit) 3.4.51.exe**

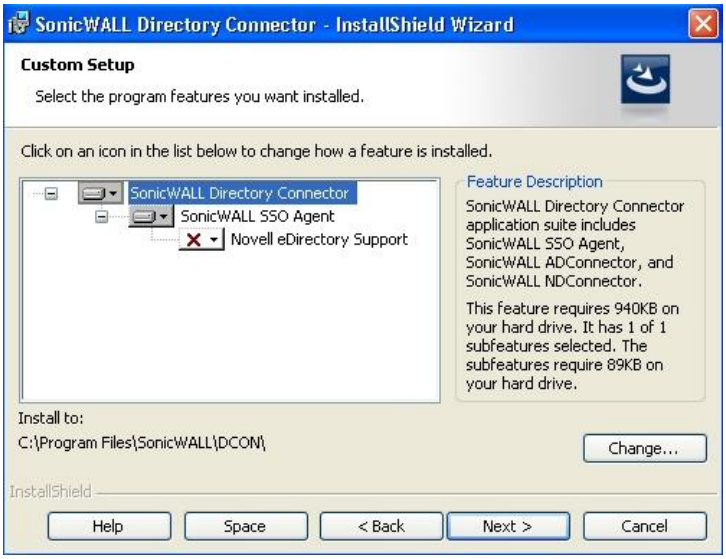
   You can find these on http://www.mysonicwall.com under Directory Services Connector.
2. Double-click the installation program to begin installation.
3. If prompted, install the Microsoft .NET framework.
4. In the Welcome screen, click **Next** to continue the installation.
5. In the License Agreement 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**.



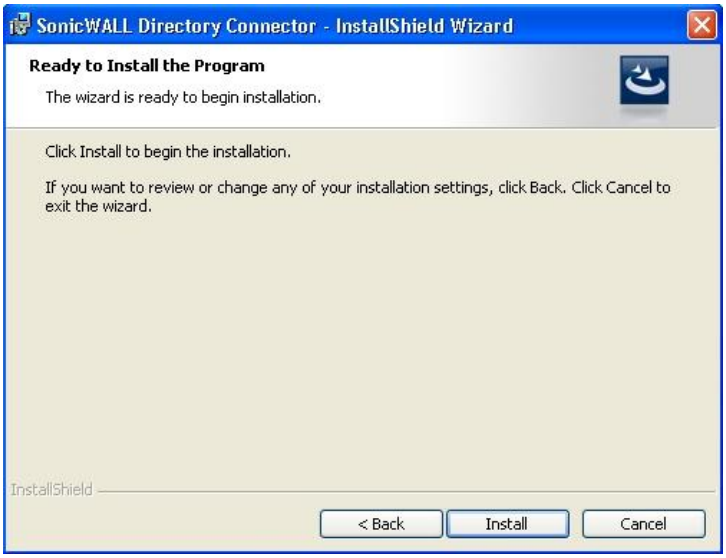
7. Select the destination folder. To use the default folder, C:\Program Files\SonicWALL\DCON, click **Next**. To specify a custom location, click **Change**, select the folder, and click **Next**.



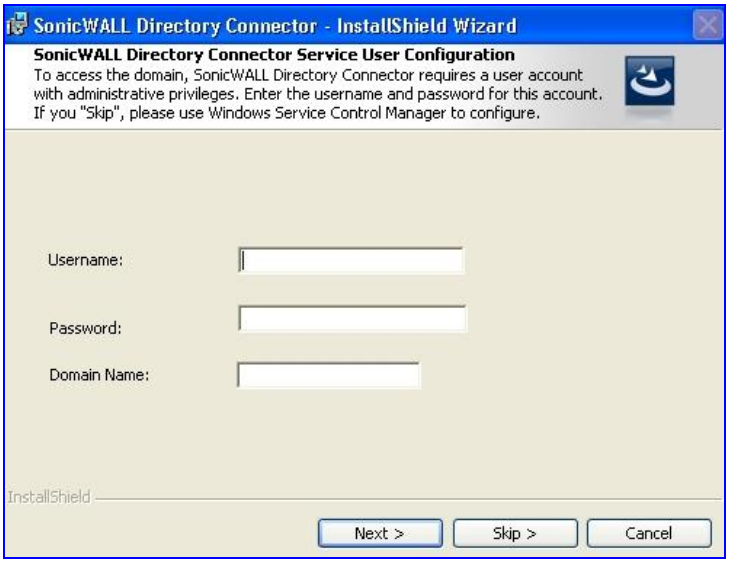
8. On the Custom Setup page, the installation icon is displayed by default next to the **SonicWALL SSO Agent** feature. Click **Next**.



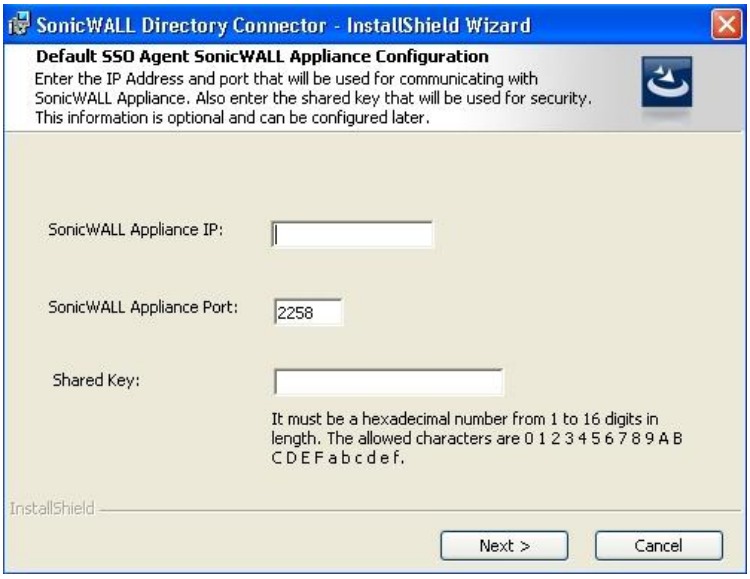
9. In the next screen, click **Install** to install Directory Connector. The status bar displays while the SonicWALL SSO Agent installs.



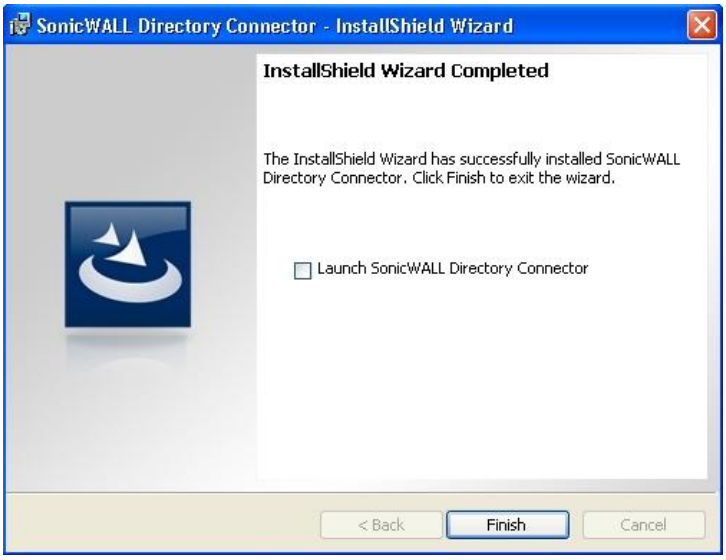
10. To configure a common service account that the SSO Agent will use to log into a specified Windows domain, enter the username of an account with administrative privileges in the **Username** field, the password for the account in the **Password** field, and the domain name of the account in the **Domain 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 **SonicWALL Appliance Port** field. Enter a shared key (a hexadecimal number from 1 to 16 digits in length) in the **Shared Key** field. Click **Next** to continue.



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

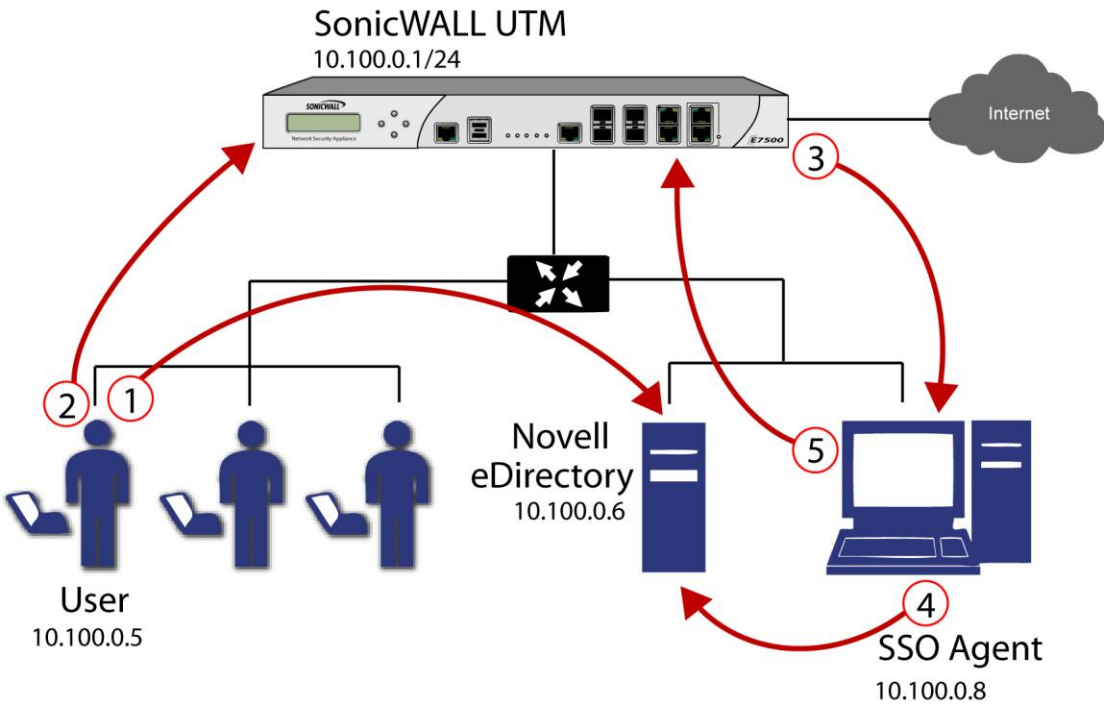


For more information about configuring and using the SonicWALL SSO Agent, see the *SonicOS Administrator's Guide* and the *SonicOS Enhanced Single Sign-On Feature Module*, available on http://www.sonicwall.com/us/Support.html.

About Novell eDirectory Support and the SonicWALL SSO Agent

Novell eDirectory together with the SonicWALL SSO Agent and a SonicWALL UTM appliance running SonicOS Enhanced 5.5 or higher provides a solution for user authentication and the management of access to network resources and online content.

SonicWALL UTM – SSO Agent – Novell eDirectory Solution Architecture



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 UTM appliance detects the request.
③ The SonicWALL appliance queries the SSO Agent.
④ The SSO Agent queries the eDirectory server about the user.
⑤ The SSO Agent communicates to the SonicWALL UTM the user's content filtering policies, 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.

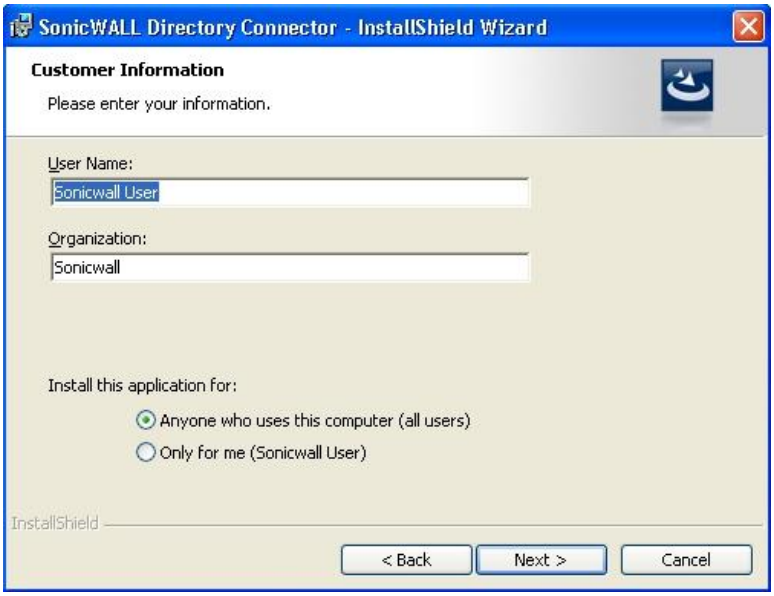
Installing the SonicWALL SSO Agent with Novell eDirectory Support

Install 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 Novell Client installed.

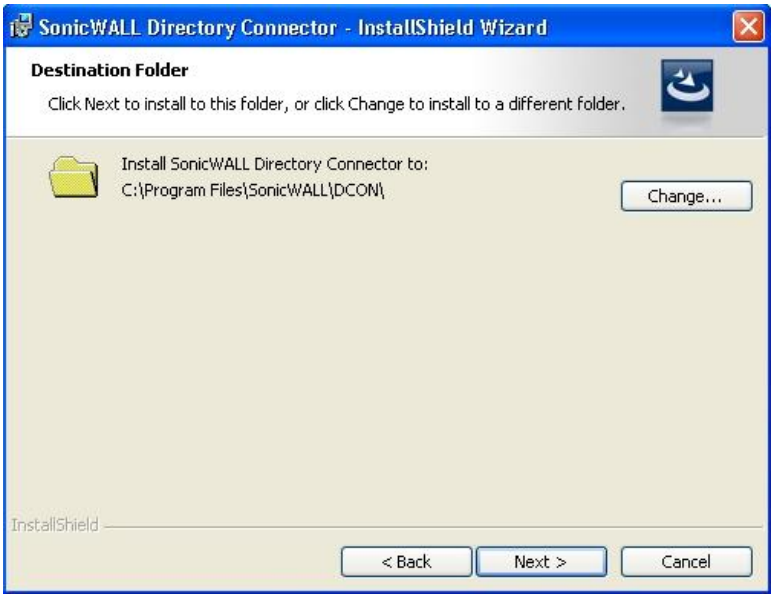
To install the SSO Agent with Novell eDirectory Support, perform the following steps:

1. Download one of the following installation programs, depending on your computer:
   - **SonicWALL Directory Connector (32-bit) 3.4.51.exe**
   - **SonicWALL Directory Connector (64-bit) 3.4.51.exe**

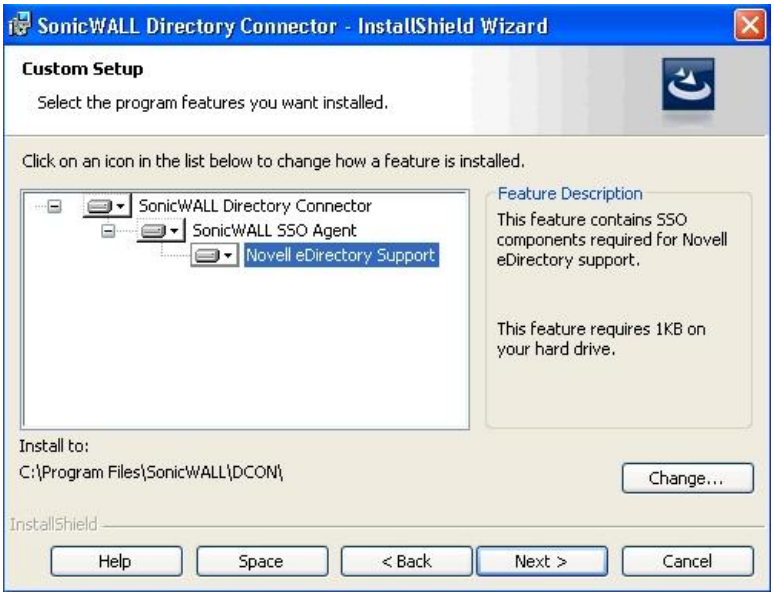
   You can find these on http://www.mysonicwall.com under Directory Services Connector.
2. Double-click the installation program to begin installation.
3. If prompted, install the Microsoft .NET framework.
4. In the Welcome screen, click **Next** to continue the installation.
5. In the License Agreement 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**.



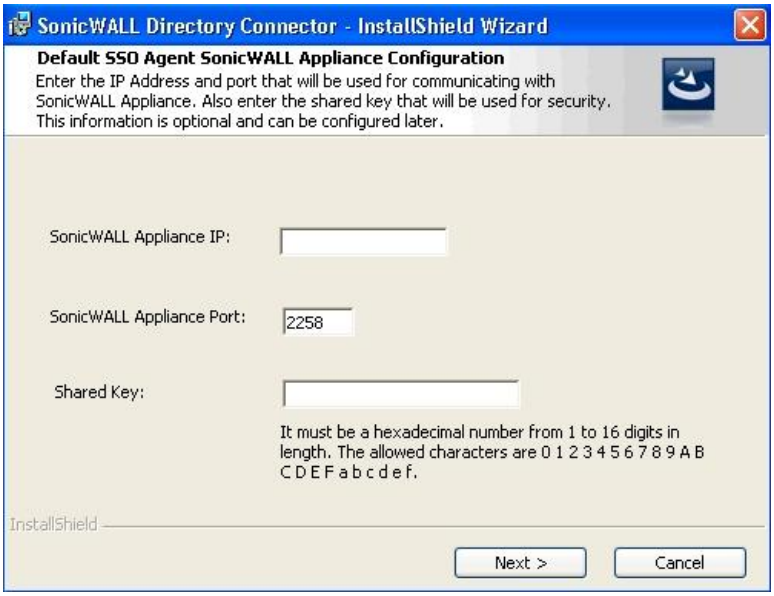
7. Select the destination folder. To use the default folder, C:\Program Files\SonicWALL\DCON, click **Next**. To specify a custom location, click **Change**, select the folder, and click **Next**.



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

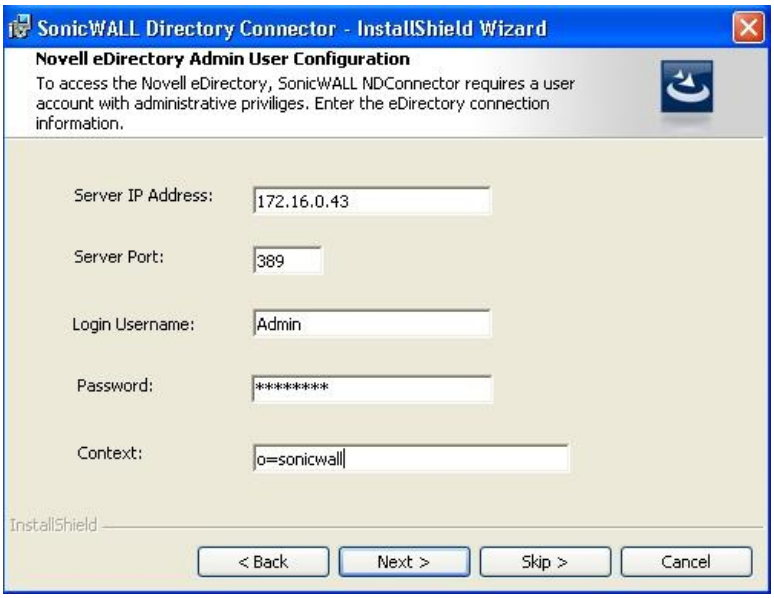


9. In the Ready to Install the Program screen, click **Install**.
10. In the Default SSO Agent SonicWALL Appliance Configuration screen, enter the SonicWALL UTM information and then click **Next**:
    - **SonicWALL Appliance IP** – Type in the SonicWALL UTM appliance IP address.
    - **SonicWALL Appliance Port** – Type in the port used by the SSO Agent to communicate with the SonicWALL UTM appliance. The default port is 2258.
    - **Shared Key** – Type in a hexadecimal number of up to 16 characters to use as the key for encrypting messages between the SSO Agent and the SonicWALL UTM appliance. You must also enter the same key when configuring the appliance to use 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 installation is complete, optionally select the **Launch SonicWALL Directory Connector** checkbox to launch the SonicWALL Directory Connector, and then click **Finish**.

    For more information about configuring and using SonicWALL SSO with Novell eDirectory support, see the *SonicOS Enhanced 5.6 Single Sign-On Feature Module* and the *SonicOS Enhanced 5.6 Administrator's Guide*, available on http://www.sonicwall.com/us/Support.html.

Related Technical Documentation

SonicWALL user guides and reference documentation is available at the SonicWALL Technical Documentation Online Library: http://www.sonicwall.com/us/Support.html

For basic and advanced deployment examples, refer to SonicOS Guides and SonicOS Technotes.

Last updated: 9/9/2011