Contents

Release Purpose ........................................................................................................................................................... 1
Platform Compatibility ................................................................................................................................................... 1
Known Issues ................................................................................................................................................................ 3
Resolved Issues ............................................................................................................................................................ 4
Enhancements in Directory Services Connector 3.6.11 ............................................................................................... 4
Overview of Dell SonicWALL Directory Services Connector ...................................................................................... 13
About SonicWALL SSO and the SSO Agent with Active Directory .............................................................. 14
About Novell eDirectory Support and the Dell SonicWALL SSO Agent .............................................................. 21
Related Technical Documentation .............................................................................................................................. 26

Release Purpose

Dell SonicWALL Directory Services Connector 3.6.11 provides several enhancements for better reliability and optimization of user identification techniques. These enhancements include the NETAPI / WMI background scanner, an option to preserve user information across SSO Agent service restarts, login notification and multi-user request optimizations, users and hosts statistics display, and the LogWatcher service for environments with multiple Domain Controllers. This release also resolves approximately 85 issues.

Platform Compatibility

SonicWALL Appliance / Firmware Compatibility

SonicWALL Directory Services Connector version 3.6.11 software is a supported release for use with the following SonicWALL platforms:

- SuperMassive 9000 series running SonicOS 6.1 and above
- SuperMassive E10000 series running SonicOS 6.0.x
- NSA 6600 / 5600 / 4600 / 3600 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: When configuring Active-Active on a SonicWALL SuperMassive E10000 Series appliance, SonicWALL Directory Services Connector version 3.4.51 or newer is required.
**Domain Controller Server Compatibility**
SonicWALL Directory Services Connector version 3.6.11 software is supported for use with Domain Controllers running the following operating systems:

- Windows Server 2012
- Windows Server 2008 R2
- Windows Server 2008
- Windows Server 2003

**Server Compatibility**
SonicWALL Directory Services Connector version 3.6.11 software is supported for installation on servers running the following operating systems:

- Windows 32-bit:
  - Windows Server 2012
  - Windows Server 2008 R2
  - Windows Server 2008
  - Windows Server 2003

- Windows 64-bit:
  - Windows Server 2012
  - Windows Server 2008 R2
  - 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 4.0
- .NET Framework 3.5
- .NET Framework 3.0
- .NET Framework 2.0

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

- Windows 8 – All versions
- 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 Directory Services Connector 3.6.11 software:

- Windows 8 – All versions
- Windows 7 – All versions
- Windows Vista – All versions
- Windows XP – All versions
- Windows 2000 Professional
- Mac OS X 10.6.0
- Linux machines using Windows domain accounts, with SSO Agent set to use **DC Security Log** as the Query Source
- Linux/Unix machines running Samba 3.0 or newer

### Known Issues

This section contains a list of known issues in the Directory Services Connector 3.6.11 release.

#### Configuration Tool

<table>
<thead>
<tr>
<th>Symptom</th>
<th>Condition / Workaround</th>
<th>Issue</th>
</tr>
</thead>
<tbody>
<tr>
<td>The <strong>Preserve users during service restart</strong> option fails with an error, displayed in the Log Viewer as: &quot;Failed in SaveConfigurationFile.; Error:Could not find a part of the path 'C:\Program Files\SonicWALL\DCON\SSO\WSLXMLPath.xml&quot; &quot;</td>
<td>Occurs when Directory Services Connector is installed on a 64-bit system, the <strong>Preserve users during service restart</strong> option is enabled, and then the agent service is restarted from the DSC Configuration Tool. Occurs because the 64-bit installer uses the 'C:\Program Files (x86)' folder, rather than 'C:\Program Files'. <strong>Workaround:</strong> Create the SonicWALL\DCON\SSO folders under 'C:\Program Files' for a full path of 'C:\Program Files\SonicWALL\DCON\SSO' for use by the preserve user information feature.</td>
<td>129224</td>
</tr>
<tr>
<td>The User Identification Mechanism incorrectly displays as NetAPI. The User Identification Mechanism should displays as Novell eDir or LDAP User.</td>
<td>Occurs when the administrator attempts to view the SSO Agent Settings. Navigate to the Users &gt; Settings page, click on the <strong>Configure</strong> button for SSO, and add Authentication Agent Settings for eDirectory. Hover the mouse on the SSO Agent Statistics to view settings.</td>
<td>115450</td>
</tr>
</tbody>
</table>

#### SSO Agent

<table>
<thead>
<tr>
<th>Symptom</th>
<th>Condition / Workaround</th>
<th>Issue</th>
</tr>
</thead>
<tbody>
<tr>
<td>The SSO Agent sends the format &quot;domain/user&quot; to the firewall appliance, but the appliance displays the format as &quot;domain.user&quot; instead.</td>
<td>Occurs when sending a packet to the firewall appliance. The SSO Agent does not keep the &quot;domain/user&quot; format.</td>
<td>117347</td>
</tr>
<tr>
<td>The Directory Connector installer does not have a text field available to enter a friendly name for the SonicWALL appliance.</td>
<td>Occurs when running the Directory Connector installer.</td>
<td>108461</td>
</tr>
<tr>
<td>Keyboard shortcuts do not work in the Directory Connector Configurator.</td>
<td>Occurs when trying to use keyboard shortcuts while configuring the SSO Agent in the Directory Connector Configurator.</td>
<td>107717</td>
</tr>
<tr>
<td>The Windows Service Users for a second firewall appliance do not display in the SSO Agent until the SSO Agent is restarted.</td>
<td>Occurs when two firewall appliances are associated with the SSO Agent. Upon switching the second appliance to the default, and then viewing the Windows Service Users, the Windows Service Users only display for the first appliance. <strong>Workaround:</strong> After setting the second firewall appliance as the default, restart the SSO Agent.</td>
<td>103858</td>
</tr>
<tr>
<td>The Directory Connector installer sometimes prompts for CSM and Novell eDirectory options that do not apply to the installation</td>
<td>Occurs when Novell eDirectory Support is inappropriately enabled during installation. A radio button should display, with an option to select the installation mode for Novell eDirectory or Windows.</td>
<td>99380</td>
</tr>
</tbody>
</table>
Resolved Issues

This section contains a list of issues that are resolved in the Directory Services Connector 3.6.11 release. A number of other issues have been resolved by the enhancements in this release.

SSO Agent

<table>
<thead>
<tr>
<th>Symptom</th>
<th>Condition / Workaround</th>
<th>Issue</th>
</tr>
</thead>
<tbody>
<tr>
<td>The SSO Agent is not responding while checking a user.</td>
<td>Occurs when checking for the user from the appliance Test tab. The SSO Agent is unable to respond due to packet drop issues in the agent.</td>
<td>125801</td>
</tr>
<tr>
<td>The CIA service task periodically stops working.</td>
<td>Occurs when the SSO Agent is set to use WMI and the failure rate is high.</td>
<td>125041</td>
</tr>
<tr>
<td>A high percentage of CPU usage is observed on the agent computer, including CPU spikes of up to 100%.</td>
<td>Occurs when the SSO Agent is set to use the DC Security Log option and multiple Domain Controllers are added.</td>
<td>123507</td>
</tr>
</tbody>
</table>

Enhancements in Directory Services Connector 3.6.11

This section describes the enhancements that are included in Dell SonicWALL Directory Services Connector 3.6.11. Directory Services Connector 3.6.11 provides several enhancements for better reliability and optimization of user identification techniques.

These enhancements include the NETAPI / WMI background scanner, an option to preserve user information across SSO Agent service restarts, login notification and multi-user request optimizations, users and hosts statistics display, and the LogWatcher service for environments with multiple Domain Controllers.

See the following sections for information about the enhancements:

- NETAPI / WMI Scanner ................................................................. 5
- Preserve User Information Across Service Restart .................. 6
- Login Notifications ................................................................. 6
- Distributed Operation Time for Multi-user Requests ............. 7
- Users and Hosts Statistics ...................................................... 7
- LogWatcher ................................................................. 8
**NETAPI / WMI Scanner**

The SSO Agent Properties page in the DSC Configuration Tool provides the Enable Scanner checkbox 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, the SSO Agent will check for the IP address in its cache. If the IP address is not present in the cache, the SSO Agent will consider the request to be the first request for that IP Address and will add the IP Address to its Scanner queue for further processing.

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

- Reply back to the appliance with an In_Progress status
- Not send any 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 via NETAPI or WMI, the agent sends a login 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.

**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 will skip any Bad IP’s and add the IP address to the back of the queue for the next fetch.
**Preserve User Information Across Service Restart**

A new option is available when the Query Source is set to DC Security Log or DC Security Log with other methods. You can select the **Preserve users during service restart** checkbox to enable this option. It causes Directory Connector to save a file containing information about previously identified users when the SSO Agent service is restarted. Upon restarting, 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. To avoid restoring outdated information, if the backup is older than 15 minutes, the information is not restored.

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 will send no user information to the appliance. If Query Source is set to DC Security Log with NETAPI or WMI, the agent will do a NETAPI or WMI query to the user PC to identify the user.

**Login Notifications**

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.
**Distributed Operation Time for Multi-user Requests**

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.

**Users and Hosts Statistics**

The Users and Hosts page of the DSC Configuration Tool displays 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.
LogWatcher

LogWatcher is a Windows service that runs on each Domain Controller. It 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.
3. The Domain Controller must have logon audit enabled.
4. The LogWatcher Service only works with SSO Agent 3.6.02 and higher.
5. The SSO Agent must be configured for LogWatcher support.

Installing LogWatcher

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.

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:

```xml
<SONICWALL_LOG_WATCHER>
  <AGENTS>
    <AGENT>
      <IP_ADDRESS>10.50.173.252</IP_ADDRESS>
      <PORT_NO>2259</PORT_NO>
    </AGENT>
    <AGENT>
      <IP_ADDRESS>10.50.173.54</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>
```
Enabling Logon Audit on the Domain Controller

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

1. Start the Group Policy Management Console.
2. As shown in the example below, browse to the following location:
   Forest: Domain Name-->Domains-->Domain Name-->Group Policy Objects (replace "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:
7. Left click on **Audit Policy**. The policy settings will be displayed in the right-hand window.

8. Double-click on **Audit account logon events** and select **Success** and **Failure**. Click **OK**.

9. Double-click on **Audit logon events** and select **Success** and **Failure**. Click **OK**.

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.
Viewing LogWatcher Information in Users and Hosts Page

The Users and Hosts page in the Directory Connector Configuration Tool 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).
Overview of Dell SonicWALL Directory Services Connector


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 Dell SonicWALL 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, Directory Services Connector 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 24 hours after installation, while the software creates a database of the user network.

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 SonicOS Administrator’s Guide and the SonicOS Enhanced 5.6 Single Sign-On Feature Module, available on [http://www.sonicwall.com/us/Support.html](http://www.sonicwall.com/us/Support.html).

To use DC Security Log mode in Dell SonicWALL Directory Services Connector, ensure that the Agent machine has the following minimum requirements:

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

**Note:** For single core processors, CPU spikes may reach up to 100% periodically while using DC Security Log mode 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.

When using DC Security Log mode, Directory Services Connector fetches security logs from the configured Domain Controller. The account that is specified to read logs must have Local Administrator privileges on the DC machine. A Domain Administrator account is equivalent, and can access the Local Administrator privileges. Please contact Dell SonicWALL support for more details on configuring permissions to non-Administrator users.
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

User Login Authorization

1. User attempts to send traffic through Dell SonicWALL appliance.

2. Dell SonicWALL appliance sends user’s IP address to the SSO agent for “User Name Request”. Blocked packets are saved.

3. The SSO agent replies with the username of the user who is logged into the workstation.

4. LDAP or Local Database is used to find group membership.

5. Based on group membership and policy match, access is granted and the Dell SonicWALL appliance allows the user traffic out. If applicable, saved packets are reinstated and sent.

Internet Access and Polling

6. The Dell SonicWALL appliance polls the SSO agent to make sure the same user is still logged on (polling time can be configured in the GUI).
When installed without the Novell eDirectory Support option, 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 via 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, 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 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 2.0 or above
- NETAPI or WMI
- The SSO Agent must run under Domain Admin privileges

About NETAPI and WMI

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 Configurator. NETAPI and WMI provide information about users that are logged into a workstation, including domain users, local users, and Windows services.

NETAPI will provide faster, though possibly slightly less accurate, performance. WMI will provide 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 will still show the user as logged in when NETAPI is used. If another user logs onto the same computer, then at that point the previous user is logged out from the Dell SonicWALL appliance.

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 timeout mechanism is included in multi-user requests from the appliance. If the request does not complete within this time, the agent silently aborts it.

User identification via the Domain Controller Security Log can be configured for 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 technical note in the Product Documentation page for supported Dell SonicWALL appliances on www.sonicwall.com.

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 Dell 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 Dell 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](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 Dell SonicWALL SSO Agent, perform the following steps:

1. Download one of the following installation programs, depending on your computer:
   - SonicWALL Directory Connector (32-bit) 3.6.11.exe
   - SonicWALL Directory Connector (64-bit) 3.6.11.exe
   You can find these on [http://www.mysonicwall.com](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**.

![Customer Information Screen]

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**.

![Destination Folder Screen]
8. On the Custom Setup page, the installation icon is displayed by default next to the **SonicWALL SSO Agent** feature. Click **Next**.

![Custom Setup screenshot](image1)

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

![Ready to Install the Program screenshot](image2)
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**.

![Configuration screen](image)

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.

![Configuration screen](image)
12. Wait for the installation to complete. The status bar displays while the SonicWALL SSO Agent installs.

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

About Novell eDirectory Support and the Dell SonicWALL SSO Agent

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

Dell SonicWALL Appliance – 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 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.
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) 3.6.11.exe
   - SonicWALL Directory Connector (64-bit) 3.6.11.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.

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

![Ready to Install the Program](image1)

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 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.

![Default SSO Agent SonicWALL Appliance Configuration](image2)
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.

![Novell eDirectory Admin User Configuration](image)

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

Related Technical Documentation

Dell SonicWALL user guides and reference documentation is available at the Dell 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 available on the website.

Last updated: 5/18/2013