Dell SonicWALL™ Directory Services Connector 4.0.18

Release Notes

June 2015

These release notes provide information about the Dell SonicWALL™ Directory Services Connector 4.0.18 release.

- About Directory Services Connector 4.0.18
- Platform compatibility
- New features
- Known issues
- Product licensing
- Technical support resources
- About Dell

About Directory Services Connector 4.0.18

Dell SonicWALL Directory Services Connector 4.0.18 is a major release that introduces new features for the Dell SonicWALL SSO Agent, including Server Session, Exchange Support, and a new Single Sign-On (SSO) Agent Cache Policy. See New features.

Platform compatibility

- Dell SonicWALL appliance / firmware compatibility
- Virtual environment compatibility
- eDirectory server compatibility
- Exchange server compatibility
- Domain controller server compatibility
- SSO Agent platform compatibility
- Client compatibility

Dell SonicWALL appliance / firmware compatibility

Dell 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
- SOHO running SonicOS 5.9.1.3 and above
- SOHO W running SonicOS 6.2.4.0 and above
- TZ600 / TZ500 / TZ400 / TZ300 running SonicOS 6.2.3.1 and above
- TZ500W / TZ400W / TZ300W running SonicOS 6.2.4.0 and above
- TZ 215 / 215W / 205 / 205W / 105 / 105W running SonicOS 5.8.1 and above
- TZ 210 / 210W / 200 / 200W / 100 / 100W running SonicOS 5.0 and above
- TZ 190 / 190W / 180 / 180W running SonicOS 4.0 and above
- PRO 2040 / 3060 / 4060 / 4100 / 5060 running SonicOS 4.0 and above

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

Virtual environment compatibility

Virtual Environments for Directory Services Recommended 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 version 4.0 software is supported for use with the following eDirectory servers:

- Novell eDirectory 8.8.5
- Novell eDirectory 8.8.7

Exchange server compatibility

SonicWALL Directory Services Connector version 4.0 software is supported for use with the following exchange servers:

- Exchange server 2010
- Exchange server 2013

Domain controller server compatibility

SonicWALL Directory Services Connector version 4.0 software 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 2008 R2 – 64-bit
- Windows Server 2008 – 32/64-bit
- Windows Server 2003 R2 – 32/64-bit

SSO Agent platform compatibility

SonicWALL Directory Services Connector and SSO Agent 4.0 software are supported for installation on 32-bit and 64-bit servers running the following operating systems:

- Windows Server 2012 – 64-bit
- Windows Server 2012 R2 – 64-bit
- Windows Server 2008 R2 – 64-bit
- Windows Server 2008 – 32/64-bit
- Windows Server 2003 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 4.5
- .NET Framework 4.0

The following Microsoft Windows operating systems and service packs are **not** supported as servers:

- Windows 2000 – All versions

***Note**: Windows Server 2008 and higher or Windows 7 and higher are recommended.*

Client compatibility

Directory Services Connector 4.0 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

New features

This section describes the new features that are included in Dell SonicWALL Directory Services Connector 4.0.

- Polling and notifications
- Client probing
- Domain controller querying
- Exchange server support
- Novell eDirectory support
- Protocols
- Installer
- Directory Services Connector Configuration Tool
- Configuration file format
- Debugging and diagnostics

Polling and notifications

The Single Sign-On (SSO) Agent works both passively and actively. In passive mode, the firewall sends requests that contain an IP address to the SSO Agent. The SSO Agent tries to identify the username of the IP address and then sends the result back to the firewall. In active mode, the SSO agent tries to detect user log in and log out events and sends notifications to the firewall. For the default configuration, both methods are used.

Client probing

In SSO Agent 4.0, 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. NetAPI is another interface based on Windows DCE-RPC service. The NetAPI method is much faster than the WMI method. Because the Windows API does not provide an interface to set the timeout for both probing methods, the default timeout is set to three seconds when the IP address is not accessible or when the connection is dropped by the Windows firewall.

Domain controller querying

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

DC security logs

In Microsoft Windows, the security Log contains records of log in and log out activity or other security-related events specified by the system's audit policy. When a domain user tries to log in to the domain network, the domain controller logs a message in the security log. Event messages are monitored by Event IDs.

Server sessions

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

Usually server sessions are a more efficient method of comparing DC Security logs. Sometimes, server sessions are not accurate. In multiple domain environments, incorrect domain names might be reported. If the user switches between two logged on usernames, the SSO Agent cannot detect it.

Enable audit logs in DC policy

Audit Logon was disabled in Windows Server 2003. Steps to enable audit logon are provided in the *Directory Services Connector Administrator’s Guide*.

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 be a normal domain user with some additional permissions granted, for access. Refer to the *Configuring a Non-Admin Domain Account for SSO Agent to Read Domain Security Logs* configuration guide located at:
https://support.software.dell.com/download/downloads?id=5371306

NetBIOS name support

Windows 2000 provides support for applications that use the NetBIOS networking APIs and the flat NetBIOS names. This allows identification of Windows 2000 domains for computers that are running Windows NT 4.0 and earlier, or those that are running Windows 95 or Windows 98. 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 admin configuration of the SSO Agent. By default, it sends the NetBIOS name.

Exchange server support

When a user logs on to a computer that is not in the domain, the DC server cannot get its user and IP information. Typically, this is handled by the client probing method. But, you may be able to use the Exchange Server to identify the user.

Suppose the user opens Outlook to send or receive mail using a domain user name and credentials. Both the DC and Exchange Server are logging messages for this activity. On the DC, Event ID 4768 is established for this action, but the IP address given is not the real source though it points to the Exchange Server. On the Exchange server, Event ID 4624 is a security log entry that contains both the user name and the source IP address. Each time Outlook receives email; there is also a 4624 event on the Exchange server. So, the SSO Agent simply monitors this event on the Exchange security log.

This works only as a supplement to the domain security log method. Although it works for machines not joining a domain, it assumes users always use Outlook after logging in.

Novell eDirectory support

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 to name just a few.

Protocols

SSO TLV protocol

The protocol is based on UDP. By default, the SSO Agent binds the UDP socket on port 2258. It receives packets from the firewall and sends packets back using this socket. If the firewall supports protocol version three or greater, the SSO Agent replies to the firewall with the same port number as the request SRC port. If the firewall only supports protocol version two, it always replies to the firewall using the configured port number (2258).

SSO user interface RPC protocol

In SSO Agent 4.0, the service component and the user interface component are completely independent. The user interface communicates with the service using HTTP on a local machine. The SSO Agent service creates an HTTP service on port 12348 of the localhost. The user interface communicates with the SSO service using this service. The content of both the HTTP requests and responses is JSON object. The protocol is referred to as JSON-RPC.

Installer

Before installing the SSO Agent, you might first need to install the .NET framework 4.0 or 4.5. The installer uses an MSI file signed by “SonicWALL Inc.” Note that the certificate expires on 03/08/2015. The installer automatically uninstalls previous SSO Agents if their version is equal to or greater than 4.0. You can have both SSO Agent 3.x and SSO Agent 4.x installed, but only one can be running because they use a common port.

Directory Services Connector Configuration Tool

The DSC Configuration Tool can be launched from the Start menu or a desktop shortcut. If the SSO Agent service is stopped, the Configuration Tool tries to start the service first.

Refresh

Refreshes the left tree.

Properties

This is the general configuration of the SSO Agent. Including:

- **Host IP and port**: the SSO agent binds the UDP socket at this IP address and port and receives the SSO protocol packets from the firewall. Note that if the host IP address is 0.0.0.0, it accepts packets from any interface. The default value of the IP address is 0.0.0.0. The default value of the port is 2258.
- **Sync Port**: the SSO agent binds an TCP socket on this port and receives an agent synchronize datagram from this port. The default value of this field is 2260.
- **Logging Level**: the SSO agent creates log files in the program data directory. The log file is useful for diagnostic and debugging purposes. The administrator can adjust the logging level through this field.
- **Max Thread Count**: the SSO Agent creates many threads at run time. Most of the threads are used for client probing. The thread count adjusts the trade-off between simultaneity and overall performance. The default value of this field is 100.
- **Cache Duration**: if a user does not log out of the computer properly, for example, pulling the power plug, the SSO Agent is not able to receive the log out message. In this case, the SSO Agent keeps the user information in its cache. It removes the user in the cache and sends a log out notification to the firewall after the cache duration time. The default time for this field is 7200, or two hours. It is a typical value that a computer refreshes the login status on DC.
- **Preserve users during service restart**: the SSO agent saves the user list to "users.xml" in the program files folder. There is a timestamp on the xml file. The SSO agent reloads this file to fill its cache if the users.xml is created within 15 minutes, otherwise it ignores the file.
- **Scan Users**: when a user is identified through the client probe method, when this field is checked, the SSO agent probes this user repeatedly until the user logs off the computer or the SSO agent can identify this user using another method, for example, a DC security log or server session. When the SSO agent detects the user logs off the computer, it sends a log out notification to the firewall.
- **Client probe method**: when the SSO agent receives an IP Address request from the firewall and the user is not found in its cache, it uses the client probe method to identify the username. This attribute specifies the client probe method to use. The SSO agent either tries to first send the WMI query then the NetAPI query, or vice versa.
- **Domain name type**: users can select the domain name types, either the NetBIOS or the FQDN. The firewall can automatically handle both domain name types.

View Logs

Viewing the logs requires Windows Explorer to open the program data folder that contains all the log files and maybe the crash dump files. In the case of troubleshooting, all files in this folder should be sent for investigation by the support team.

Users and Hosts

The Users and Hosts page displays some statistical information and all the users in the cache. You can search and sort the users, as well as manually removing a user from the cache.

Diagnostic Tools

You can manually identify IP addresses using the WMI or NetAPI method by inputting multiple IP addresses separated by commas or an IP address range. The results can be exported to a CSV file.

Windows Service Users

The Windows Service Users page displays all the service users configured by the administrator. The users might be used by services on the end-users computer. The SSO Agent ignores all events whose usernames are in this list.

Service Logon Accounts

The WMI, NetAPI, and DC Security Log methods require the domain administrator privilege. The service should be run with a domain administrator account. You can setup an account name and password on this page.

Restart Service

You can manually restart the service.

Dell SonicWALL appliances

When you click a Dell SonicWALL appliance item, all the configured appliances are listed on the right panel. You can see the friendly name, IP, port, and status from that grid view.

You should add at least one Dell SonicWALL appliance. Fill in the correct appliance IP and port. The shared key should be evenly numbered in length and can only contain the following characters: 0-9, a-f, A-F. It should be exactly the same as what is configured on the firewall.

Domain controllers

When you click a Domain Controllers item, all the configured DCs are listed on the right panel. You can see the IP, domain name, and status from that grid view.

The SSO Agent can autodiscover all the domain controllers. It tries to find the DCs that the host machine belongs to using a DNS query. You can also manually add the DC one-by-one. Input a valid DC IP Address and domain name.

For each DC server, the administrator can configure monitoring methods. There are two methods, the security log method and the server session method. If security log method is enabled, you should choose either the event subscription method or the pulling method. You can also configure all the DC servers at the same time by clicking the “configure all” menu item.

Exchange servers

When you click on an Exchange Server item, all the configured Exchange servers are listed in the right panel. You can see the friendly name, IP address, and status from that grid view. You can add, modify, and remove exchange servers. For each Exchange server, the administrator can choose to use the subscription method or the pulling method to read the event logs from the server. You can also configure all the Exchange servers at the same time by clicking the “configure all” menu item.

Novell eDirectory servers

When you click a Novell eDirectory Servers item, all the configured eDirectory servers are listed in the right panel. You can view the IP address, basic configuration, and status from that grid. You can add, modify, and remove the eDirectory server by inputting the correct IP address, port, user dn, password, base dn, and polling interval. You can test the connection before clicking **OK**.

Remote SSO Agents

When you click a Remote SSO Agent item, all the configured Remote SSO Agents are listed in the right panel. You can see the friendly name, IP address, port, and status from that grid view. You can add, modify, and remove the remote SSO agents by inputting the correct IP address and sync port. The SSO agent synchronizes the user cache to the remote agent each time the IP-user mapping is added or removed.

When an SSO Agent starts up, it sends the reset RPC to all the remote agents. When a remote agent receives this reset RPC, it sends its user cache to the requesting agent. Thereafter, the remote agent sends any incremental changes.

Configuration file format

Under the application installation directory is the main configuration file, Config.xml. All the password fields are encrypted by a private algorithm (blowfish encryption and then base64 encoding.) The “users.xml” file in the application installation directory contains all the users saved from the cache during the service restart.

Debugging and diagnostics

Load Test

The Load Test feature allows you to preload a static set of IP-to-username mappings in a user-defined test file. The SSO Agent loads the test file at the service start time and checks and reloads the file every 60 seconds.

Crash dump

When the SSO Agent service crashes, the crash dumps are located at “C:\ProgramData\Dell SonicWALL.”

Logging files

The agent can log up to five logs at a time and stores them at “C:\ProgramData\Dell SonicWALL\SSOAgent.” The files are named as follows:

- SSOAgent.log - This is the main log file
- SSOPacket.log - This is the packets log between the firewall and agent
- Rpc.log - This is the RPC log between the UI and agent service
- SecurityEvent.log - This represents the DC/Exchange security event log
- SessionTable.log - This will show the results returned by the NetSessionEnum API

More logs are created with higher logging levels. Debug is the highest level.

Known issues

The following is a list of known issues in this release.

Single Sign On Agent

Known issue	Issue ID
The Users and Hosts UI often displays the log on information of the last user rather than the current user's information when logging in to the client PC as a subdomain user. Occurs when a Windows XP user logs on and off a Server Session. On the Users and Hosts screen, the previous local admin user name is still returned by the query.	148858
Server sessions may return incorrect user information when logging in users through a client. Occurs when using server session and a local administrator logs out of a domain PC as say Sub1 and another user logs in to the same PC later as Sub2. The previous local admin user name (Sub1) is still returned by the session server query	149533
Log off notifications are not available for certain client machines Occurs when using Linux client machines. SSO Agents are unable to detect log off/power off information from Linux clients.	149546
Webmail users are logged off after two hours even when the browser is left open. Occurs when the SSO Agent deletes the user because it did not receive a login event (4624) during these two hours. As a result, the SSO Agent clears the user from the cache after the default cache duration (two hours). Even when a user logs in again, there are still no login events (4624) in the exchange security log because the SSO Agent is not detecting the user login.	149608
Test the user through the WMI/NetAPI overrides the identification method in users and hosts. Occurs after a domain user is detected by the Agent through the DC Security log, execute a test query from the firewall and test the user with NetAPI/WMI. The NetAPI/WMI test result overrides the cache status for this user, and the next time you execute the test query through DC for this user, the agent incorrectly returns 'No User found.' The test query through NetAPI/WMI should not override the DC Security login on the Agent side.	149704
No warning is displayed when the SSO Agent port does not match the port set on the appliance. Occurs when the agent port is configured to be a different port number than that set in the appliance. The agent port should be consistent with the appliance port to allow communication.	150235

Product licensing

Dell SonicWALL Directory Services Connector and Single Sign-On Agent are included with your SonicOS license and Dell SonicWALL network security appliance. Dell SonicWALL network security appliances must be registered on MySonicWALL to enable full functionality and the benefits of Dell SonicWALL security services, firmware updates, and technical support.

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 http://software.dell.com/support/.

The site enables you to:

- View Knowledge Base articles at:

  https://support.software.dell.com/kb-product-select
- View instructional videos at:

  https://support.software.dell.com/videos-product-select
- Engage in community discussions
- Chat with a support engineer
- Create, update, and manage Service Requests (cases)
- Obtain product notifications

About Dell

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

Contacting Dell

Technical support:
Online support

Product questions and sales:
(800) 306-9329

Email:
info@software.dell.com

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 web site (software.dell.com) for regional and international office information.

Patents

For more information about applicable patents, refer to http://software.dell.com/legal/patents.aspx.

Trademarks

Dell, the Dell logo, and SonicWALL are trademarks of Dell 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.

Last updated: 6/29/2015

232-002910-00 Rev. A