SonicWall® Directory Connector with SSO 4.1.6

Release Notes

November 2017

These release notes provide information about the SonicWall® Directory Connector with SSO 4.1.6 release.

Topics:

• About Directory Connector 4.1.6
• Supported Platforms
• New Features
• Resolved Issues
• Known Issues
• Product Licensing
• SonicWall Support

About Directory Connector 4.1.6

Directory Connector 4.1.6 is a major release that introduces the Linux SSO Agent and provides other new features. This release also fixes a number of known issues from previous releases. See New Features and Resolved Issues.

This release provides the features and contains all the resolved issues that were included in previous releases of SonicWall Directory Connector with SSO. For more information, see the previous release notes, available on MySonicWall.


Supported Platforms

Topics:

• SSO Agent Platform Compatibility
• Virtual Environment Compatibility
• SonicWall Appliance / Firmware Compatibility
• Exchange Server Compatibility
• Domain Controller Server Compatibility
• Novell eDirectory Server Compatibility
• Terminal Server Compatibility
• Client Compatibility

SSO Agent Platform Compatibility

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

**Supported Windows Platforms**

On Windows, SonicWall Directory Connector with SSO and SSO Agent 4.1.6 software are supported for installation on 32-bit and 64-bit servers running the following operating systems:

- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2
- Windows Server 2008
- Windows Server 2003 R2
- Windows 10
- Windows 8
- Windows 7

**NOTE:** Internet Explorer 8 or higher is required on the server when running the Directory Connector 4.1.6 Configuration Tool. On Windows Server 2003, IE6 is the default version of Internet Explorer, so you must upgrade IE in order to run the new SSO Agent user interface. However, the SSO Agent service does not have any IE version requirement.

**NOTE:** In a production environment, SonicWall recommends using Windows Server rather than Windows 7, 8, or 10.

**Supported Linux Platforms**

On Linux, SonicWall Directory Connector with SSO and SSO Agent 4.1.6 software are supported for installation on 64-bit platforms running the following operating systems:

- CentOS 7
- CentOS 6
- Ubuntu 16.04
- Ubuntu 14.04
- Fedora 25

**.NET Framework Compatibility**

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

- .NET Framework 4.5
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:

<table>
<thead>
<tr>
<th>Windows Server (32-bit / 64-bit)</th>
<th>CPU</th>
<th>Memory</th>
</tr>
</thead>
<tbody>
<tr>
<td>2016</td>
<td>Intel Xeon (4 processors)</td>
<td>4 GB</td>
</tr>
<tr>
<td>2012 / 2012R2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2008 / 2008R2</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

SonicWall Appliance / Firmware Compatibility

Directory Connector 4.1.6 is supported with the following SonicWall appliances and firmware versions:

- SuperMassive™ 9200 / 9400 / 9600 running SonicOS 6.1 and above
- SuperMassive 9800 running SonicOS 6.2.7.7 and above
- SuperMassive E10200 / E10400 / E10800 running SonicOS 6.0.x
- NSA 2650 running SonicOS 6.5 and above
- NSA 2600 / 3600 / 4600 / 5600 / 6600 running SonicOS 6.1 and above
- NSA E-Class E5500 / E6500 / E7500 / E8500 / E8510 running SonicOS 5.0 and above
- NSA 240 / 2400 / 3500 / 4500 / 5000 running SonicOS 5.0 and above
- NSA 220 / 220W / 250M / 250MW running SonicOS 5.8.1 and above
- 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
- SOHO running SonicOS 5.9.1.3 and above
- SOHO W running SonicOS 6.2.4.0 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.
Exchange Server Compatibility

SonicWall Directory Connector with SSO version 4.1.6 software is supported for use with the following Exchange servers:

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

Domain Controller Server Compatibility

SonicWall Directory Connector with SSO version 4.1.6 software is supported for use with domain controllers running the following Microsoft Windows operating systems:

- Windows Server 2016 – 64-bit
- 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

Novell eDirectory Server Compatibility

SonicWall Directory Connector with SSO version 4.1.6 software is supported for use with the following Novell eDirectory versions:

- Novell eDirectory 8.8.5 – 64-bit
- Novell eDirectory 8.8.7 – 64-bit

Terminal Server Compatibility

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

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

Client Compatibility

Directory Connector 4.1.6 is compatible with the following client operating systems on 32-bit and 64-bit platforms for the purpose of determining the logged in user name and other information necessary for user authentication:

- Windows 10
- Windows 8
- Windows 7
New Features

This section describes the new features included in Directory Connector 4.1.6.

Topics:

- Linux SSO Agent
- HTML-Based User Interface
- Terminal Server IP Virtualization Support
- Non-Cross Domain-Independent Credentials for DC, TS, and Exchange Servers
- Dashboard and Statistics on Status Page
- Static Users List Import/Export
- Users and Hosts Lists Export
- Third-party Integration Support – SSO API

Linux SSO Agent

SonicWall Directory Connector with SSO 4.1.6 introduces the Linux SSO Agent. The Agent is supported on a variety of Linux platforms, including CentOS 6 and 7, Ubuntu 14.04 and 16.04, and Fedora 25.

The Linux Agent is based on the previous Samba (SMB2) support and the performance is similar to the Windows SSO Agent. All of the main features in previous versions of the SSO Agent are implemented in the Linux SSO Agent. A few features are missing from the Linux Agent, including:

- DC Security Log Subscription and Server Session server monitoring methods
- Domain Controller auto discovery
- Terminal Server support

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

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

The Linux SSO Agent uses a web user interface that you can connect to at http://127.0.0.1:8080 on the local system where the Agent is installed. For security, the web user interface is not accessible using the system IP address. The web interface communicates with the service through JSON RPC using the RPC port 12348.

HTML-Based User Interface

In Directory Connector 4.1.6, the entire user interface has been rewritten as an HTML-based graphical user interface using the Ext JS framework. Ext JS is a JavaScript application framework for building interactive cross platform web applications.

The Linux SSO Agent user interface uses a web user interface that you can connect to using your browser, while the Windows SSO Agent is still displayed as a Windows form. Other than the carrier, the two SSO Agent user interfaces are very similar.
Terminal Server IP Virtualization Support

This feature provides an alternative method of identifying users logged into Terminal Servers which is expected to replace the SonicWall Terminal Server Agent in future releases.

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

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

Non-Cross Domain-Independent Credentials for DC, TS, and Exchange Servers

When adding a Domain Controller, Terminal Server, or Exchange Server in Directory Connector 4.1.6, you can specify the corresponding user name and password. These credentials are independent of one another and do not have to be in the same domain. The domain is specified as part of the user name, such as SSODC3\Administrator for a particular Domain Controller.

Dashboard and Statistics on Status Page

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

Static Users List Import/Export

The **Static Users** page of the user interface displays all the static users configured in the SSO Agent. You can manually add and remove a user on this page. In Directory Connector 4.1.6 you can import and export the whole user list.

To import a list of users from a CSV file, click the **Upload** button.

**Importing a Static User List:**

To export a list of users to a CSV file, click the **Export** button. The user list is saved as `C:\Program Files\SonicWall\SSOAgent\static.csv`. 
Exporting a Static User List:

Users and Hosts Lists Export

The Users and Hosts page of the user interface displays statistics and all the users in the cache. You can search and sort the users and can manually remove a user from the cache on this page. In Directory Connector 4.1.6 you can export the user list.

To export the list of cached users to a CSV file, click the Export button. The user list is saved as C:\Program Files\SonicWall\SSOAgent\users.csv.
Exporting from User and Hosts:

Third-party Integration Support – SSO API

The SSO API command line tool is introduced in Directory Connector 4.1.6.

**NOTE:** SonicOS 6.5.0.1 or higher is required for SSO API support.

You can use the SSO API tool to insert or delete a static user remotely or locally. This supports the integration of third-party applications with the SonicWall SSO Agent.

**SSO API Commands:**

Resolved Issues

This section provides a list of resolved issues in this release.

<table>
<thead>
<tr>
<th>Resolved Issue</th>
<th>Issue ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Users, although authenticated via DC logs, are not recognized via NetAPI even though the SSO Agent sends the user information to the firewall. SonicOS displays “SSO agent did not respond”. Occurs when using Single Sign-On with a SuperMassive 9800, which is a multi-blade appliance. After the firewall sends a request to query a user name, the SSO Agent first replies with a response, then sends the notification after retrieving the user information, but the response and notification do not always go to the same blade.</td>
<td>191774</td>
</tr>
<tr>
<td>The WMI query failure log messages do not include the host IP address. Occurs when SonicOS requests the query and the SSO Agent logs the failure in the SSOAgent.log file, without the host IP address. However, when using the Agent’s built-in Diagnostic Tool the WMI query failure log message does include the IP.</td>
<td>185097</td>
</tr>
</tbody>
</table>

Known Issues

This section provides a list of known issues in this release.

<table>
<thead>
<tr>
<th>Known Issue</th>
<th>Issue ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Linux SSO Agent sometimes cannot be restarted normally. Occurs after using WMI or NetAPI to authenticate about 10,000 users, but not always.</td>
<td>196223</td>
</tr>
<tr>
<td>If domain user, user1, logs into a client and then initiates an RDP connection to another destination using domain user, user2, as the credentials, user1 is replaced by user2 in the Users and Hosts page of the Directory Connector Configuration Tool. Occurs in a Windows farm environment with IP Virtualization enabled and using DHCP as the IP pool provider, when specifying the destination of the RDP connection by the farm name rather than by the IP address.</td>
<td>196023</td>
</tr>
<tr>
<td>The Users and Hosts screen in Directory Services Connector often displays the information of the last logon user rather than the current user’s information. Also, the last logon user is displayed with the wrong domain. Occurs when two domain controllers are added in the SSO Agent, one with a domain name (domain.com) and the other with a subdomain name (sub.domain.com). Both are in Server Session mode. The first client logon is displayed correctly, but subsequent logons by a subdomain user are incorrectly displayed with the domain, not the subdomain, and sometimes show the previous logon user name.</td>
<td>148858</td>
</tr>
<tr>
<td>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.</td>
<td>149533</td>
</tr>
</tbody>
</table>
Known Issue | Issue ID |
---|---|
Log off notifications are not available for certain client machines. | 149546 |
Occurs when using Linux client machines. SSO Agents are unable to detect log off/power off information from Linux clients. | |
Webmail users are deleted from the Users and Hosts table after two hours even when sending and receiving emails every 15 minutes. After the user is deleted, the Agent sometimes does not detect the user logging in again. | 149608 |
Occurs when the SSO Agent does not receive a login event during the two hours and clears the user from the cache after the default cache duration of two hours. When the user logs in again, there are still no login events in the Exchange security log and the SSO Agent does not detect the user login. | |

Product Licensing

SonicWall Directory Connector with SSO and Single Sign-On Agent are included with your SonicOS license and SonicWall network security appliance. SonicWall network security appliances must be registered on MySonicWall to enable full functionality and the benefits of SonicWall security services, firmware updates, and technical support. Log in or register for a MySonicWall account at https://mysonicwall.com.

SonicWall Support

Technical support is available to customers who have purchased SonicWall products 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. To access the Support Portal, go to https://www.sonicwall.com/support.

The Support Portal enables you to:

- View knowledge base articles and technical documentation
- View video tutorials
- Access MySonicWall
- Learn about SonicWall professional services
- Review SonicWall Support services and warranty information
- Register for training and certification
- Request technical support or customer service

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