WatchGuard® SSL v3.2 Update 3 Release Notes

Supported Devices	SSL 100 and 560
WatchGuard SSL OS Build	489931
Revision Date	18 November 2015

Introduction

WatchGuard® is pleased to announce the release of WatchGuard SSL OS v3.2 Update 3 for the WatchGuard SSL 100 and SSL 560.

We recommend all WatchGuard SSL customers install the v3.2 Update 3 release because it includes component upgrades to address several known vulnerabilities. See the Resolved Issues section for more information.

Highlights of the WatchGuard SSL v3.2 release include:

- Windows 8 and 64-bit Internet Explorer Support
- Outlook Anywhere Support
- Nested Group Support
- Access Client Settings Synchronization
- Access Client History Menu
- Optimized Assessment Scan
- Confirmation for Startup Commands
- DNS Suffix Assignment
- Log File Rotation Deletion

Windows 8 and 64-bit Internet Explorer Support

The SSL device now fully supports the Windows 8 operating system (32-bit and 64-bit). It is important to note that there a known issue with SMB traffic from an Access Client installed on Windows 8 that can cause a memory leak.

The SSL device also supports the 64-bit Internet Explorer with new ActiveX loaders for Assessment, Abolishment, and the Access Client.

Outlook Anywhere Support

You can now configure and use Outlook Anywhere with the SSL device. See Add an Outlook Anywhere Resource in the online help for detailed instructions on how to configure the SSL device for use with Outlook Anywhere.

The WatchGuard SSL device only supports basic authentication with Outlook Anywhere, and you must make sure that the Exchange Server and Outlook Client are configured to use basic authentication. NTLM is not supported..

Nested Group Support

The SSL device now supports nested groups (a user group that belongs to another group) within directory services. Nested groups are now processed correctly when access rules are applied, and appear correctly within reports and the group display in the admin Web UI.

Access Client Settings Synchronization

With this feature, you can store and synchronize individual Access Client preferences, history, and favorite resources on the SSL device. This feature is enabled by default. To configure client synchronization on the SSL device, click **User Management > Global User Account Settings**, then select the **User Client Settings Sync** tab.

On the Access Client, there are two methods to synchronize your client settings: automatic and manual. By default, automatic synchronization is disabled on the Access Client. To enable and configure automatic synchronization on the Access Client, select **Preferences**, then select the **Synchronization** tab. Select **Enable Automatic Synchronization** to automatically synchronize to the SSL device when you start an SSL tunnel and when you make any changes to your settings or favorites while connected to the tunnel.

To perform a manual synchronization, click **Synchronize Now** to immediately synchronize with the SSL device while connected to the tunnel. If you are not connected, a pop-up authentication dialog appears, and the client will synchronize to the SSL device after successfully authentication.

Client Favorites

Administrators can also add favorites globally for new users, or for a specific user that can be synchronized to their Access Client settings. To add favorites that will be synchronized to new users, click **User Management > Global User Account Settings**, select the **User Client Settings Sync** tab, then click **Add Favorite Resource**.

To manage favorites for a specific user, select **User Management > User Accounts**, select a specific user, then select the **Favorites** tab.

Access Client History Menu

A **History** menu option has been added to the Access Client. When a user loads a tunnel successfully, the details of the tunnel configuration are automatically saved in the History. This allows the user to easily open a recently accessed tunnel resource. The History menu can contain a maximum of 15 items.

Optimized Assessment Scan

The SSL device now caches the results of assessment access rules to improve the efficiency of assessing connections where multiple access rules are applied globally or applied to many resources.

To configure the behavior of assessment results caching, select **Manage System > Assessment**, then select the **General Settings** tab. These options are enabled when you create a corresponding assessment access rule, and allow you to collect and cache Windows, process, network, anti-virus, firewall, and anti-spyware information. If you remove the original access rules, these options remain enabled for caching purposes. You can disable these options to improve client scanning efficiency during assessment when you no longer require these assessment options.

Confirmation for Startup Commands

A **Confirm Command** option has been added to the **Startup** tab of a tunnel resource. When enabled, the end-user is prompted to confirm the command before it is run. If this option is disabled, the command is run automatically without confirmation. By default, this option is enabled for all resource wizards except RDP Access and SSH Access, where the command text is not readable.

DNS Suffix Assignment

The DNS suffix for a connection is now always applied, even if an IP address assignment fails. The DNS suffix is assigned automatically if DNS forwarding is enabled in the advanced settings of the tunnel resource. The DNS suffix is assigned based on your configured **DNS Search Order** field on the **Manage System > Network Configuration** page.

Log File Rotation Deletion

You can now configure how many log files to keep on the system before they are deleted. This prevents excessive log files from filling up your disk space. For each type of log, in the **Log File Rotation** section you can configure the **Max Files in Rotation**. The default is 90.

Before You Begin

The WatchGuard SSL devices and WG SSL OS v3.2 software enforce these software licensing rules:

- **Activation** — You must activate your WatchGuard SSL device with LiveSecurity to receive a license. If you do not have a valid license, you can complete the setup procedure using the default license. The license you get from LiveSecurity includes access to end-point integrity software updates.
- **User pack upgrades** — You must activate user upgrades with LiveSecurity to receive a license that gives you higher user capacity.
- **Software upgrades** — You must have a current LiveSecurity subscription to install software upgrades.

System Requirements

WatchGuard SSL Component	Microsoft Windows XP SP3 (32-bit)	Microsoft Windows XP SP2 (64-bit)	Microsoft Windows Vista (32-bit and 64-bit)	Microsoft Windows 7 & 8 (32-bit and 64-bit)	Microsoft Windows Server 2003	Mac OS X v10.7.3 (Lion)
WatchGuard SSL Web UI *Supported Browsers: IE 7, 8, 9, and 10, Firefox, Chrome*	✓	✓	✓	✓	✓	✓
WatchGuard SSL Client Software	✓	✓	✓	✓	✓	✓ * Static tunnels only

Installation

When you install your WatchGuard SSL device for the first time, use the instructions in the *WatchGuard SSL Quick Start Guide* included with your device. To download a copy of the latest guide, go to the Quick Start Guides page.

The following software components are available:

- WatchGuard SSL Operating System v3.2 Update 3
- Access Client Installation Software — Optional Access Client installation file for customers that require the Access Client to be installed manually on their end users' computers. Available for Windows 32-bit and Windows 64-bit operating systems.
- Mobile ID Client Installation Software — Optional software for administrators who want to distribute the Mobile ID clients to their end users. Available for Windows, Java, and Linux. This software has not been updated for the v3.2 release. You can continue to use the previously released Mobile ID Client software with SSL OS v3.2.

The Access Client software (including the ActiveX and Java access client) does not operate correctly when started from Internet Explorer 7 or later version in protected mode. To make sure that the browser is not in protected mode, in the Internet Options configuration, add the address of the SSL Application Portal to the list of trusted sites. Then, verify that the Internet Options configuration does not require protected mode for trusted sites.

To download the software:

1. Go to the WatchGuard Software Downloads page.
2. Select the SSL device model for which you want to download software

Upgrade from Previous Version

Before you upgrade, go the WatchGuard Software Downloads Center. Download and extract the SSL OS v3.2 Update 3 software update on the computer you use to connect to your SSL device.

You can upgrade from any previous version of the WatchGuard SSL OS.

To update the OS for your device:

1. Log in to the Web UI.
2. Select **Manage System > Device Update**.
   The Update OS page appears.
3. In the **Update the OS** section, click **Browse** to locate the software update file.
4. Click **Update**.
   The OS is updated and the device reboots. This can take several minutes.

After the device update is complete, log in to the WatchGuard SSL Web UI again. While the software version remains v3.2, you will see an updated build number for Update 3 (489931) on the System Status page.

Upgrade the Installed Access Client

If your end users have the Access Client software installed on their computers and you want to use the *.msi* installer to install the new Access Client software, you must manually uninstall the Access Client software from the computer before the *.msi* installer can install the new client software. If you use the *.exe* installer, there is no need to manually uninstall the older client software first.

Set up the Access Client for a Standard Windows User

The Access Client requires elevated access privileges to perform certain administrative tasks, such as to install a driver and to assign an IP address to a network adapter. In Access Client versions prior to SSL v3.1.1, users were required to log in to their Windows operating system as an administrative user before they could install or use the Access Client.

Current releases of the Access Client allow Windows standard users (users without administrator privileges) to connect to tunnel resources. Administrator privileges are still required for the initial installation of the Access Client software. The Access Client software includes a component, called the WatchGuard Access Client Helper Service, which performs the tasks that require elevated access privileges. This allows a user without administrator privileges to use the Access Client.

See Set up the Access Client for a Standard User for detailed installation instructions.

Resolved Issues in SSL v3.2 Update 3

- The SSL OS OpenSSL library has been updated to version 0.9.8zg and support for the SSLv3 protocol has been disabled in the Web UI to address vulnerabilities associated with POODLE (CVE-2014-3566). *[83673]*
- The SSL OS glibc library has been updated to address vulnerabilities associated with GHOST (CVE-2015-0235). *[84296]*
- The Web UI has been updated to address vulnerabilities associated with Logjam (CVE-2015-4000). *[85993]*
- The Web UI has been updated to address vulnerabilities associated with FREAK (CVE-2014-8730). *[84758]*
- Access to the Web UI is no longer prevented because of a weak Diffie-Hellman public key when using current Chrome and Firefox web browsers *[86707]*
- This release resolves an issue that caused resources to fail to load from the Application Portal with the error message "Could not load and start configuration. (error=5040001)". *[88331]*
- You can now successfully launch fileshare resources from the Application Portal that use unicode in their names. *[88681]*

Resolved Issues in SSL v3.2 Update 2

- Multiple OpenSSL vulnerabilities identified by security advisory FreeBSD-SA-14:14.openssl (CVE-2014-0195, CVE-2014-0221, CVE-2014-0224, and CVE-2014-3470) are resolved.

Resolved Issues in SSL v3.2 Update 1

- This release includes a new certificate for Java applets to replace the certificate that expires on 8 April 2014.
- This release resolves a compatibility issue with Java version 7u51 and later. *[78675, 78670, 78615, 78611, 79713]*
- The SSL device uses several Java applets that receive critical updates in this release:
  - Java-based Access Client
  - Java-based Endpoint Protection
  - Web Authentication client
  - RDP client for terminal services
  - SSHterm client for SSL
- This release resolves an issue that prevented SecureMatrix authentication from working with Java 7. *[71361]*
- IE 11 is now correctly recognized when loading a tunnel. *[79714]*
- An issue has been resolved that caused incorrect HTTP SMS messages. *[70978]*
- The Session Control setting **Duplicate user name logon reverse action** now works correctly on standalone access clients. *[43329]*
- The Log Viewer no longer truncates multi-line log messages. *[67939]*
- Complex access rules no longer cause exception errors. *[72594]*
- An issue has been resolved that caused configuration changes to fail. *[65723]*
- An issue has been resolved that caused configured resources to disappear with an access point stack trace. *[72024]*
- Access rulesnow work correctly for web resources that contain a question mark (?) in the URL path. *[59411]*
- This release resolves resource Access Error 1031601 that occured on web resources to a host that used Digest Access Authentication (RFC2069). *[71749]*
- System Status now shows the serial number and device type (SSL100 or SSL560). *[70933]*
- Users no longer experience a "0 Cache, No Store" error when they try to get access to web resources. *[72863]*
- Access rules based on group membership now work correctly. Users now only see resources when they are a member of the group specified in the access rule. *[73533]*
- The Login page no longer unexpectedly fails with an exception error when you click the Resource Access tab. *[73625]*
- Users are no longer added to the active user list when they are denied logon because of the Duplicate User Logon setting. *[73982]*
- This release resolves an issue that caused a properJavaRDP resource to fail with a 1032009 Permission Denied message. *[73732]*
- The properJavaRDP and SSH resources now work correctly when the SSL device portal port is set to a port number other than 443. *[69265, 73297]*
- You can now create multiple resources with the same host and port. *[73743]*
- Web resources no longer fail for connections to a Zentyal virtual machine server. *[74942]*
- This release resolves an issue that caused a long delay when you applied an Access Rule to a resource. *[74959]*

- The number of login attempts is no longer incremented when a user clicks Submit multiple times very quickly. *[74782]*
- The **Monitor System > Log Viewer > View Log** feature now displays as a web page that operates on all browsers instead of a dialog box. *[74650]*
- You can now use a host name when you configure a resource host. *[28287]*
- You can now use a host name when you configure a file share resource. *[55866]*
- An issue has been resolved that caused the Access Client to crash when requesting configuration information. *[76562]*
- The Access Client can now successfully map drives when the map share path includes the "/" character. *[76599]*
- When you create a Microsoft Windows File Share resource that uses a host name, you can now use the "/" character in the startup command. *[76628]*
- You no longer see a security warning when you use SecureMatrix authentication. *[77807]*
- The SSL device can now act as a RADIUS server for external authentication requests [*73402]*
- File share drives no longer fail to map when you use a host name instead of an IP address. This applies to resources with and without Single Sign-On (SSO) enabled. *[76564]*
- File share authentication with SSO no longer fails when a user authenticates with User Principle Name (UPN) format, such as user@example.com. *[75241]*
- When a tunnel resource uses an access rule based on group membership, the resource no longer shows an authentication failure when you use the installed Access Client without first logging in to Application Portal. *[74352]*

Resolved Issues in SSL v3.2

System

- Inactive timeouts no longer occur when you transfer large files over HTTP or FTP. *[40456]*
- Feature keys are now installed correctly when the licensee's company name contains special characters. *[40490]*
- The log viewer reload button now works correctly on the Google Chrome web browser. *[44916]*
- A device upgraded from v3.1.1 to a later version now correctly enters recovery mode when invoked from the front panel. *[57363]*
- When using the SMS channel, the SSL device now correctly recognizes when no phone number is provided and does not send an SMS message. *[64851]*
- Mobile Text Authentication now correctly switches to the next SMS channel when an error is detected with the original SMS channel. *[64852]*
- TFTP File transfers over 32MB now complete. *[66004]*
- The User Audit Report now correctly displays resource names in the Resources Used column. *[67322]*
- Changes to SMS channel settings no longer cause intermittent system errors. *[67522]*
- User manual linking errors no longer occur when the system is using a non-US time zone region. *[67570]*
- Reports now display a descriptive tunnel resource name. *[67653]*
- A listener configured for a different port than 443 can now be correctly accessed from an external client. *[67887]*
- Group access rules now work correctly after groups have been reorganized in a directory tree. When the group is moved, you must open the group access rule and save it again. The SSL device will then re-search the group and apply the new group location for the access rule. *[68233]*
- You can now enter "0" in the Max Logon Retries option to disable account locking in the Global User Account Settings page. *[68421]*

- The SSL device no longer attempts new authentication connections to an LDAP server when the user has already connected. *[69917]*

Client

- A tunnel configuration saved as a favorite in the Access Client now correctly includes the server port information. *[37330]*
- For improved Access Client performance, the client tunnel connection limit has been increased to 128 per tunnel from 60. *[39097]*
- Additional pop-up certificate warnings do not occur when the Access Client is launched from a web browser after you have already connected to the web portal. *[65015]*
- Access Client instability has been mitigated when accessing file shares. *[66227]*
- Proxy detection delays no longer occur when launching a tunnel with the Access Client on Internet Explorer. *[66705]*
- The standalone Access Client can now correctly access mapped drive file shares with the $uid option set. *[67099]*
- Connection timeouts have been reduced when assessment is run on an Access Client before a connection is allowed. *[67127]*
- A certificate warning no longer occurs during assessment on the standalone Access Client when you have already connected via a tunnel. *[67128]*
- A scroll bar now appears on the Java RDP client when the RDP session is larger than the host screen size. *[67415]*
- You are no longer prompted for authentication when you launch the Access Client from the web portal and you have already connected to a resource. *[67726]*
- Timeouts no longer occur when the Access Client acquires an IP address from an IP pool. *[67938]*
- Access Client DNS suffix assignment is now always applied, even if an IP assignment fails. *[68075]*
- Unresponsive page errors no longer occur when you load a tunnel with a low bandwidth client using the Google Chrome web browser. *[68113]*
- Drives are now correctly mapped when you access a file share resource that uses a mapped drive letter already in use. *[68403]*
- Verification is now performed to prevent the Access Client from installing on the wrong 32 or 64-bit OS platform. *[68422]*
- The Access Client no longer crashes during an update. *[69929]*
- You can now update the Access Client from a port other than the default port 443. *[69936]*

Nested User Groups

- User groups now display correctly when you view the users of a nested group. *[37706]*
- Access rules and policies for user groups now work with nested groups. *[67461]*
- Nested groups are now processed and reported in the User Policy Analysis Report. *[68123]*

Web Resource and Outlook Web Access

- Proxy errors no longer occur when connecting to a web resource. *[44289]*
- Notification errors no longer occur when using an OWA 2010 web resource. *[45346]*
- Outlook configured for RPC over HTTP (such as Outlook Anywhere) now works. *[55909]*
- Outlook Web Access now works when IIS is configured to accept a client certificate. *[69946]*

Known Issues and Limitations

You can find information about known issues for WatchGuard SSL software, including workarounds where available, on the WatchGuard website. To see Known Issues, log in to the WatchGuard website and use the filters available on the Technical Search > Knowledge base tab.

Product Documentation

The WatchGuard SSL appliances include a context-sensitive help system. You can find updates to the help system, as well as a complete documentation set for the product, online at http://www.watchguard.com/wgrd-help/documentation/overview. There are no documentation updates for this release.

Technical Assistance

For technical assistance, contact WatchGuard Technical Support by telephone or on the Web at http://www.watchguard.com/support. When you contact Technical Support, you must supply your registered Product Serial Number, LiveSecurity key or Partner ID.

	Phone Number
U.S. End Users	877.232.3531
International End Users	+1 206.613.0456
Authorized WatchGuard Resellers	206.521.8375