FORCEPOINT

Release Notes

Revision A

Stonesoft SSL VPN 1.5.211

Contents

About this release

This document contains important information about the current release. We strongly recommend that you read the entire document.

Resolved issues

These issues have been resolved since Stonesoft SSL VPN version 1.5.208. For a list of issues that have been fixed in earlier releases, see the Release Notes for the specific release.

Issue	Description
Security vulnerabilities in OpenSSL library (#135442)	The OpenSSL library included in the SSL VPN engine was updated to address discovered security vulnerabilities.
/data partition might become full (#116834)	The file /data/home/root/.sg-sslvpn-client/remote.pem might grow until the /data partition becomes full.
Only up to 32 certificate authorities are used even if configuration contains more (#116806)	If client certificate authentication methods are configured with more than 32 certificate authorities, client certificates are only matched against 32 authorities.
Selecting certificate to be used in Access Client might fail (#116893)	Using certificate authentication while authenticating directly from the Access Client might fail, even if the same certificate can be used when logging in through the web portal.

System requirements

Stonesoft appliances

Stonesoft SSL VPN version 1.5.211 is supported on all Stonesoft SSL VPN appliances.

Installation of 32-bit and 64-bit engine software, or upgrade to 64-bit engine software is supported only on the following SSL VPN appliances:

- SSL-1035
- SSL-1302
- SSL-3201
- SSL-3202

For older appliance models, use 32-bit engine software.

Mirrored configurations between 32-bit and 64-bit engines are not supported.

Upgrade instructions

When upgrading mirrored systems, see the upgrade instructions in the *SSL VPN Administrator's Guide*, which is available at https://support.forcepoint.com.

It is recommended that you publish the configuration after a successful upgrade.

Upgrade from previous version

Upgrade Stonesoft SSL VPN from 1.5.x to 1.5.211 through the Web Console. After the upgrade, log in to the SSL VPN Administrator and publish the updated configuration if the Publish button is highlighted.

Upgrade from prior versions

Upgrade Stonesoft SSL VPN from 1.4.x to 1.5.211 through the Web Console. After the upgrade, log in to the SSL VPN Administrator interface and publish the updated configuration if the Publish button is highlighted.

Direct upgrade from other versions to Stonesoft SSL VPN 1.5.211 has not been tested, but might work.

Build version

The Stonesoft SSL VPN 1.5.211 build version is 2032.

Product binary checksums

sslgw_engine_1.5.211.2032_i386.zip

SHA1SUM:

`f30e9b133ecb6da3ea014cdbe9280862731fa006`

sslgw_engine_1.5.211.2032_x86-64.zip

SHA1SUM:

`f893a23fe67e2b043294d23f6ee8f8d3ede36a56`

Compatibility

Requirements

- Administration of Stonesoft SSL VPN version 1.5.211 requires the use of a workstation with a TCP/IP network configured and a web browser installed.
- To use the Application Portal, the connecting client must have TCP/IP configured and a web browser installed.
- To use Tunnel Resources, such as client/server TCP/UDP-based applications, the connecting client must have TCP/IP configured and a web browser compatible with Java or ActiveX technologies installed.
- To use the Stonesoft Web authentication method, the client must support Java technology to display the clickable webpad.
- To use the Stonesoft MobileID (Synchronized or Challenge) authentication method, the client must have MobileID software installed and seeded.

Directory services

User information can be stored in an internal user directory, or one of the following external directory services can be used:

- Microsoft Active Directory 2003
- Microsoft Active Directory 2008
- Novell eDirectory
- OpenLDAP
- Sun Java System Directory Server
- Oracle Internet Directory (authentication only)
- Tivoli Directory Server (authentication only)
- IBM RACF LDAP (authentication only)
- OpenDS 2.x
- OpenDJ

NOTE – You must use an external Directory Service or the new OpenDJ Directory Service for a mirrored pair configuration. For additional information, see the *SSL VPN Administrator's Guide*.

Access Client

When using the Access Client on Windows 7 or Windows 8, the following requirements apply:

Requirement	Description
Access Client on Microsoft Windows 7 and Windows 8 requires administrator rights	The Access Client requires administrator rights the first time it is used on Windows Vista, Windows 7, and Windows 8. The Access Client automatically upgrades afterwards. Alternatively, you can use remote software distribution or installation systems and the provided Access Client MSI package.
Stonesoft ActiveX Client Loader requirements	To run the ActiveX Access Client loader successfully with Windows Vista UAC, you must add the HTTPS address of the Access Point server to the list of trusted sites in Internet Explorer.
Drive letter mapping in Microsoft Windows 7 and Windows 8	A single drive letter (for example, `F:`) cannot be used as a startup command in Windows Vista, Windows 7, and Windows 8. All commands must be executed using "runas" to elevate to administrator mode, because the mapping is done in administrator mode, and "`F:`" is not a valid executable. Use the following startup command instead: `explorer /root, F:` This command works on Windows 7 and Windows 8.
Java Runtime Environment	To run the Stonesoft Java Access Client, use Sun Java 1.6 Update 2 or higher.

When using the Access Client on Linux or Mac OS, the following requirements apply:

Requirement	Description

Access Client on Linux and Mac OS platforms does not connect to a SSL VPN Access Point without a trusted certificate to validate the gateway certificate on the client	The Linux and Mac OS Access Clients can be downloaded through a Java Loader or an essp:// protocol handler in the browser. Before resources can be used, the client must verify the SSL VPN gateway certificate using the public certificate of the signer. One of the following files must be present:
	`$HOME/.sg-sslvpn-client/trust.pem`
	`$HOME/.sg-sslvpn-client/server.pem`
	If the SSL VPN gateway uses a self-signed certificate, the trust.pem file should include the self-signed certificate. Otherwise, the public CA certificate that issued the gateway certificate.
	Alternatively, only the server certificate can be placed in file server.pem.

For additional information about libraries and components to install, see the *Stonesoft SSL VPN Administrator's Guide*.

Feature requirements and compatibility

Feature	Compatible browsers or operating systems
Stonesoft SSL VPN Application Portal	Any JavaScript enabled web browser
Stonesoft Administrator	Any JavaScript enabled web browser
Stonesoft Web Authentication Method	Any Java compliant browser
Stonesoft MobileID Free Authentication Software Token	• Microsoft Windows 7 (32 and 64 bit), Windows 8 • Linux (distribution independent, 32 and 64 bit) • Apple MAC OS X 10.6.x (Snow Leopard), 10.7.x (Lion) • Apple iOS (iPhone and iPad) • Android 2.x, 3.x and 4.x • WinPhone • Java • BlackBerry • Symbian "Belle"
Access Client	• Microsoft Windows 7 32/64 bit • Microsoft Windows 8 • Apple Mac OS X 10.6.x (Snow Leopard) 10.7.x (Lion) • Linux Fedora 32/64 bit • Linux Ubuntu 32/64 bit • Linux Suse 32/64 bit
Stonesoft Endpoint Security (Assessment)	• Microsoft Windows 7 32/64 bit • Microsoft Windows 8 • Apple Mac OS X 10.6.x (Snow Leopard) 10.7.x (Lion), 10.8.x (Mountain Lion)
Stonesoft Endpoint Security (Abolishment)	• Microsoft Windows 7 32/64 bit • Microsoft Windows 8

Known issues

For a list of known issues in this product release, see knowledge base article 12203.

Find product documentation

On the Forcepoint support website, you can find information about a released product, including product documentation, technical articles, and more.

You can get additional information and support for your product on the Forcepoint support website at https://support.forcepoint.com. There, you can access product documentation, knowledge base articles, downloads, cases, and contact information.