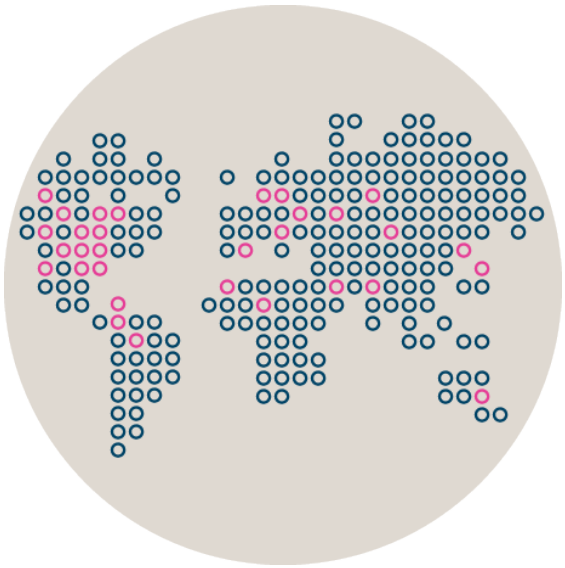

Stonesoft Management Center

Release Notes for Version 5.5.1

Updated: December 19, 2013

STONESOFT

Table of Contents

What's New

Enhancements

Enhancements that have been made since Stonesoft Management Center version 5.5.0 are described in the table below.

Enhancement	Description
Number of Group members visible in Configuration view	It is now possible to see directly in the Groups view (Configuration > Security Engines > Network Elements > Groups) how many Groups and other elements belong to each Group element.

Fixes

The problems described in the table below have been fixed since Stonesoft Management Center version 5.5.0. A workaround solution is presented for earlier versions where available.

Synopsis	Description	Workaround for Previous Versions
Web Start fails to open the Management Client with Java JRE 7u45 (#99696)	Starting the Management Client through Web Start fails when you have Java Runtime Environment (JRE) version 7u45 installed on the client computer.	There are three possible workarounds: - Install the Management Client locally on your computer. - Downgrade the JRE to an older version. - Install the older JRE version (JRE 1.7u40) in a different location (e.g.: /home/legacy/) and use the javaws binary to launch the JNLP URL (e.g.: /home/legacy/JDK_1.7.0_40/bin/javaws.exe http://localhost/smcclient.jnlp).
Java Web Start fails to open the Management Client with JRE 7u25 (#95930)	Starting the Management Client through Java Web Start fails when you have Java Runtime Environment (JRE) version 7u25 installed on the client computer.	Install the Management Client locally on your computer or downgrade the JRE to an older version (e.g. JRE 7u21).
Management database installation may fail on Windows 2008 (#93078)	Management database installation may fail with a "Permission denied" error for the pg_log folder in Windows 2008 R2 if you are logged in with an administrator account that has a different name than the PostgreSQL service account.	Use the PostgreSQL service account for installing the SMC or contact Stonesoft Support for more information on the issue.

Synopsis	Description	Workaround for Previous Versions
Automatic CA Renewal fails in environments with multiple Domains (#91375)	The Automatic CA Renewal feature checks that engines from all of the Domains have received the new CA before the CA is updated. In SMC 5.4.0 or higher, the system fails to check engines from Domains other than the Shared Domain and attempts to update the CA, even though the engines in the other Domains have not yet received the new CA. This results in a lost connection between the engines in the Domains other than the Shared Domain and the SMC. You must then make initial contact again between the engines and the Management Server.	N/A
Deleting element fails with error "Move to Trash Failed" (#82416)	In an environment with multiple Management Servers, deleting an element may fail with the error "Move to Trash Failed".	1. Open the element properties and click OK. 2. Delete the element.
Policy Editor in Preview mode may not show latest edits (#92745)	When in Preview mode, the Policy Editor may not show the latest edits. After switching to Edit mode, the latest changes are visible in the Policy Editor.	N/A
Info panel in policy editing view not updated (#92602)	The Info panel shows names and IP addresses of network elements when you click the Source or Destination cell, and Service names with ports when you click the Service cell of a rule. When you switch between the different cells, the labels in the Info panel are not updated.	Close the policy and open the policy for editing again.
Logging option for Correlation Situation is ignored (#93421)	If you set the Logging option to something other than "None" on the Inspection tab in the Inspection Policy, the Correlation Situation matches the event in the traffic, but the Log Level setting is ignored. For example, setting the Log Level to "Alert" for the "Suspicious traffic" category does not result in an alert from a match to the event in the traffic.	Make sure that a Correlation Situation with the Log Server as the context has a Logging option set to something other than "None" in the Inspection Policy.
Dynamic update package activation fails when upgrading to SMC 5.5.0 (#94186)	If you have dynamic update package 520 or newer activated when you upgrade to SMC 5.5.0, the new SMC version fails to reactivate the dynamic update package. This may cause the policy installation to fail after the upgrade.	Activate the newer dynamic update package after the upgrade. If it is not available, reactivate the one that was activated before the SMC upgrade.
Elements for TLS Inspection are not shown in Management Client (#94714)	After upgrading the SMC, the Client Protection Certificate Authority and Server Credentials are not shown on the Add-Ons tab of the engine element properties. However, the elements are still referenced.	Contact Stonesoft Support for a workaround.
Virtual Security Engines consume Management Server license node count (#95508)	Only the Master Engine counts against the node limit that is defined in the Management Server license. However, in SMC 5.5.0, Virtual Security Engines also consume the node limit.	Contact Stonesoft Order Services to temporarily increase the Management Server license node count if needed.
Policy installation on multiple firewalls with different versions may fail (#96330)	Installing the same Policy on multiple firewalls at the same time may fail if the firewalls run different software versions, especially if the firewalls run different major versions.	Install the Policy one firewall at time.

Synopsis	Description	Workaround for Previous Versions
Tasks that involve Log Server may fail in environment with multiple Management Servers (#89480)	In an environment with multiple Management Servers, Tasks that involve Log Servers may fail after changing the active Management Server. The following error is displayed: "Reason: Unexpected Error". The affected Tasks include the Log Export Task and the Log Server Backup Task, for example.	Change the active Management Server again. Tasks usually start working again automatically after the active Management Server is changed again.
Type-ahead search does not find IP addresses of Networks or Address Ranges (#96449)	Type-ahead search finds the IP addresses of Host elements, but does not find the IP addresses of Network or Address Range elements.	N/A
Firewall element not shown in other Domain after moving from Shared Domain (#82740)	After moving a Firewall element from the Shared Domain to another Domain, the System Status view and the Domain Overview may not show the Firewall element.	Restart the Management Server service.
Engine elements with references to temporary filters cannot be deleted (#93628)	Upgrading a legacy combined Sensor-Analyzer to an IPS engine or deleting an engine element may fail with the following error details: "An element that is still referenced by others cannot be deleted. The referenced elements() are:" The list of referenced elements is empty or contains the engine element itself. This may happen due to temporary filters that reference the engine element.	Contact Stonesoft Support for a workaround.

In addition, SMC 5.5.1 includes fixes to these known issues that were already fixed in SMC 5.4.6:

- Importing Route-Based VPN fails (#92003)
- Adding multiple CVIs and NDIs from the same network address range has unintended results (#92050)
- Link Aggregation and Tunnel Interfaces cannot be configured for the same firewall (#92225)
- "View as Table" lists all Domains (#92593)
- Policy upload fails if the policy contains a jump rule to an empty sub-policy (#92724)
- Engines that belong to other Domains visible in Overviews (#93583)
- Deleting DNS element in Firewall DNS settings causes database error (#94568)
- "Notify when engine upgrade becomes available" option does not work (#92693)
- Administrator with "Manage Users" permission cannot open user properties (#91770)
- Various Firewall-related actions may fail due to problems with VPN end-points (#90121)
- No users shown when browsing LDAP Domain on external LDAP Server without Stonesoft-specific attributes (#92283)
- Expressions with None or Any may create incorrect configuration for 5.4 Firewall engine (#94779)

For more information, see the SMC 5.4.6 Release Notes.

Other Changes

Change	Description
Changes in entropy generation for SMC installation (only in 5.5.1_8530)	The Linux /dev/random random number generator is used as the entropy source for internal long-term key pair generation. As a result, the first service start-up and possible later certificate renewal operations are blocked until the required amount of entropy is available. Depending on the environment, this may take up to a few minutes. It is then not possible to install this SMC version in environments that do not have an input device (mouse or keyboard).

Change	Description
Option for SMC Load Sharing removed (since 5.5.1)	It is no longer possible to configure Management Servers in active-active mode. Only one Management Server can be active at a time.
SMS Alert Sending (since 5.5.0)	There is no longer support for directly attached SMS modems for sending alert notifications. Instead of directly attached SMS modems, customers can use HTTP- or SMTP-based alert notification methods.
Configure Updates and Upgrades moved to Management Server properties (since 5.5.0)	There is no longer a separate Configure Updates and Upgrades dialog. The settings are now found in the Management Server properties dialog.
Simplified License view (since 5.5.0)	The view that lists licenses in the SMC has been reorganized with more simplified labels.
Changes to Tasks branches (since 5.5.0)	The Running Tasks and Executed Tasks branches have been merged into a single History branch. There are now only two branches for Tasks: Definition and History. The Definition branch shows custom Task Definitions and predefined System Task Definitions. By default, the History branch shows Tasks that are currently running. Optionally, you can also view Executed Tasks in the History branch. System Tasks are not shown in the History branch unless the Show Executed Tasks option is enabled.
Configuration parameters related to “SMS notifications based on HTTP” no longer supported (since 5.5.0)	In SMC 5.5, the following parameters in the LogServerConfiguration.txt, AuthenticationServerConfiguration.txt, and the SGGlobal.txt files are no longer supported: • SMS_HTTP_MESSAGE_FIELD • SMS_HTTP_PHONE_FIELD • SMS_HTTP_ACCOUNT_FIELD • SMS_HTTP_USER_PWD • SMS_HTTP_ADDON_QUERY_STRING • SMS_HTTP_PWD_FIELD The options can now be configured in the Management Client.

System Requirements

Basic Management System Hardware Requirements

- Intel Core family processor or higher recommended or equivalent on a non-Intel platform
- A mouse or pointing device (for Management Client only)
- SVGA (1024x768) display or higher (for Management Client only)
- Disk space for Management Server: 6 GB
- Disk space for Log Server: 50 GB
- Memory requirements for 32-bit operating systems:
  - 2 GB RAM for Server (3 GB minimum if all components are installed on the same server)
  - 1 GB RAM for Management Client
- Memory requirements for 64-bit operating systems:
  - 6 GB RAM for Server (8 GB minimum if all components are installed on the same server)
  - 2 GB RAM for Management Client

Operating Systems

Stonesoft Management System supports the following operating systems and versions:

- Microsoft® Windows Server 2008™ SP2 and R2 (32-bit and 64-bit)*
- Microsoft® Windows 7™ SP1 (32-bit and 64-bit)*
- Microsoft® Windows Vista™ SP2 (32-bit and 64-bit)*
- Microsoft® Windows Server 2003™ SP2 (32-bit)*
- CentOS 6 (for 32-bit and 64-bit x86)
- Red Hat Enterprise Linux 6 (for 32-bit and 64-bit x86)
- SUSE Linux Enterprise 11 SP1 (for 32-bit and 64-bit x86)

*) Only the U.S. English language version has been tested, but other locales may work as well.

Build Version

Stonesoft Management Center version 5.5.1 build version is 8530.

This release contains Stonesoft Dynamic Update package 533.

Compatibility

Minimum

Stonesoft Management Center version 5.5 is compatible with the following Stonesoft component versions:

- Stonesoft Firewall engine version 5.1.0 or higher
- Stonesoft IPS engine version 4.3.0 or higher
- Stonesoft SSL VPN version 1.4.0 or higher

Native Support

To utilize all the features of Stonesoft Management Center version 5.5, the following Stonesoft component versions are required:

- Stonesoft Security Engine version 5.5 or higher
- Stonesoft Firewall engine version 5.5 or higher
- Stonesoft IPS engine version 5.5 or higher
- Stonesoft SSL VPN version 1.5 or higher

Installation Instructions

Note – The sgadmin user is reserved for Stonesoft use on Linux, so it must not exist before the Stonesoft Management Center is installed for the first time.

The main installation steps for the Stonesoft Management Center and the Firewall, IPS or Layer 2 Firewall engines are as follows:

1. Install the Management Server, the Log Server(s), and optionally the Web Portal Server(s) and Authentication Server(s).
2. Import the licenses for all components (you can generate licenses on our web site at https://my.stonesoft.com/managelicense.do).
3. Configure the Firewall, IPS, or Layer 2 Firewall elements with the Management Client using the Security Engine Configuration view.
4. Generate initial configurations for the engines by right-clicking each Firewall, IPS or Layer 2 Firewall element and selecting **Save Initial Configuration**.
5. Make the initial connection from the engines to the Management Server and enter the one-time password provided during Step 4.
6. Create and upload a policy on the engines with the Management Client.

The detailed installation instructions can be found in the product-specific installation guides. For a more thorough explanation of using Stonesoft Management Center, refer to the Management Client *Online Help* or the *Stonesoft Administrator's Guide*. For background information on how the system works, consult the *Stonesoft Management Center Reference Guide.* All guides are available for download at www.stonesoft.com/en/customer_care/documentation/current/.

Upgrade Instructions

Note – Stonesoft Management Center (Management Server, Log Server, Web Portal Server and Authentication Server) must be upgraded before the engines are upgraded to the same major version.

Stonesoft Management Center version 5.5.1 requires an updated license if upgrading from version 5.1 or earlier. Unless the automatic license updates functionality is in use, request a license upgrade on our website at https://my.stonesoft.com/managelicense.do and activate the new license using the Stonesoft Management Client before upgrading the software.

To upgrade an earlier version of the Stonesoft Management Center to Stonesoft Management Center version 5.5.1, we strongly recommend that you stop all the Stonesoft services and take a backup before continuing with the upgrade. After taking the backup, run the appropriate setup file depending on the operating system. The installation program detects the old version and does the upgrade automatically.

Versions earlier than 4.0.0 require upgrade to version 4.0.0 – 5.1.4 before upgrading to version 5.5.

Caution – Before you upgrade to SMC 5.5, note the known issues #80132 and #91528 related to upgrades in the following table.

Known Issues

The current known issues of Stonesoft version 5.5.1 are described in the table below. For an updated list of known issues, consult our website at http://www.stonesoft.com/en/customer_care/kb/.

Synopsis	Description	Workaround
Changing notification settings for Management Server requires restart (#96962)	After changing notification settings in the Management Server properties, the new settings are taken into use only after the Management Server service is restarted.	N/A
Saving an IPS or Layer 2 Firewall element that has different Logical Interfaces fails (#96914)	You cannot save IPS or Layer 2 Firewall elements that have different Logical Interfaces defined for different VLANs under one inline pair.	N/A
NAT configuration for Virtual Security Engines may be incorrectly generated (#97116)	In some situations, the NAT configuration for Virtual Security Engines may be incorrectly generated. This may result in some connections using the wrong NAT definition.	At policy installation, deselect the 'Keep Previous Configuration Definitions' option in the Upload Policy Task Properties dialog.
Remote upgrade does not work for all old engine versions (#80132)	Remote upgrade does not work for all old engine versions. This issue is fixed in engine versions: - Firewall/VPN 5.1.10 - Firewall/VPN 5.2.8 - Firewall/VPN 5.3.4 - IPS 5.2.104 - All engine versions 5.4 and 5.5 and higher.	Upgrade the engine locally (see the Firewall/VPN Installation Guide or the IPS and Layer 2 Firewall Installation Guide) or contact Stonesoft Support.
Management Server may not start due to incorrect default memory settings (#96508)	The Management Server service may not start because the incorrect amount of memory is reserved for it. The following error messages may be displayed: "Error: Could not create the Java Virtual Machine." "Error: A fatal exception has occurred. Program will exit."	Reduce the maximum memory value from 1048 to 512 by setting this row in the SGConfiguration.txt file: MANAGEMENT_MAX_MEMORY_IN_MB=512
256-bit security strength for management connections is not compatible with SSL VPN (#93100)	The SSL VPN is not compatible with Management Servers that use 256-bit security strength for management connections (introduced in version 5.5.0). The SSL VPN cannot contact the Management Server when 256-bit security strength for management connections is enabled. Monitoring, logging, and statistics related to the SSL VPN do not work.	Do not enable 256-bit security strength for management connections if you want to monitor the SSL VPN through the SMC.
IPS alerts are not displayed for IPS log data type (#91116)	IPS alerts are not visible if you select “IPS” as the log data type in the Logs view. This problem affects IPS engine versions 5.4.0 or higher.	Select “Security Engine” as the log data type in the Logs view instead.

Synopsis	Description	Workaround
Remote upgrade to Security Engine version 5.4 or higher fails when upgrade is started from Engine Upgrades > Firewall (#91528)	When a remote upgrade to Security Engine version 5.4 or higher is started from the Other Elements > Engine Upgrades > Firewall branch of the Administration Configuration view, the upgrade fails.	Start the upgrade from the Other Elements > Engine Upgrades > Security Engine branch of the Administration Configuration view.
Initial contact between SMC 5.4 and version 5.2 Combined Sensor-Analyzers may fail (#92367)	Initial contact between SMC 5.4 and version 5.2 Combined Sensor-Analyzers may fail due to failed POS license binding. This issue has been found in SMC 5.4.4 and 5.4.5, and IPS 5.2 versions. This issue does not affect Single Sensors or Sensor Clusters.	N/A
Initial license counter is displayed even if appliance has permanent license (#90404)	The initial license counter is started when a new appliance makes initial contact with the Management Server. Even if the policy has been installed on the appliance, and the appliance has then received its permanent license, the Initial Contact Date shows “xx days left”. To verify that the appliance has the correct license, check the Licenses view. The license should be shown as “Bound”.	You can safely ignore the initial license counter if the correct license is bound to the element and a policy is installed.
Traffic that matches a rule that applies the Forward VPN action may also match a NAT rule (#84207)	Traffic that matches a rule that applies the Forward VPN action may also match a NAT rule after a policy has been installed with SMC 5.4. Matching traffic is not correctly forwarded. The logs show that NAT was applied to the traffic.	Add a NAT rule that matches the traffic forwarded from one VPN tunnel to another before the NAT rule that incorrectly matches the traffic. Leave the NAT cell empty.
Firewall Policy tree is not displayed correctly (#75857)	Some Firewall Policies or the whole sub-tree of Firewall Policies may not be displayed in the Security Engine Configuration view.	Select Tools > Collapse All and Tools > Expand All to make all the Firewall Policies reappear.
Access rules containing non-HTTP-based applications do not work with 5.3 Firewalls (#81846)	Dynamic update packages 450 and later include non-HTTP-based Applications that can be placed in Access rules. If you try to upload a policy containing this type of rules to an engine of version 5.3 or lower, the rules are ignored because support for non-HTTP-based Application identification is introduced in engine version 5.4.	Do not use non-HTTP-based Applications if your target engines are not yet upgraded to version 5.4.
Proof-of-serial licenses are not always bound correctly (#49192)	When the appliance makes initial contact with the Management Server, the appliance is not always recognized correctly. As a result, the proof-of-serial code and the appliance name do not appear in the Info Panel. The SMC is then not able to automatically retrieve the license for the appliance.	Right-click the engine element, and select Tools > Get DMI Info. If that does not help, save the initial configuration for the appliance again.

Synopsis	Description	Workaround
Policy validation may fail to detect NDI addresses in NAT rules (#75021)	NDI addresses should never be used as NAT addresses. Using an NDI address as a NAT address (including indirectly through NAT chains that involve an NDI address that is used as a NAT address) produces a cluster load balancing configuration where certain connections can be handled only by a specific node. The load balancing entries may come from NAT rules that were used in previous policies and are still active, even though they no longer exist in the policy. Policy validation may fail to detect this type of NAT rule, especially with complicated and cross-referenced NAT configurations.	To remove load balancing entries that refer to previous NAT rules, install the policy but do not enable the “Keep previous configuration settings” option. Firewall engines starting from 5.3.4 (5.1.10 and 5.2.8) prevent situations in which fail-over between nodes fails due to load balancing entries that link NDI addresses to NAT. Policy installation fails with the following error message: “Load balancing configuration contains invalid flag combinations”.
Connection monitoring may not work correctly with older engine versions (#69925)	The system may fail to show the active connections in the Connection Monitoring view if the Firewall engine version is 5.1.0 or lower.	Upgrade the Firewall engine to version 5.2.0 or higher.
System Report schedules are deleted when upgrading from SMC 5.1.4 to 5.2.1 or higher (#65027)	If you upgrade from SMC 5.1.4 to 5.2.1 (or higher) you lose all the existing Report schedules for the System Report in the upgrade. You must reschedule the System Report’s report operation after the upgrade. This issue concerns only schedules that relate to the “System Report” Report Design.	N/A
Policy upload fails because NAT rule contains an invalid definition (#64461)	Customers upgrading to SMC 5.2.2 or higher may get a message at policy installation about an invalid static source or destination NAT definition that prevents installing the policy. The reason for the issue is that the size of the original address range is different than the size of the translated address range in a static NAT rule. One explanation for this can be that the Broadcast and Network Addresses Included option is selected for one network but not for the other network used in the NAT definition.	Make sure that the original and translated address ranges are of the same size in the Network Address Translation dialog.
Dynamic update package activation and policy upload do not work (#50716)	The Management Server database may be corrupted, preventing update activation and policy upload if dynamic update package 218 has been active at some point in the Management Server history. Usually the symptoms of the problem appear after upgrading to a new version.	Contact Stonesoft Support for a workaround.
DHCP REBIND requests are not allowed by default (#29987)	If DHCP clients fail to renew IP addresses from the server that originally allocated the addresses, the clients attempt to broadcast DHCP REBIND messages to the network, requesting that some other DHCP server renew the IP address. The DHCP Relay Sub-Policy does not allow these packets by default.	Add a stateless rule before the jump to the DHCP Relay Sub-Policy to allow DHCP packets from the DHCP clients to the broadcast address: Source: [Address range of your DHCP pool] Destination: DHCP Broadcast Destination Service: BOOTPS (UDP) Action: Allow Options: No connection state tracking

Synopsis	Description	Workaround
Upgrade of online node in standby cluster never reaches 100% (#49342)	When upgrading an online node in a standby-mode cluster, the Management Server keeps waiting for the node to come back online after upgrade, even though the normal behavior is that the node stays in standby mode after reboot.	Close the upgrade window and ignore the message about waiting for the node to come online.
Listening ports under 1024 are not supported for Web Start and Web Portal Servers in Unix environments (#38834)	Web Start and Web Portal Servers are not able to listen to port numbers under 1024 in Unix environments.	N/A
Firewall engines with dynamic control IP address do not support manual blacklisting (#16597)	Firewall engines that have a dynamic control IP address do not support manual blacklisting.	N/A

Copyright and Disclaimer

Trademarks and Patents

Stonesoft Corporation

Itälahdenkatu 22A
FI-00210 Helsinki
Finland

Tel. +358 9 476 711
Fax +358 9 4767 1349

Stonesoft Inc.

1050 Crown Pointe Parkway
Suite 900
Atlanta, GA 30338
USA

Tel. +1 770 668 1125
Fax +1 770 668 1131