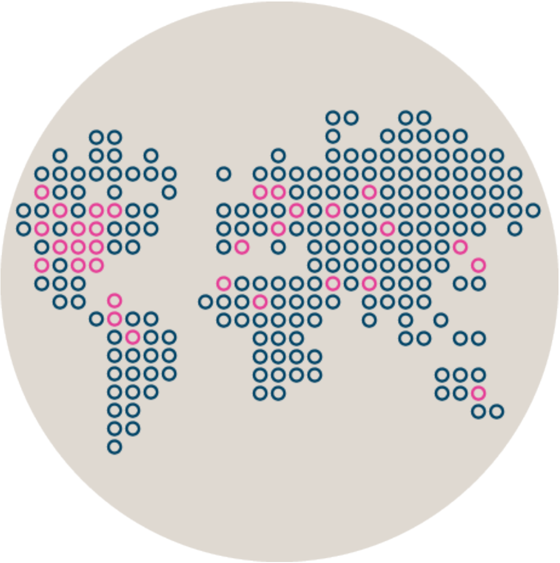

Stonesoft Management Center

Release Notes for Version 5.5.2

Updated: September 5, 2013

STONESOFT

Table of Contents

What's New

Fixes

The problems described in the table below have been fixed since Stonesoft Management Center version 5.5.1. A workaround solution is presented for earlier versions where available.

Synopsis	Description	Workaround for Previous Versions
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.
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.
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
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
Policy installation fails for engines that use legacy licenses with restricted IP address counts (#97334)	Policy installation fails for engines that use legacy licenses that restrict IP address counts. The engine refuses the configuration with an error similar to the following: "FATAL: setting up license-excluded interface 1 failed". The issue can also occur if an interface that is excluded from IP counting has been defined even if no licenses that restrict IP address counts are used.	Remove the "Exclude from IP Counting" setting in the Routing view if you do not use licenses that restrict IP address counts.
Forwarding of Alert Notifications sent by e-mail may stop randomly (#97408)	The forwarding of Alert Notifications sent by e-mail may stop randomly if the e-mail message cannot be formed using the e-mail template.	Restart the Management Server and the Log Server.

Synopsis	Description	Workaround for Previous Versions
Policy installation fails if license does not have VPN feature (#97440)	Policy installation fails with a license that does not include a VPN feature. This occurs even when the policy that is installed does not include a VPN configuration. The following error message is displayed: "The license for <firewall> node 1 does not support VPNs. Remove the VPN configuration."	Request an evaluation license. See http://www.stonesoft.com/en/customer_care/downloads/evaluation_licenses/.
Unresolved variable in e-mail alert notifications sent from Management Server installed separately from Log Server (#97453)	Starting from SMC 5.5.0, alert notifications are sent by the Management Server. When the Management Server is installed on a different server than the Log Server(s), alert notifications sent by e-mail may have unresolved variables.	If the Management Server and Log Server(s) run on the same operating system, copy the <SG_HOME>/data/notification folder from the Log Server to the Management Server. If the servers run on different operating systems, contact Stonesoft Support.
Management Server restart breaks automatic IPS blacklisting (#97591)	Starting from version 5.4, IPS blacklisting entries are sent through the Management Server. Restarting the Management Server breaks automatic blacklisting.	Create a manual blacklisting entry from the Management Server for the Firewall. After this, automatic blacklisting works until the next time the Management Server is restarted.
POS-bound licenses appear Unassigned in SMC 5.5.1 (#97749)	POS-bound licenses appear to have the "Unassigned" status in SMC 5.5.1. In the "Bound To" column of the License view, you can still see the element to which the license is assigned, and the policy installation succeeds without license-related errors.	To verify which license is assigned to an engine, use the "sg-status" command on the engine command line.
Cannot save IPS or Layer 2 Firewall element with multiple Logical Interfaces in VLANs under the same physical Inline Interface pair (#96914)	Saving an IPS or Layer 2 Firewall element fails when different Logical Interfaces are used for different VLANs under the same physical Inline Interface 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.
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
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 for Previous Versions
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.
Web Portal Users may not be able to view log details (#92704)	Web Portal Users may see an "Internal Error" message when trying to view the details of a log entry.	Restart the Web Portal Server.
SMC uploads inspection configuration to FW-105 if Inspection Policy is selected (#87325)	The FW-105 license does not allow deep inspection. If inspection is enabled in the Access rules, the user is notified of the license limitation. If inspection is not enabled but an Inspection Policy is selected, the inspection configuration is uploaded to the engine. This causes the policy installation to be slow, and it may even fail. It may also temporarily cause a high load and high memory consumption.	On the Inspection tab of the Firewall Policy, select "No Inspection Policy".
Route-Based VPN configuration not generated if same Firewall referenced by several Internal Security Gateways (#97980)	If the same Firewall is referenced by Internal Security Gateway elements, Route-Based VPN tunnels are not created when a policy is installed on the Firewall.	If possible, use the same Internal Security Gateway element to represent the Firewall in all VPNs.
Adding new rule to policy may fail (#96553)	Due to a problem with the Insert Points, adding a new rule to the NAT rules in a Firewall Policy or to the Exceptions in the Inspection Policy may fail with the following error: "Management Center Error, Index: X, Size: X".	If the parent Firewall Template Policy or the parent Inspection Template Policy is a system Template Policy, duplicate the system Template Policy and move the new Template Policy under the system Template Policy. Edit the parent Firewall Template Policy or the parent Inspection Template Policy and add a new Insert Point immediately above the existing Insert Point in the NAT rules or the Exceptions. You can then add rules to the Firewall Policy or Inspection Policy using the new Insert Point.
Moving External Security Gateway to another Domain does not move associated Geolocation (#90568)	Moving an External Security Gateway element to another Domain does not move the associated Geolocation element and corrupts the Geolocation element. Deleting an External Security Gateway element also corrupts the associated Geolocation element.	Remove the Geolocation from the properties of the External Security Gateway element before moving or deleting the External Security Gateway element.

Other Changes

Change	Description
SMC Load Sharing option 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 more 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 Licenses 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 5.5.2 build version is 8537.

This release contains Stonesoft Dynamic Update package 540.

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 the 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 5.5.2 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 5.5.2, 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 lower than 4.0.0 require upgrade to version 4.0.0 – 5.1.4 before upgrading to version 5.5.

Known Issues

The current known issues of Stonesoft version 5.5.2 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
Web Portal Users not able to view logs on Log Servers that are not in the Shared Domain (#97625)	Web Portal Users are not able to view logs that are stored on Log Servers that belong to a particular Domain. The issue does not affect Log Servers that belong to the Shared Domain.	Use the Management Client to view logs.
An administrator who is not a superuser cannot see data in Overviews (#97356)	An administrator who is not a superuser but has been granted permissions to "ALL Elements" cannot see data in Overviews. This occurs even when the administrator has been granted all permissions and all roles. Overviews are based on counter data, and it is not possible to configure permission restrictions for counter data. This means that administrators either have access to all counter data or to no counter data.	The "ALL Elements" Access Control List does not include SSL gateways or elements that represent third-party devices. Administrators who are not superusers can see data in Overviews if they have been granted the following elements: - "ALL Elements" - "ALL SSL VPN Gateways" - "ALL Third-Party Devices"
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.
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.

Synopsis	Description	Workaround
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.
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.
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

These materials, Stonesoft products, and related documentation are protected by copyright and other laws, international treaties and conventions. All rights, title and interest in the materials, Stonesoft products and related documentation shall remain with Stonesoft and its licensors. All registered or unregistered trademarks in these materials are the sole property of their respective owners. No part of this document or related Stonesoft products may be reproduced in any form, or by any means without written authorization of Stonesoft Corporation.

Stonesoft provides these materials for informational purposes only. They are subject to change without notice and do not represent a commitment on the part of Stonesoft. Stonesoft assumes no liability for any errors or inaccuracies that may appear in these materials or for incompatibility between different hardware components, required BIOS settings, NIC drivers, or any NIC configuration issues. Use these materials at your own risk. Stonesoft does not warrant or endorse any third party products described herein.

THESE MATERIALS ARE PROVIDED "AS-IS." STONESOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, AS TO THE INFORMATION CONTAINED HEREIN. IN ADDITION, STONESOFT MAKES NO EXPRESS OR IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE WITH RESPECT TO THE INFORMATION CONTAINED IN THESE MATERIALS. IN NO EVENT SHALL STONESOFT BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL OR INCIDENTAL DAMAGES, INCLUDING, BUT NOT LIMITED TO, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING FROM THE USE OF THESE MATERIALS, EVEN IF ADVISED IN ADVANCE OF THE POSSIBILITY OF SUCH DAMAGES.

Trademarks and Patents

Stonesoft, the Stonesoft logo and StoneGate are all trademarks or registered trademarks of Stonesoft Corporation. Multi-Link technology, Multi-Link VPN, and the Stonesoft clustering technology-as well as other technologies included in Stonesoft-are protected by patents or pending patent applications in the U.S. and other countries. All other trademarks or registered trademarks are property of their respective owners.

Stonesoft Corporation

Itälahdenkatu 22A
FI-00210 Helsinki
Finland

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

STONESOFT

Stonesoft Inc.

1050 Crown Pointe Parkway
Suite 900
Atlanta, GA 30338
USA

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