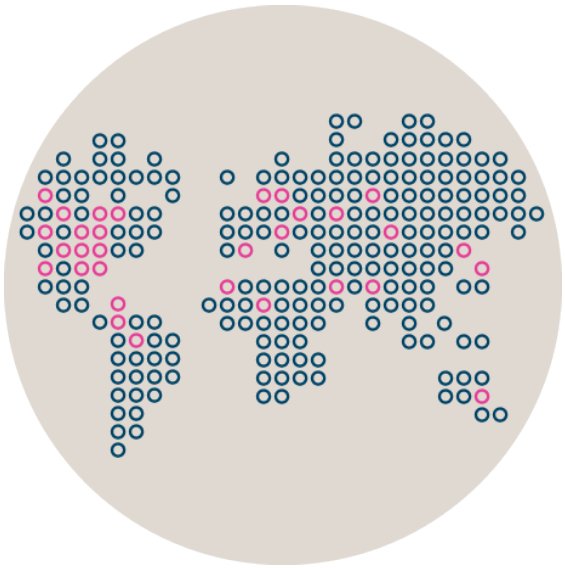

Stonesoft Management Center

Release Notes for Version 5.5.3

Updated: October 7, 2013

STONESOFT
A McAfee Group Company

Table of Contents

What's New **3**

Enhancements 3

Fixes 3

Other Changes 5

System Requirements **6**

Basic Management System Hardware Requirements 6

Operating Systems 6

Build Version **6**

Compatibility **7**

Minimum 7

Native Support 7

Installation Instructions **8**

Upgrade Instructions **8**

Known Issues **9**

What's New

Enhancements

Enhancements that have been made since Stonesoft Management Center version 5.5.2 are described in the table below.

Enhancement	Description
The administrator name can be up to 120 characters (since 5.5.3)	The administrator name was limited to 20 characters. Starting from Stonesoft Management Center 5.5.3, the name can be up to 120 characters.
Rule comment length extended (since 5.5.3)	Rule comments were limited to 256 characters. Starting from Stonesoft Management Center 5.5.3, rule comment has been extended.

Fixes

The problems described in the table below have been fixed since Stonesoft Management Center version 5.5.2. A workaround solution is presented for earlier versions where available.

Synopsis	Description	Workaround for Previous Versions
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.
Administrator who is not 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"
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.
Error message related to FW/VPN 315 L license limitation not correct (#98609)	Policy installation on L-model appliances may fail with the following error message: "The license for Firewall Node X does not support Multi-Link. Remove the Multi-Link configuration or upgrade the license." However, the error may be due to the fact that the engine license does not allow clustering for load balancing or another feature that is not supported by the license.	Make sure that license-limited features are not configured, even if the license includes Multi-Link.

Synopsis	Description	Workaround for Previous Versions
User Groups and group members not displayed for OpenLDAP Servers (#98530)	When browsing OpenLDAP Servers, User Groups and their members are not displayed. However, both Users and User Groups can still be used in rules.	N/A
Search Users does not find group names (#98589)	The Search Users tool only finds users, not groups. The result is the same with database queries to the Internal Domain and LDAP queries to external LDAP domains.	User group information can be found by browsing the domain information in the User Authentication view.
Browsing an OpenLDAP Server with many users may freeze the Management Client (#98365)	Browsing an OpenLDAP server may freeze the Management Client UI for several minutes if there is a large number of users (tens of thousands or more).	N/A
Editing a Firewall element may create duplicate directly connected routes (#98165)	Editing a Firewall element that has originally been created with version 5.3 or lower and saving changes may add duplicate directly connected routes to the Routing view of the Firewall. Duplicate network elements cannot be removed from the view.	- Edit the Interface under which the duplicate element exists in the Routing view by changing the IP address to a different network. - After changing the IP address, the original directly connected routes may be removed. - Change the Interface IP addresses back. The directly connected networks automatically appear in the Routing view.
Filters may not work for Web Portal Users (#85210)	Web Portal Users may see an "Unexpected Internal Error" message when they select Filters for exporting or browsing logs. The same Filter works correctly when used through the Management Client.	N/A
When VPN Certificate Authority is renewed, alert about trusting new IPsec CA is displayed even if no VPN certificates are used (#95015)	After a new VPN Certificate Authority has been created, the new IPsec CA certificate is uploaded to the engine nodes. If a VPN certificate has been created for an engine, but the engine policy does not refer to a VPN certificate, the following alert is displayed for the engine: "Refresh policy for Internal Gateway to trust new VPN Certificate Authority". Refreshing the policy on the engine does not remove the alert, as VPN-related certificates are not uploaded to the engine if only pre-shared key authentication is used.	Contact Stonesoft support for a workaround.
New blacklist entries cannot be created directly in Active Alerts view (#98597)	When you right-click an alert in the Active Alerts view, the right-click menu does not include the option "New Blacklist Entry". Prior to version 5.5, new blacklist entries could be created by using the right-click menu for active alerts.	Create new blacklist entries in the System Status view by right-clicking an element and selecting Blacklist > New Entry.
Create Rule option not available in Active Alerts view (#98480)	If you right-click an alert in the Active Alerts view, there is no option to create a rule.	You can select Create Rule if you right-click an alert in the Logs view.

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 5.5.3 build version is 8539.

This release contains Stonesoft Dynamic Update package 543.

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 the 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 using 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 5.5.3 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 5.5.3, 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 5.5.3 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
SMC installation or upgrade may fail due to incorrect time zone (#98732)	Stonesoft Management Center installation or upgrade may fail if the system used to install or upgrade is set to the "Europe/Busingen" time zone.	Manually set your system to another time zone.
Browsing logs from granted elements may fail for administrators with restricted permissions (#89876)	In rare cases, browsing the logs from granted elements may fail for administrators with restricted permissions. The Logs view is empty and the error message "Failed to create the query" is displayed in the Query panel.	Restart or log in again to the Management Client to resolve the issue. If it does not help, restart the Management Server.
Alert threshold not switched off after its duration ends (#99041)	An alert threshold can be used to define a limit for the number of alerts that match a particular entry in an Alert Chain. After the limit has been reached, matching alerts are blocked. However, the alert threshold fails to switch off automatically once its defined duration has ended. As a result, alerts are not forwarded even after the alert threshold is no longer effective.	Install the Alert Policy.
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.
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 rule to an engine that is version 5.3 or lower, the rule is ignored because support for non-HTTP-based Application identification is introduced only in engine version 5.4.	Do not use non-HTTP-based Applications if your target engines are not yet upgraded to version 5.4.

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.
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
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
A McAfee Group Company

Stonesoft Inc.

1050 Crown Pointe Parkway
Suite 900
Atlanta, GA 30338
USA

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