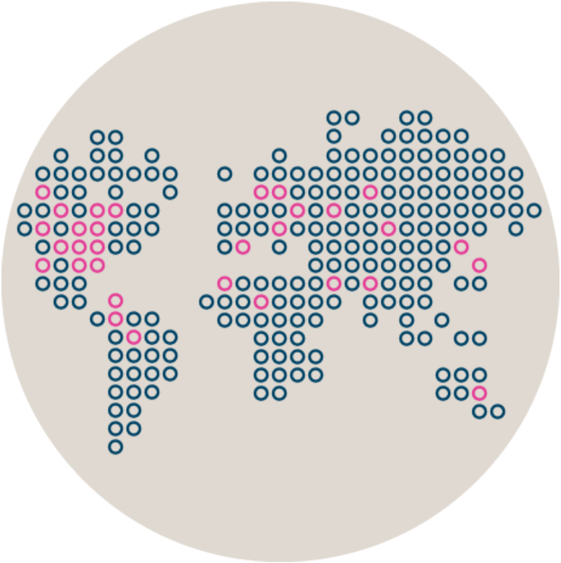

Stonesoft Management Center

Release Notes for Version 5.5.0

Created: May 6, 2013

STONESOFT

Table of Contents

What's New

Features

Features that have been added since Stonesoft Management Center version 5.4.5 are described in the table below.

Feature	Description
Support for Virtual Firewalls	Virtual Security Engines are logically separate engines that run as virtual engine instances on a physical engine device. You can now use a physical Security Engine device as a Master Engine to provide resources for Virtual Security Engines. This means that the same Master Engine can simultaneously have different security policies, separate routing tables and overlapping IP addresses for different interfaces (reserved by different Virtual Security Engines). Virtual Security Engines do not require individual licenses. Instead, the Security Engine license for the Master Engine defines how many Virtual Resources can be created. The number of Virtual Resources limits the number of Virtual Security Engines. Virtual Security Engines can currently be used only in the Firewall role. Virtualization works across several SMC Domains. For example, the Master Engine can be in the Shared Domain and the Virtual Security Engines can be in one or several other Domains.
SMC Load Sharing	With SMC Load Sharing, there is no longer the concept of active and standby Management Servers. All Management Servers are always active, and all changes to the Management database are replicated between the Management Servers. Domains form the boundaries for SMC Load Sharing. Administrators can change which Management Server controls which Domain. Changes to a Domain can be made only when logged in to the Management Server that controls that Domain. However, the changes are visible even if you are logged in to another Management Server. The full benefits of SMC Load Sharing require the SMC Domains feature. Otherwise, there is one Domain (the Shared Domain) and it can only be controlled by one Management Server. If you already have licenses for SMC High Availability and Domains, no additional licenses are needed for SMC Load Sharing. The benefits of SMC Load Sharing include: • All Management Servers are in use all the time. • Increased scalability. You can now manage up to 5000 engine nodes within a single management system. • Better 24/7 management support for geographically distributed environments. For example, you can have one Domain for a network operation center in New York and another Domain for a network operation center in Singapore. If you want to edit elements in a Domain, you must log in to the Management Server that controls the Domain. You can change the Management Server that controls the Domain at the end of the shift.
IPFIX/NetFlow forwarding and reception	SMC 5.5 is able to generate IPFIX data and NetFlow v9 data and forward the data to third-party SIEM products. IPFIX/NetFlow forwarding is configured in the Log Server properties. SMC 5.5 is also able to receive IPFIX and NetFlow v5 and v9 data. This enhancement is an extension of the current Third-Party Monitoring feature set that SMC provides. IPFIX/NetFlow reception is configured in the properties of third-party elements (such as Hosts, Routers, and different types of Server elements).

Enhancements

Enhancements that have been made since Stonesoft Management Center version 5.4.5 are described in the table below.

Enhancement	Description
New Active Alerts view	The Active Alerts view has been re-implemented. Active Alerts are now aggregated by severity and Situation name by default. This makes it easier to acknowledge several alerts that are identical. It is also easier to see all the different types of alerts that have been received.
Easier syslog forwarding	In SMC 5.5 and higher, syslog forwarding can be configured directly through the Management Client in the Log Server properties. It is now possible to configure several TCP and UDP forwarding settings for each Log Server. The current log forwarding settings (configured in the LogServerConfiguration.txt file) are automatically migrated. If you have used filters in your existing log forwarding settings, we recommend that you replace them with the filters you can now define in the Log Server properties.
Type-ahead element creation	When you start typing an element name in a policy cell, a tooltip opens. The tooltip lists all the elements that match your search criteria. The tooltip includes shortcuts to create elements such as Hosts, Networks, and Services. If you did not find an element with the IP address that you were looking for, you can create a Host element for that IP address by selecting the shortcut that is displayed in the "New" menu next to the type-ahead search field.
Obsolete elements	In SMC versions lower than 5.5, deleted elements were sent to the Trash branch in environments with multiple Management Servers. In version 5.5, elements to be deleted are first marked as obsolete. They are shown in the Obsolete Elements branch from which they can be deleted permanently. The Obsolete Elements branch is displayed regardless of the number of Management Servers. If an element has references, you can mark the element as obsolete, but you must remove the references to permanently delete the element. In an environment with one Management Server, you can delete an element permanently by pressing Shift and right-clicking the element.
Support for X-Forwarded-For (XFF) logs	The X-Forwarded-For (XFF) HTTP header field is commonly used to identify the IP address of a client that uses an HTTP proxy or load balancer to connect to a web server. SMC 5.5.0 includes new log fields and statistics that allow you to see the originating XFF Client and the detected XFF Proxies.
Improved security strength of Management connections	You can now use 256-bit encryption for the connection between Security Engines and the Management Server. This requires both the Security Engines and the Management Server to be version 5.5 or higher. You must also use an Internal ECDSA Certificate Authority to sign certificates for system communication.
Internal ECDSA Certificate Authority	The Elliptic Curve Digital Signature Algorithm (ECDSA) is a digital signature algorithm that uses elliptic curve cryptography. It is now possible to use an Internal ECDSA Certificate Authority to sign the certificates that components use to identify each other in system communications. When you start using an ECDSA Certificate Authority, you must recertify all SMC servers and you may also need to make initial contact between the engines and the Management Server. Engines with versions lower than 5.5 and SSL VPN gateways cannot communicate with the SMC when an ECDSA Certificate Authority is used.
Loopback Interfaces	A Loopback IP address allows the firewall to communicate with itself. It is now possible to configure any IP address that is not already used as a Cluster Virtual IP Addresses (CVI) or Node Dedicated IP Addresses (NDI) on another interface as a loopback IP address. You can add several loopback IP addresses to each Firewall. Loopback IP addresses can also be used as End-Point IP addresses in policy-based VPNs and in the Route-Based VPN.

Simplified log filtering dialogs	Separate log filtering dialogs now make it easier to change the comparison criteria for log filtering. For example, IP filter dialogs allow users to easily change the log field and comparison operators.
Improved traffic accounting statistics	In SMC 5.5 and higher, Stonesoft engines report accounted traffic amounts periodically–every 15 minutes by default. Previously, traffic amounts were reported only when connections were closed and this caused high traffic peaks to statistics.
Top Rate stacked bars statistics	There is a new type of graph that allows administrators to see top rate bar statistics distributed by secondary ranking criteria. You can now see, for example, the top applications per user as a single graph. This new graph is available only when you have two compatible top rate statistics items within the same statistics section.
New options in QoS Policies	Multiple enhancements have been made to the current bandwidth management and traffic prioritization features. The new QoS Mode option in the properties of a Physical, VLAN, ADSL, Tunnel, or SSID Interface allows you define in more detail how QoS is applied to the interface. • You can now read and/or write DSCP markers for traffic without configuring Access rules to apply a QoS class to the traffic. The matching is done based only on the QoS Policy. • QoS Class-based statistics items are now available even when QoS is not used for bandwidth management and traffic prioritization. The QoS class for the packet comes from the QoS Classes that are applied in the Access rules. New Active Queue Management (AQM) features reduce the volume of dropped or retransmitted packets when there is network congestion. AQM monitors the average queue size and uses a scheduling algorithm to determine the statistical probability for dropping incoming packets. It is now possible to assign a weight to QoS Classes so that different QoS Classes with the same priority can be assigned to the queue according to their weight when the QoS Class Guarantee is reached and traffic must be queued. This allows more granular control of traffic prioritization, but does not act as a guarantee.
DHCP Server lease time can be set for engines 5.4.3 or higher	SMC 5.5 includes a new option that allows the administrator to specify the lease time of the leases set by a DHCP Server. This option works with engines 5.4.3 and higher.

Fixes

The problems described in the table below have been fixed since Stonesoft Management Center version 5.4.5. A workaround solution is presented for earlier versions where available.

Synopsis	Description	Workaround for Previous Versions
Not possible to browse more than 1000 users stored in Active Directory (#22881)	When Active Directory is used as an external user database, it is impossible to browse more than 1000 users with the Management Client.	Increase the maximum value of the LDAP search results in SGConfiguration.txt. For example: LDAP_SEARCH_MAX_RESULT_CONSTRAINT=5000 See the instructions at Microsoft MSDN library for how to handle the configuration of the Active Directory server when a large number of users are queried.
Internal user database not updated after Management Server time change (#42603)	New or updated user information may not be automatically updated in the internal user database on firewall engines if the Management Server time has changed while the Management Server service is running.	Restart the Management Server service.
Address elements are not sorted numerically when sorted by IP address (#86531)	When sorted by IP address, network or host elements are not sorted numerically. For example, 10.100.0.0 is listed before 10.20.0.0.	N/A
Active alerts are not always displayed (#82149)	Although the Management Client indicates that there are active alerts, displaying the active alerts may fail. The Acknowledge All action may not reset the number of active alerts.	Restart the Management Server service.
Scheduled Reports stop running if E-mail or Post Process actions fail (#88861)	If Post Process script execution or e-mail sending fail when a Report runs automatically, the Task no longer runs automatically according to the schedule.	Edit the options on the Task tab of the Report Operation Properties to schedule the Report to run automatically again.
No users shown when browsing LDAP Domain on external LDAP Server without Stonesoft-specific attributes (#91456)	If the schema of an external LDAP Server has not been updated with Stonesoft-specific attributes, no users are shown when browsing the LDAP Domain in the Management Client.	N/A
User Monitoring view fails to show user entries (#90289)	The User Monitoring view may fail to show User entries. The view displays a “Connecting to server…” message.	N/A
Snapshots shown with identical names in Snapshot Comparison dialog (#91271)	Snapshots are shown with identical names in the Snapshot Comparison dialog. The date of each Snapshot is not shown.	N/A
“View Rule” option in logs does not work as expected for Inspection Exception rules (#92610)	When you select “View Rule” from the right-click menu of an Inspection Exception rule with a Situation match, the log entry may point to the Situations tree or to a rule in an unexpected template.	Search the Inspection Policy for the correct rule tag.

Other Changes

Change	Description
SMS Alert Sending	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 techniques.
Configure Updates and Upgrades moved to Management Server properties	There is no longer a separate Configure updates and upgrades dialog. Instead, those settings can be found in the Management Server properties dialog.
Simplified License view	The view that lists licenses in the SMC has been reorganized with more simplified labels.
Changes to Tasks branches	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	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 5.5.0 build version is 8514.

This release contains Stonesoft Dynamic Update package 521.

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 5.5.0 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 5.5.0, 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 5.5.0 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
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.
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
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 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.
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 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.
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
Incorrect HTTP Protocol Agent configuration for Security Engine in Firewall/VPN role (#89219)	SMC 5.4 creates an incorrect HTTP Protocol Agent configuration for Security Engines in the Firewall/VPN role. This causes HTTP traffic to consume more resources than before. IPv6 HTTP does not work.	Do not use the HTTP Protocol Agent if it is possible to allow HTTP traffic without the Protocol Agent.
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.
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.

Synopsis	Description	Workaround
SMC Web Start does not work after JRE upgrade from version 7 u4 to 7 u5 (#83161)	SMC Web Start may fail to launch the Management Client login dialog after a JRE upgrade from version 7 u4 to 7 u5. The following message is shown in the details of the related error message: “Unsigned application requesting unrestricted access to system”.	Start the command prompt shell and run these commands: javaws -uninstall javaws -clearcache Alternatively, open the javaws -viewer and manually delete applications, resources, and deleted applications from the cache.
Web Start Management Client fails to start on Mac OS X (#87359)	Recent Mac OS X updates have disabled Java from browsers. You must install an Oracle Java package to enable Java in your browser. However, after the package is installed, the Web Start Management Client does not work via the browser. This issue has also been seen on Ubuntu Linux. The problematic Java update is 1.7u9.	Use a newer version of Java.
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.
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.

Synopsis	Description	Workaround
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
Add from Routing action in the Diagram Editor is slow (#44989)	The Add from Routing action in the Diagram Editor is slow in large environments.	N/A
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