Alcatel-Lucent Security Management Server

SMS | 9.1.340

PATCH RELEASE NOTES

SMS 9.1.340 PATCH RELEASE
SEPTEMBER 2009
ISSUE 2

Limited warranty

Alcatel-Lucent provides a limited warranty to this product.

Contents

List of tables

About this document

Purpose

This document describes the feature content for the 9.1.340 patch of the Alcatel-Lucent Security Management Server. Included in this document are brief descriptions of each new feature, resolved issues, known issues, and installation and upgrade notes specific to this release.

Reason for reissue

The table that follows specifies dates and reasons for reissue of release notes.

Table 1 Release notes reissue history

Issue number	Date of issue	Description of changes
1	09/09/2009	First issue of this patch release notes document
2	09/22/2009	Add known issue number 0923791 to Table 5-1, “Known issues and workarounds” (p. 5-2)

Supported systems

The following Alcatel-Lucent VPN Firewall Brick™ Security Appliance models are supported by the current Alcatel-Lucent Security Management Server (SMS) release:

- VPN Firewall Brick™ Model 20 Security Appliance
- VPN Firewall Brick™ Model 50 Security Appliance
- VPN Firewall Brick™ Model 80 Security Appliance
- VPN Firewall Brick™ Model 150 Security Appliance
- VPN Firewall Brick™ Model 350 Security Appliance
- VPN Firewall Brick™ Model 500 Security Appliance
- VPN Firewall Brick™ Model 700 Basic and VPN Security Appliance
- VPN Firewall Brick™ Model 1100/1100A Security Appliance
- VPN Firewall Brick™ Model 1200 Basic and HS Security Appliance

Safety information

For safety information on installing and upgrading SMS software please see the *Alcatel-Lucent Security Management Server (SMS) 9.1 Installation Guide.*

For safety information on hardware, please see the safety instructions in the Brick model user's guides.

Conventions used

The following text conventions may be used throughout this document.

Table 2 Text conventions

Text appearance	Description of use
variable text	A variable name or string for which you will substitute your own information.
`filename`	A specific filename or path.
URL or URI	An Internet address or resource.
`Command`	Commands or button names. Literal text for values that the user types in fields or selects from predefined sets of values or fields
GUI	Exact window names and GUI text.
`screen text`	Message text displayed on the user interface.

Technical support

For technical support, contact your local Alcatel-Lucent customer support team. See the Alcatel-Lucent Support web site **http://alcatel-lucent.com/support/** for contact information.

How to order

To order Alcatel-Lucent documents, contact your local sales representative or use the Online Customer Support Site (OLCS) web site **https://support.alcatel-lucent.com/portal/olcsHome.do**.

How to comment

To comment on this document, go to the Online Comment Form (**http://www.infodoc.alcatel-info.com/comments/**) or e-mail your comments to the Comments Hotline (**comments@alcatel-lucent.com**).

1 Overview

Overview

Purpose

This chapter lists the feature content and other release information including test results for the 9.1.340 patch of the Alcatel-Lucent Security Management Server.

Introduction to release content

This document contains information on the following:

- Resolved issues
- Security related resolved issues
- Known issues
- Installation instructions
- Special notes
- Download locations

Test results

As of 09/09/2009, this 9.1.340 patch has passed testing and has been released for production.

2 Release components

Overview

Purpose

This chapter describes software and documentation deliverables included in this release.

Software deliverables

Software included in this release

The 9.1.340 software patch includes:

- Updates to Alcatel-Lucent Security Management Server 9.1 for Windows 2000, Windows XP, Windows 2003.
- Updates to Alcatel-Lucent Security Management Server 9.1 for Solaris 8, 9, or 10.
- Updates to SMS 9.1 Software Documentation
- Remote Navigator
- SNMP MIBs

How to obtain software

For software downloads, please logon to your account at **https://vpn-firewall-brick.alcatel-lucent.com/**.

Documentation deliverables

Documentation available for the 9.1.340 patch

Table 2-1 Documentation list

Document ID	Document title
260-100-017R9.1	*Alcatel-Lucent Security Management Server (SMS) Release 9.1 Administration Guide, Issue 7*
260-100-018R9.1	*Alcatel-Lucent Security Management Server (SMS) Release 9.1 Installation Guide, Issue 3*
260-100-016R9.1	*Alcatel-Lucent Security Management Server (SMS) Release 9.1 Policy Guide, Issue 8*
260-100-019R9.1	*Alcatel-Lucent Security Management Server (SMS) Release 9.1 Reports, Alarms, and Logs, Issue 6*
260-100-022R9.1	*Alcatel-Lucent Security Management Server (SMS) Release 9.1 Technical Overview, Issue 1*
260-100-020R9.1	*Alcatel-Lucent Security Management Server (SMS) Release 9.1 Tools and Troubleshooting Guide, Issue 7*

To obtain documentation

Alcatel-Lucent SMS product documentation is available to customers through OnLine Customer Support (OLCS).

To access documentation:

1. Go to **https://services.support.alcatel-lucent.com/services/vpnfirewallbrick/**.

   Note: If you do not already have a service contract account you will be prompted to create an account.
2. Select **Register for Access** on the right hand side of the page.
3. Select **Customer**
4. Select **Yes, I accept the Terms of use**
5. Select **Next**
6. Enter your name and contact information
7. Select **Next**

Note: The login ID and password is separate from the login ID and password used to access the registration website. The account creation process can take 1 to 12 hours. A temporary login ID and password will be emailed once the account is approved.

To navigate to OLCS:

8. Go to **https://support.alcatel-lucent.com/portal/productIndexByCat.do**.
9. Select **Product Index**
10. Select the alphabetic section for the product or solution for which you require documentation. For example, for VPN Firewall, select **U-Z** and scroll to the **V** section to select **VPN Firewall Brick**.
11. To obtain manuals, select **Manuals and Guides**. To obtain release notes, select **Release Information**.

Note: Online product manuals are accessible from the SMS GUI.

3 New features

Overview

Purpose

This chapter provides new feature descriptions, interface changes, and alarm changes included in the 9.1.340 patch.

New features

Support for replacement Brick 700 models

Support is added for the new Brick 700 hardware including the 700 basic and 700 VPN.

Note: For 9.1 releases, the new second generation Model 700 Brick device (cool-grey box) can only be managed and supported by the 9.1.340 patch release or subsequent 9.1 releases of the Alcatel-Lucent Security Management Server (SMS) application.

If you are replacing an existing first generation Model 700 Brick device (black box) with a new Model 700 Brick device (cool-grey box) you will need to re-bootstrap the Brick using the **`mkfloppy`** process to create a new floppy or USB drive, or using the floppyless bootstrap method to load a new boot image via the Brick serial port.

For details about creating Brick boot media and activating a Brick device, refer to the *Configuring and Activating an Alcatel-Lucent VPN Firewall Brick™ Security Appliance* chapter in the *SMS Administration Guide*.

Note: To manually force 100 Mbps or 10 Mbps, a cat-5 cross-over cable is required.

Enhancements

No enhancements are included with this release.

Interface changes

Changes to Northbound Interfaces

No interface changes are included with this release.

Changes to Southbound Interfaces

The SMS has no southbound interfaces.

Alarm changes

No alarm changes are included with this release.

4 Resolved issues

Overview

Purpose

This chapter describes the resolved issues in this release.

Resolved issues

The following table includes resolved issues associated with security and other fixes for this release. The resolved issues are listed with an internal ID number, title, and a description of what has been fixed.

Security related

No security related issues are included with this release.

Other resolved issues

Table 4-1 Resolved issues

Internal ID	Title	Description of issue
0923715	The Brick replaces some source MAC addresses it should not replace.	In most cases, simple bridged packets should not have their source MAC addresses replaced by the Brick, but in some uni-directional cases, it does.

5 Known issues

Overview

Purpose

This chapter describes known issues and workarounds (if available) for this release.

Known issues and workarounds

The following are known issues and workarounds (if available) in this release.

Table 5-1 Known issues and workarounds

Fault ID	Title	Description of issue	Workaround
0620266	Multi-site SMS issues	Under load conditions, sometimes the SMS does not allow any more administrators to login and/or the GUI will hang if an administrator tries to open a new Status Monitor window.	Restart the SMS services.
0620263		If there is a flood of console alarm messages (e.g. when the loss of a major communications link causes a lot of VPN Firewall device Lost alarms), the links between SMS machines or Compute Servers may go down temporarily.	None. Links are automatically re-established.
0721637		Loss of Database synchronization puts the Multi-Site environment in a hung state. The Self-Repair Database feature alleviates a lot of such situations, however, some still exist.	Stop services on all Secondary SMSs. Do a manual DbSetup of all secondary SMSs and then start services.
0620250	Link to Primary SMS bouncing	Under load conditions, sometimes the Secondary SMS is unable to maintain a connection to the Primary SMS and the link state bounces up and down every few minutes.	Restart the SMS services on the Primary SMS.
0620264	Database process memory growth	Adding, deleting, or updating a large number of VPN Firewall devices may cause the database process memory to grow and exceed its limit.	Increase the Database Max Heap size in the Tunable Parameters in the Configuration Assistant. Restart the SMS services if the database process exceeds its memory limit.

Fault ID	Title	Description of issue	Workaround
0721966	Upgrading a Secondary SMS may fail.	Upgrading a Secondary SMS causes the installation process to fail and generates an error indicating that the connection to the Primary SMS cannot be closed.	**Clean installation:** Install both the Primary SMS and the Secondary SMS with the GA software version first, then upgrade to the desired patch. **Installing a new Secondary:** If the Primary SMS is already running the patch version, and then an install is performed for a new Secondary SMS from scratch, a Primary license key must be used to install the GA software version and the patch, then a Secondary license key must be substituted in the *<smsroot>\swkeys* file and run dbsetup.
0722260	Solaris upgrade does not generate FIPs warning.	Upgrade on Solaris does not generate the warning that FIPs-enabled bricks will no longer support 512-bit certificates.	None
0722267	Incorrect warning message at installation.	When upgrading to a release later than 9.1.249, and if the initial clean install of the SMS is prior to 9.0.187, a new Certificate Authority is generated. 512-bit VPN certificates must also be replaced after this upgrade. During the upgrade process, a warning to this effect is provided. However, in any case where the initial clean install of the SMS is 9.0.187 or later, a new Certificate Authority is not generated when upgrading to 9.1.249 or later, but 512-bit VPN certificates would still need to be replaced after this upgrade. In this instance, the warning should make no reference to the Certificate Authority and re-floppying Bricks.	Ignore the erroneous warning message.

Fault ID	Title	Description of issue	Workaround
0923761	The Brick Model 1200 may not come back up after disabling the motherboard interface.	If the e7 port of a Brick Model 1200 is disabled using the **Physical Ports** tab, sometimes the Brick does not come up again when re-enabled.	Reboot the Brick.
0923791	Forcing link speed causes the Brick to failover.	When a Brick port is changed from 1 Gig to 100 Mb/sec or 10 Mb/sec, the active Brick changes the speed to the configured value, but the standby Brick may maintain its gig link. When this happens, the active Brick yields to the standby due to `inferior link` and causes a Brick failover to occur. This speed mismatch persists on the active Brick until it is rebooted.	Reboot the active Brick after the failover.
None	Possible Brick Panic	Some Brick models may panic and reboot if using QoS when Jumbo Frames are enabled. This seems to be most likely on Brick Models 700 and 1200 Basic.	Do not use QoS and Jumbo Frames on the same Brick.

Note: These issues are not new to this patch release, they are existing issues that have been discovered.

Upgrade Issues in Patch 9.1.340

If the network is configured such that traffic from one machine to another one is routed through the VPN Firewall device twice (e.g. from the source through the VPN Firewall device to a router and then back through the VPN Firewall device to the destination), then the VPN Firewall device may need to be reconfigured to allow this to continue to work properly. Prior to version 9.1.170, the VPN Firewall device would delete the session entry when it saw the packet pass through the same zone the second time and recreate it based upon rules. This in turn created a number of issues as strict TCP, QOS, and some application filters would not work properly and performance would generally be poor.

As of version 9.1.170, this no longer occurs and the packet is usually dropped. If, however, the VPN Firewall device is reconfigured so that the packet passes through a different zone on each pass, then this will continue to work and the issues associated with the previous configuration will no longer exist.

In order to upgrade to 9.1.170 or later without affecting traffic, make these changes before installing the software upgrade.

Note: Installing this patch will cause IKEv1 LAN-to-LAN tunnels between the VPN Firewall device and a previous version of the VPN Firewall device to fail until both are upgraded or until the encryption algorithm is changed to a value other than AES-CBC_192/256. This occurs only if the previous patch was prior to 9.1.249. Upgrading from 9.1.249 or later does not cause this issue.

Self Repairing Database Feature

The Self Repairing Database feature has been added to alleviate the current database synchronization issues. This feature detects the loss of database synchronization capability early and attempts to self repair the databases by downloading the new database from the Primary and performing a silent database setup on the Secondary.

Two new configurable parameters in the config.ini file have been added to control the Self Repair Database feature.

- secondary.enableSelfRepair- If set to true, this parameter enables the auto repair feature. To turn this feature off, set this parameter to false. The default value is true.
- secondary.forceDbSetupAfter- Once the feature is turned on, the Secondary will look for a stalled database. When a situation that requires a self-repair is detected, the system waits for a few minutes before starting the self repair. The variable secondary.forceDbSetupAfter in the config.ini file specifies this value in minutes. The default value is 60 minutes. This variable can be set to start the self repair in less than 60 minutes after a hung/stalled condition if preferred.

FIPS Installations Only

If you are upgrading to this patch from Release 9.1.299, and 512-bit Certificates have already been replaced, the warning generated during upgrade to this patch may be ignored. This warning is generated only using the windows version of this patch.

6 System requirements

Overview

Purpose

This chapter describes software and hardware requirements.

Software requirements

Microsoft® Windows 2000 Pro SP4, 2000 Server SP4, XP Professional SP1 and SP2, 2003 Server SP2

- NTFS file system

Solaris 8, 9, and 10

Software licensing keys

For information on obtaining SMS installation keys please see the *Alcatel-Lucent Security Management Server (SMS) Release 9.1 Installation Guide.*

Hardware requirements

The following minimum hardware specifications for Windows and Solaris are required to run the SMS software.

Table 6-1 Windows minimum requirements

Type	Minimum Requirement
Processor	400MHz Pentium Processor or greater
RAM	512 MB or greater
Swap Space	Greater than or equal to RAM
Fixed Storage	1 GB or greater space on an NTFS partition
Removeable Storage	CD-ROM Drive
Floppy Drive	3.5” Floppy Drive
Network Interface	Ethernet Interface Card
Monitor	1024 x 768 x 65,535 color display

Note: A floppy drive is required only if managing VPN Firewall device Models 20, 80, 350, 500, 1000, or 1100/1100A.

Table 6-2 Solaris minimum requirements

Type	Minimum Requirement
Processor	Sun Ultra SPARC 5 (330 MHz Processor)
RAM	512 MB or greater
Swap Space	Greater than or equal to RAM
Fixed Storage	500 MB disc space
Removeable Storage	CD-ROM drive
Floppy Drive	3.5” Floppy drive
Network Interface	Ethernet Interface Card

Note: A floppy drive is required only if managing VPN Firewall device Models 20, 80, 350, 500, 1000, or 1100/1100A.

7 Installation and upgrade notes

Overview

Purpose

This chapter includes information on how to install the 9.1.340 patch for the Alcatel-Lucent Security Management Server software.

Performing upgrades

This section outlines how to load the latest patch for SMS 9.1.340 on an Alcatel-Lucent Security Management Server.

Install on Windows 2000, Windows XP, Windows 2003

If you are unsure which product you are using, perform the following while logged into the SMS:

a. Click on the **HELP** tab.

b. Click on About. A dialog box will be displayed that indicates the current SMS software version.

c. Exit from the Alcatel-Lucent Security Management Server.

1. Download the *LSMSPatch-9.1.340.exe* file for the Alcatel-Lucent Managed Firewall product to a temporary directory where you have at least 130.0 Mb of space.
2. Once the download is complete, double click the *LSMSPatch-9.1.340.exe* or appropriate file and follow the installation instructions to install the software.

   Note: All SMS services will automatically stop during the installation. They will restart once the installation is done. It is also important to exit out of the GUI and other SMS applications or close any windows that are using the SMS File system for the upgrade to be successful.
3. After the software has been successfully installed, launch the SMS Navigator and login to the SMS.
4. To verify successful installation of the software, perform the following:

   a. Click on the **HELP** tab.

   b. Click on About. A dialog box will display the version number of the VPN Firewall device and the SMS. This should update the version to 9.1.340.
5. To update and activate the new software on a firewall appliance, follow the steps below:

   a. Access the **Devices** menu and select **BRICKS**.

   b. Highlight the desired VPN Firewall device in the **Navigator** View. Right Click and select **Software Download**.

   c. Click **OK** in the response window **Do you want to download software to brick: <*Brickname*>**. The server will copy the updated VPN Firewall device's OS to the selected VPN Firewall device. The process takes approximately three minutes.

   d. After the download to the VPN Firewall device is done, a message is displayed as a reminder that the VPN Firewall device must be rebooted for these changes to take effect. Please reboot the VPN Firewall device.

For added protection, it is also recommend that you create an updated floppy disk for the VPN Firewall device.

a. Insert a floppy disk into the disk drive on the Alcatel-Lucent Security Management Server.

b. Access the **Devices** menu and select **BRICKS**.

c. Highlight the desired VPN Firewall device in the **Navigator** View. Right Click and select **`Make/Package Floppy`**.

d. In the response window, click **OK**. The server will copy the VPN Firewall boot files to the floppy.

e. When the process is completed, please remove the floppy from the SMS and store it in a safe location.

To download the SMS Windows software now, please logon to your account at **https://vpn-firewall-brick.alcatel-lucent.com/**.

Install on Solaris 8, 9, or 10

If you are unsure which product version you are using, perform the following while logged into the SMS:

a. Click on the **HELP** tab

b. Click on About. A dialog box will be displayed that indicates the current SMS software version.

c. Exit from the Alcatel-Lucent Security Management Server.

1. Please download *lsmspatch-9.1.340.tar* for Alcatel-Lucent Security Management Server product.
2. Once the download is complete, move it to a temporary directory where at least 600.0 MB of space exists.

   `mv` *`lsmspatch-9.1.340.tar /tmp`*

   `cd` */tmp*
3. Use the **`tar`** command to expand the file as follows:

   `tar` *`xvf lsmspatch-9.1.340.tar`*
4. Execute a **`pkgadd`** command as follows:

   `pkgadd` *`-d . LUsms`*
5. The first message will indicate `This appears to be an attempt to install the same architecture and version of a package which is already installed. This installation will attempt to overwrite this package.` And the following prompt is displayed:

`Do you want to continue with the package of <LUsms> [y,n,?].`

Type **`y`**.

Note: All SMS services will automatically stop during the installation. They will restart once the installation is done. It is also important to exit out of the GUI and other SMS applications or close any windows that are using the SMS File system for the upgrade to be successful.

6. After the software has been successfully installed, launch your SMS Navigator and login to the SMS.
7. To verify successful installation of the software, perform the following:
   a. Click on the **HELP** tab.
   b. Click on About. A dialog box will display the version number of the VPN Firewall devices and the SMS. The software should update the version to 9.1.340.
8. To update and activate the new software on a firewall appliance, follow the steps below:
   a. Access the **Devices** menu and select **BRICKS**.
   b. Highlight the desired VPN Firewall device in the **Navigator** View. Right Click and select **Software Download**.
   c. Click **OK** in the response window `Do you want to download software to brick: <Brickname>`. The server will copy the updated VPN Firewall devices OS to the selected VPN Firewall device. The process takes approximately three minutes.
   d. After the download to the VPN Firewall device is done, a message is displayed as a reminder that the VPN Firewall device must be rebooted for these changes to take effect. Please reboot the VPN Firewall device.

For added protection, we also recommend an updated floppy disk be created for the VPN Firewall device.

   a. Insert a floppy disk into the disk drive on the Lucent Security Management Server.
   b. Access the **Devices** menu and select **BRICKS**.
   c. Highlight the desired VPN Firewall device in the **Navigator** View. Right Click and select **`Make/Package Floppy`**.
   d. In the response window, click OK. The server will copy VPN Firewall device boot files to the floppy.
   e. When the process is completed, please remove the floppy from the SMS and store in a safe location.

To download the SMS Solaris software now, please logon to your account at **https://vpn-firewall-brick.alcatel-lucent.com/**.

Software checksums

Table 7-1 SMS checksums

Filename	Checksum
LSMSPatch-9.1.340.exe	83cd226f86ac1de8ddaffbebc291f220
lsmspatch-9.1.340.tar	32df4b267c0f83e7b0157837e29766a9