



syslog-ng Store Box 5.0

Upgrade Guide

## Copyright 2018 One Identity LLC.

### ALL RIGHTS RESERVED.

This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of One Identity LLC .

The information in this document is provided in connection with One Identity products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of One Identity LLC products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, ONE IDENTITY ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL ONE IDENTITY BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF ONE IDENTITY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. One Identity makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. One Identity does not make any commitment to update the information contained in this document.

If you have any questions regarding your potential use of this material, contact:

One Identity LLC.  
Attn: LEGAL Dept  
4 Polaris Way  
Aliso Viejo, CA 92656

Refer to our Web site (<http://www.OneIdentity.com>) for regional and international office information.

### Patents

One Identity is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at <http://www.OneIdentity.com/legal/patents.aspx>.

### Trademarks

One Identity and the One Identity logo are trademarks and registered trademarks of One Identity LLC. in the U.S.A. and other countries. For a complete list of One Identity trademarks, please visit our website at [www.OneIdentity.com/legal](http://www.OneIdentity.com/legal). All other trademarks are the property of their respective owners.

### Legend

-  **WARNING:** A WARNING icon indicates a potential for property damage, personal injury, or death.
-  **CAUTION:** A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.
-  **IMPORTANT, NOTE, TIP, MOBILE, or VIDEO:** An information icon indicates supporting information.

SSB Upgrade Guide  
Updated - July 2018  
Version - 5.0

# Contents

|   |           |
|---|-----------|
| <b>Preface</b> .....                                  | <b>4</b>  |
| <b>Prerequisites and Notes</b> .....                  | <b>5</b>  |
| Upgrade path to SSB 5 LTS .....                       | 5         |
| Pyramid hardware is not supported .....               | 5         |
| SNMP v3 trap settings .....                           | 6         |
| Changes in the prevention of disk space fill-up ..... | 6         |
| SNMP high disk utilization trap .....                 | 7         |
| Upgrade checklist .....                               | 7         |
| <b>Upgrading to SSB 5 LTS</b> .....                   | <b>10</b> |
| Upgrading SSB (single node) .....                     | 10        |
| Upgrading an SSB cluster .....                        | 11        |
| Updating the SSB license .....                        | 12        |
| <b>Troubleshooting</b> .....                          | <b>14</b> |
| <b>About us</b> .....                                 | <b>15</b> |
| Contacting us .....                                   | 15        |
| Technical support resources .....                     | 15        |

## Preface

Welcome to syslog-ng Store Box (SSB) version 5 LTS and thank you for choosing our product. This document describes the process to upgrade existing SSB installations to SSB 5 LTS. The main aim of this paper is to aid system administrators in planning the migration to the new version of SSB.

**⚠ CAUTION:**

**Read the entire document thoroughly before starting the upgrade.**

Upgrading to SSB 5 LTS is not supported if you have SSB deployed on any of the following Pyramid hardware: SSB N1000, SSB N1000d, SSB N5000, SSB N10000. For details, see [Prerequisites and Notes](#) on page 5.

As of June 2011, the following release policy applies to syslog-ng Store Box:

- *Long Term Supported or LTS releases* (for example, SSB 4 LTS) are supported for 3 years after their original publication date and for 1 year after the next LTS release is published (whichever date is later). The second digit of the revisions of such releases is 0 (for example, SSB 4.0.1). Maintenance releases to LTS releases contain only bugfixes and security updates.
- *Feature releases* (for example, SSB 4 F1) are supported for 6 months after their original publication date and for 2 months after succeeding Feature or LTS Release is published (whichever date is later). Feature releases contain enhancements and new features, presumably 1-3 new features per release. Only the last of the feature releases is supported (for example, when a new feature release comes out, the last one becomes unsupported).

**⚠ CAUTION:**

**Downgrading from a feature release to an earlier (and thus unsupported) feature release, or to the previous LTS release is not supported.**

# Prerequisites and Notes

## Upgrade path to SSB 5 LTS

Upgrading to SSB 5 LTS is tested and supported using the following upgrade path:

- *The latest SSB 4 LTS maintenance version (for example, 4.0.7) -> SSB 5 LTS*  
Always upgrade to the latest available maintenance version of SSB 4 LTS before upgrading to SSB 5 LTS.
- *The latest maintenance version of the previous feature release (in this case, SSB 4 F9) -> SSB 5 LTS*

From older releases, upgrade to 4 LTS first. For details, see [How to upgrade to syslog-ng Store Box 4 LTS](#).

## Pyramid hardware is not supported

SSB 5 LTS is not supported on the following hardware: SSB N1000, SSB N1000d, SSB N5000, SSB N10000.

In case you have SSB deployed on other, newer hardware or you have SSB 4 LTS, those will not be affected in any way. The version policy applies to those. For details, open the [SSB product page on the Support Portal](#) and navigate to **Product Life Cycle & Policies > Product Support Policies > Software Product Support Lifecycle Policy**.

If you wish to take advantage of new features and remain supported beyond the end date of the Extended Support phase, you need to upgrade your hardware. For assistance with your hardware upgrade, [contact our Sales Team](#). For further inquiries, [contact our Support Team](#).

If you do not know the type of your hardware or when it was purchased, complete the following steps:

1. Log in to SSB.
2. Navigate to **Basic Settings > Troubleshooting > System debug**, click **COLLECT AND SAVE CURRENT SYSTEM STATE INFO**, and save the file.
3. Log in to the [support portal](#) and submit a ticket.
4. In the **Summary** field, enter Determining hardware type.
5. Upload the file you downloaded from SSB in Step 2.
6. We will check the type of your hardware and notify you.

# SNMP v3 trap settings

The MD5 authentication method and the DES encryption method are no longer available as SNMP trap settings, when configuring SSB to:

- Send alerts to a central monitoring server via SNMP v3.
- Forward log messages to an SNMP destination using the SNMP v3 protocol.

Due to the removal of support for these authentication and encryption methods, certain configuration changes automatically take effect when you upgrade your SSB to version 5 LTS from 4.0. They are as follows:

- MD5 authentication method:
  - If you have **Basic Settings > Management > SNMP trap settings > SNMP v3 > Authentication method** set to **MD5**, that will automatically be set to **SHA1**.
  - If you have **Log > Destinations > SNMP destination > SNMP trap settings > SNMP v3 > Authentication method** set to **MD5**, that will automatically be set to **SHA1**.
- DES encryption method:
  - If you have **Basic Settings > Management > SNMP trap settings > SNMP v3 > Encryption method** set to **DES**, that will automatically be set to **AES**.
  - If you have **Log > Destinations > SNMP destination > SNMP trap settings > SNMP v3 > Encryption method** set to **DES**, that will automatically be set to **AES**.

Note that these automatic changes may require you to reset the relevant configuration options at your end, following an upgrade to version 5 LTS from 4.0.

## Changes in the prevention of disk space fill-up

The following changes have been introduced in SSB 4 F8 regarding the prevention of disk space fill-up:

- The default value of **Basic Settings > Management > Disk space fill up prevention > Disconnect clients when disks are** has changed from 0 to 90. If you had 0 specified, then following the upgrade, it will change to 90. This means that disk fillup prevention will be turned on by default, with clients getting disconnected once disk utilization exceeds 90%.
- Another change concerns the value 100. Starting from version 4 F8, you are only

allowed to set values between 1-99. This means that if you had 100 specified before the upgrade, then that will change to 99 following the upgrade.

For more information on preventing disk space from filling up, see ["Preventing disk space fill up" in the Administration Guide](#).

## SNMP high disk utilization trap

The following changes have been introduced regarding the SNMP trap that is sent when disk utilization exceeds a pre-configured value:

- In the `dismanEventMIB` trap, the value of `dskDevice` has changed from `rootfs` to `none`. This only concerns the disk with index 1.  
In case you had some filters or alerts set on the value `rootfs`, then those will not work anymore.
- The `dismanEventMIB` trap sends out path information in a new field called `dskPath`.

## Upgrade checklist

The following list applies to all configurations:

- You have backed up your configuration and your data.  
For more information on creating configuration and data backups, see ["Data and configuration backups" in the Administration Guide](#).
- For added safety, you have also exported the current configuration of SSB.  
For detailed instructions, refer to ["Exporting the configuration of SSB" in the Administration Guide](#).
- You have a valid [support portal](#) account.  
To download the required firmware files, you need a valid [support portal](#) account. To create an account, navigate to the [support portal](#) and follow the instructions on screen (you will need to enter your product's asset number, which is the license number or serial number you have been provided previously).
- You have downloaded the new 5 LTS license file from [support portal](#). As license files are specific to each long term release, upgrading to SSB 5 LTS removes any earlier license.

**⚠ CAUTION:**

**SSB now strictly checks if you have a High Availability license when running SSB in High Availability mode. You cannot upgrade to 5 LTS or later when using a single-node license in a HA environment. After upgrading to 5 LTS or later, an SSB node can be converted to HA only if a valid HA license is installed. HA licenses include the following line:**

Licensed-Options: Highavailability

**To buy a valid HA license, contact your sales representative or [contact our Sales Team](#).**

- You have downloaded the latest SSB core firmware and boot firmware from the [Downloads page](#).

For a detailed description of the different firmwares, see "[Firmware in SSB](#)" in the [Administration Guide](#).

- You have read the Release Notes (changelog) of the firmware(s) before updating. The Release Notes might include additional instructions specific to the firmware version.

The Release Notes are available on the [Downloads page](#).

If you have a high availability cluster:

- You have IPMI access to the slave node. You can find detailed information on using the IPMI interface in the following documents:
  - For SSB T1, see the [SMT IPMI User's Guide](#).
  - For SSB T4 and T10, see the [X9 SMT IPMI User's Guide](#).
- You have verified on the **Basic Settings > High Availability** page that the HA status is not degraded.
- *If you have a high availability cluster with geocustering enabled:*

Perform the firmware upload steps an hour before the actual upgrade. Geocustering can introduce delays in master-slave synchronization, and the slave node might not be able to sync the new firmware from the master node on time.

If you are upgrading SSB in a virtual environment:

- You have created a snapshot of the virtual machine before starting the upgrade process.
- You have configured and enabled console redirection (if the virtual environment allows it).

During the upgrade, SSB displays information about the progress of the upgrade and any possible problems to the console, which you can monitor with IPMI (ILOM) or console access.

We recommend that you test the upgrade process in a non-productive (virtual, etc.) environment first.

Upgrading SSB requires a reboot. We strongly suggest that you perform the upgrade on the productive appliance during maintenance hours only, to avoid any potential data loss.

# Upgrading to SSB 5 LTS

## Upgrading SSB (single node)

### Purpose:

If you want to upgrade a SSB cluster, see [Upgrading an SSB cluster](#) on page 11. To upgrade a standalone SSB node to version 5 LTS, complete the following steps.

### Prerequisites:

Read the following warnings before starting the upgrade process.

### Steps:

1. Update the core firmware of SSB using the web interface.
  - a. Navigate to **Basic Settings > System > Core firmwares**.
  - b. Upload the new core firmware.
  - c. When the upload is finished, select the **After reboot** option for the new firmware.  
*Do not reboot SSB yet.*
2. Upload the boot firmware of SSB using the web interface.
  - a. Navigate to **Basic Settings > System > Boot firmwares**.
  - b. Upload the new boot firmware.
  - c. When the upload is finished, select the **After reboot** option for the new firmware.
3. *Recommended step.* To help troubleshoot potential issues following the upgrade, collect and save system information (create a debug bundle) now.  
Navigate to **Basic Settings > Troubleshooting > System debug** and choose **Collect and save current system state info**.
4. Navigate to **Basic Settings > System > System Control > This node**, and

choose **Reboot**.

SSB attempts to boot with the new firmware. Wait for the process to complete.

5. Log in to the SSB web interface to verify that the upgrade was successful.  
Navigate to **Basic Settings > System > Version details** and check the version numbers of SSB. In case you encounter problems, you can find common troubleshooting steps in [Troubleshooting](#) on page 14.
6. Upload the new license file. For details, see [Updating the SSB license](#) on page 12.

## Upgrading an SSB cluster

### Prerequisites:

Make sure that you have physically connected the IPMI interface to the network and that it is properly configured. This is important because you can only power the slave node on through the IPMI interface. For details on configuring the IPMI interface, see "[Out-of-band management of SSB](#)" in the [Administration Guide](#).

#### CAUTION:

**SSB now strictly checks if you have a High Availability license when running SSB in High Availability mode. You cannot upgrade to 5 LTS or later when using a single-node license in a HA environment. After upgrading to 5 LTS or later, an SSB node can be converted to HA only if a valid HA license is installed. HA licenses include the following line:**

Licensed-Options: Highavailability

**To buy a valid HA license, contact your sales representative or [contact our Sales Team](#).**

### Steps:

1. Update the core firmware of SSB using the web interface.
  - a. Navigate to **Basic Settings > System > Core firmwares**.
  - b. Upload the new core firmware.
  - c. When the upload is finished, select the **After reboot** option for the new firmware.  
*Do not reboot SSB yet.*
2. Upload the boot firmware of SSB using the web interface.
  - a. Navigate to **Basic Settings > System > Boot firmwares**.
  - b. Upload the new boot firmware.
  - c. When the upload is finished, select the **After reboot** option for the new

firmware.

*Do not reboot SSB yet.*

3. *Recommended step.* To help troubleshoot potential issues following the upgrade, collect and save system information (create a debug bundle) now.

Navigate to **Basic Settings > Troubleshooting > System debug** and choose **Collect and save current system state info**.

4. Navigate to **Basic Settings > High availability**, and verify that the new firmware is displayed for the slave node. This might take a few minutes.

Note that at this stage, the slave node is not using the new firmware yet.

5. Navigate to **Basic Settings > System > High availability > Other node** and click **Shutdown**.

6. Restart the master node: choose **This node > Reboot**.

SSB attempts to boot with the new firmware. Wait for the process to complete.

7. Log in to the SSB web interface to verify that the master node upgrade was successful.

Navigate to **Basic Settings > System > Version details** and check the version numbers of SSB. In case you encounter problems, you can find common troubleshooting steps in [Troubleshooting](#) on page 14.

8. Upload the new license file. For details, see [Updating the SSB license](#) on page 12.

9. Use the IPMI interface to reboot the slave node.

The slave node attempts to boot with the new firmware, and reconnects to the master node to sync data. During the sync process, certain services (including Heartbeat) are not available. Wait for the process to finish, and the slave node to boot fully.

10. Navigate to **Basic Settings > System > High availability & Nodes** and verify that the slave node is connected, and has the same firmware versions as the master node.

**NOTE:**

When upgrading an SSB cluster, the upgrade process on the slave node will only be completed once a takeover has been performed.

## Updating the SSB license

### Steps:

1. Download the new 5 LTS license file from [support portal](#).
2. Navigate to **Basic Settings > System > License**.
3. Click **Browse** and select the new license file.

You can upload compressed licenses (for example, .zip archives).

4. Click **Upload**, then **Commit**.

## Troubleshooting

If you experience any strange behavior of the web interface, first try to reload the page by holding the SHIFT key while clicking the Reload button of your browser to remove any cached version of the page.

In the unlikely case that SSB encounters a problem during the upgrade process and cannot revert to its original state, SSB performs the following actions:

- Initializes the network interfaces using the already configured IP addresses.
- Enables SSH access to SSB, unless SSB is running in sealed mode. That way it is possible to access the logs of the upgrade process, which helps the Support Team to diagnose and solve the problem. Note that SSH access will be enabled on every active interface, even if management access has not been enabled for the interface.

In case the web interface is not available within 30 minutes of rebooting SSB, check the information displayed on the local console and [contact our Support Team](#).

One Identity solutions eliminate the complexities and time-consuming processes often required to govern identities, manage privileged accounts and control access. Our solutions enhance business agility while addressing your IAM challenges with on-premises, cloud and hybrid environments.

## Contacting us

For sales or other inquiries, visit <https://www.oneidentity.com/company/contact-us.aspx> or call +1-800-306-9329.

## Technical support resources

Technical support is available to One Identity customers with a valid maintenance contract and customers who have trial versions. You can access the Support Portal at <https://support.oneidentity.com/>.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request
- View Knowledge Base articles
- Sign up for product notifications
- Download software and technical documentation
- View how-to-videos at [www.YouTube.com/OneIdentity](http://www.YouTube.com/OneIdentity)
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product