Upgrading to IBM Security Identity Manager Version 7.0.1.7 Cookbook

Version 1.0

Acknowledgements

This document is created by:

Anilkumar Hegde
Nandkishor Gitte

Table of Contents

Introduction

This cookbook describes the upgrade paths, before upgrade considerations, procedure to upgrade to IBM® Security Identity Manager (ISIM), Version 7.0.1.7 and after upgrade configurations.

Supported upgrade paths

To upgrade to the IBM® Security Identity Manager, Version 7.0.1.7, the following upgrade paths are supported.

- Version 7.0.0 to Version 7.0.1.7
- Versions 7.0.0.2 and 7.0.0.3 to Version 7.0.1.7
- Version 7.0.1 and 7.0.1.1 to Version 7.0.1.7
- Version 7.0.1.3 and higher to Version 7.0.1.7

Chapter 1. Upgrading from Version 7.0.0 to Version 7.0.1.7

Direct upgrade from IBM Security Identity Manager, Version 7.0.0 to IBM Security Identity Manager, Version 7.0.1.7 is not supported. You must first upgrade from IBM Security Identity Manager, Version 7.0.0 to IBM Security Identity Manager, Version 7.0.1 and then upgrade from IBM Security Identity Manager, Version 7.0.1 to IBM Security Identity Manager, Version 7.0.1.7.

Upgrade from Version 7.0.0 to Version 7.0.1

In IBM Security Identity Manager, Version 7.0.1, the following new features are introduced:

- Application interface

  In IBM Security Identity Manager, Version 7.0.0, both the virtual appliance local management interface and the IBM Security Identity Manager application run on the same network interface. In IBM Security Identity Manager, Version 7.0.0.2, application interface was introduced to provide an additional level of security. That means, in IBM Security Identity Manager, Version 7.0.1, virtual appliance local management interface, and IBM Security Identity Manager application run on separate network interface.
- Port Standardization

  In IBM Security Identity Manager, Version 7.0.1, ISIM application ports are standardized. Before ISIM 7.0.1, the ISIM application on each node used to run on a different port. From ISIM 7.0.1 and later, the IBM Security Identity Manager application on each node runs on the same port, which is 9082.

Complete the pre-upgrade preparations, upgrade procedure, and the post-upgrade configurations.

Pre-upgrade preparations

- You must attach at least three network cards or interfaces to set up the virtual machine for the IBM Security Identity Manager, Version 7.0.1. Out of the three network cards, two network cards are required for the virtual appliance local management interface and one for the IBM Security Identity Manager application.

  Note: Set VMXNET 3 as the network adapter for better results. You can also use the E1000 adapter to set up the virtual machine.
- Acquire at least one new network address (IP address) for the IBM Security Identity Manager application.
- Change your external servers such as load balancer to point to the new network address.
- Change your external servers such as load balancer or IBM Security Access Manager junction, to use the port 9082.

Upgrade the virtual appliance

Complete the procedure to upgrade the virtual appliance. See Procedure to upgrade the virtual appliance.

Post-upgrade configurations

Complete the following configurations.

- Assign a new network address to the IBM Security Identity Manager application.
- Configure the application interface for the IBM Security Identity Manager application from **Manage > Application Interfaces** in the virtual appliance.
- If you use IBM Security Access Manager for Single Sign-On, reconfigure your Single Sign-On Configuration in the IBM Security Identity Manager virtual appliance from **Configure > Single Sign-On Configuration**.

Upgrade from Version 7.0.1 to Version 7.0.1.7

See Upgrading from Version 7.0.1 to Version 7.0.1.7

Chapter 2. Upgrading from Versions 7.0.0.2 and 7.0.0.3 to Version 7.0.1.7

In the later versions of IBM Security Identity Manager, Version 7.0.0.2 and 7.0.0.3, the following new features are introduced:

- Fully qualified domain name (FQDN) for application interface

  You can specify FQDN to generate a self-signed application server certificate by using the specified FQDN. However, if a custom certificate is used in IBM Security Identity Manager, Version 7.0.1, then the self-signed certificate is not generated and your custom certificate is imported from IBM Security Identity Manager, Version 7.0.1.
- Separate interface gateway for application interface

  You can specify a separate interface gateway for each application interface, which enables each interface to run a separate subnet.
- Port Standardization

  In IBM Security Identity Manager, Version 7.0.1, ISIM application ports are standardized. Before ISIM 7.0.1, the ISIM application on each node used to run on a different port. From ISIM 7.0.1 and later, the IBM Security Identity Manager application on each node runs on the same port, which is 9082.
- Non-secure communication to the IBM Security Identity Manager application is closed.
- Simple Network Management Protocol (SNMP) port standardization

  SNMP port is standardized in IBM Security Identity Manager, Version 7.0.1.3. Before ISIM 7.0.1.3, there was provision to set SNMP server port of your own choice. From 7.0.1.3 onwards, SNMP server is configured to run always on port 161.

Complete the pre-upgrade preparations, upgrade procedure, and the post-upgrade configurations.

Pre-upgrade preparations

- Ensure that you get the DNS registered FQDN for the IBM Security Identity Manager application interface.
- Acquire the interface gateway from your network administrator.
- Ensure that you update all your external applications to communicate with the IBM Security Identity Manager over the secure channel.
- Change your external SNMP clients to use the updated SNMP port, which is 161.
- Change your external servers such as load balancer or IBM Security Access Manager junction, to use the port 9082.

Upgrade the virtual appliance

Complete the procedure to upgrade the virtual appliance. See Procedure to upgrade the virtual appliance.

Post-upgrade configurations

Configure the application interface for the IBM Security Identity Manager application from **Manage > Application Interfaces** in the virtual appliance.

Chapter 3. Upgrading from Version 7.0.1 and 7.0.1.1 to Version 7.0.1.7

Starting IBM Security Identity Manager, Version 7.0.1.3, the following new features were introduced:

- Fully qualified domain name (FQDN) for application interface

  You can specify FQDN to generate a self-signed application server certificate by using the specified FQDN. However, if a custom certificate is used in IBM Security Identity Manager, Version 7.0.1, then the self-signed certificate is not generated and your custom certificate is imported from IBM Security Identity Manager, Version 7.0.1.
- Separate interface gateway for application interface

  You can specify a separate interface gateway for each application interface, which enables each interface to run a separate subnet.
- Non-secure communication to the IBM Security Identity Manager application is closed.
- Simple Network Management Protocol (SNMP) port standardization

  SNMP port is standardized in IBM Security Identity Manager, Version 7.0.1.3. Prior to IBM Security Identity Manager, Version 7.0.1.3, a provision to set SNMP server port was a user's choice. From IBM Security Identity Manager, Version 7.0.1.3 onwards, SNMP server is configured to run always on the port 161.

Complete the pre-upgrade preparations, upgrade procedure, and the post-upgrade configurations.

Pre-upgrade preparations

- Ensure that you get the DNS registered FQDN for the IBM Security Identity Manager application interface.
- Acquire the interface gateway from your network administrator.
- Ensure that you update all your external applications to communicate with the IBM Security Identity Manager over the secure channel.
- Change your external SNMP clients to use the updated SNMP port, which is 161.

Upgrade the virtual appliance

Complete the procedure to upgrade the virtual appliance. See Procedure to upgrade the virtual appliance.

Post-upgrade configurations

Configure the application interface for the IBM Security Identity Manager application from **Manage > Application Interfaces** in the virtual appliance.

Chapter 4. Upgrading from Version 7.0.1.3 and higher to Version 7.0.1.7

Pre-upgrade preparations

N/A

Upgrade the virtual appliance

Complete the procedure to upgrade the virtual appliance. See Procedure to upgrade the virtual appliance.

Post-upgrade configurations

N/A

Procedure to upgrade the virtual appliance

Copy the package files for upgrading through USB device

Install the firmware update to upgrade the IBM Security Identity Manager virtual appliance. Before you apply the firmware update to upgrade the IBM Security Identity Manager virtual appliance, back up your data tier, which is all the databases and the directory server.

The IBM Security Identity Manager virtual appliance has two partitions with separate firmware on each partition. The partitions are swapped during the firmware updates to roll back the firmware updates when required. Either of the partition can be active on the IBM Security Identity Manager virtual appliance.
In the factory-installed state, Partition 1 is active and contains the firmware version of the current released product. When you apply a firmware update, the update is installed on Partition 2 and your policies and settings are copied from Partition 1 to Partition 2.
The IBM Security Identity Manager virtual appliance restarts the system by using Partition 2, which is now the active partition.

Complete these steps:

1. Download the isim_*.zip package from the IBM Fix Central.
2. Extract the isim_*.pkg build to a location of your choice.
3. Access the command-line interface (CLI) of the virtual appliance with either an ssh session or the console.
4. Copy the isim_*.pkg to a USB device.
5. Attach the USB device to your virtual system.
6. Access the command-line interface (CLI) of the virtual appliance to transfer the firmware.
   - For upgrade from IBM® Security Identity Manager virtual appliance, Version 7.0.1 or later, run this command: **isim > upgrade > transfer**
   - For upgrade from earlier versions of IBM® Security Identity Manager virtual appliance, Version 7.0.1, run this command: **isim > firmware_update > transfer_firmware**

Copy the package files for upgrading through firmware update transfer utility

The IBM Security Identity Manager virtual appliance allows only firmware updates by USB device. Starting at firmware release 7.0.0.2 (7.0.0-ISS-SIM-FP0002), firmware (.pkg) files can be transferred with the attached Java™ utility. A USB device is no longer required to update the virtual appliance. You must install the firmware release 7.0.0.2 (7.0.0-ISS-SIM-FP0002) or later before you can install the firmware release 7.0.0.3 or later with this utility. This utility performs the same function as the command-line interface (CLI) command of the virtual appliance.

Complete these steps:

1. Download the isim_*.zip package from the IBM Fix Central.
2. Extract the isim_*.pkg build to a location of your choice.
3. Copy the utility to a system where Java, Version 1.7 is installed.
4. Copy these files to the file system.
   - The .pkg firmware update file.
   - The keystore (jks) file.
5. Run the following Java command to upload the .pkg file.
   Usage:
   ```
   java -jar FileUpload.jar Hostname AdminId AdminPassword Truststore_Filepath Truststore_Password <Absolute path to pkg file>
   ```
   Example:
   ```
   java -jar FileUpload.jar isimsys.ibm.com admin admin /Downloads/temptrust.jks WebAS
   /Downloads/7.0.1-ISS-SIM-FP0007.pkg
   ```
6. Use the supplied temptrust.jks file if you did not update the default certificates. If you previously updated the default certificate on the virtual appliance, temptrust.jks does not work. Use an updated jks file that is based on your updated certificate.

Install the IBM Security Identity Manager virtual appliance

The IBM Security Identity Manager virtual appliance version upgrade can be installed only by using the command-line interface (CLI).

Complete these steps:

1. Access the command-line interface (CLI) of the virtual appliance to install the firmware with the following command.

   Note: Run this command after you transfer the .pkg file.

   a. For upgrade from IBM® Security Identity Manager virtual appliance, Version 7.0.1 or later, run this command:

      isim > upgrade > install

   b. For upgrade from earlier versions of IBM® Security Identity Manager virtual appliance, Version 7.0.1, run this command:

      isim > firmware_update > install_firmware

2. Select the index of the firmware update that you want to install to the virtual system and press Enter.

   The results are as follows:

   a. The upgrade process formats Partition 2 and installs the new firmware update on it.

   b. When you apply the firmware update, your policies and settings are copied from Partition 1 to Partition 2.

3. Type the reboot command and press Enter to restart the virtual system. Partition 2 is now the active partition. After the virtual appliance restarts from the Partition 2, all the configuration that were part of Partition 1, is applied to the Partition 2.
4. For the Identity data store, clear the Service Integration Bus before you restart the IBM Security Identity Manager. See Reconfiguring the data store connection.
5. Restart the IBM Security Identity Manager.
6. Optional: Back up Partition 2 in to Partition 1 after the successful completion of the firmware upgrade. The backup process overwrites the information that is in Partition 1.

   Do the following actions:

   a. Check and fix any errors if the upgrade process failed.

   b. Use Partition 1 to set it as the active partition and restart it.

   Partition 1 now becomes the active partition.

References

For more information about the IBM Security Identity Manager, Version 7.0.1.7 features and functions, see http://www.ibm.com/support/knowledgecenter/SSRMWJ_7.0.1.7/com.ibm.isim.doc/kc-homepage.htm