SOPHOS

Upgrading SUM

Staged Rollout Procedure

Sophos Limited

April 2014

1 Content

2 Staged Rollout Procedure

Starting with SUM 4.2, the management support of different UTM versions from the Sophos UTM Manager has changed. Please find more information in the knowledgebase article 120690.

In summary, SUM 4.2 and future versions manage UTM devices in two modes:

- Full management mode
- Legacy mode

The difference between legacy mode and full-management mode is, that you are not allowed to make configurations in SUM for your UTM. If SUM and UTM are not on corresponding versions, the central management session falls into legacy mode.

This document gives you detailed instructions what to do and which things are important to consider. If you have not updated your SUM to 4.2 and UTMs to 9.2 we recommend to do this as soon as possible. If you are not able to update all of your UTMs to version 9.2 then we recommend a staged rollout. Please note that, for the staged rollout, a second SUM with a second license is necessary.

2.1 Staged Rollout

It is important to plan ahead the staged rollout and aspire for the entire process to be finished in the shortest time period acceptable by the organization. This will ensure getting the most benefit from new features, improvements, and bug fixes, while reducing the chances of management complexity and configuration synchronization issues.

To perform the staged rollout, proceed as follows:

1. Create a backup of your current SUM.
2. Install a second SUM.
3. Restore the backup from the previous SUM.
4. Connect your UTMs to the new SUM.
5. Finalizing staged rollout

In the following chapters the recommended steps are described in detail.

2.1.1 Creating a Backup

Before installing or upgrading SUM it is necessaty to create a backup with the current system state. Proceed as follows:

1. Log on to SUM WebAdmin.
2. Navigate to *Management* > *Backup/Restore* > *Backup/Restore*.
3. Enter a comment into the comment field (optional).

4. Click *Create Backup Now*.

► The backup appears in the list of available backups.

5. Click on the download icon ( ).
   The 'Download options' dialog appears.

6. If you want to download the backup encrypted activate the checkmark next to *Encrypt before downloading* and enter a password.

7. Click *Download backup*.
   You will be asked if you really want to download.

8. Click *Save file*.

► The backup file will be downloaded. Use this backup to restore the configuration for your new SUM later on.

2.1.2 Installing SUM

Within the staged rollout Sophos recommends to install a second SUM. Aim is to have a SUM with a version < 4.2 and one with a version >= 4.2.

To install SUM, proceed as follows:

1. Navigate to the Sophos downloads area.

2. Click at Sophos UTM Manager on *Get full package*.
   A web form opens.

3. Fill out the web form and submit it.
   You will get an email containing installation instructions and your MyUTM account information.

4. Follow the instructions in the email.

Note – It is also possible to mount the ISO-file on a virtual drive instead of burning it onto a CD-ROM.

Note – Give SUM an IP-address of your network environment so that it's reachable from your UTMs and the management PC.

5. After installation open the new SUM in your web browser and perform the basic system setup by following the displayed steps.

2.1.3 Restoring the backup

Import and restore the backup of your old SUM. Proceed as follows:

1. Log on to your new SUMs' WebAdmin.

2. Navigate to *Management > Backup/Restore > Backup/Restore*.

3. In the Import backup area click on the folder icon.
   The dialog 'Upload file' opens.

4. Click *Browse* and select the backup you created with your old SUM.

5. Click *Start Upload*.
   The file will be uploaded.

6. If the file is encrypted enter the password.

7. Click *Import backup*.
   The backup file will be imported and is visible in the *Available backups* list.

8. Restore the backup by clicking on the restore icon ( ) next to the currently imported backup.
   You will be asked if you really want to restore.

9. Confirm the question with *Ok*.

► The backup will be restored.

If you have problems restoring a backup you have the possibility to import the configurations. This is described in Importing Configurations.

2.1.4 Connecting UTMs to SUM

If you are in a mixed environment and want to be able to monitor all UTMs in one SUM you have to add a second SUM to each of your UTMs. Aim is to have UTM <= 9.1 which can be managed by a SUM <=4.1 and monitored by a (second) SUM >= 4.2 and the other way round.

To add a second SUM to your UTM, proceed as follows:

1. Log on to your UTM.

2. Open the tab *Management > Central Management > Sophos UTM Manager*.

3. Add your second SUM for monitoring at *Settings for a Second SUM (optional)*.

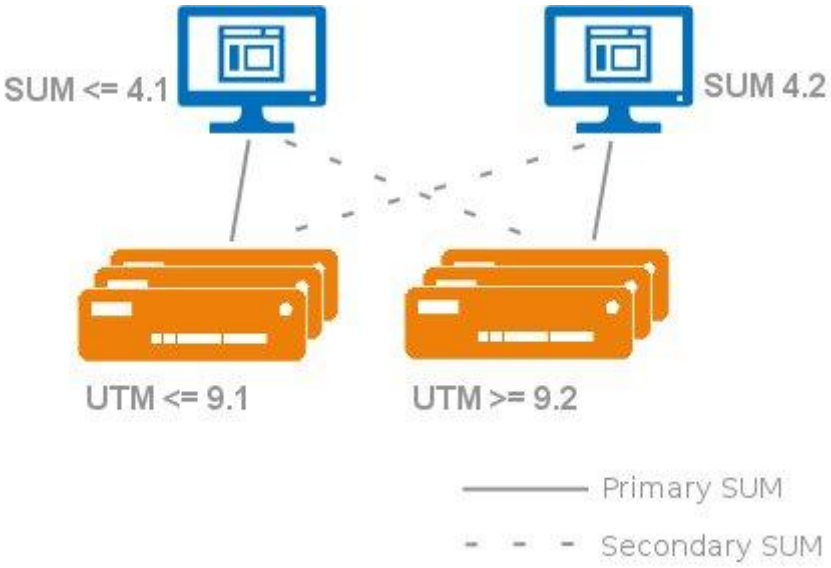
► The UTM connects to the second SUM and can be monitored.

2.1.5 Finalizing staged rollout

The staged rollout is finished when all UTMs have been upgraded to a current version and thus are managed in ‘full management mode’ and are using SUM 4.2 installation as the primary SUM server. Afterwards the now unused SUM <= 4.1 can be turned off permanently. It’s up to your decision if you want to re-configure your new SUM to the IP address initially used by the old SUM but remember if you do that you would have to manually change the SUM host in all connected UTMs individually.

2.2 Managing configuration changes

It is advised that during a staged-rollout period configuration changes on legacy mode UTMs are kept to a minimum. If changes are made from an old version of SUM to legacy mode UTMs the changes have to be merged back into the new version of SUM manually after the UTM is upgraded.



Configuration with two SUMs

1. Track changes you make in SUM <= 4.1 as long as the UTM is in legacy mode, and manually update in SUM 4.2 after the UTM is upgraded. Please write down and comment your changes to the legacy mode UTMs (in a spreadsheet for example). After the UTM is upgraded to the latest supported full management mode version (>= 9.2), apply specific changes for this device in SUM >= 4.2.

2. Re-deploy the configuration once a legacy mode UTM is upgraded. In this case, after upgrade the new UTMs, configuration will be overridden with the current SUM managed configuration for the group the UTM belongs to.

3 Best practice tips

3.1 Alternative method for switching UTMs between two SUM servers

Another method for easy switching UTMs between two SUM server versions would be using a firewall DNAT.

Most often the SUM machine will not be directly connected to the internet (having an official IP address), but is placed in a DMZ or LAN segment behind a firewall. The firewall in front of the SUM is configured to do Destination NAT (DNAT, forward NAT, port forwarding) of incoming packets of port 4433/tcp to the SUM – these packets are establishing the communication between a UTM and SUM.

You should have a DNAT rule with the following attributes:

```
Original Source: ANY/Internet
Original Destination: Firewall(External WAN Address)
Original Port: 4433/TCP
Translated Source: <no translation>
Translated Destination: SUM4.1_IP
Translated Port: <no translation>
```

In this case, you can avoid changing the SUM server IP addresses on each UTM manually.

Add an additional DNAT rule on the firewall for the updated UTMs with the following attributes:

```
Original Source: Group of updated UTMs
Original Destination: Firewall(External WAN Address)
Original Port: 4433/TCP
Translated Source: <no translation>
Translated Destination: SUM4.2_IP
Translated Port: <no translation>
```

To configure this using an UTM as firewall, proceed as follows:

1. Log on to UTM.
2. Navigate to *Definitions & Users* > *Network Definitions* > *Network Definitions*.
3. Click on *New network definition*, select type *DNS host* and create a definition for each of your UTMs.
4. Click on *New network definition*, select type *Network group*.
5. Add the DNS host definition to this network group, every time you upgrade a UTM.
6. Navigate to *Network Protection* > *NAT* > *NAT* and click on *New NAT rule…*.
7. Place the new rule before (above) the existing NAT rule for the old SUM.
8. Set the rule type to *DNAT (Destination)*.
9. Insert your new network group as the source at *For traffic from*.

10. Insert the pre-defined service definition *Sophos UTM Manager (SUM)* by adding it into the *Using service* field.
11. Insert your WAN address into the *Going to* field.
12. As action for *Change the destination to* use the network definition with the internal IP address of your new SUM.
13. Insert the pre-defined service definition *Sophos UTM Manager (SUM)* by adding it into the *And the service to* field.
14. Activate the checkbox next to *Automatic Firewall rule*.
15. Click *Save*.

Now all UTMs you upgraded to new version will match this first DNAT rule, thus the port 4433-packets are forwarded to the new SUM server. No local change on the UTMs is needed.

4 Additional Scenarios

4.1 SUM was upgraded to 4.2 before UTMs were upgraded to 9.2

In case the SUM was already upgraded to a higher version only to realize your UTMs fall into legacy mode, you have to re-install the old SUM version or to upgrade your UTMs, too. To re-install the old SUM version, proceed as follows:

1. Install a fresh instance of the SUM version you had before.
2. Restore configuration from the SUM backup of the old SUM.
3. If a configuration backup copy is not available you will have to rebuild the SUM configuration by importing from UTMs.

4.2 Importing Configurations

You need this function only if no backups are available and if you have matching corresponding versions of UTM and SUM or in case you installed a second SUM and for any reason you can import the configurations from your UTMs.

Note – It is only possible to import configurations of matching versions.

To import configurations, proceed as follows:

1. Open the Gateway Manager of the requested SUM.
2. Navigate to *Configuration* > *Import* > *Type Selection*.
3. Select the requested gateways.
   Only the matching devices will be displayed for selection.
4. Select the requested global object types.
5. Click *Apply* to save your changes.
   The objects are now visible in the *Import* list.
6. Open the Import list (*Configuration* > *Import* > *Import*).
7. Select the requested objects.
8. Click *Import*.

► The selected objects will be imported and displayed in the Gateway Manager.

Note – If you import objects which already exist, they will be marked with '(2)'.

4.3 Mixed-environment managed from an MSP

The MSP SUM is slightly different as it manages licenses. The basic procedures and managing of fully-managed UTMs and legacy-mode UTMs is the same except for the steps needed to change the SUM host IP address. Please follow these steps:

1. Follow *Staged Rollout Procedure* instructions.
2. Under *Definitions & User > Network Definitions*: change the IP address of the SUM *host object* to the new SUM IP address.

► After 2-3 minutes the UTM is going to connect to that SUM.