Use Security Packages

For supported software information. click [here](#).

A security package (SPack) is a software bundle that supports predefined services and objects that you can use in firewall configurations to protect network devices from security threats. An SPack includes databases for services such as applications, URL categories, URL reputations, IP reputations, IDS and IPS signature definitions, firmware, and antivirus definitions for Versa Secure SD-WAN and Security Service Edge (SSE). For more information, see [SPack Services](#) below.

There are different types of SPacks, which are called flavors:

- Premium—Contains the complete antivirus, IDS, IPS, and URL filtering database. You can use this flavor for all security deployments.
  To install a premium SPack, a minimum of 8 GB of RAM is recommended, as the premium full package size ranges from 900 MB to 1.1 GB. If the amount of RAM is low, an error message displays during the installation. Note that you cannot install a premium SPack on two-core 4-GB VOS devices.
- Sample—Contains only important security configurations to load the features and contains a basic antivirus, IPS, and URL filtering database. The package size is less than 100 MB. The sample SPack database contains fewer signatures and is not recommended for unified threat management (UTM) deployments.

The SPack flavor depends on the type of software license subscription that you have. For more information, see [Licenses and Entitlement](#).

When you first deploy headend and branch network components, an SPack is preinstalled on a Versa Director node, which acts as the centralized patch and lifecycle management server. The Versa Managed Services team downloads, maintains, and installs SPacks for managed headends. For on-premise headends and private SASE deployments, enterprise administrators manage SPacks.

Versa Networks updates SPacks frequently and supports automatic updates. You can also update SPacks manually. Each update contains the latest signatures to protect against newly discovered threats. You should update the SPack regularly, and it is recommended that you use the automatic update. Updating the SPack has no operational impact on a running Director node or Versa Operating System^{TM} (VOS^{TM}) device.

SPack updates also include updates to the application identification library on VOS devices, which allow the application identification library to recognize additional applications. For more information, see [Upgrade the Application Engine Protocol Bundle](#) below.

This article defines the SPack services, describes how to download and install an SPack on the Director node, how to

upload an SPack, and how to configure SPack updates on VOS devices. It also describes how to install updates for the application identification library.

SPack Services

Note: Versa tests SPack updates only on VOS versions that are actively supported. Updating SPacks on EOS versions is not supported.

The following table provides information about the services in an SPack:

Service	Description	Database Update Frequency
Antivirus	Antivirus software receives information about supported file types and protocols from SPack, as well as database updates. SPack is updated for new malware database updates and these updates contain different hashes from all file types. Antivirus SDK contains different signatures to detect viruses and is periodically updated through SPack. Antivirus also receives security tags through SPack to allow certain application identifiers (AppIDs). For more information, see Configure Antivirus.	With each SPack release.
Application identifiers (AppIDs)	The AppID service uses application signatures that the SPack provides to identify applications.	Every three months (third-party database).
File filtering	File filtering service receives signatures to identify different file types. You use use file filtering to reduce the risk of attacks from unwanted and malicious files. For more information, see Configure File Filtering.	In case of specific code update.
IDS and IPS	Intrusion detection system (IDS) is the process of examining the network for indications of vulnerabilities and for detecting inappropriate or anomalous activity. Intrusion prevention system (IPS) is the process of stopping vulnerabilities by responding to	Weekly.

	inappropriate or anomalous activity. The IDS/IPS signature component in SPack updates signature files. These signatures are patterns that match known threats and enable IPS to identify and respond to security incidents in real time. This ensures that IPS remains up-to-date to effectively identify potential threats. IDS/IPS provides the following features: ◦ Threat prevention—IDS/IPS detects threats and actively blocks or mitigates them. On identifying a malicious activity, IPS takes immediate action, such as dropping harmful packets, blocking traffic, or resetting connections. ◦ Inline operation—IDS/IPS operates inline with the network traffic, that is, it controls the flow of data in real time. This allows it to prevent attacks before reaching the target. ◦ Signature- and anomaly-based detection—IDS/IPS uses a database of signatures or behavior-based rules to identify threats. You can also configure it to respond to specific types of attacks. For more information, see [Configure Intrusion Detection and Prevention](#).	
IP filtering	IP filtering performs IP address lookup in the SPack IP reputation database. The SPack database contains reputation and geo-location associated with specific IP addresses. As IP reputations change frequently, it is recommended that you use the	With each SPack release.

	latest SPack. If an access policy is associated with a predefined IP filtering profile or a user-defined reputation-based action profile, the latest SPack ensures proper enforcement profile actions. For more information, see [Configure IP Filtering](#).	
URL filtering	SPack enables lookup of any URL for category and reputation for URL filtering. SPack comprises the top one million URL categories and reputations from Versa feed. URL filtering uses URL reputation manager (URM) to answer cloud lookup request by sending these requests to urm.versanow.net. URM provides the following features: ◦ Supports load balancing for multi-region architecture based on latency. ◦ Supports IPv6. ◦ Provides caching abilities to enable faster response. For more information, see [Configure URL Filtering](#).	Continuous updates for URL-related intelligence.

Configure the SPack Download Parameters

You can download SPacks from an SPack cloud server. On the Director node, you can schedule when to download an SPack. You can update the full SPack, which downloads the full database repository, or you can perform an incremental update, which downloads only the updates from the last downloaded SPack to the latest one. When Versa Networks updates an SPack, the SPack server provides real-time updates, regardless of whether you have configured a full or an incremental download on the Director node.

You configure SPack download parameters to do the following:

- Define the URL from which to download SPacks
- Select a full download or an incremental update to the currently installed SPack
- Schedule a time to download an updated SPack

To configure the SPack download parameters:

1. For Releases 22.1.1 and later:

    a. In Director view, select the Administration tab in the top menu bar.

    b. Select Inventory > Software Images in the left menu bar.
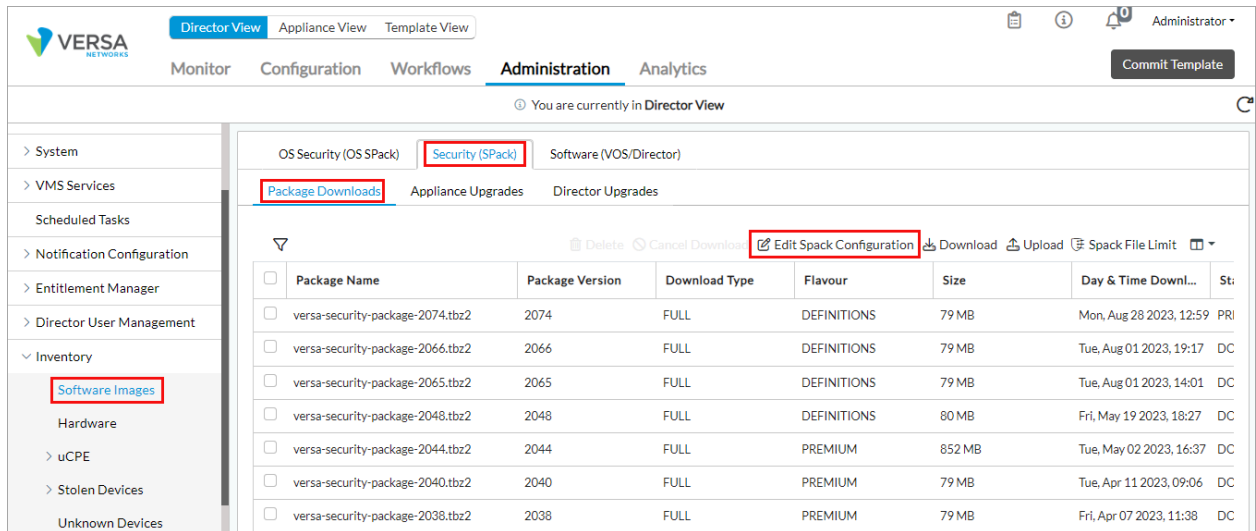
    c. Select the Security (SPack) tab, and then select the Package Download tab. The main screen displays the SPack files that have already been downloaded.

    d. Click Edit SPack Configuration. The Edit SPack Configuration popup window displays.

2. For Releases 21.2 and earlier:

    a. In Director view, select the Administration tab in the top menu bar.

    b. Select Inventory 📄 > Security Packages 🛡 in the left menu bar. The main screen displays the SPack files that have already been downloaded.
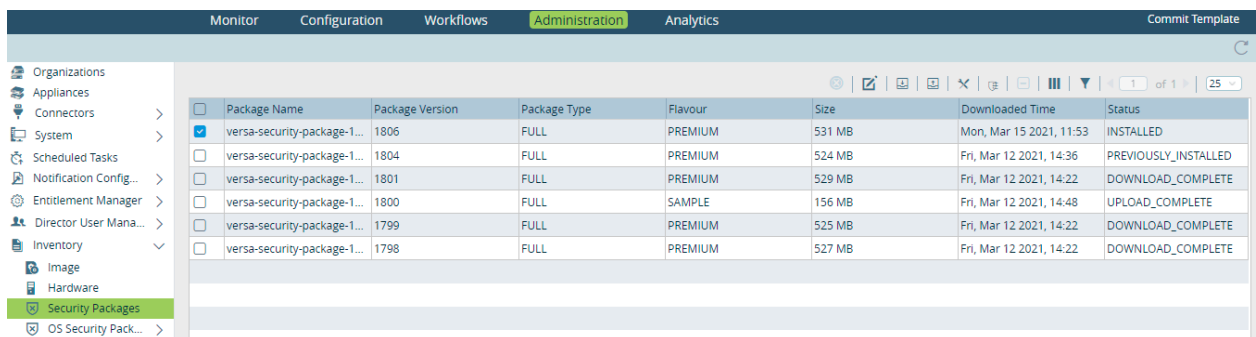
    c. Click the 📝 Edit icon to edit the preconfigured SPack configuration. The Edit SPack Configuration popup window displays.

3. In the Edit SPack Configuration popup window, enter information for the following fields.

Edit Security (S-Pack) Configuration ✕

URL *

> https://spack.versanetworks.com/versa-updates

Download Timeout   Download Type

> [   ]   Full   ⌄

Flavor

> Premium   ⌄

☑ Schedule Download

Start Time *   Interval (sec) *

> 01/08/2024 09:04:19 AM 📅   3600

OK   Cancel

Field	Description
URL	Enter the URL from which to download SPacks. Use the URL https://spack.versanetworks.com/versa-updates.
Download Timeout	Enter the time, in minutes, after which the download times out. *Range*: 300 through 3600 minutes (5 through 60 hours) *Default*: 300 minutes
Download Type	Select the type of SPack download: ◦ Full—Download the full database repository. A full download overwrites the SPack that is installed on the Director node. ◦ Incremental—Download only an update to the currently installed SPack. To determine whether an incremental update is available, check the release notes for the SPack version.
Flavor	(For Releases 21.1.1 and later.) Select the type of SPack database to download: ◦ Premium—Download an SPack database that contains the complete antivirus, IPS, and URL filtering database. You can use the premium SPack database for all security deployments. To install a premium SPack, a minimum of 8 GB of RAM is recommended. If the amount of RAM is low, an error message is displayed during the installation. Note that you cannot install a premium SPack on two-core 4-GB VOS devices. ◦ Sample—Download an SPack database that contains a basic antivirus, IPS, and URL filtering database. The sample SPack database contains fewer signatures, and it is not recommended for UTM deployments.
Schedule Download (Group of Fields)	Click to schedule a time at which to download SPacks. For Releases 20.2.3 and later, a scheduled download downloads the SPack and automatically installs it on the Director node at the scheduled time. To view information about the download and the Director update, click the Tasks icon in the horizontal

	menu bar. For more information, see View SPack Log Messages, below.
◦ Start Time	Enter the time at which to begin downloading the SPack.
◦ Interval	Enter a time interval after which the Director node attempts the next SPack download. This interval defines the time between two downloads. For example, if the interval is 900 seconds, the Director node attempts the next SPack download after 15 minutes. *Default*: 900 seconds (for Releases 21.2.1 and later) *Range*: 0 to 4294967295 seconds *Recommended Value:* It is recommended that you configure an interval of 900 seconds or greater.

4. Click OK.

When an SPack download completes successfully, the Status column in the main pane displays the status DOWNLOAD_COMPLETE.

Set the SPack File Limit

When you schedule an SPack download to a Director node, the Director node retains the last five SPacks by default. When this limit is reached, the Director node deletes the oldest SPack.

To change the number of SPacks that the Director node retains:

1. For Releases 22.1.1 and later:
   a. In Director view, select the Administration tab in the top menu bar.
   b. Select Inventory > Software Images in the left menu bar.
   c. Select the Security (SPack) tab, and then select the Package Download tab.

	Package Name	Package Version	Download Type	Flavour	Size	Day & Time Downl...	St
☐	versa-security-package-2074.tbz2	2074	FULL	DEFINITIONS	79 MB	Mon, Aug 28 2023, 12:59	PRI
☐	versa-security-package-2066.tbz2	2066	FULL	DEFINITIONS	79 MB	Tue, Aug 01 2023, 19:17	DC

    d. Click SPack File Limit. The Set SPack File Limit popup window displays.

2. For Releases 21.2 and earlier:

    1. In Director view, select the Administrator tab in the top menu bar.

    2. Select Inventory 🗎 > Security Package ⊗ in the left menu bar.

    3. Click the ⊞ SPack File Limit icon. The Set SPack File Limit popup window displays.

3. In the Set SPack File Limit popup window, enter the maximum number of SPacks to retain on the Director node. The default is 5. You configure the file limit to be any value, but keep in mind the memory availability on the Director node.

4. Click OK.

Manually Download an SPack to the Director Node

Note that to download an SPack manually from a cloud server to the Director node, the Director node must have access to the internet.

For Releases 21.2.1 and later, you can upload an SPack file that you have downloaded to your computer.

For Releases 21.1.1 and later, a VOS device supports fully qualified domain names (FQDNs) and IP addresses advertised by SaaS providers. These FQDNs and IP addresses are installed as part of the SPack and are updated periodically as part of SPack updates.

To download an SPack manually from a cloud server to the Director node:

1. For Releases 22.1.1 and later:

    a. In Director view, select the Administration tab in the top menu bar.

    b. Select Inventory > Software Images in the left menu bar.

    c. Select the Security (SPack) tab, and then select the Package Downloads tab.

    d. Click Download. The Download Security Package popup window displays.

2. For Releases 21.2 and earlier:

    a. In Director view, select the Administration tab in the top menu bar.

    b. Select the Inventory 📄 > Security Package 🛡️ in the left menu bar.

    c. Click the 🔽 Download icon. The Download Security Package popup window displays.

3. In the Download Security Package popup window, in the Package field, select the SPack version to download to the Director node. The list displays all the SPack versions that are available to download.
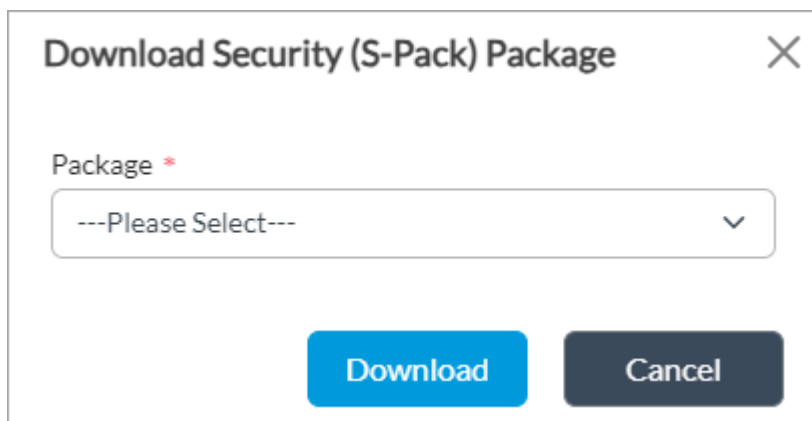
4. Click Download to start downloading the SPack to the Director node.

When the SPack download completes successfully, the Status column in the main pane displays the status DOWNLOAD_COMPLETE.

Manually Download an SPack without a Director Node

If the Director node is installed in a closed environment that does not have access to the internet, you can manually

download an SPack to your system using a browser or by issuing a shell command.

Note: To download the SPack, you must use the exact SPack version number.

To download an SPack from the shell on a Linux or MacOS system, issue the following command. In the example below, 2119 is the SPack version number. Either type the command on a single line or use a backslash (\) to indicate that the command continues on the next line.

```
wget \
'https://spack.versanetworks.com/versa-updates?action=download-spack-version-ex&current-api-
version=11&current-version=2119&flavor=premium' \
-O 'versa-security-package-2119.tbz2'
```

To download an SPack using a web browser:

1. Copy the following line into the URI field of the browser. In this example, the SPack version number is 2119.

```
https://spack.versanetworks.com/versa-updates?action=download-spack-version-ex&current-api-
version=11&current-version=2119&flavor=premium
```

2. When the browser prompts you to choose a filename, enter the name versa-security-package-2119.tbz2.

Manually Upload an SPack

For Releases 21.2.1 and later.

You can download an SPack to a local computer and then manually upload it to a Director node. One case to do this is when the Director node does not have internet access. The SPack filename must start with the string versa-security-package and the filename extension must be .tbz2. If you are also uploading an SPack checksum file, the filename must start with the string versa-security-package, and the filename extension must be .sha1.

To upload an SPack manually from a local computer to the Director node:

1. For Releases 22.1.1 and later:
   a. In Director view, select the Administration tab in the top menu bar.
   b. Select Inventory > Software Images in the left menu bar.
   c. Select the Security (SPack) tab, and then select the Package Downloads tab.

   d. Click Upload. The Upload Security Package popup window displays.

2. For Releases 21.2 and earlier:

    a. In Director view, select the Administration tab in the top menu bar.

    b. Select the Inventory 🗎 > Security Package 🛡 in the left menu bar.

    c. Click the ⬆ Upload icon. The Upload Security Package popup window displays.

3. Enter information for the following fields.

Field	Description
Upload Type	Select the type of SPack to upload. Ensure that you select the same type as the SPack file that you want to upload. ◦ Full—Download the full database repository. A full download overwrites the SPack that is installed on the Director node. ◦ Incremental—Upload only an update to the currently installed SPack. To determine whether an incremental update is available, check the release notes for the SPack version.
Flavor	Select the type of SPack database to download. Ensure that you select the same flavor as the SPack file that you want to upload. ◦ Premium—Upload an SPack database that contains the complete antivirus, IPS, and URL filtering database. You can use the premium SPack database for all security deployments. To install a premium SPack, a minimum of 8 GB of RAM is recommended. If the amount of RAM is low, an error message is displayed during the installation. Note that you cannot install a premium SPack on two-core 4-GB VOS devices. ◦ Sample—Upload an SPack database that contains a basic antivirus, IPS, and URL filtering database. The sample SPack database contains fewer signatures, and it is not recommended for UTM deployments.
Upload Security (SPack)File	Click Browse File, and then select the SPack file to upload from the local computer. Note that filename must start with the string versa-security-package and the filename extension must be .tbz2.
Upload Checksum File	Click Browse File, and then select the checksum file for the SPack to upload from the local computer. The filename must start with the string versa-security-package, and the filename extension must be .sha1

4. Click Upload.

To display information about the manual SPack upload, click the Tasks icon in the horizontal menu bar. For more information, see View SPack Log Messages, below.

Install an SPack on a VOS Device

For Releases 22.1.1 and later.

1. In Director view, select the Administration tab in the top menu bar.
2. Select Inventory > Software Images in the left menu bar.
3. Select the Security (SPack) tab, and then select the Upgrade Appliances tab.

4. Select the VOS device or devices on which to install the SPack, or select the box to the left of the Appliance Name column to select all devices. The Package Version column in the table displays the current SPack version installed on each device.
5. Click Upgrade Appliances. The Upgrade Appliances Security Package popup window displays. Enter information for the following fields.

Field	Description
Download Type (Required)	Select the type of package to download: ◦ Full—Select a new SPack. Select this option if an SPack is not alrea ◦ Incremental—Select to upgrade the SPack on the VOS device.
Flavor	Select the type of SPack database to download: ◦ Premium—Download an SPack database that contains the complete can use the premium SPack database for all security deployments. T of RAM is recommended. If the amount of RAM is low, an error mess that you cannot install a premium SPack on two-core 4-GB VOS dev ◦ Sample—Download an SPack database that contains a basic antivir sample SPack database contains fewer signatures, and it is not reco
Security Package (SPack) Version (Required)	Select the the SPack from the list of downloaded SPacks. The list displa
Schedule Upgrade	Click to schedule a date and time for the upgrade to occur. Enter the date and enter the time in the format *hh*:*mm*:*ss* (hours:minutes:seconds, using
Selected Appliances	Displays the device or devices that you selected to upgrade.

6. Click Upgrade. If you have not set a schedule for the upgrade, the SPack upgrade occurs immediately.

Install an SPack on a VOS Device for Releases 21.2.1 and Earlier

1. In Director view, select the Administration tab in the top menu bar.

2. Select the Inventory 📄 > Security Package 🛇 in the left menu bar.

3. In the main pane, check the Package Version and Status to identify the last downloaded SPack.

4. Select the last downloaded SPack. You can also download an older SPack

5. Click the ✖ Install icon. In the Install Security Package popup window, enter information for the following fields.

Field	Description
Package	Displays the SPack version that you selected in the main pane. This is the SPack to be installed.
Appliance	Select the VOS device on which to install the SPack. You can select multiple devices.
Update Director	Click to install the downloaded SPack version on the Director node.

6. Click Install to initiate the SPack installation.

Install an SPack on a Director Node

For Releases 22.1.1 and later.

1. In Director view, select the Administration tab in the top menu bar.
2. Select Inventory > Software Images in the left menu bar.
3. Select the Security (SPack) tab, and then select the Director Upgrades tab. The Current Version box displays information about the SPack that is currently installed on the Director node.
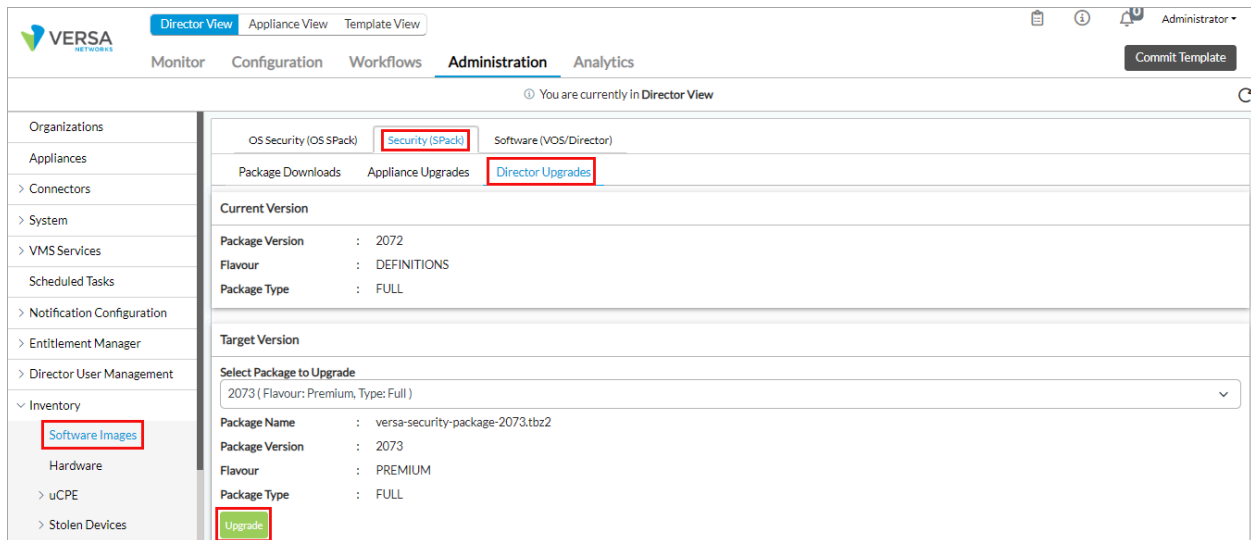
4. Select the package to which to upgrade the Director node to in the Select Package to Upgrade under Target Version field.

5. Click Upgrade.

Configure Automatic SPack Updates

On a VOS device, you can configure SPack updates to occur automatically, either at a regularly scheduled time or once at a specific time (called a real-time update).

To configure automatic SPack updates on a VOS device:

1. In Director view:
   a. Select the Configuration tab in the top menu bar.
   b. Select Devices > Devices in the horizontal menu bar.
   c. Select a VOS device in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Others > System > Security Package Update in the left menu bar. The main pane displays the automatic security update settings for the VOS device.

4. Click the ✎ Edit icon. In the Add/Edit Automatic Security Update Setting popup window, enter information for the fields.

Edit Automatic Security Update Setting ✕

Common Settings

URL

https://spack.versanetworks.com/versa-updates

Download Timeout | Routing Instance
300 | --Select-- ⌄

Flavor Type

Premium ⌄

☐ **Scheduled Update**

Start Time | Download Type
HH:MM:SS | Incremental ⌄

Interval

☐ **Realtime Update**

Start Time | Interval (seconds)
HH:MM:SS |

OK   Cancel

Field	Description
Common Settings (Group of Fields)	
◦ URL	Enter the URL of the server from which to download the SPack.
◦ Download Timeout	Enter the time, in minutes, after which the download times out.
◦ Routing Instance	Select the routing instance to use to reach the SPack server.
◦ Flavor Type	Select the type of SPack database to download: ◦ Premium—Download an SPack database that contains the complete antivirus, IPS, and URL filtering database. You can use the premium SPack database for all security deployments. To install a premium SPack, a minimum of 8 GB of RAM is recommended. If the amount of RAM is low, an error message is displayed during the installation. Note that you cannot install a premium SPack on two-core 4-GB VOS devices. ◦ Sample—Download an SPack database that contains a basic antivirus, IPS, and URL filtering database. The sample SPack database contains fewer signatures, and it is not recommended for UTM deployments.
Scheduled Update (Group of Fields)	Click to schedule a regular, periodic SPack update. When you select this option, if a new SPack is available, it is downloaded and installed automatically. Updating the SPack regularly ensures that it is always up to date and so can protect the VOS devices from the latest threats.
◦ Start Time	Enter the time at which to first check whether an SPack update is available.
◦ Download Type	Select the type of download: ◦ Full—Download the complete SPack. A full download overwrites the SPack that is installed on the VOS device. It is recommended that you configure a full download. ◦ Incremental—Download only an update to the currently installed SPack. Incremental updates are possible only in some cases, depending on

	the SPack version. If an incremental update from the installed SPack to the latest SPack is not supported, the VOS device automatically performs a full update, to download the complete SPack and to overwrite the SPack that is currently installed on the VOS device. To determine whether an incremental update is available, check the release notes for the SPack version.
◦ Interval	Enter how often to check whether a new security package is available. You can specify the interval in months, days, hours, minutes, and seconds. Note that a month is treated as 30 days.

Edit Automatic Security Update Setting ✕

Premium ⌄

☑ **Scheduled Update**

Start Time | Download Type
HH:MM:SS | Full ⌄

Interval

Months	00
Days	01
Hours	00	nterval (seconds)
Minutes	00
Seconds	00

OK

OK   **Cancel**

The following examples illustrate when the VOS device checks for the availability of a new security package:

- Start Time: 02:00:00, Interval: 1 day—VOS device checks for SPack updates at 2 a.m. every day, and if one is available, automatically updates to the newer SPack version.
- Start Time: 22:00:00, Interval: 1 month—VOS device checks for SPack updates at 10 p.m. every 30 days, and if one is available, automatically updates to the newer SPack

	version. So, if you enable the automatic SPack update on the 7th of the month, let's say, April 7, the first check for an SPack version update happens at 10 p.m. on April 7, the next check happens at 10 p.m. on May 7, and so forth.
Real-Time Update (Group of Fields)	Click to schedule an SPack update at a specific time. Real-time updates ensure that critical updates are downloaded to the VOS device before the next SPack upgrade is available to be downloaded.
◦ Start Time	Enter the time at which to perform the real-time SPack update.
◦ Interval	Enter a time interval, in seconds, after which the VOS device again attempts to download the SPack if an earlier download attempt fails. *Range:* 900 through 86390 seconds (15 minutes through just under 24 hours)

5. Click OK.

Upgrade the Application Engine Protocol Bundle

For Releases 21.2.1 and later.

The application engine protocol bundle, also known as the application identification library (AIL), is a database that contains signatures to detect and identify more than 4700 applications. The application identification library is provided as part of the VOS software and is preinstalled on each Versa branch CPE device.

Updates to the application identification library on VOS devices are provided in security pack (SPack) updates. The updates allow the application identification library to recognize additional applications.

Note that application identification library updates are not installed automatically as part of the SPack upgrade or as part of a VOS software upgrade. You must manually upgrade the library. The upgrade affects the operation of the VOS device, because after you upgrade the library, you must restart the services on the VOS device.

To upgrade an application engine protocol bundle:

1. In Director view:
    1. Select the Configuration tab in the top menu bar.
    2. Select Templates > Device Templates in the horizontal menu bar.
    3. Select a device name in the main panel. The view changes to Appliance view.

2. Select Administration in the top menu bar.

3. Select Organization > Security Package in the left menu bar.
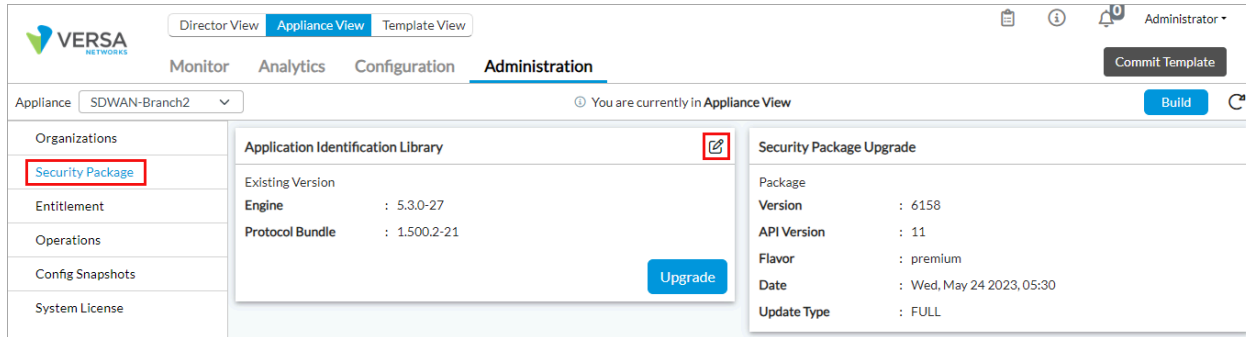
4. In the Application Identification Library pane, click the Edit ✎ icon. The Upgrade Protocol Bundle popup window displays.
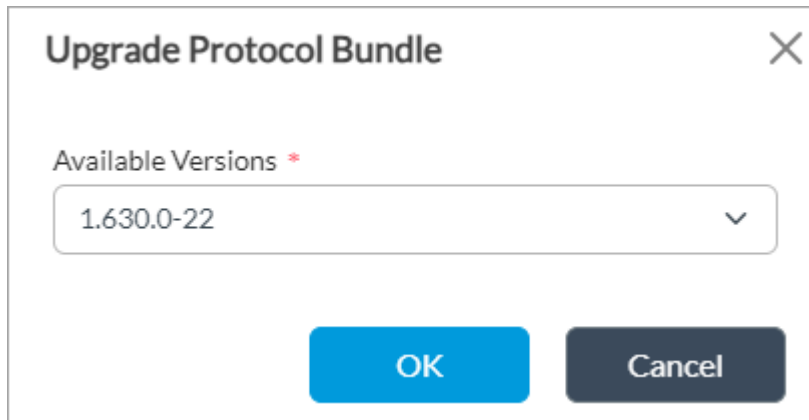
5. Select the protocol bundle to which to upgrade.

6. Click OK. The Application Identification Library table displays the new version.
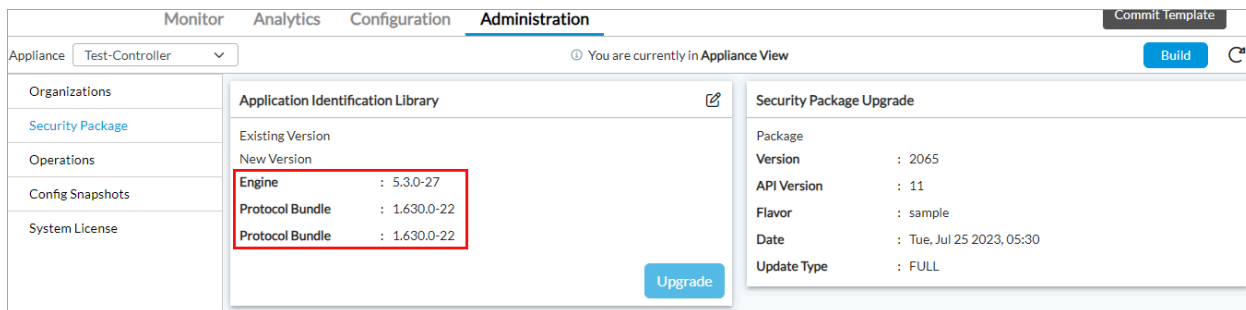
7. Click Upgrade. The following message displays, indicating that when you upgrade the protocol bundle, the Versa services are restarted.

Upgrade Protocol Bundle

Are you sure you want to upgrade? Appliance services will be restarted.

[Confirm] [Cancel]
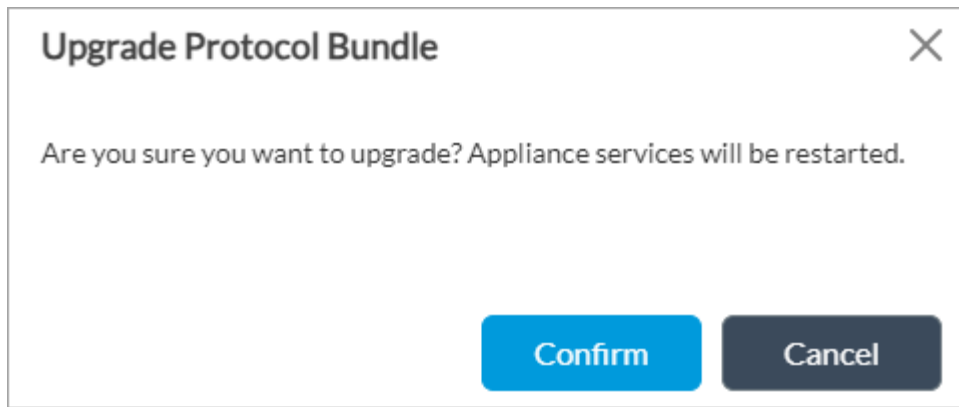
8. Click Confirm to upgrade the protocol bundle.

View Application Engine Protocol Bundle Information

You can view the following information related to the application engine protocol bundle:

- Bundle version at both the provider and tenant level
- Currently installed version
- Appliances that match the selected bundle version

To view information related to the application engine protocol bundle:

1. In Director view, select the Monitor tab in the top menu bar.
2. Select a provider organization in the left menu bar to display provider-level information. The following screen displays.

Asset Summary			VIEW DETAILS
CATEGORY	UP	DOWN	TOTAL
SDWAN Branches	2	0	2
SDWAN Controllers	1	0	1
Hub Controllers	0	0	0
Router Firewalls	0	0	0
SDWAN Hubs	0	0	0
uCPEs	0	0	0
Sub Organizations	-	-	5
Directors	-	-	1
Analytics Cluster	-	-	0

Recent Events   VIEW DETAILS

CRITICAL	MAJOR	MINOR
1	0	0

INDETERMINATE	WARNING
0	0

Refresh every 5 minutes

Provider Health			
CATEGORY	UP	DOWN	DISABLED
Config Sync Status	2	1	0
Reachability Status	2	1	0
Service Status	1	2	0
Interfaces	21	2	0
BGP Adjacencies	42	6	0
IKE Status	24	-	0
Paths	96	0	0

System Summary	
Hardware Information	3
Software Version	2
Hardware Model	1
Security Packages	2
OS Security Packages	2
App ID Protocol Bundle Version	2

Services	
SFW	1
SDWAN	18
NGFW	12
IPsec	10
CGNAT	12
Secure Access	10

3. To view tenant-level information, select a tenant in the left menu bar. The following screen displays.

4. In the System Summary pane, click AppID Protocol Bundle Version. The screen displays the currently installed version, along with the number of devices on which that version is installed. In the screenshot below, Version 1.500.2-21 is installed on two devices.

5. Click the version number to display the devices on which that version is installed, or click Back to return to the previous screen.

View SPack Information

To view information about the SPack, including the version, type (flavor), and download type:

1. In Director view:

    a. Select the Administration tab in the top menu bar.

    b. Select Appliances in the left menu bar.

    c. Select a device name in the main panel. The view changes to Appliance view.

2. Select Organizations > Security Package in the left menu bar. The Security Package Upgrade pane displays information about the installed SPack version.

To display information about the SPack from the CLI, issue the following command:

```
admin@Branch-cli> show security security-package information
```

For example:

```
admin@Branch-cli> show security security-package information
Version          1988
API Version      11
Flavor           premium
Release Date     2022-09-19
Update Type      full
```
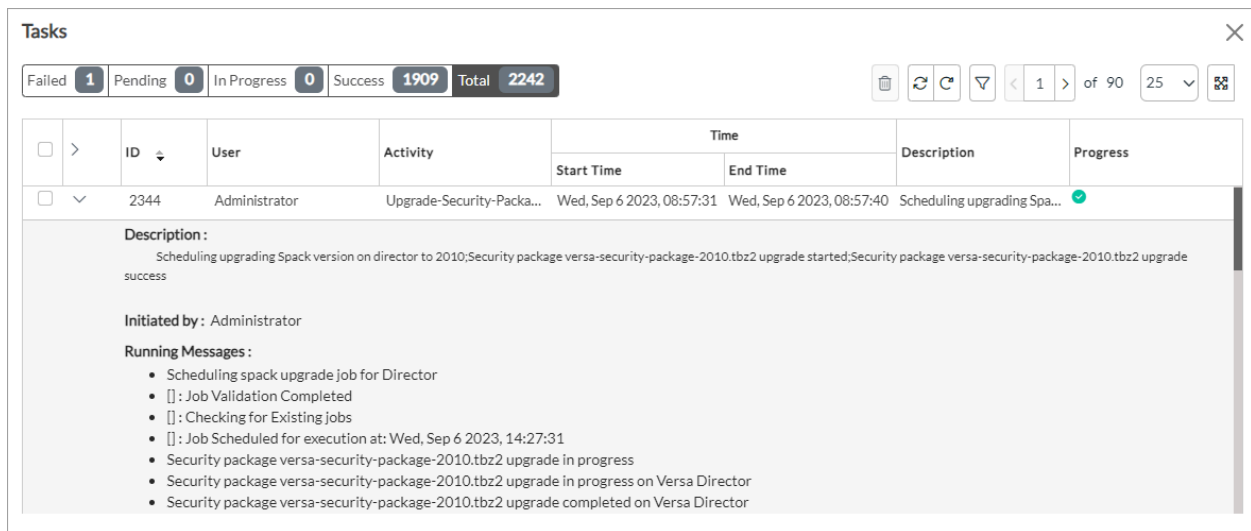
View SPack Log Messages

To check SPack download and install log messages:

1. In Director view:

    a. Select the Administration tab in the top menu bar.

    b. Select Appliances in the left menu bar.

    c. Select a device name in the main panel. The view changes to the Appliance view.

2. Click the [icon] Tasks icon in the horizontal menu bar.
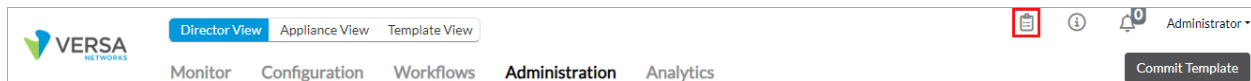
3. The Tasks popup window displays. This window lists all SPack download tasks, including failed, pending, in progress, successful, and total number of tasks.

The following sample output shows the status of the scheduled SPack download:

The following sample output shows the status of of a scheduled upgrade to the Director node:

The following sample output shows the status of a manual SPack upload:

Supported Software Information

Releases 20.2 and later support all content described in this article, except:

- Releases 20.2.3 adds support for scheduled SPack downloads the SPack and automatically installing the SPack on the Director node.

- Releases 21.1.1 supports VOS devices dynamically querying and downloading the FQDNs and IP addresses advertised by SaaS providers; you can upgrade the application engine protocol bundle and manually upload an SPack file from your computer.

- Release 21.2.1 allows you to upload an SPack file that you have downloaded in your computer and upgrade an application engine protocol bundle; adds default interval for scheduled SPack download.

- Release 22.1.1 moves the SPack GUI to > Software Images > Security (SPack) tab; you can upgrade a Director node from the Director Upgrades tab.

Additional Information

Licenses and Entitlement
Use OS Security Packages