
Configure Layer 7 Objects



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

When users connect to the network from a fixed location and access resources using specific port numbers, firewalls can use IP addresses and port numbers to enforce policies. However, with wireless networking and mobile devices, a user can connect to the network from multiple devices simultaneously, and it is no longer practical to identify a user, an application, or a device based on a static IP address and port number.

You can use Layer 7 application identification, sometimes referred to as AppID, to identify users, applications, and devices. Application identification identifies applications at different network layers based on the protocol rather than based on the IP address and port number. Because application identification does not depend on port number to identify an application, it can detect applications even on non-standard ports.

Application identification applies an application signature to traffic that is allowed by a security policy. The application signature, which is based on the application's properties and its transaction characteristics, allows the Versa Operating System™ (VOS™) device to identify the application.

Application identification provides an effective detection capability for evasive applications such as Facebook, Skype, Torrent, and WhatsApp.

To configure application identification, you configure application objects on VOS devices. The VOS software provides predefined application objects for a variety of application categories, each with risk levels and productivity ratings. You can also configure custom application objects. In NGFW security access policies (also called access lists, or ACLs) and in SD-WAN policies, you can reference application objects so that the policies can identify network applications, verify traffic against the security policy, and then allow only the desired traffic on the network.

You use both application objects and URL filtering to provide security for network applications based on risk level. In NGFW security access policies and in SD-WAN policies, you can define match criteria based on Layer 7 information, such as the application, and based on URL categories. (Note that NGFW can use Layer 2 through Layer 7 policies.) In these policies, you can use both predefined and custom application objects.

This article describes how to view predefined applications objects and how to configure the following Layer 7 objects:

- Custom application signature objects
- Custom application group objects
- Custom application filter objects

- Predefined application objects with customized attributes
- Custom URL category objects

Risk Levels in Application Signatures

Each application has an application signature that identifies the risk assigned to the application by the Versa Networks security research team. The risks are grouped into five levels, with Level 1 being the lowest risk and Level 5 being the highest risk. On configuration and monitoring screens, each risk level is identified by a number in a colored box.

The following table describes the risk levels.

Risk Level	Box Color	Description
1 (lowest risk)	Green	<ul style="list-style-type: none"> • Business-based SaaS applications • Business systems • Databases • Email • ERP applications • ICS protocols • Internet utilities • Medical protocols, such as DICOM • Networking (at the protocol level) • Office programs • Software updates • VoIP • VPN tools
2	Blue	<ul style="list-style-type: none"> • Audio streaming • Authentication services • Backup and restore applications • Collaboration application • Conferencing applications • Remote-access tools • Social business applications, such as Amazon

Risk Level	Box Color	Description
		<ul style="list-style-type: none"> • Software development applications • Well-known games
3	Yellow	<ul style="list-style-type: none"> • Neutral; default Versa values
4	Orange	<ul style="list-style-type: none"> • Instant-messaging applications • Online internet conferencing tools • Photo and video sharing • Proxy applications • Social networking applications
5 (highest risk)	Red	<ul style="list-style-type: none"> • File-sharing applications

View Predefined Application Signatures




The Versa Networks Security Research team defines all predefined application service objects. VOS devices currently support approximately 4,500 application signatures (also called application service objects or application objects), which include specific applications or SaaS groups of applications for cloud providers. The predefined service objects and application signatures are updated regularly through the Versa security package (SPack) updates, and you can update them at any time, by installing the latest SPack. Installing an SPack has no impact to operation of the Director nodes and VOS devices. For more information, see [Use Security Packages](#).

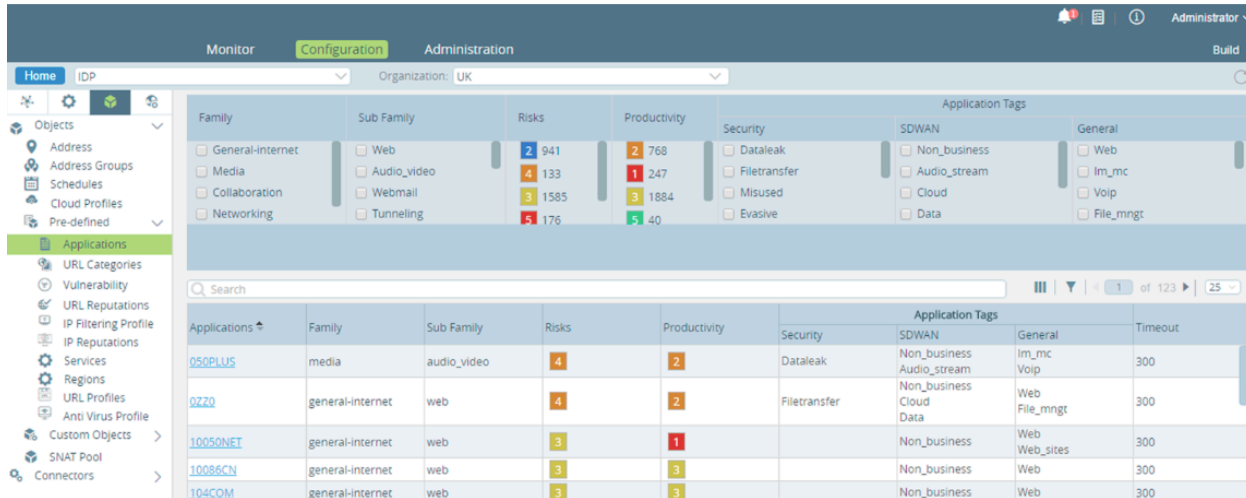
To provide feedback for adding modifying the predefined objects, send email to support@versa-networks.com.

If the predefined applications do not meet your requirements, you can define custom application signatures, as discussed in [Create a Custom Application Signature](#) below.

To display the predefined application service objects and application signatures:

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 device in the main pane. The view changes to Appliance view.

- d. Or, select the Administration tab in the top menu bar, select Appliances in the left menu bar, and select a device in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Objects & Connectors  > Objects  > Predefined Objects  > Applications in the left menu bar. The Application dashboard displays. It lists various attributes of each application definition, including the application's relative security risk and productivity rating, the tags that you can apply for each of the application by assigning a security type, SD-WAN attributes, and general attribute.



Family	Sub Family	Risks	Productivity	Security	SDWAN	General
General-Internet	Web	2 941	2 768	Dataleak	Non_business	Web
Media	Audio_video	4 133	1 247	Filetransfer	Audio_stream	Im_mc
Collaboration	Webmail	3 1585	3 1884	Misused	Cloud	Voip
Networking	Tunneling	5 176	5 40	Evasive	Data	File_mngt

Applications	Family	Sub Family	Risks	Productivity	Security	SDWAN	General	Timeout
050PLUS	media	audio_video	4	2	Dataleak	Non_business Audio_stream	Im_mc Voip	300
0ZZ0	general-Internet	web	4	2	Filetransfer	Non_business Cloud Data	Web File_mngt	300
10050NET	general-Internet	web	3	1		Non_business	Web Web_sites	300
10086CN	general-Internet	web	3	3		Non_business	Web	300
104COM	general-Internet	web	3	3		Non_business	Web	300

For information about configuring predefined and custom application signatures, see [Configure Security Access Policy Rules](#).

Configure Custom Application Objects

To create custom application objects and signatures, you create a customer application signature for a tenant, and then you create an IPS signature to identify the custom application.

Create a Custom Application Signature

You can create custom application signatures on a per-tenant basis. This means that multiple tenants can define an application object that have the same application name, but that have different signatures, and vice versa.

You can use custom application objects multiple times in the configuration, such as when you define application group objects and NGFW policy rules.





When you configure an application filter object based on application attribute match information, the application filter matches both predefined and custom applications, based on the application attributes. For more information, see [Configure Security Access Policy Rules](#).

To create a custom application signature:

https://docs.versa-networks.com/Secure_SD-WAN/01_Configuration_from_Director/Security_Configuration/Configure_Layer_...

Updated: Wed, 23 Oct 2024 08:19:34 GMT

Copyright © 2024, Versa Networks, Inc.

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 device in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Objects & Connectors  > Objects  > Custom Objects  > Applications in the left menu bar.
4. Click the  Add icon. In the Add Application window, enter information for the following fields.

Add Application
✕

Name *

Description *

Precedence *
Application Timeout (sec)
☐ App Match IPs

Attributes
Match Information

Family	Sub-Family	Risk	Productivity	Application Tags		
				Security	SDWAN	General
<input checked="" type="radio"/> Business-syste...	<input checked="" type="radio"/> Antivirus	<input checked="" type="radio"/> 1	<input checked="" type="radio"/> 1	<input type="checkbox"/> Anonymizer	<input type="checkbox"/> Audio_stream	<input type="checkbox"/> Aaa
<input type="radio"/> Collaboration	<input type="radio"/> Application-se...	<input type="radio"/> 2	<input type="radio"/> 2	<input type="checkbox"/> Bandwidth	<input type="checkbox"/> Business	<input type="checkbox"/> Adult_content
<input type="radio"/> General-intern...	<input type="radio"/> Audio_video	<input type="radio"/> 3	<input type="radio"/> 3	<input type="checkbox"/> Dataleak	<input type="checkbox"/> Cloud	<input type="checkbox"/> Advertising
<input type="radio"/> Media	<input type="radio"/> Authentication...	<input type="radio"/> 4	<input type="radio"/> 4	<input type="checkbox"/> Evasive	<input type="checkbox"/> Data	<input type="checkbox"/> Analytics
<input type="radio"/> Networking	<input type="radio"/> Behavioral	<input type="radio"/> 5	<input type="radio"/> 5	<input type="checkbox"/> Filetransfer	<input type="checkbox"/> Non_business	<input type="checkbox"/> Anonymizer
	<input type="radio"/> Compression			<input type="checkbox"/> Malware	<input type="checkbox"/> Video_stream	<input type="checkbox"/> Audio_chat
	<input type="radio"/> Database			<input type="checkbox"/> Misused		<input type="checkbox"/> Basic
	<input type="radio"/> Encrypted			<input type="checkbox"/> Tunnel		<input type="checkbox"/> Blog
				<input type="checkbox"/> Vulnerable		<input type="checkbox"/> Cdn

OK
Cancel

Field	Description
Name	Enter a name for the application.
Description	Enter a text description for the application.
Precedence	Enter a unique priority number to use when multiple applications match the traffic. The application with a higher precedence value is matched first.
Application Timeout	Enter how long to wait, in seconds, for the application to timeout because of inactivity.
Application Match IPS	Click to enable the matching of applications using an IPS signature.

5. Select the Attributes tab, and enter information for the following fields.

Field	Description
Family	Select the application's family type.
Subfamily	Select the application's subfamily.
Risk	Click to assign a risk level to the application. For more information, see Risk Levels in Application Signatures , above.
Productivity	Click to assign a productivity value to the application. Red (1) indicates the lowest productivity value, and green (5) indicates the highest productivity value.
Application Tags	Click to assign a tag to the application for classification purposes: <ul style="list-style-type: none"> ◦ General ◦ SD-WAN ◦ Security

6. Select the Match Information tab, and then click to choose the match criteria information for the application. In the Add Match Information window, enter information for the following fields.

Field	Description
Name	Enter a name for the match rule name for the custom application.
Host Pattern	Enter the host pattern to detect.
Protocol Value	Enter the applications protocol value to detect.
Source Address	Enter the source IP address of the application on which the rule is applicable.
Destination Address	Enter the destination IP address of the application on which the application rule is applicable.
Source Port	<p>Click to enable, and assign a custom source port for the application:</p> <ul style="list-style-type: none"> ◦ Range—Select to enable the Low and High fields, and then enter the lowest and highest source port numbers on which the security policy is applicable. ◦ Value—Select to enable the Source Port Value field, and then enter the application port on which the security policy is applicable.
Destination Port	<p>Click to enable, and assign a custom destination port for the application:</p> <ul style="list-style-type: none"> ◦ Range—Select to enable the Low and High fields, and then enter the lowest and highest destination port numbers on which the security policy is applicable. ◦ Value—Select to enable the Source Port Value field, and then enter the application port on which the security policy is applicable.

7. Click OK.

Create an IPS Signature To Identify a Custom Application

To identify a custom application, the IPS signature must include the following

- <classtype:aap-id;>.
- <pktnum:[<|>]number;>—pktnum has a format similar to the dsize keyword. Use pktnum to restrict IPS to detect the application in the first few packets of the session.





- <appid:app_name;> keyword,—app_name must match the name of the custom application. For example, if the custom application name is enterprise-internal-1, configure appid as appid:enterprise-internal-1
- <versa_parent_appid;> keyword—The value for this keyword is the application reported by the Qosmos engine or VOS device. This keyword helps to identify the application in appid. For example, if the custom application name is enterprise-internal-1 and the application reported by Versa appliance without your custom signature is http, in the custom signature, configure versa_parent_appid as versa_parent_appid:http and the appid as appid:enterprise-internal-1.

Configure Custom Application Group Objects

To simplify the creation of security policy, you can group applications that require the same security settings into an application group.

You can create custom application group objects on a per-tenant basis. You can associate a custom application group with one or more predefined or custom applications. You can use a custom application group in NGFW and SD-WAN policy rules to specify match criteria for Layer 7 applications.

To create a custom application group:

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 in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Objects & Connectors  > Objects  > Custom Objects  > Application Group in the left menu bar
4. Click the  Add icon. In the Add Application Group popup window, enter information for the following fields.

Add Application Group [X]

Name *

Description

Tags

☐ **Applications *** [Add] [Remove] [Search]

-
-
-
-
-

OK **Cancel**

Field	Description
Name	Enter a name for the application group. This name appears in the application list when you define the security policy.
Description	Enter a text description of the application group.
Tags	Enter a keyword or phrase to use to filter the application group.
Applications	Click the Add icon, and select from the predefined and custom applications.

- Click OK.

Configure Custom Application Filter Objects






You can create custom application filter objects on a per-tenant basis. You can associate a custom application filter with one or more filter conditions that match information based on the attributes of a predefined or custom application. You can use a custom application filter objects in NGFW and SD-WAN policy rules to specify match criteria for Layer 7 application.

To create a custom application filter:

https://docs.versa-networks.com/Secure_SD-WAN/01_Configuration_from_Director/Security_Configuration/Configure_Layer_...

Updated: Wed, 23 Oct 2024 08:19:34 GMT

Copyright © 2024, Versa Networks, Inc.

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 in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Objects & Connectors  > Objects  > Custom Objects  > Application Filters  in the left menu bar
4. Click the  Add icon. In the Add Application Filter popup window, enter information for the following fields.

Add Application Filter

Family

☐ Business-system
 ☐ Collaboration
 ☐ General-Internet

Sub Family

☐ Antivirus
 ☐ Application-service
 ☐ Audio_video

Risks

230 1 938 2 1187 3 133 4 176 5

Productivity

247 1 760 2 1493 3 124 4 40 5

Application Tags - Security

☐ Anonymizer
 ☐ Bandwidth
 ☐ Dataleak

Application Tags - SDWAN

☐ Audio_stream
 ☐ Business
 ☐ Cloud

Application Tags - General

☐ Aaa
 ☐ Adult_content
 ☐ Advertising

Name *
Description

NO FILTERS SELECTED

Applications	Family	Sub Family	Risks	Productivity	Application Tags		
					Security	SDWAN	General
01NET	general-inter...	web	2	2		Non_business	Web
050PLUS	media	audio_video	4	2	Dataleak	Audio_stream Non_business	Im_mc Voip
0ZZ0	general-inter...	web	4	2	Filetransfer	Cloud Data Non_business	File_mngt Web
10050NET	general-inter...	web	3	1		Non_business	Web Web_sites
10086CN	general-inter...	web	3	3		Non_business	Web
104COM	general-inter...	web	3	3		Non_business	Web
1111TW	general-inter...	web	3	1		Non_business	Web
114LA	general-inter...	web	3	3		Non_business	Web

OK

Cancel




Field	Description
Name	Enter a name for the application filter name. This name appears in the application list when you define the security policy.
Description	Enter a text description of the application filter.
Family	Select the application's family type.
Subfamily	Select the application's subfamily.
Risk	Click to assign a risk level to the application. For more information, see Risk Levels in Application Signatures , above.
Application Tags	Click to assign a tag to the application for classification purposes: <ul style="list-style-type: none"> ◦ General ◦ SD-WAN ◦ Security

5. Click OK.

Configure Attributes of Predefined Application Objects

The Versa security research team creates predefined applications with associated attribute information, such as family, subfamily, risk, productivity, and tags. To customize the predefined attribute information, you can override the attribute information on a per-tenant basis. For example, on a given VOS device, you can tag the Skype application as business traffic for one tenant and as non-business traffic for another tenant.

To configure the attributes of a predefined application object:

- In Director view:
 - Select the Administration tab in the top menu bar.
 - Select Appliances in the left menu bar.
 - Select a device in the main pane. The view changes to Appliance view.
- Select the Configuration tab in the top menu bar.
- Select Objects & Connectors  > Objects  > Predefined Objects  > Applications in the left menu bar.
- In the lower half of the dashboard, click an application to edit its configuration. You can edit the Risk value, Productivity value, Application Tags, and Timeout value to reconfigure the application. The timeout configuration applies only to TCP sessions.

5. Click OK.





Configure URL Category Objects

You can use predefined URL categories, and you can create and configure custom URL categories.

View Predefined URL Categories

VOS devices approximately 83 predefined URL categories, which are updated regularly through the Versa SPack updates. For more information, see [Use Security Packages](#). If the predefined URL categories do not meet your requirements, you can define custom ones based on URL strings or pattern matches.

To view the predefined URL categories:

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 in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Objects & Connectors  > Objects  > Predefined Objects  > URL Categories  in the left menu bar.



Name	Version
real_estate	1
computer_and_internet_security	2
financial_services	3
business_and_economy	4
computer_and_internet_info	5
auctions	6
shopping	7
cult_and_occult	8
travel	9
abused_drugs	10
adult_and_pornography	11
home_and_garden	12
military	13
social_network	14
dead_sites	15

For information about configuring predefined and custom URL categories, see [Configure Security Access Policy Rules](#).






Configure Custom URL Categories

You can create custom URL category objects on a per-tenant basis. Each custom URL category has a unique name and defines information about the URLs to match using a string match or a pattern match. You also associate a reputation value with the URL category. You can use a custom URL category in NGFW and SD-WAN policy rules to specify match

criteria for a Layer 7 URL category. You can also specify custom URL categories in the category-based action rules and reputation-based action rules of a URL-filtering profile.



For information about configuring predefined and custom URL categories, see [Configure Security Access Policy Rules](#).

To define a custom URL category and use it with a URL filtering profile or as a match criteria in a policy rule:



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 in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Objects & Connectors  > Objects  > Custom Objects  > URL Categories  in the left menu bar.
4. Click the  Add icon to add a new category. In the Add URL Category popup window, enter information for the following fields.

Field	Description
Name	Enter a name for the URL category name. This name is displayed in the category list when defining the URL-filtering policies and in the match criteria for URL categories in policy rules.
Description	Enter a text description of the URL category.
Tags	Enter a keyword or phrase that allows you to filter the URL category. This is useful when you have many URL categories and want to view those that are tagged with a particular keyword.
Confidence	<p>Enter a confidence value for the category. This value is used to break the tie when multiple URL categories match a single URL. A higher confidence value takes precedence.</p> <p><i>Range: 1 through 100</i></p>
URL File	<p>Select a URL file to upload a CSV file that contains multiple strings and patterns. Each line in the file contains either a string or a regex pattern for the URL and the reputation associated with the URL.</p> <p>Entries in the CSV file have one of the following formats:</p> <ul style="list-style-type: none"> ◦ <i>string,URL,reputation</i> ◦ <i>pattern,URL,reputation</i> <p>For example:</p> <ul style="list-style-type: none"> ◦ Using a string— <i>string,www.versa-networks.com/,high_risk</i> ◦ Using a regex pattern— <i>pattern,.*versa-networks*,high_risk</i>. If you include a backslash (\) or an open curly brace ({} in the regex pattern, you must escape it by preceding it with a backslash.

5. Select the URL Patterns tab, and enter information for the following fields.

Field	Description
Pattern	Enter a URL pattern to match and group the URLs. You can include regex patterns. For example, use the <code>www.versa-networks.com</code> pattern or use a wildcard like <code>*.versa-networks</code> . If you include a backslash (<code>\</code>) or an open curly brace (<code>{</code>) in the regex pattern, you must escape it by preceding it with a backslash.
Reputation	Select a predefined reputation from the list and assign it to the URL match pattern.
 Add icon	Click the  Add icon to add additional patterns.

6. Select the URL Strings tab, and enter information for the following fields.

Field	Description
String	Enter a URL string that you want to group.
Reputation	Select a predefined reputation from the list and assign it to the URL string.
 Add icon	Click the  Add icon to add additional patterns.

7. Click OK.

Troubleshoot Application Identification

To troubleshoot application identification-related security issues, issue the following CLI commands:

- **show orgs org-services *tenant-name* application-identification list detail**
- **show orgs org-services *tenant-name* application-identification list tag**
- **show orgs org-services *tenant-name* application-identification list sla**
- **show orgs org-services *tenant-name* application-identification statistics application brief**
- **show orgs org-services *tenant-name* application-identification statistics application detail**
- **show orgs org-services *tenant-name* application-identification statistics application top10**
- **show orgs org-services *tenant-name* application-identification statistics application-group**
- **show orgs org-services *tenant-name* application-identification statistics application-filter**

https://docs.versa-networks.com/Secure_SD-WAN/01_Configuration_from_Director/Security_Configuration/Configure_Layer_...

Updated: Wed, 23 Oct 2024 08:19:34 GMT

Copyright © 2024, Versa Networks, Inc.

Supported Software Information

Releases 20.2 and later support all content described in this article.

Additional Information

[Configure NGFW](#)

[Configure SD-WAN Policy](#)

[Configure Stateful Firewall](#)

[Configure URL Filtering](#)

[Use Security Packages](#)