






Configure Security Scanners

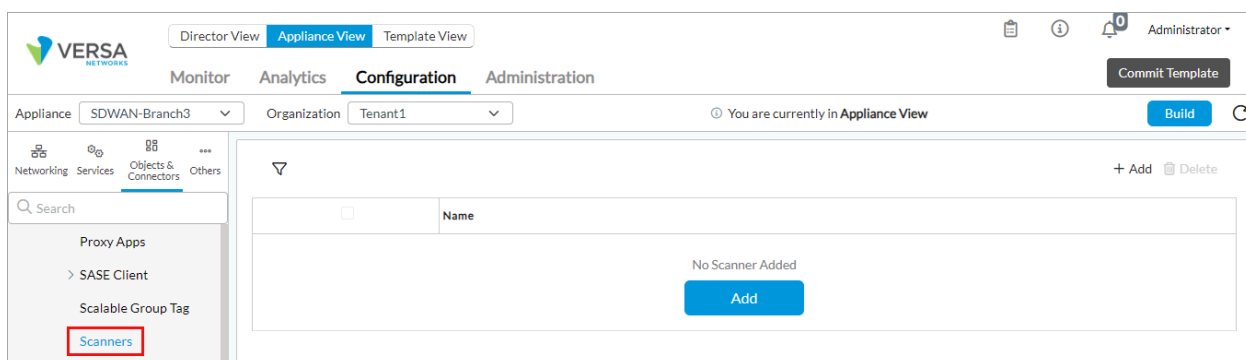
 For supported software information, click [here](#).


On Versa Operating System™ (VOS™) devices, you can configure scanners, which are protocol parsers, for the HTTP, IMAP, POP3, and SMTP protocols. A security scanner scans the list of configuration parameters associated with the protocol. For example, you can configure the maximum content length for an HTTP protocol scanner.

The primary role of the configuration parameters for each protocol scanner is to detect anomalies and then take the required default action. You can enforce the anomaly rule in the security policy and configure the action for that rule. For more information, see [Configure Vulnerability Rules](#). Ensure that you select the rule type as Anomaly Rule and that you set an appropriate action in the predefined action filters.

To configure a security scanner for a tenant:

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 Administration > Appliance, and then click on the appliance in the main pane.
4. Select Objects & Connectors  > Objects  > Custom Objects  > Scanners  in the left menu bar.



5. Click the  Add icon to add and modify the build in security scanner. In the Add Scanner popup window, enter information for the following fields.

Add Scanner

Name

http

Config Parameters

Name	Value	
accept_encoding_max_length	80	+
No Records to Display		

OK

Cancel

Field	Description
Name	<p>Select the name of a predefined security parser:</p> <ul style="list-style-type: none"> ◦ av—Antivirus ◦ http ◦ imap ◦ pop3 ◦ smtp ◦ stream
Configuration Parameters (Group of Fields)	
<ul style="list-style-type: none"> ◦ Name 	<p>Select the configuration parameter for the selected security parser:</p> <ul style="list-style-type: none"> ◦ av <ul style="list-style-type: none"> ▪ compressed-file-size-limit—Enter the size of a compressed file. The default is 2 MB. To scan compressed files larger than 2 MB, you must also change the default value of the normal-file-size-limit option. For example, to change the compressed file of size 25 MB, change both the compressed-file-size-limit and normal-file-size-limit file sizes to 25 MB. ▪ file-cache-enable—Select to optimize antivirus scanning. All files are scanned and stored in the antivirus cache for 15 days, which is the default. ▪ max-entries-in-cache—Enter the number of entries in the antivirus cache. The default is 1048576. ▪ normal-file-size-limit—Enter the file size. The default is 10 MB. The VOS antivirus software does not scan files that are larger than 10 MB unless you increase the value of this option. ◦ http <ul style="list-style-type: none"> ▪ accept_encoding_max-length—The default is 80. ▪ accept_language_max-length—The default is 80. ▪ accept_overflow_max_length—The default is 256.

	<ul style="list-style-type: none"> ▪ <code>accept_ranges_max_length</code>—The default is 80. ▪ <code>authorization_max_length</code>—The default is 128. ▪ <code>connection_max_length</code>—The default is 80. ▪ <code>content_encoding_max_length</code>—The default is 80. ▪ <code>content_language_max_length</code>—The default is 80. ▪ <code>content_location_max_length</code>—The default is 80. ▪ <code>content_max_length</code>—The default is 16384. ▪ <code>content_md5_max_length</code>—The default is 80. ▪ <code>content_range_max_length</code>—The default is 80. ▪ <code>content_type_max_length</code>—The default is 80. ▪ <code>cookie_max_length</code>—The default is 2048. ▪ <code>disable_response_verification</code>—The default is 0. ▪ <code>referer_max_length</code>—The default is 8192. ▪ <code>req_chunk_max_length</code>—The default is 10. ▪ <code>req_content_max_length</code>—There is no default value. ▪ <code>res_chunk_max_length</code>—The default is 10. ▪ <code>res_content_max_length</code>—There is no default value. ▪ <code>server_max_length</code>—The default is 80. ▪ <code>set_cookie_max_length</code>—The default is 2048. ▪ <code>user_agent_max_length</code>—The default is 512. ▪ <code>verb_max_length</code>—The default is 16. ▪ <code>url_max_length</code>—The default is 8192. ◦ <code>imap</code> <ul style="list-style-type: none"> ▪ <code>max_literal_size</code>—The default is 124. ▪ <code>max_tag_size</code>—The default is 20. ◦ <code>pop3</code> <ul style="list-style-type: none"> ▪ <code>max_command-len</code>—The default is 4. ▪ <code>max-command-line-len</code>—The default is 255.
--	---

	<ul style="list-style-type: none"> ▪ max_reply-line-len—The default is 512. ◦ smtp <ul style="list-style-type: none"> ▪ auth_command_max_count—The default is 1. ▪ chunk_size_max_len—The default is 2147483647. ▪ command_line_max_len—The default is 65535. ▪ email_domain_max_len—The default is 64. ▪ helo_command_max_count—The default is 1. ▪ rcpt_to_max_num—The default is 128. ◦ stream <ul style="list-style-type: none"> ▪ stream_3whs_ack_in_wrong_dir—The default is 1. ▪ stream_3whs_async_wrong_seq—The default is 1. ▪ stream_3whs_right_seq_wrong_ack_evasion—The default is 1. ▪ stream_3whs_synack_in_wrong_direction—The default is 1. ▪ stream_3whs_synack_resend_with_different_ack—The default is 1. ▪ stream_3whs_synack_resend_with_diff_seq—The default is 0. ▪ stream_3whs_synack_toserver_on_syn_rcv—The default is 1. ▪ stream_3whs_synack_with_wrong_ack—The default is 1. ▪ stream_3whs_synack_flood—The default is 1. ▪ stream_3whs_syn_resend_diff_seq_on_syn_rcv—The default is 1. ▪ stream_3whs_syn_toclient_on_syn_rcv—The default is 1. ▪ stream_3whs_wrong_seq_wrong_ack—The default is 1. ▪ stream_4whs_synack_with_wrong_ack—The default is 1. ▪ stream_4whs_synack_with_wrong_syn—The default is 1. ▪ stream_4whs_wrong_seq—The default is 1.
--	---

	<ul style="list-style-type: none"> ▪ stream_4whs_invalid_ack—The default is 1. ▪ stream_closewait_ack_out_of_window—The default is 1. ▪ stream_closewait_fin_out_of_window—The default is 1. ▪ stream_closewait_pkt_before_last_ack—The default is 1. ▪ stream_closewait_invalid_ack—The default is 1. ▪ stream_closing_ack_wrong_seq—The default is 1. ▪ stream_closing_invalid_ack—The default is 1. ▪ stream_est_packet_out_of_window—The default is 0. ▪ stream_est_pkt_before_last_ack—The default is 0. ▪ stream_est_synack_resend—The default is 1. ▪ stream_est_synack_resend_with_different_ack—The default is 1. ▪ stream_est_synack_resend_with_diff_seq—The default is 1. ▪ stream_est_synack_toserver—The default is 1. ▪ stream_est_syn_resend—The default is 1. ▪ stream_est_syn_resend_diff_seq—The default is 1. ▪ stream_est_syn_toclient—The default is 1. ▪ stream_est_invalid_ack—The default is 0. ▪ stream_fin_invalid_ack—The default is 1. ▪ stream_fin1_ack_wrong_seq—The default is 1. ▪ stream_fin1_fin_wrong_seq—The default is 1. ▪ stream_fin1_invalid_ack—The default is 1. ▪ stream_fin2_ack_wrong_seq—The default is 1. ▪ stream_fin2_fin_wrong_seq—The default is 1. ▪ stream_fin2_invalid_ack—The default is 1. ▪ stream_fin_but_no_session—The default is
--	---

	<p>0.</p> <ul style="list-style-type: none"> ▪ stream_fin_out_of_window—The default is 1. ▪ stream_lastack_ack_wrong_seq—The default is 1. ▪ stream_lastack_invalid_ack—The default is 1. ▪ stream_rst_but_no_session—The default is 0. ▪ stream_timewait_ack_wrong_seq—The default is 1. ▪ stream_timewait_invalid_ack—The default is 1. ▪ stream_shutdown_syn_resend—The default is 1. ▪ stream_pkt_invalid_timestamp—The default is 1. ▪ stream_pkt_invalid_ack—The default is 1. ▪ stream_pkt_broken_ack—The default is 0. ▪ stream_rst_invalid_ack—The default is 1. ▪ stream_pkt_retransmission—The default is 1. ▪ stream_reassembly_segment_before_base_seq—The default is 0. ▪ stream_reassembly_no_segment—The default is 0. ▪ stream_reassembly_seq_gap—The default is 0. ▪ stream_reassembly_overlap_different_data—The default is 1.
◦ Value	Enter a value for the protocol scanner parameter.

6. Click OK.

Supported Software Information

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

Additional Information

[Configure Vulnerability Rules](#)