


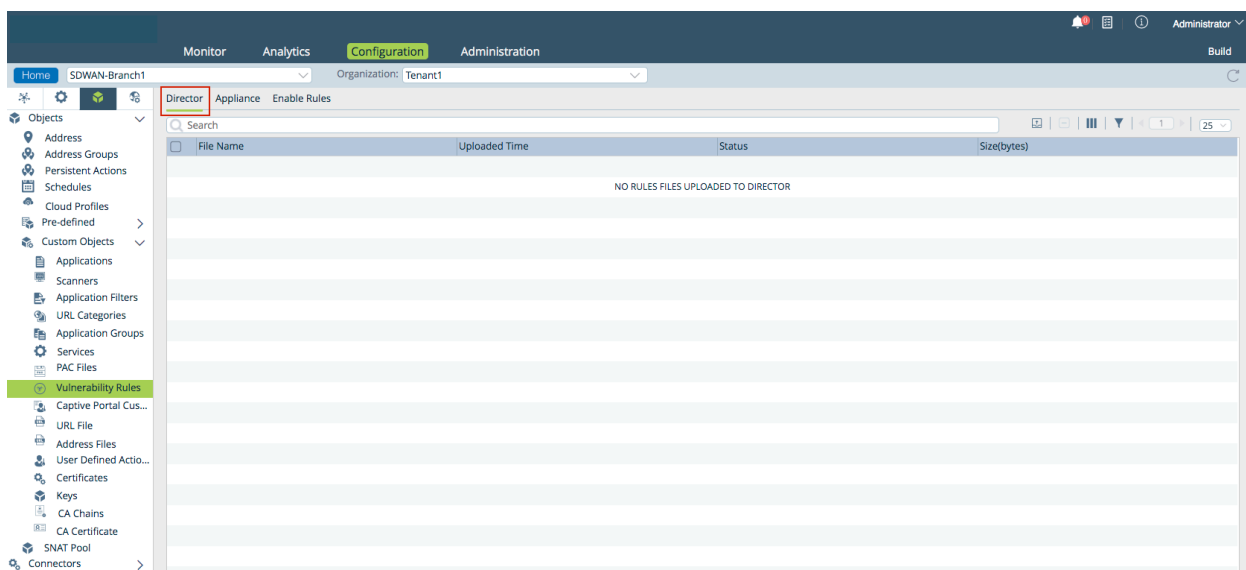
Configure Vulnerability Rules

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

Vulnerability rules determines the level of protection against buffer overflows, illegal code execution, and other attempts to exploit system vulnerabilities. You can define rules separately for Director nodes and Versa Operating System™ (VOS™) devices.

To configure vulnerability rules for a Director node:

1. In Director view:
 - a. Select the Configuration tab in the top menu bar.
 - b. Select Templates > Device Templates in the horizontal menu bar.
 - c. Select an organization in the left navigation panel.
 - d. Select a template 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 > Vulnerability Rules in the left menu bar. The main pane displays, with the Director tab selected.



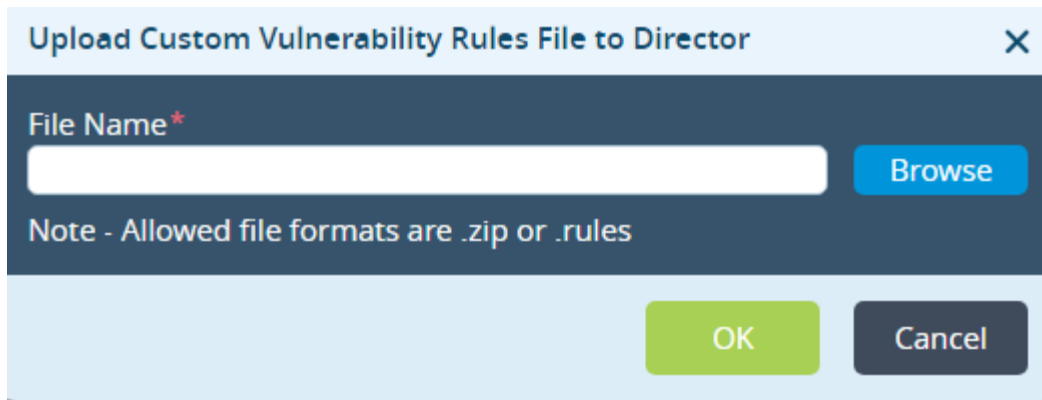
4. Click the  Upload File icon. In the Upload Custom Vulnerability Rules File to Director, click Browse and select

https://docs.versa-networks.com/Management_and_Orchestration/Versa_Director/Configuration/Configure_Vulnerability_Rules

Updated: Thu, 24 Oct 2024 10:45:01 GMT

Copyright © 2024, Versa Networks, Inc.

the file.



Upload Custom Vulnerability Rules File to Director

File Name*

Browse

Note - Allowed file formats are .zip or .rules

OK Cancel

5. Click OK.

Supported Software Information

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

Additional Information

[Configure Intrusion Detection and Prevention](#)