TITANIA NIPPER

Titania Nipper Cisco PSIRT Audit Guide

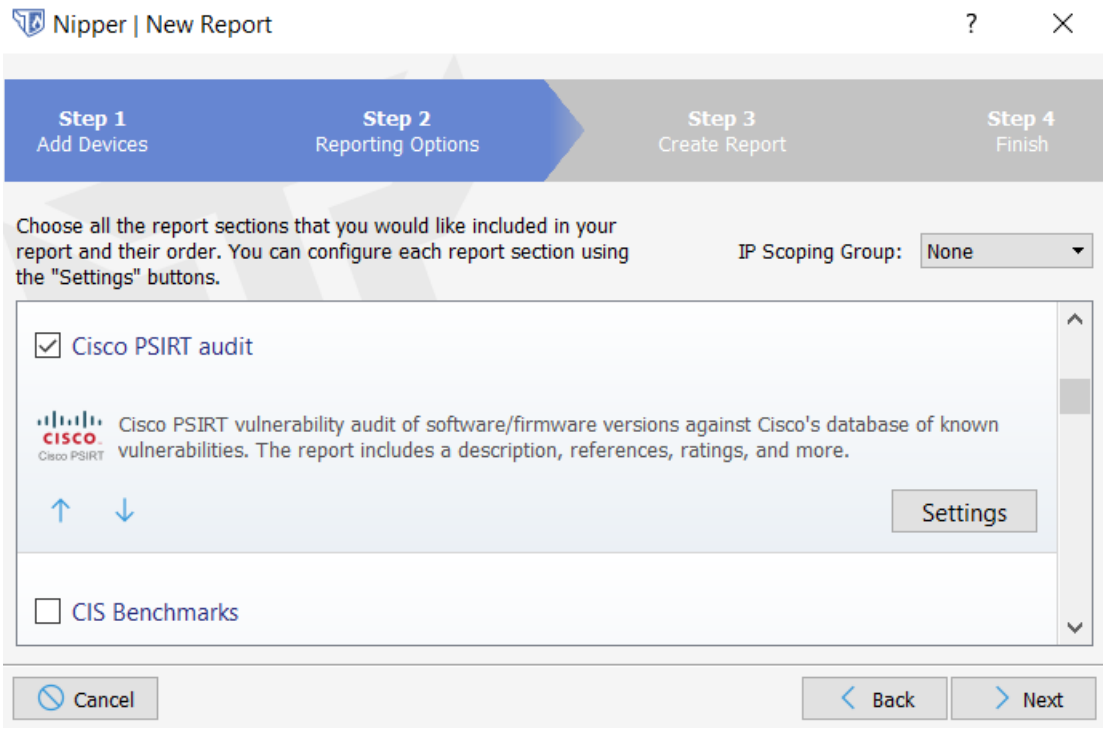
Software Version: 2.13.X

Last updated: October 10, 2023

Nipper – Cisco PSIRT Audit

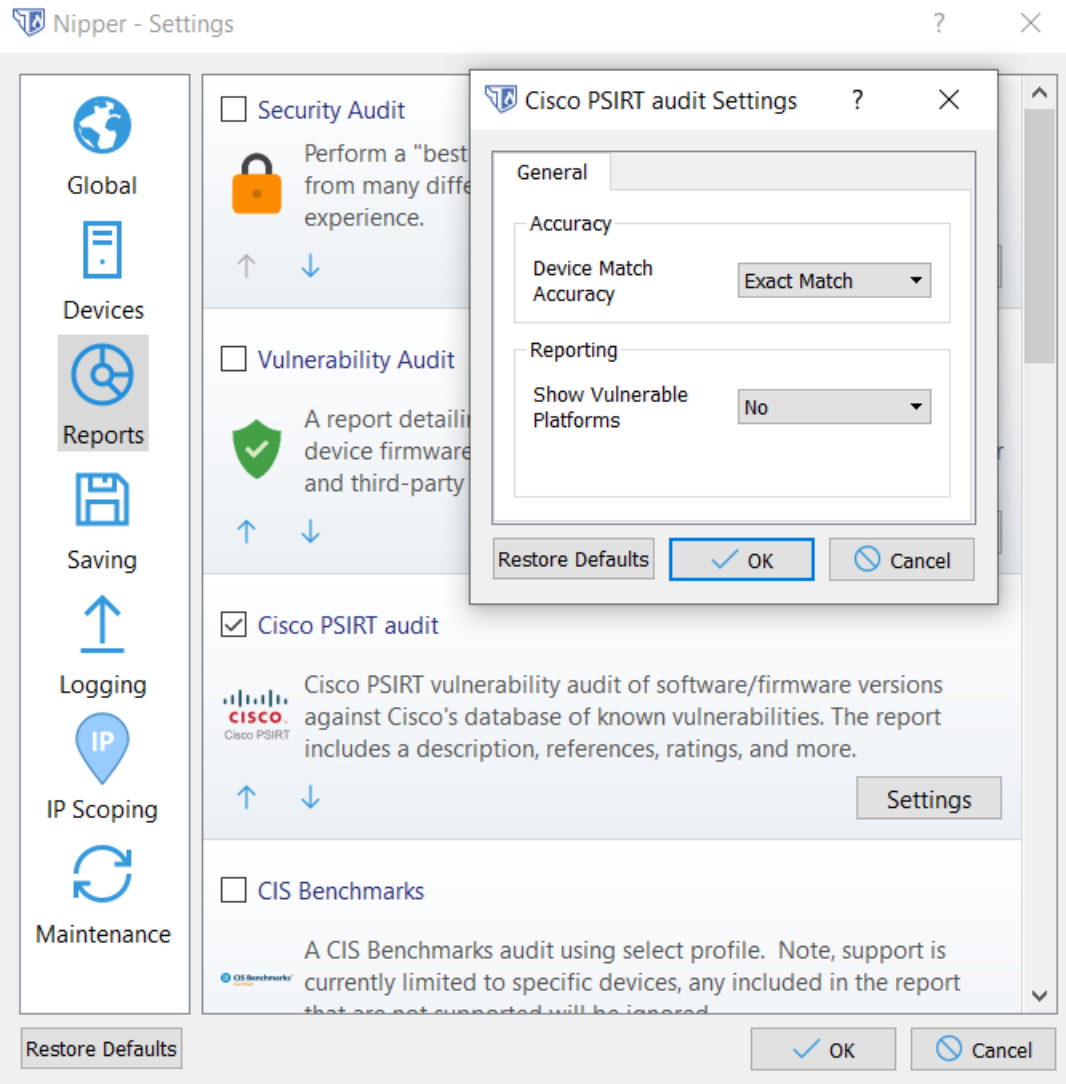
PSIRT Plugin

The latest release of Nipper includes a Cisco-specialized report plugin.



The Cisco PSIRT (Product Security Incident Response Team) plugin analyses devices against Cisco's community-managed list of security advisories, reporting identified vulnerabilities with detailed information, including Cisco's SIR (Security Impact Rating) and the respective CVSS (Common Vulnerability Scoring System) base score for each vulnerability.

The accuracy with which this plugin matches your device(s) against vulnerabilities can also be managed in the settings for the Plugin.



The Cisco PSIRT is a dedicated, global team that manages the receipt, investigation, and public reporting of information about security vulnerabilities and issues related to Cisco products and networks. Cisco defines a security vulnerability as an unintended weakness in a product that could allow an attacker to compromise the integrity, availability, or confidentiality of the product. The Cisco PSIRT adheres to ISO/IEC 29147:2014.

The on-call Cisco PSIRT works 24 hours a day with Cisco customers, independent security researchers, consultants, industry organizations, and other vendors to identify possible security vulnerabilities and issues with Cisco products and networks.

The full Cisco Vulnerability policy can be viewed online here.

There is also a new help guide detailing how to update the PSIRT resource file utilized within Nipper's Help & Information section, to ensure up-to-date PSIRT security advisory information is readily available. This is accomplished using Nipper's internal Resource Manager.