This Tenable Integrations Policy ("Policy") defines the categories of Tenable product integrations as well as the support policy for each. The intent of this Policy document is to provide information that aids customers in planning and preparing for their organization's support needs.

Integrations Overview

Tenable offers integrations with a variety of technology partners as part of its Cyber Exposure ecosystem. Tenable alongside its ecosystem partners creates the world's richest set of Cyber Exposure data to analyze, gain context, and take decisive action to better understand and reduce cyber risk. These integrations are provided free of charge from Tenable to allow customers to gain the greatest benefit from Tenable products. Tenable is committed to working with the technology ecosystem to maintain integrations that keep pace with changes over time.

Tenable Integrations fall into four major categories:

NASL Integrations: These are Nessus-based integrations developed by Tenable that are handled and updated via Tenable Plugins. Examples of NASL-Based Integrations include Privileged Access Management (PAM), Mobile Device Management (MDM), and Patch Management.

Tenable Embedded Integrations: Tenable Embedded Integrations are developed by Tenable and embedded in a Tenable UI. By design, only the latest versions are available. Examples include Tenable VM cloud connectors Tenable Cloud Security Integrations and Tenable Container Security connectors.

Third-Party Platform Integrations, developed by Tenable: These are integrations developed for use on third party platforms. Third-Party Platform integrations can be either Tenable supported (Ex. Jira, Splunk, ServiceNow) or Community supported. Those that are Community Supported are open source and hosted and distributed via Github.

Third-Party Platform Integrations, developed by a Third-Party: These are integrations that are developed by a Third-Party partner, but are also validated by Tenable.

Tenable Integration Support

Tenable provides basic support with the exception of open-source integrations which are community-supported. With the exception of Integrations hosted by Tenable partners, only the latest version of Integrations will be made available for download. Any bugs are fixed via new releases, therefore customers should be on the most current version before contacting Tenable support. Given that Tenable integrations are distributed in "code" form, there is limited opportunity for customization outside of the features provided in the integration.

Tenable reserves the right to End of Life any Tenable Integration at any time. An Integration End of Life will be handled via a product bulletin and where possible, proactive notification. Please sign up for the Tenable Product Lifecycle Community Group to be automatically notified of product End of Life: Product Lifecycle Management

Table 1: Support Matrix

Integration Type	Developed By	Supported By
NASL integrations	Tenable	Tenable
Tenable Embedded Integrations	Tenable	Tenable
Third Party Integrations developed by Tenable	Tenable	Tenable
Third Party Integrations developed by Tenable, Open Source	Tenable	Community/Github
Third Party Integrations developed by Third Party	Third Party	Third Party

For more specific information on all Tenable Integrations, please visit https://www.tenable.com/partners/technology.

For Tenable Integration downloads, please visit https://www.tenable.com/downloads/integrations.

Tenable Technical Support

Technical support is necessary to ensure your technical issues or usage questions are resolved in a timely manner. Tenable support experts are available 24 hours a day, 7 days a week, and are available via a variety of convenient methods, including the Tenable Support Portal, phone, email and chat.

Customers with Tenable Technical Support are entitled to a number of predetermined technical support contacts who may: create cases, search the knowledge base, review product documentation, and download software updates. For more details, please refer to the Tenable Technical Support Guide.

Customer Notifications

In an effort to make End of Life information readily available, it will be shared in multiple ways and multiple locations:

- Tenable Community Group: Product Lifecycle Management
- Specific Product End of Life Bulletins
- Tenable Product Documentation, Release Notes, Downloads page
- Tenable Community Notifications
- Tenable Product Documentation
- Customer and Partner Newsletters

For More Information

For more information about the Tenable product offering, please visit the following pages:
Tenable Attack Surface Management: https://www.tenable.com/products/tenable-asm
Tenable Cloud Security: https://www.tenable.com/products/tenable-cs
Tenable One: https://www.tenable.com/products/tenable-one
Tenable Vulnerability Management: https://www.tenable.com/products/tenable-io
Tenable Lumin: https://www.tenable.com/products/tenable-lumin
Tenable Nessus: https://www.tenable.com/products/nessus
Tenable Security Center: https://www.tenable.com/products/tenable-sc
Tenable Identity Exposure: https://www.tenable.com/products/tenable-ad
Tenable OT Security: https://www.tenable.com/products/tenable-ot
Tenable Core: https://docs.tenable.com/Core.htm

Version 1.0a, Updated: 3/12/2024