Tenable FedRAMP FAQ

The following are frequently asked questions about Tenable FedRAMP.

Q: How does FedRAMP work for customers who use both Tenable.sc and Tenable.io FedRAMP?
   
   - You can add Tenable.io FedRAMP scanners to Tenable.sc the same way you add internal, local, or remote Nessus scanners. For more information, see the Add a Tenable.io Scanner.
   
   - Beginning in August 2021, you can use Tenable.io FedRAMP for Nessus Agent management by Tenable.sc. For more information, see Manage Agent Scans.
   
   - With Tenable.io FedRAMP, you cannot use Tenable.sc for reporting.

Q: Does Tenable.io FedRAMP support any other platform integrations?

   - A: Yes. Beginning in August 2021, Customers can export Tenable.io data onto other platforms. However, once the data leaves Tenable.io, it is your responsibility to keep the data encrypted and stored in a way that is compliant with FedRAMP requirements.

   The following platforms are supported in FedRAMP:

   - QRadar
   - ServiceNow
   - JIRA
   - Splunk

Q: Can I automatically migrate data from commercial Tenable.io or Tenable.sc into Tenable.io FedRAMP?

   - A: There is not automated process for migrating data into or from Tenable.io. Tenable recommends working with Tenable Professional Services to assist with migration.

A: Currently, there is no timeline for future FedRAMP authorization levels. Once Tenable.io becomes FedRAMP certified at the Moderate authorization level, Tenable plans to investigate authorization at higher levels. DoD impact levels require a separate process with a DoD sponsor. Although the FedRAMP Moderate and DoD IL 2 controls are equivalent, an Authority to Operate must be formalized with a DoD agency sponsor.