Tenable and QianXin Integration Guide

Last Revised: November 20, 2023

Table of Contents

Welcome to Tenable for QiAnXin

This document describes how to configure Tenable for integration with the Qianxin Privileged Account Management System.

Qianxin Privileged Account Management System is a privileged access management (PAM) software solution that stores, manages and monitors credentials. Benefits of integrating with Qianxin PAM include:

- A built-in password safe to securely store target passwords
- Advanced account monitoring
- Management of account lifecycle

QiAnXin Integrations

View one of the following options for Qianxin integration steps:

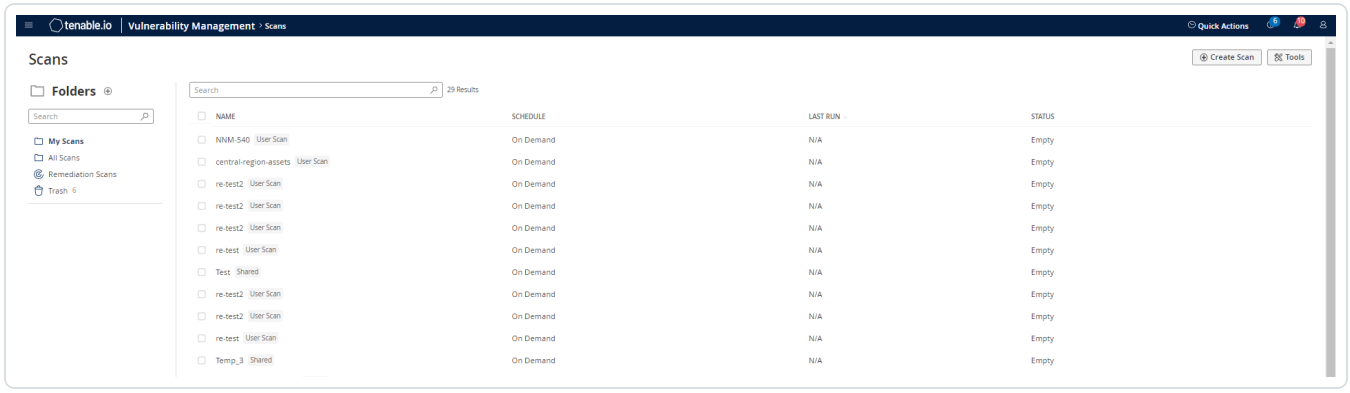
- Database Integration
- SSH Integration
- Windows Integration

Database Integration

To configure database integration:

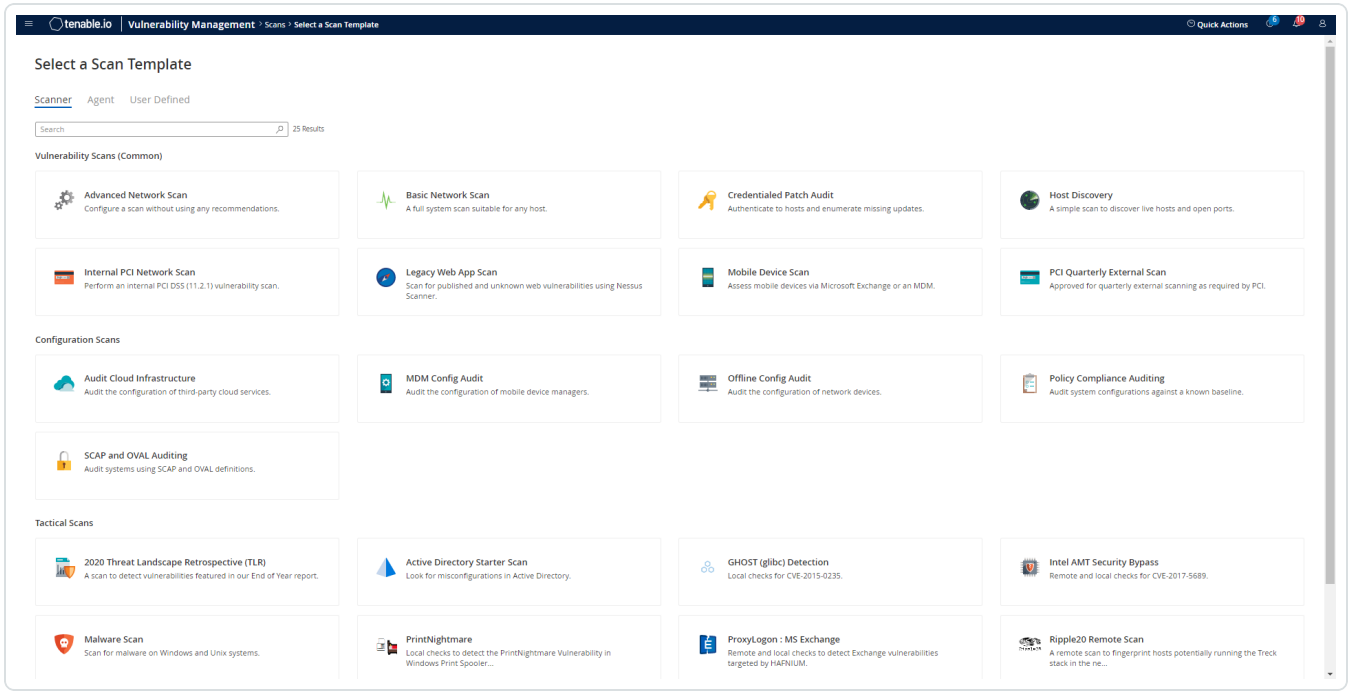
1. Log in to the Tenable user interface.
2. Click **Scans**.

   The **My Scans** page appears.



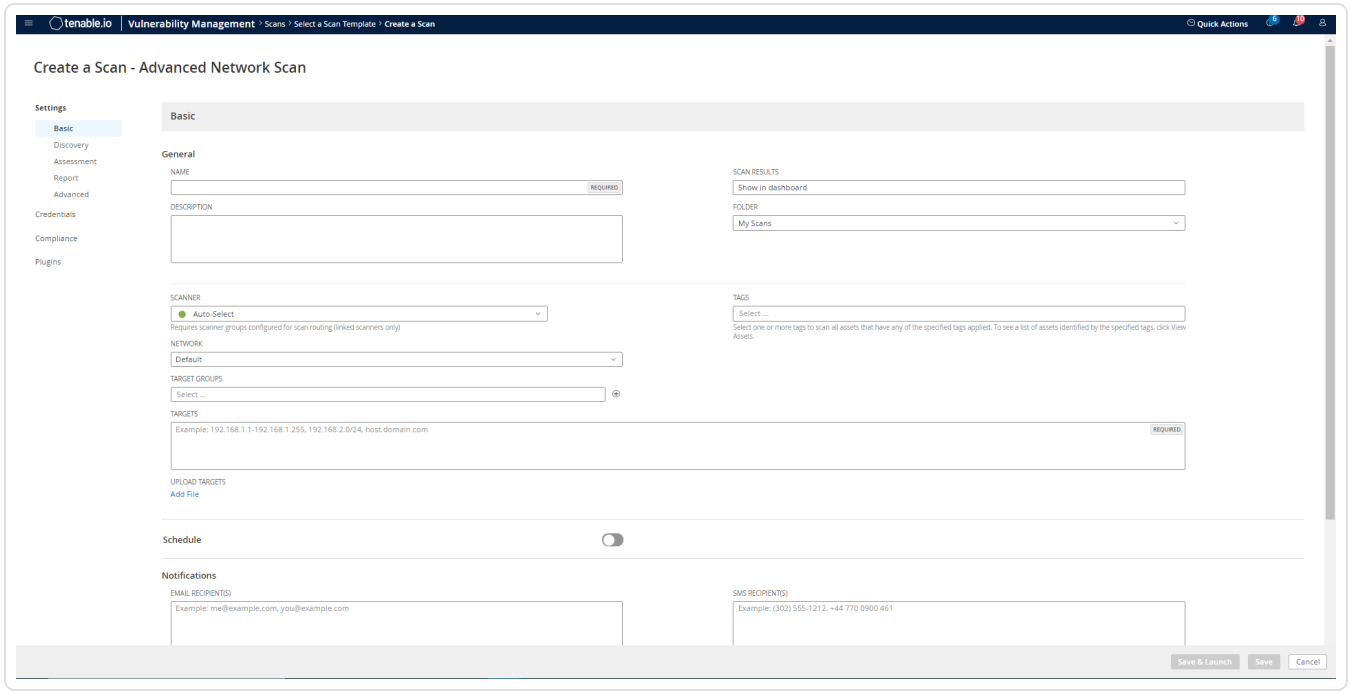
3. Click **+ New Scan.**

   The **Select a Scan Template** page appears.

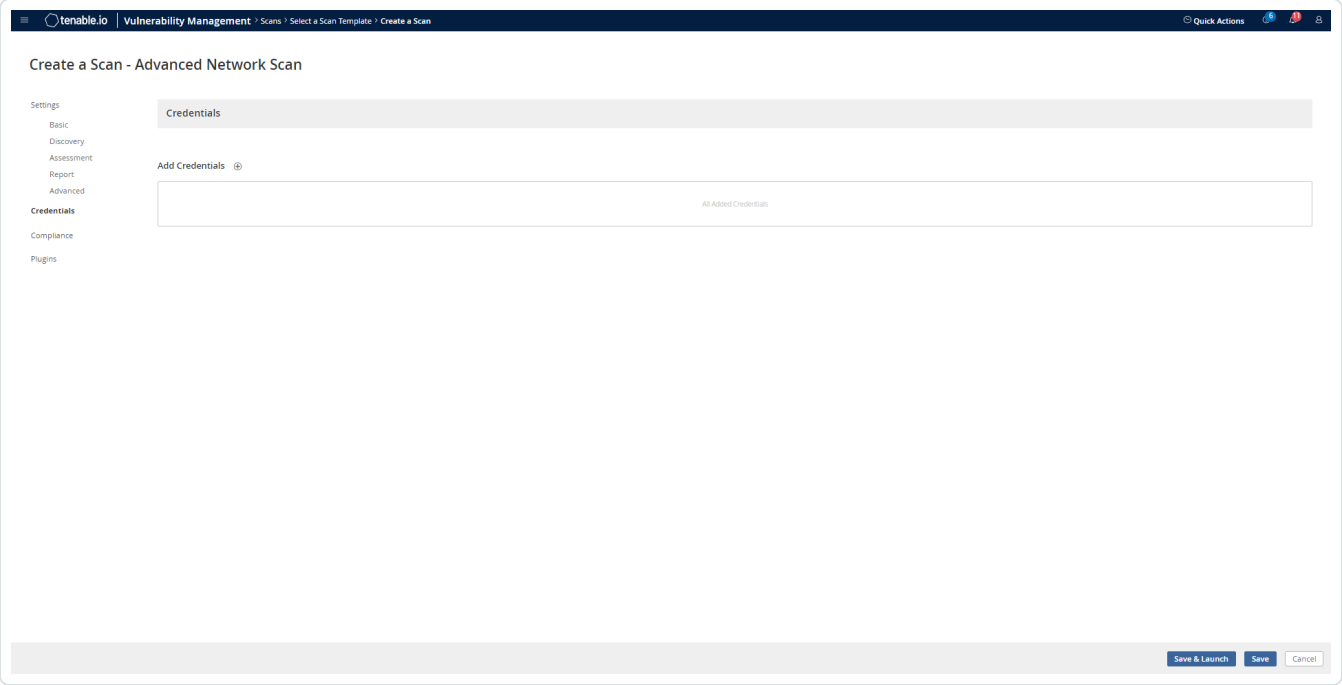


4. Select a scan template. For demonstration, the **Advanced Network Scan** template is used.

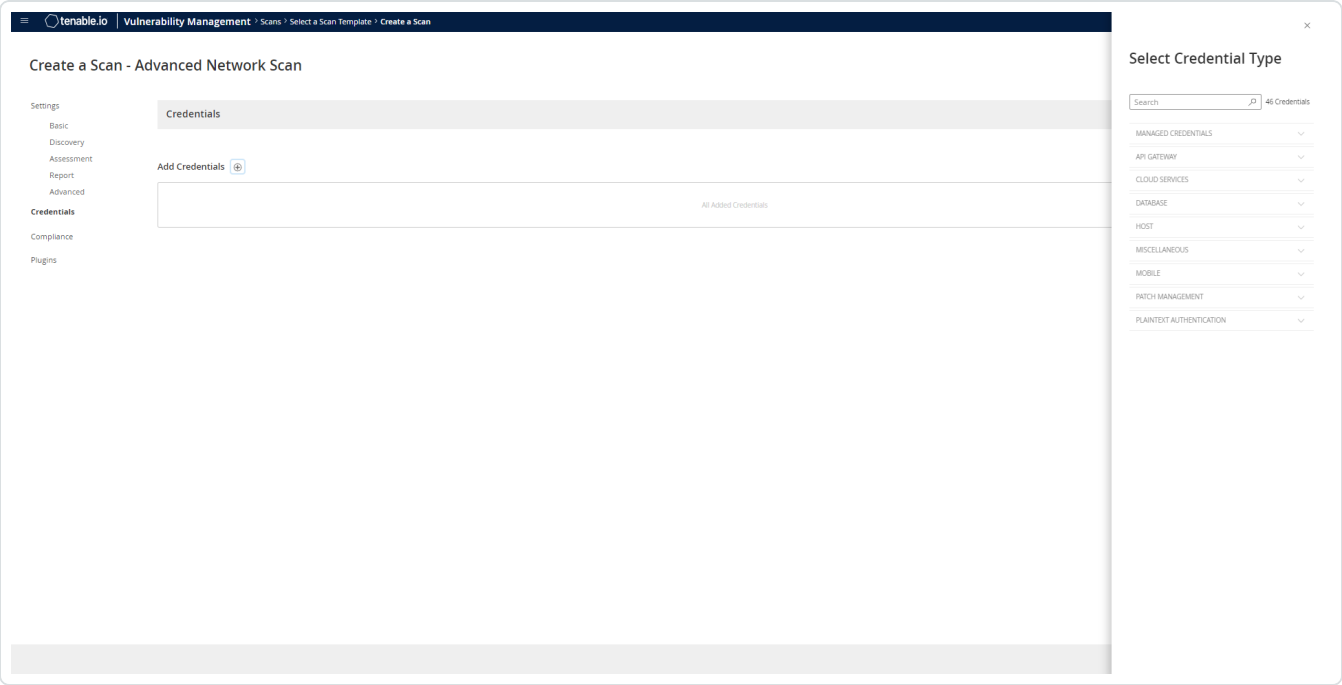
The scan configuration page appears.



5. In the **Name** box, type a name for the scan.
6. In the **Targets** box, type an IP address, hostname, or range of IP addresses.
7. (Optional) Add a description, folder location, scanner location, and specify target groups.
8. Click the **Credentials** tab.

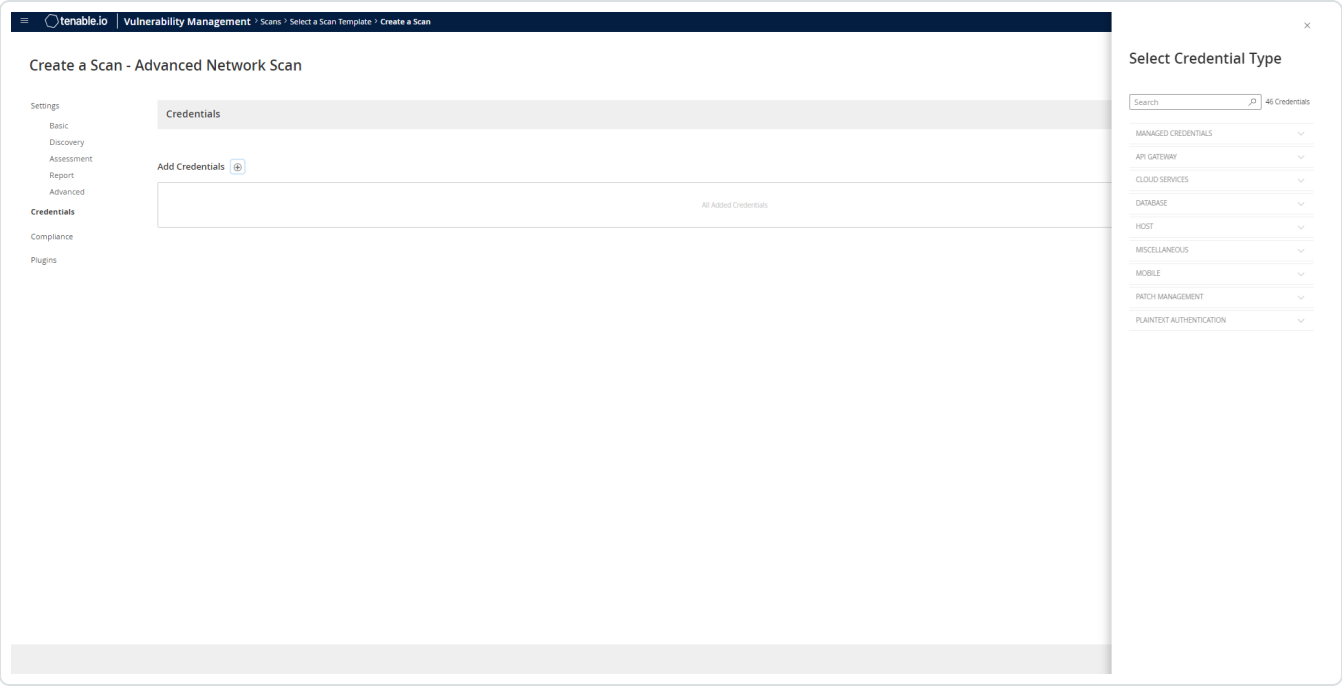


The **Credentials** pane appears.

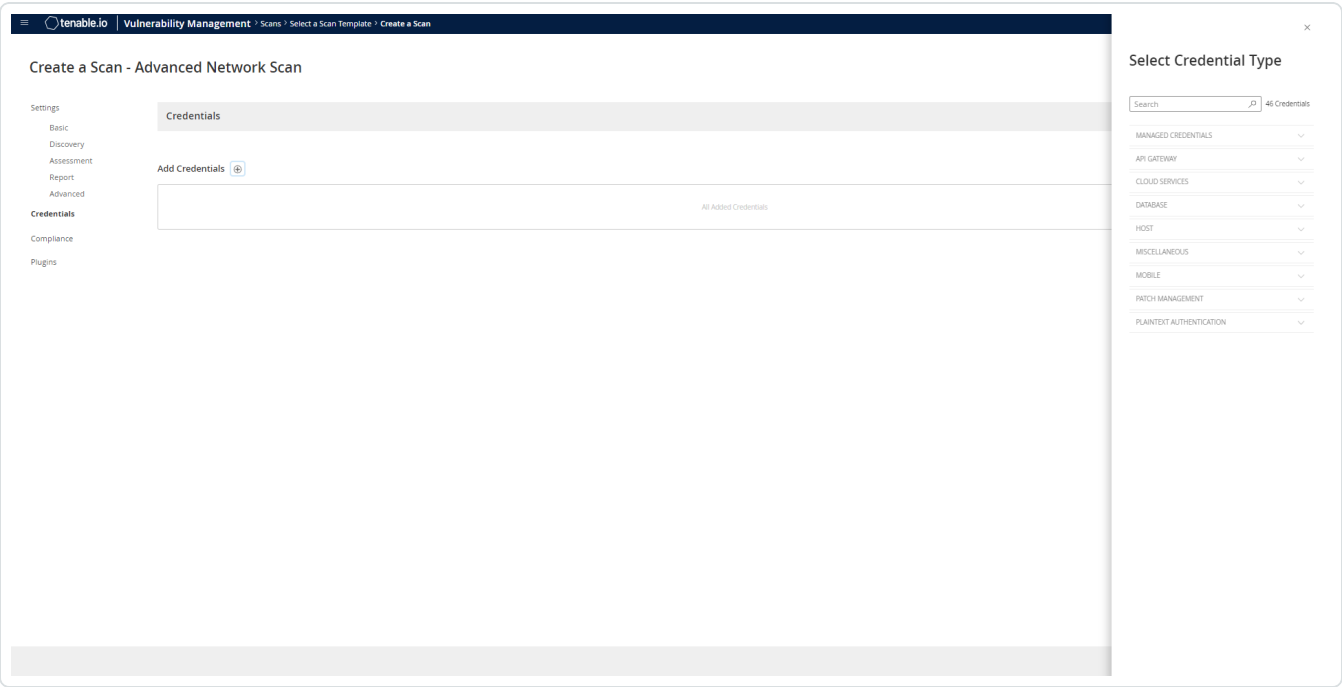


9. Click the **Database** option.

   The **Database** options appear.



10. From the **Database Type** drop-down, select **Oracle**.



11. From the **Auth Type** drop-down, select **Qianxin**.

    The **Qianxin** field options appear.

12. Configure each field for the **Database** authentication.

Option	Description	Required
Qianxin Host	The IP address or URL for the Qianxin host.	yes
Qianxin Port	The port on which the Qianxin API communicates. By default, Tenable uses 443.	yes
Qianxin API Client ID	The Client ID for the applicable Qianxin A2A Application for Oauth 2.0 API authentication.	yes
Qianxin API Secret ID	The Secret ID for the applicable Qianxin A2A Application for Oauth 2.0 API authentication.	yes
Qianxin Credential ID or Identifier	The credential ID or identifier for the credential you are requesting to retrieve.	yes
Private Key File	The Private Key used to decrypt encrypted sensitive data from A2A. **Note:** You can enable encryption of sensitive data in the A2A Application Authorizations. If enabled, you must provide a private key file in the scan credentials. This can be downloaded from the applicable A2A application in Qianxin.	Required if you have enabled encryption of sensitive data in A2A Application Authorizations.
HTTPS	This is enabled by default.	yes
Verify SSL Certificate	This is disabled by default.	no

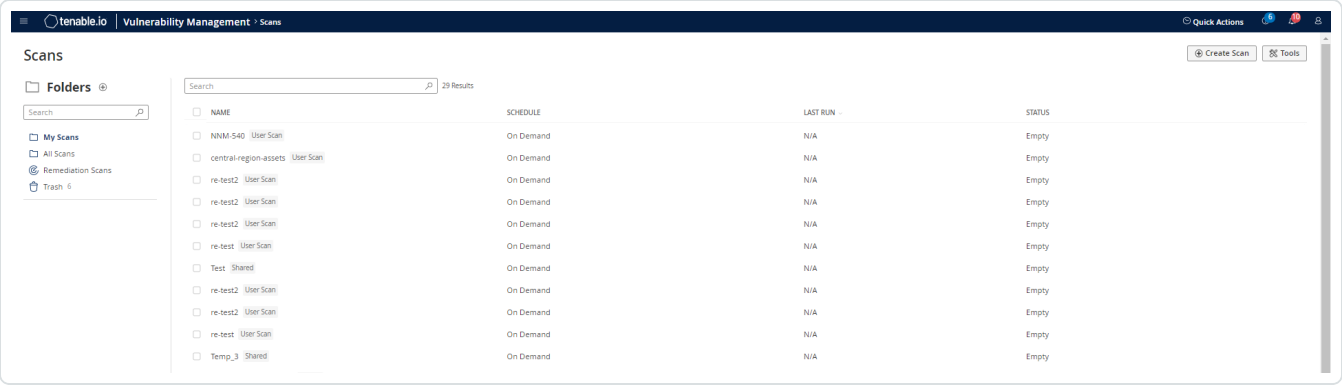
13. Click **Save**.

SSH Integration

To configure SSH integration:

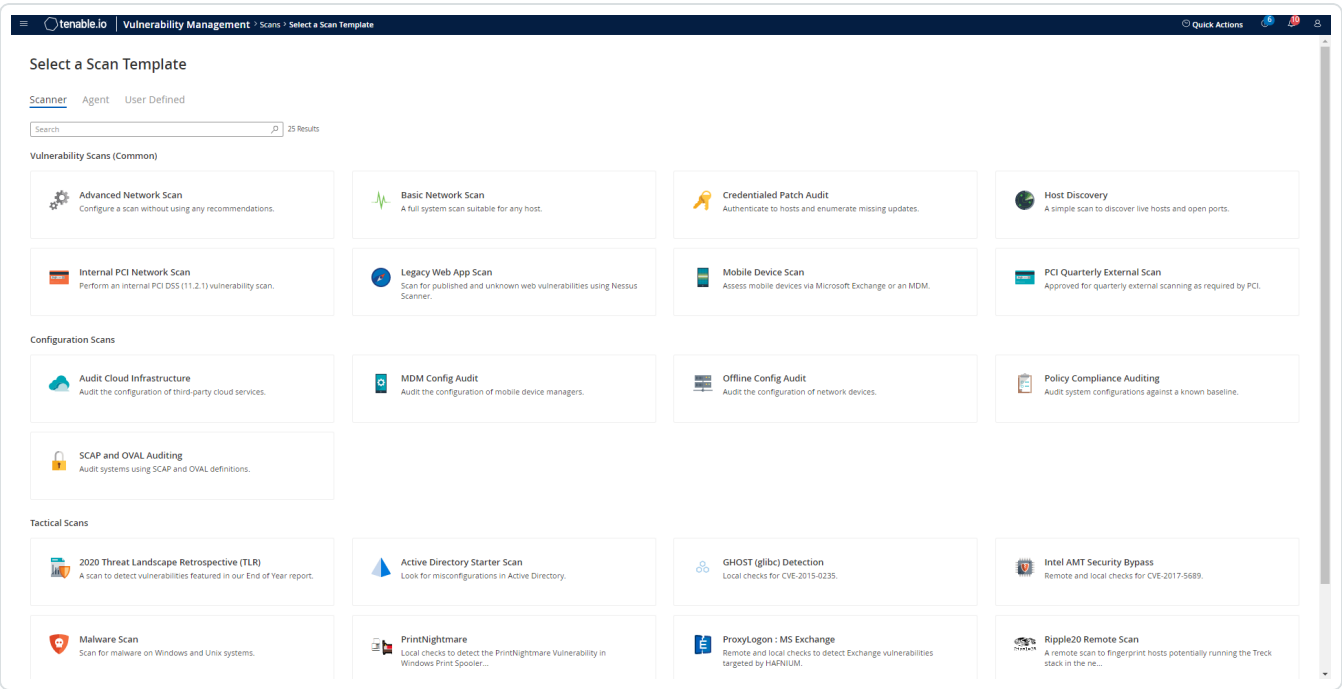
1. Log in to the Tenable user interface.
2. Click **Scans**.
3. Click **+ New Scan**.

   The **My Scans** page appears.

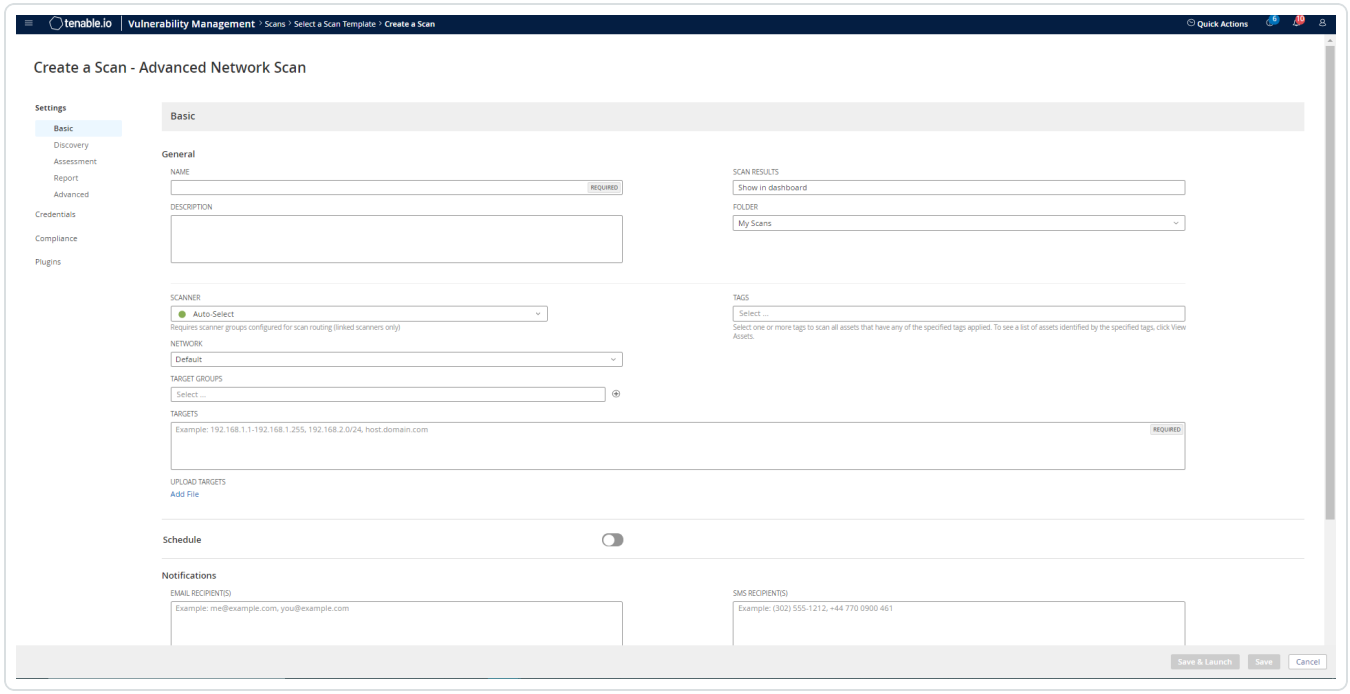


4. Select a scan template.

   The **Scan Templates** page appears.

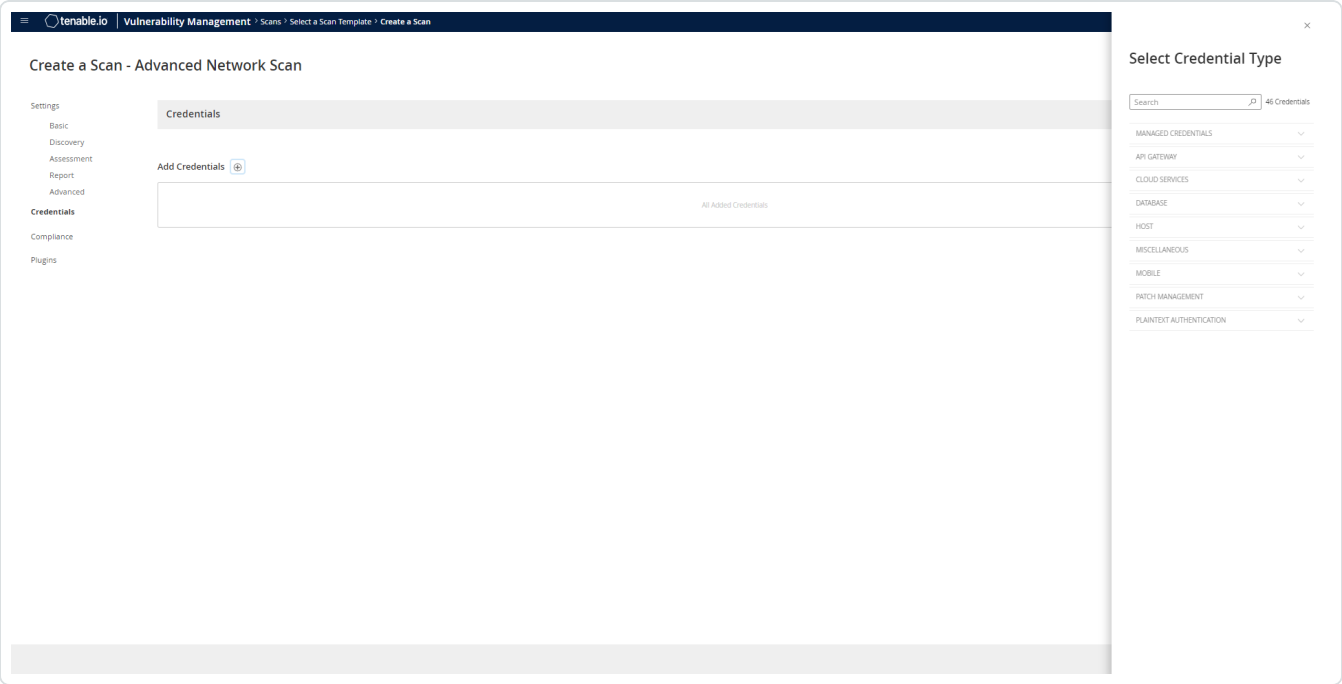


The scan configuration page appears.



5. In the **Name** box, type a name for the scan.
6. In the **Targets** box, type an IP address, hostname, or range of IP addresses.
7. (Optional) Add a description, folder location, scanner location, and specify target groups.
8. Click the **Credentials** tab.

   The Credentials options appear.



9. In the **Select a Credential** menu, select the **Host** drop-down.
10. Select **SSH**.

    The **Qianxin** field options appear.
11. Configure each field for **SSH** authentication.

Option	Description	Required
Qianxin Host	The IP address or url for the Qianxin host.	yes
Qianxin Port	The port on which the Qianxin API communicates. By default, Tenable uses 443.	yes
Qianxin API Client ID	The Client ID for the applicable Qianxin A2A Application for Oauth 2.0 API authentication.	yes
Qianxin API Secret ID	The Secret ID for the applicable Qianxin A2A Application for Oauth 2.0	yes

Option	Description	Required
	API authentication.	
Qianxin Credential ID or Identifier	The credential ID or identifier for the credential the you are requesting to retrieve.	yes
Use SSH Key for Target Authentication	The user can select this option to retrieve the SSH Key to authenticate to the target if configuration is applicable in Qianxin.	Required if authenticating to target with SSH Key.
Private Key File	The Private Key used to decrypt encrypted sensitive data from A2A. **Note:** You can enable encryption of sensitive data in the A2A Application Authorizations. If enabled, you must provide a private key file in the scan credentials. This can be downloaded from the applicable A2A application in Qianxin.	Required if you have enabled encryption of sensitive data in A2A Application Authorizations.
Escalate Privileges with	The Private Key used to decrypt encrypted sensitive data from A2A. **Note:** Tenable supports multiple options for privilege escalation, including su, su+sudo and sudo. For example, if you select sudo, more fields for sudo user, Escalation Account Name, and Location of su and sudo (directory) are provided and can be completed to support authentication and privilege escalation through Qianxin. The Escalation Account Name field is then required to complete your privilege escalation.	Required if you wish to escalate privileges.

Option	Description	Required
	Note: For more information about supported privilege escalation types and their accompanying fields, see the Nessus User Guide, the Tenable Vulnerability Management User Guide, or the Tenable Security Center User Guide.	
Escalation account credential ID or identifier	If the escalation account has a different username or password from the least privileged user, enter the credential ID or identifier for the escalation account credential here.	no
HTTPS	This is enabled by default.	yes
Verify SSL Certificate	This is disabled by default.	no

12. Click **Save**.

Windows Integration

To configure Tenable with Qianxin using Windows integration:

1. Log in to Tenable Vulnerability Management.
2. In the upper-left corner, click the ☰ button.

   The left navigation plane appears.
3. In the left navigation plane, click **Settings**.

   The **Settings** page appears.
4. Click the **Credentials** widget.

   The **Credentials** page appears. The credentials table lists the managed credentials you have permission to view.
5. Click the ⊕ button next to the **Credentials** title.

   The credential form plane appears.
6. In the **Host** section, click **Windows**.

   The selected credential options appear.
7. In the **Authentication Method** drop-down, select **Qianxin**.

   The **Qianxin** options appear.

8. Configure the **Qianxin** credentials.

Option	Description	Required
Qianxin Host	The IP address or URL for the Qianxin host.	yes
Qianxin Port	The port on which the Qianxin API communicates. By default, Tenable uses 443.	yes
Qianxin API Client ID	The Client ID for the applicable Qianxin A2A Application for Oauth 2.0 API authentication.	yes
Qianxin API Secret ID	The Secret ID for the applicable Qianxin A2A Application for Oauth 2.0 API authentication.	yes
Domain	The domain to which the username belongs.	no
Qianxin Credential ID or Identifier	The credential ID or identifier for the credential the you are requesting to retrieve.	yes
Private Key File	The Private Key used to decrypt encrypted sensitive data from A2A. **Note:** You can enable encryption of sensitive data in the A2A Application Authorizations. If enabled, the user must provide a private key file in the scan credentials. This can be downloaded from the applicable A2A application in Qianxin.	Required if you have enabled encryption of sensitive data in A2A Application Authorizations.
HTTPS	This is enabled by default.	yes

Option	Description	Required
Verify SSL Certificate	This is disabled by default.	no

9. Click **Save**.