Tenable and QiAnXin Integration Guide

Last Revised: June 24, 2024

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 that securely stores 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

Tenable provides full database support for Qianxin integrations. Complete the following steps to configure database credentials for scans with Qianxin.

For more information on Tenable scans, see the Nessus User Guide, the Tenable Vulnerability Management User Guide, or the Tenable Security Center User Guide.

To configure Qianxin database for Tenable Vulnerability Management or Tenable Nessus:

1. Log in to your Tenable user interface.
2. In the upper-left corner, click the ☰ button.

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

   The **Scans** page appears.
4. In the upper-right corner of the page, click the [→**Create a Scan** button.

   The **Select a Scan Template** page appears.
5. Select a scan template.

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

The **Settings** pane appears.

10. Click the **Database** option.

    The **Database** options appear.

11. In the **Database Type** drop-down box, select **Oracle**.

12. In the **Auth Type** drop-down box, click Qianxin.

    The Qianxin options appear.

13. Configure each option 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 embedded account application created in QiAnXin PAM	yes
QiAnXin API Secret ID	The Secret ID for the embedded account application created in QiAnXin PAM	yes
Username	The username to log in to the hosts you want to scan.	yes
Host IP	Specify the host IP of the asset containing the account to use. If not specified, the scan target IP is used.	no
Platform	Specify the platform (based on asset type) of the asset containing the account to use. If not specified, a default target is used based on credential type (for example, for Windows credentials, the default is WINDOWS). Possible values: • **ACTIVE_DIRECTORY** – Windows	no

Option	Description	Required
	Domain Account • **WINDOWS** – Windows Local Account • **LINUX** – Linux Account • **SQL_SERVER** – SQL Server Database • **ORACLE** – Oracle Database • **MYSQL** – MySQL Database • **DB2** – DB2 Database • **HP_UNIX** – HP Unix • **SOLARIS** – Solaris • **OPENLDAP** – OpenLDAP • **POSTGRESQL** – PostgreSQL	
Region ID	Specify the region ID of the asset containing the account to use.	Only if using multiple regions
Use SSL	When enabled, Tenable uses SSL for secure communication. This is enabled by default.	no
Verify SSL Certificate	When enabled, Tenable verifies that the SSL Certificate on the server is signed by a trusted CA.	no

14. Do one of the following:
    - If you want to save without launching the scan, click **Save**.
    - If you want to save and launch the scan immediately, click **Save & Launch**.

    > **Note:** If you scheduled the scan to run at a later time, the **Save & Launch** option is not available.

To configure Qianxin database for Tenable Security Center:

1. Log in to Tenable Security Center.
2. Click **Scanning** > **Credentials** (administrator users) or **Scans** > **Credentials** (organizational users).

   The **Credentials** page appears.
3. Click **Add**.

   The **Credential Templates** page appears.
4. In the **Miscellaneous**, **API Gateway**, **Database**, **SNMP**, **SSH**, or **Windows**, or **Web Authentication** sections, click the tile for the specific method you want to configure.

   The **Add Credentials** configuration page appears.
5. In the **Name** box, type a name for the credentials.
6. In the **Description** box, type a description for the credentials.
7. (Optional) Type or select a **Tag**. For more information, see Tags in the *Tenable Security Center User Guide*.
8. Configure each option 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 embedded account application created in QiAnXin PAM	yes
QiAnXin API Secret ID	The Secret ID for the embedded account application created in QiAnXin PAM	yes
Username	The username to log in to the hosts you want to scan.	yes
Host IP	Specify the host IP of the asset containing the account to use. If not specified, the scan target	no

Option	Description	Required
	IP is used.	
Platform	Specify the platform (based on asset type) of the asset containing the account to use. If not specified, a default target is used based on credential type (for example, for Windows credentials, the default is WINDOWS). Possible values: • **ACTIVE_DIRECTORY** – Windows Domain Account • **WINDOWS** – Windows Local Account • **LINUX** – Linux Account • **SQL_SERVER** – SQL Server Database • **ORACLE** – Oracle Database • **MYSQL** – MySQL Database • **DB2** – DB2 Database • **HP_UNIX** – HP Unix • **SOLARIS** – Solaris • **OPENLDAP** – OpenLDAP • **POSTGRESQL** – PostgreSQL	no
Region ID	Specify the region ID of the asset containing the account to use.	Only if using multiple regions
Use SSL	When enabled, Tenable uses SSL for secure communication. This is enabled by default.	no
Verify SSL Certificate	When enabled, Tenable verifies that the SSL	no

Option	Description	Required
	Certificate on the server is signed by a trusted CA.	

9. Click **Submit**.

   Tenable Security Center saves your configuration.

SSH Integration

Tenable provides full SSH support for Qianxin integrations. Complete the following steps to configure SSH credentials for scans with Qianxin.

For more information on Tenable scans, see the Nessus User Guide, the Tenable Vulnerability Management User Guide, or the Tenable Security Center User Guide.

To configure Qianxin SSH for Tenable Vulnerability Management or Tenable Nessus:

1. Log in to your Tenable user interface.
2. In the upper-left corner, click the ☰ button.

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

   The **Scans** page appears.
4. In the upper-right corner of the page, click the [→**Create a Scan** button.

   The **Select a Scan Template** page appears.
5. Select a scan template.

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

The **Credentials** pane appears.

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

    The **Settings** pane appears.

12. In the **Auth Type** drop-down box, click **Qianxin**.

    The Qianxin options appear.

13. Configure each option for the **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 embedded account application created in QiAnXin PAM.	yes
QiAnXin API Secret ID QiAnXin API Client Secret	The Secret ID for the embedded account application created in QiAnXin PAM.	yes
QiAnXin Username	The username to log in to the hosts you want to scan.	yes
Host IP QiAnXin Asset Address	Specify the host IP of the asset containing the account to use. If not specified, the scan target IP is used.	no
QiAnXin Asset Platform	Specify the platform (based on asset type) of the asset containing the account to use. If not specified, a default target is used based on credential type (for example, for Windows credentials, the default is WINDOWS). Possible values:	no

Option	Description	Required
	• **ACTIVE_DIRECTORY** – Windows Domain Account • **WINDOWS** – Windows Local Account • **LINUX** – Linux Account • **SQL_SERVER** – SQL Server Database • **ORACLE** – Oracle Database • **MYSQL** – MySQL Database • **DB2** – DB2 Database • **HP_UNIX** – HP Unix • **SOLARIS** – Solaris • **OPENLDAP** – OpenLDAP • **POSTGRESQL** – PostgreSQL	
QiAnXin Region ID	Specify the region ID of the asset containing the account to use.	Only if using multiple regions
Escalate Privileges with	Use the drop-down menu to select the privilege elevation method, or select “Nothing” to skip privilege elevation. **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 only required if the escalation password differs from the normal	Required if you wish to escalate privileges.

Option	Description	Required
	login password. **Note:** For more information about supported privilege escalation types and their accompanying fields, see the Nessus User Guide or the Tenable Vulnerability Management User Guide.	
Escalation Account Username	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
Use SSL	When enabled, Tenable uses SSL for secure communication. This is enabled by default.	no
Verify SSL Certificate	When enabled, Tenable verifies that the SSL Certificate on the server is signed by a trusted CA.	no
Privilege Escalation	The privilege escalation method you want to use to increase users' privileges after initial authentication. Your **Privilege Escalation** selection determines the specific options you must configure. For more information, see Privilege Escalation.	no

14. Do one of the following:
    - If you want to save without launching the scan, click **Save**.
    - If you want to save and launch the scan immediately, click **Save & Launch**.

      Note: If you scheduled the scan to run at a later time, the **Save & Launch** option is not available.

To configure Qianxin SSH for Tenable Security Center:

1. Log in to Tenable Security Center.
2. Click **Scanning** > **Credentials** (administrator users) or **Scans** > **Credentials** (organizational users).

   The **Credentials** page appears.
3. Click **Add**.

   The **Credential Templates** page appears.
4. In the **Miscellaneous**, **API Gateway**, **Database**, **SNMP**, **SSH**, or **Windows**, or **Web Authentication** sections, click the tile for the specific method you want to configure.

   The **Add Credentials** configuration page appears.
5. In the **Name** box, type a name for the credentials.
6. In the **Description** box, type a description for the credentials.
7. (Optional) Type or select a **Tag**. For more information, see Tags in the *Tenable Security Center User Guide*.
8. Configure each option for the **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 embedded account application created in QiAnXin PAM.	yes
QiAnXin API Secret ID QiAnXin API Client Secret	The Secret ID for the embedded account application created in QiAnXin PAM.	yes
QiAnXin Username	The username to log in to the hosts you want to scan.	yes
Host IP	Specify the host IP of the asset containing the	no

Option	Description	Required
QiAnXin Asset Address	account to use. If not specified, the scan target IP is used.	
QiAnXin Asset Platform	Specify the platform (based on asset type) of the asset containing the account to use. If not specified, a default target is used based on credential type (for example, for Windows credentials, the default is WINDOWS). Possible values: • **ACTIVE_DIRECTORY** – Windows Domain Account • **WINDOWS** – Windows Local Account • **LINUX** – Linux Account • **SQL_SERVER** – SQL Server Database • **ORACLE** – Oracle Database • **MYSQL** – MySQL Database • **DB2** – DB2 Database • **HP_UNIX** – HP Unix • **SOLARIS** – Solaris • **OPENLDAP** – OpenLDAP • **POSTGRESQL** – PostgreSQL	no
QiAnXin Region ID	Specify the region ID of the asset containing the account to use.	Only if using multiple regions
Escalate Privileges with	Use the drop-down menu to select the privilege elevation method, or select “Nothing” to skip privilege elevation.	Required if you wish to escalate

Option	Description	Required
	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 only required if the escalation password differs from the normal login password. **Note:** For more information about supported privilege escalation types and their accompanying fields, see the Nessus User Guide or the Tenable Vulnerability Management User Guide.	privileges.
Escalation Account Username	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
Use SSL	When enabled, Tenable uses SSL for secure communication. This is enabled by default.	no
Verify SSL Certificate	When enabled, Tenable verifies that the SSL Certificate on the server is signed by a trusted CA.	no
Privilege Escalation	The privilege escalation method you want to use to increase users' privileges after initial authentication. Your **Privilege Escalation** selection determines the specific options you must configure. For more information, see Privilege Escalation.	no

9. Click **Submit**.

   Tenable Security Center saves your configuration.

Windows Integration

Tenable provides full Windows support for Qianxin integrations. Complete the following steps to configure Windows credentials for scans with Qianxin.

For more information on Tenable scans, see the Nessus User Guide, the Tenable Vulnerability Management User Guide, or the Tenable Security Center User Guide.

To configure Qianxin Windows for Tenable Vulnerability Management or Tenable Nessus:

1. Log in to your Tenable user interface.
2. In the upper-left corner, click the ☰ button.

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

   The **Scans** page appears.
4. In the upper-right corner of the page, click the [→**Create a Scan** button.

   The **Select a Scan Template** page appears.
5. Select a scan template.

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

   The **Credentials** pane appears.
10. In the **Select a Credential** menu, select the **Host** drop-down.
11. Select **Windows**.

    The **Settings** pane appears.

12. In the **Auth Type** drop-down box, click **Qianxin**.

    The Qianxin options appear.

13. Configure each option for the **Windows** 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 embedded account application created in QiAnXin PAM.	yes
QiAnXin API Secret ID QiAnXin API Client Secret	The Secret ID for the embedded account application created in QiAnXin PAM.	yes
Domain	The domain to which the username belongs.	no
QiAnXin Username	The username to log in to the hosts you want to scan.	yes
Domain	The domain to which the username belongs.	no
Host IP QiAnXin Asset Address	Specify the host IP of the asset containing the account to use. If not specified, the scan target IP is used.	no
QiAnXin Asset Platform	Specify the platform (based on asset type) of the asset containing the account to use. If not specified, a default target is used based on credential type (for example, for Windows credentials, the default is WINDOWS). Possible values: • **ACTIVE_DIRECTORY** – Windows Domain Account	no

Option	Description	Required
	• **WINDOWS** – Windows Local Account • **LINUX** – Linux Account • **SQL_SERVER** – SQL Server Database • **ORACLE** – Oracle Database • **MYSQL** – MySQL Database • **DB2** – DB2 Database • **HP_UNIX** – HP Unix • **SOLARIS** – Solaris • **OPENLDAP** – OpenLDAP • **POSTGRESQL** – PostgreSQL	
QiAnXin Region ID	Specify the region ID of the asset containing the account to use.	Only if using multiple regions.
Use SSL	When enabled, Tenable uses SSL for secure communication. This is enabled by default.	no
Verify SSL Certificate	When enabled, Tenable verifies that the SSL Certificate on the server is signed by a trusted CA.	no

14. Do one of the following:
    - If you want to save without launching the scan, click **Save**.
    - If you want to save and launch the scan immediately, click **Save & Launch**.

    > **Note:** If you scheduled the scan to run at a later time, the **Save & Launch** option is not available.

To configure Qianxin Windows for Tenable Security Center:

1. Log in to Tenable Security Center.
2. Click **Scanning** > **Credentials** (administrator users) or **Scans** > **Credentials** (organizational users).

   The **Credentials** page appears.
3. Click **Add**.

   The **Credential Templates** page appears.
4. In the **Miscellaneous**, **API Gateway**, **Database**, **SNMP**, **SSH**, or **Windows**, or **Web Authentication** sections, click the tile for the specific method you want to configure.

   The **Add Credentials** configuration page appears.
5. In the **Name** box, type a name for the credentials.
6. In the **Description** box, type a description for the credentials.
7. (Optional) Type or select a **Tag**. For more information, see Tags in the *Tenable Security Center User Guide*.
8. Configure each option for the **Windows** 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 embedded account application created in QiAnXin PAM.	yes
QiAnXin API Secret ID QiAnXin API Client Secret	The Secret ID for the embedded account application created in QiAnXin PAM.	yes
Domain	The domain to which the username belongs.	no
QiAnXin Username	The username to log in to the hosts you want to scan.	yes

Option	Description	Required
Domain	The domain to which the username belongs.	no
Host IP QiAnXin Asset Address	Specify the host IP of the asset containing the account to use. If not specified, the scan target IP is used.	no
QiAnXin Asset Platform	Specify the platform (based on asset type) of the asset containing the account to use. If not specified, a default target is used based on credential type (for example, for Windows credentials, the default is WINDOWS). Possible values: • **ACTIVE_DIRECTORY** – Windows Domain Account • **WINDOWS** – Windows Local Account • **LINUX** – Linux Account • **SQL_SERVER** – SQL Server Database • **ORACLE** – Oracle Database • **MYSQL** – MySQL Database • **DB2** – DB2 Database • **HP_UNIX** – HP Unix • **SOLARIS** – Solaris • **OPENLDAP** – OpenLDAP • **POSTGRESQL** – PostgreSQL	no
QiAnXin Region ID	Specify the region ID of the asset containing the account to use.	Only if using multiple regions.

Option	Description	Required
Use SSL	When enabled, Tenable uses SSL for secure communication. This is enabled by default.	no
Verify SSL Certificate	When enabled, Tenable verifies that the SSL Certificate on the server is signed by a trusted CA.	no

9. Click **Submit**.

   Tenable Security Center saves your configuration.