Tenable and ARCON Integration Guide

Last Revised: April 09, 2025

Table of Contents

Welcome to Tenable for ARCON

Integrating Tenable applications with ARCON provides an effective solution for managing, controlling, and monitoring privileged user activities. ARCON provides technology security teams with centralized policy framework to authorize privileges based on roles and responsibilities.

You can integrate ARCON with Tenable Nessus Manager, Tenable Vulnerability Management, or Tenable Security Center.

The benefits of integrating Tenable applications with ARCON include:

- A centralized control point through which all network connections and traffic is routed
- Offers a rule and role-based restricted privileged access to target systems
- Streamlines the life cycles of secrets making them easier to incorporate through various strategies

For additional information about ARCON, see the ARCON website.

Requirements

To integrate Tenable with ARCON you must meet the following requirements.

Tenable Product

You must have an active account for at least one of the following Tenable products to integrate with ARCON: Tenable Vulnerability Management or Tenable Nessus Manager.

Tenable User Role

You must have the appropriate role for your Tenable account:

Tenable Vulnerability Management - Standard, Scan Manager, Administrator, or System Administrator

Tenable Nessus Manager - Standard, Administrator, or System Administrator

ARCON Requirements

You must have an active ARCON account.

Nessus and ARCON

You can integrate Nessus with Arcon using Database, SSH, or Windows credentials. View the corresponding section to configure your Tenable Nessus application with ARCON.

Configure Tenable Nessus with ARCON (Database)

Configure Tenable Nessus with ARCON (SSH)

Configure Tenable Nessus with ARCON (Windows)

Configure Tenable Nessus with ARCON (Database)

In Tenable Nessus Manager, you can integrate with Arcon using database credentials. Complete the following steps to configure Nessus with ARCON in database.

> **Required User Role:** Standard, Administrator, or System Administrator

To integrate Tenable Nessus with ARCON using database credentials:

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 **Cassandra**, **Oracle**, **DB2**, **MongoDB**, **PostgreSQL**, **MySQL**, **SQL Server**, or **Sybase ASE**.

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

    The ARCON options appear.

13. Configure each option for the **Database** authentication.

Option	Default Value
Arcon host	(Required) The Arcon IP address or DNS address. **Note:** If your Arcon installation is in a subdirectory, you must include the subdirectory path. For example, type *IP address or hostname/subdirectory path*.
Arcon port	The port on which Arcon listens.
API User	(Required) The API user provided by Arcon.
API Key	(Required) The API key provided by Arcon.
Authentication URL	The URL Tenable Nessus Manager uses to access Arcon.
Password Engine URL	The URL Tenable Nessus Manager uses to access the passwords in Arcon.
Username	(Required) The username to log in to the hosts you want to scan.
Arcon Target Type	(Optional) The name of the target type. . Depending on the Arcon PAM version you are using and the system type the SSH credential has been created with, this is set to **linux** by default. Refer to the

Option	Default Value
	Arcon PAM Specifications document (provided by Arcon) for target type/system type mapping for the correct target type value.
Checkout Duration	(Required) The length of time, in hours, that you want to keep credentials checked out in Arcon. Configure the **Checkout Duration** to exceed the typical duration of your Tenable Vulnerability Management scans. If a password from a previous scan is still checked out when a new scan begins, the new scan fails. **Note:** Configure the password change interval in Arcon so that password changes do not disrupt your Tenable Vulnerability Management scans. If Arcon changes a password during a scan, the scan fails.
Use SSL	When enabled, Tenable Nessus Manager uses SSL through IIS for secure communications. You must configure SSL through IIS in Arcon before enabling this option.
Verify SSL	When enabled, Tenable Nessus Manager validates the SSL certificate. You must configure SSL through IIS in Arcon before enabling this option.
Targets to Prioritize Credentials	Specify IPs or CIDR blocks on which this credential is attempted before any other credential. To specify multiple IPs or CIDR blocks, use a comma or space-separated list. Using this setting can decrease scan times by prioritizing a credential that you know works against your selected targets. For example, if your scan specifies 100 credentials, and the successful credential is the 59th credential out of 100, the first 58 credentials have to fail before the 59th credential succeeds. If you use **Targets To Prioritize Credentials**, you configure the scan to use the successful credential first, which allows the scan to access the

Option	Default Value
	target faster.

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.

Configure Tenable Nessus with ARCON (SSH)

In Tenable Nessus Manager, you can integrate with Arcon using SSH credentials. Complete the following steps to configure Tenable Nessus with ARCON using SSH.

> **Required User Role:** Standard, Administrator, or System administrator

To integrate Tenable Nessus with ARCON using SSH credentials:

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 **ARCON**.

    The ARCON options appear.
13. Configure each option for the **SSH** authentication.

Option	Default Value
Arcon host	(Required) The Arcon IP address or DNS address. **Note:** If your Arcon installation is in a subdirectory, you must include the subdirectory path. For example, type *IP address or hostname/subdirectory path*.
Arcon port	The port on which Arcon listens.
API User	(Required) The API user provided by Arcon.
API Key	(Required) The API key provided by Arcon.
Authentication URL	The URL Tenable Nessus Manager uses to access Arcon.
Password Engine URL	The URL Tenable Nessus Manager uses to access the passwords in Arcon.
Username	(Required) The username to log in to the hosts you want to scan.
Arcon Target Type	(Optional) The name of the target type. . Depending on the Arcon PAM version you are using and the system type the SSH credential has been created with, this is set to **linux** by default. Refer to the

Option	Default Value
	Arcon PAM Specifications document (provided by Arcon) for target type/system type mapping for the correct target type value.
Checkout Duration	(Required) The length of time, in hours, that you want to keep credentials checked out in Arcon. Configure the **Checkout Duration** to exceed the typical duration of your Tenable Vulnerability Management scans. If a password from a previous scan is still checked out when a new scan begins, the new scan fails. **Note:** Configure the password change interval in Arcon so that password changes do not disrupt your Tenable Vulnerability Management scans. If Arcon changes a password during a scan, the scan fails.
Use SSL	When enabled, Tenable Nessus Manager uses SSL through IIS for secure communications. You must configure SSL through IIS in Arcon before enabling this option.
Verify SSL	When enabled, Tenable Nessus Manager validates the SSL certificate. You must configure SSL through IIS in Arcon before enabling this option.
Targets to Prioritize Credentials	Specify IPs or CIDR blocks on which this credential is attempted before any other credential. To specify multiple IPs or CIDR blocks, use a comma or space-separated list. Using this setting can decrease scan times by prioritizing a credential that you know works against your selected targets. For example, if your scan specifies 100 credentials, and the successful credential is the 59th credential out of 100, the first 58 credentials have to fail before the 59th credential succeeds. If you use **Targets To Prioritize Credentials**, you configure the scan to use the successful credential first, which allows the scan to access the

Option	Default Value
	target faster.

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.

What to do next:

To verify the integration is working:

1. On the **Scans** page, click the **Launch** button to initiate an on-demand scan.
2. Once the scan completes, select the completed scan and look for **Plugin ID 97993** and the corresponding message - *It was possible to log into the remote host via SSH using 'password' authentication*. This result validates that authentication was successful.

Configure Tenable Nessus with ARCON (Windows)

In Tenable Nessus Manager, you can integrate with Arcon using Wndows credentials. Complete the following steps to configure Nessus with ARCON in Windows.

> **Required User Role:** Standard, Administrator, or System Administrator

To integrate Tenable Nessus with ARCON using Windows credentials:

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 **ARCON**.

    The ARCON options appear.

13. Configure each option for the **Windows** authentication.

Option	Default Value
Arcon host	(Required) The Arcon IP address or DNS address. **Note:** If your Arcon installation is in a subdirectory, you must include the subdirectory path. For example, type *IP address or hostname/subdirectory path*.
Arcon port	The port on which Arcon listens.
API User	(Required) The API user provided by Arcon.
API Key	(Required) The API key provided by Arcon.

Option	Default Value
Authentication URL	The URL Tenable Nessus Manager uses to access Arcon.
Password Engine URL	The URL Tenable Nessus Manager uses to access the passwords in Arcon.
Username	(Required) The username to log in to the hosts you want to scan.
Arcon Target Type	(Optional) The name of the target type. . Depending on the Arcon PAM version you are using and the system type the SSH credential has been created with, this is set to **linux** by default. Refer to the Arcon PAM Specifications document (provided by Arcon) for target type/system type mapping for the correct target type value.
Checkout Duration	(Required) The length of time, in hours, that you want to keep credentials checked out in Arcon. Configure the **Checkout Duration** to exceed the typical duration of your Tenable Vulnerability Management scans. If a password from a previous scan is still checked out when a new scan begins, the new scan fails. **Note:** Configure the password change interval in Arcon so that password changes do not disrupt your Tenable Vulnerability Management scans. If Arcon changes a password during a scan, the scan fails.
Use SSL	When enabled, Tenable Nessus Manager uses SSL through IIS for secure communications. You must configure SSL through IIS in Arcon before enabling this option.
Verify SSL	When enabled, Tenable Nessus Manager validates the SSL certificate. You must configure SSL through IIS in Arcon before enabling this option.
Targets to	Specify IPs or CIDR blocks on which this credential is attempted

Option	Default Value
Prioritize Credentials	before any other credential. To specify multiple IPs or CIDR blocks, use a comma or space-separated list. Using this setting can decrease scan times by prioritizing a credential that you know works against your selected targets. For example, if your scan specifies 100 credentials, and the successful credential is the 59th credential out of 100, the first 58 credentials have to fail before the 59th credential succeeds. If you use **Targets To Prioritize Credentials**, you configure the scan to use the successful credential first, which allows the scan to access the target faster.

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.

What to do next:

To verify the integration is working:

1. On the **Scans** page, click the **Launch** button to initiate an on-demand scan.
2. Once the scan completes, select the completed scan and look for the following message - *Microsoft Windows SMB Log In Possible: 10394*. This result validates that authentication was successful.

Tenable Vulnerability Management and ARCON

You can integrate Tenable Vulnerability Management with ARCON using Windows credentials or SSH credentials. View the corresponding section to configure your Tenable Vulnerability Management application with ARCON.

Configure Tenable Vulnerability Management with ARCON (Database)

Configure Tenable Vulnerability Management with ARCON (SSH)

Configure Tenable Vulnerability Management with ARCON (Windows)

Configure Tenable Vulnerability Management with ARCON (Database)

In Tenable Vulnerability Management, you can integrate with ARCON using database credentials.

Complete the following steps to configure Tenable Vulnerability Management with ARCON using database.

> **Required User Role:** Standard, Scan Manager, or Administrator

To integrate Tenable Vulnerability Management with ARCON using database credentials:

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 **Cassandra**, **Oracle**, **DB2**, **MongoDB**, **PostgreSQL**, **MySQL**, **SQL Server**, or **Sybase ASE**.
12. In the **Auth Type** drop-down box, click **ARCON**.

    The ARCON options appear.
13. Configure each option for the **Database** authentication.

Option	Default Value
Arcon host	(Required) The Arcon IP address or DNS address. **Note:** If your Arcon installation is in a subdirectory, you must include the subdirectory path. For example, type *IP address or hostname/subdirectory path*.
Arcon port	The port on which Arcon listens.
API User	(Required) The API user provided by Arcon.
API Key	(Required) The API key provided by Arcon.
Authentication URL	The URL Tenable Vulnerability Management uses to access Arcon.
Password Engine URL	The URL Tenable Vulnerability Management uses to access the passwords in Arcon.
Username	(Required) The username to log in to the hosts you want to scan.
Arcon Target Type	(Optional) The name of the target type. . Depending on the Arcon

Option	Default Value
	PAM version you are using and the system type the SSH credential has been created with, this is set to **linux** by default. Refer to the Arcon PAM Specifications document (provided by Arcon) for target type/system type mapping for the correct target type value.
Checkout Duration	(Required) The length of time, in hours, that you want to keep credentials checked out in Arcon. Configure the **Checkout Duration** to exceed the typical duration of your Tenable Vulnerability Management scans. If a password from a previous scan is still checked out when a new scan begins, the new scan fails. **Note:** Configure the password change interval in Arcon so that password changes do not disrupt your Tenable Vulnerability Management scans. If Arcon changes a password during a scan, the scan fails.
Use SSL	When enabled, Tenable Vulnerability Management uses SSL through IIS for secure communications. You must configure SSL through IIS in Arcon before enabling this option.
Verify SSL	When enabled, Tenable Vulnerability Management validates the SSL certificate. You must configure SSL through IIS in Arcon before enabling this option.
Targets to Prioritize Credentials	Specify IPs or CIDR blocks on which this credential is attempted before any other credential. To specify multiple IPs or CIDR blocks, use a comma or space-separated list. Using this setting can decrease scan times by prioritizing a credential that you know works against your selected targets. For example, if your scan specifies 100 credentials, and the successful credential is the 59th credential out of 100, the first 58 credentials have to fail before the 59th credential succeeds. If you use **Targets**

Option	Default Value
	To Prioritize Credentials, you configure the scan to use the successful credential first, which allows the scan to access the target faster.

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.

Configure Tenable Vulnerability Management with ARCON (SSH)

In Tenable Vulnerability Management, you can integrate with ARCON using SSH credentials. Complete the following steps to configure Tenable Vulnerability Management with ARCON using SSH.

> **Required User Role:** Standard, Scan Manager, or Administrator

To integrate Tenable Vulnerability Management with ARCON using SSH credentials:

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 **ARCON**.

    The ARCON options appear.
13. Configure each option for the **SSH** authentication.

Option	Default Value
Arcon host	(Required) The Arcon IP address or DNS address. **Note:** If your Arcon installation is in a subdirectory, you must include the subdirectory path. For example, type *IP address or hostname/subdirectory path*.
Arcon port	The port on which Arcon listens.
API User	(Required) The API user provided by Arcon.
API Key	(Required) The API key provided by Arcon.
Authentication URL	The URL Tenable Vulnerability Management uses to access Arcon.
Password Engine URL	The URL Tenable Vulnerability Management uses to access the passwords in Arcon.
Username	(Required) The username to log in to the hosts you want to scan.

Option	Default Value
Arcon Target Type	(Optional) The name of the target type. . Depending on the Arcon PAM version you are using and the system type the SSH credential has been created with, this is set to **linux** by default. Refer to the Arcon PAM Specifications document (provided by Arcon) for target type/system type mapping for the correct target type value.
Checkout Duration	(Required) The length of time, in hours, that you want to keep credentials checked out in Arcon. Configure the **Checkout Duration** to exceed the typical duration of your Tenable Vulnerability Management scans. If a password from a previous scan is still checked out when a new scan begins, the new scan fails. **Note:** Configure the password change interval in Arcon so that password changes do not disrupt your Tenable Vulnerability Management scans. If Arcon changes a password during a scan, the scan fails.
Use SSL	When enabled, Tenable Vulnerability Management uses SSL through IIS for secure communications. You must configure SSL through IIS in Arcon before enabling this option.
Verify SSL	When enabled, Tenable Vulnerability Management validates the SSL certificate. You must configure SSL through IIS in Arcon before enabling this option.
Targets to Prioritize Credentials	Specify IPs or CIDR blocks on which this credential is attempted before any other credential. To specify multiple IPs or CIDR blocks, use a comma or space-separated list. Using this setting can decrease scan times by prioritizing a credential that you know works against your selected targets. For example, if your scan specifies 100 credentials, and the successful credential is the 59th credential out of 100, the first 58 credentials

Option	Default Value
	have to fail before the 59th credential succeeds. If you use **Targets To Prioritize Credentials**, you configure the scan to use the successful credential first, which allows the scan to access the target faster.

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.

What to do next:

To verify the integration is working:

1. On the **Scans** page, click the **Launch** button to initiate an on-demand scan.
2. Once the scan has completed, select the completed scan and look for **Plugin ID 97993** and the corresponding message - *It was possible to log into the remote host via SSH using 'password' authentication*. This validates that authentication was successful.

Configure Tenable Vulnerability Management with ARCON (Windows)

In Tenable Vulnerability Management, you can integrate with ARCON using Windows credentials. Complete the following steps to configure Tenable Vulnerability Management with ARCON using Windows.

> **Required User Role:** Standard, Scan Manager, or Administrator

To integrate Tenable Vulnerability Management with ARCON using Windows credentials:

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 **ARCON**.

    The ARCON options appear.

13. Configure each option for the **Windows** authentication.

Option	Default Value
Arcon host	(Required) The Arcon IP address or DNS address. **Note:** If your Arcon installation is in a subdirectory, you must include the subdirectory path. For example, type *IP address or hostname/subdirectory path*.
Arcon port	The port on which Arcon listens.

Option	Default Value
API User	(Required) The API user provided by Arcon.
API Key	(Required) The API key provided by Arcon.
Authentication URL	The URL Tenable Vulnerability Management uses to access Arcon.
Password Engine URL	The URL Tenable Vulnerability Management uses to access the passwords in Arcon.
Username	(Required) The username to log in to the hosts you want to scan.
Arcon Target Type	(Optional) The name of the target type. . Depending on the Arcon PAM version you are using and the system type the SSH credential has been created with, this is set to **linux** by default. Refer to the Arcon PAM Specifications document (provided by Arcon) for target type/system type mapping for the correct target type value.
Checkout Duration	(Required) The length of time, in hours, that you want to keep credentials checked out in Arcon. Configure the **Checkout Duration** to exceed the typical duration of your Tenable Vulnerability Management scans. If a password from a previous scan is still checked out when a new scan begins, the new scan fails. **Note:** Configure the password change interval in Arcon so that password changes do not disrupt your Tenable Vulnerability Management scans. If Arcon changes a password during a scan, the scan fails.
Use SSL	When enabled, Tenable Vulnerability Management uses SSL through IIS for secure communications. You must configure SSL through IIS in Arcon before enabling this option.
Verify SSL	When enabled, Tenable Vulnerability Management validates the SSL

Option	Default Value
	certificate. You must configure SSL through IIS in Arcon before enabling this option.
Targets to Prioritize Credentials	Specify IPs or CIDR blocks on which this credential is attempted before any other credential. To specify multiple IPs or CIDR blocks, use a comma or space-separated list. Using this setting can decrease scan times by prioritizing a credential that you know works against your selected targets. For example, if your scan specifies 100 credentials, and the successful credential is the 59th credential out of 100, the first 58 credentials have to fail before the 59th credential succeeds. If you use **Targets To Prioritize Credentials**, you configure the scan to use the successful credential first, which allows the scan to access the target faster.

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.

What to do next:

Verify the integration is working.

1. On the **Scans** page, click the **Launch** button to initiate an on-demand scan.
2. Once the scan completes, click the completed scan.

   The scan details appear.

   Look for a message similar to the following- *Microsoft Windows SMB Log In Possible: 10394*. This result validates that authentication was successful.

Tenable Security Center and ARCON

You can integrate Tenable Security Center with Arcon using Windows credentials or SSH credentials. View the corresponding section to configure your Tenable Security Center application with ARCON.

Configure Tenable Security Center with ARCON (Windows)

Configure Tenable Security Center with ARCON (SSH)

Configure Tenable Security Center with ARCON (Windows)

In Tenable Security Center, you can integrate with ARCON using Windows credentials. Complete the following steps to configure Tenable Security Center with ARCON using Windows.

Required Tenable Security Center User Role: Any

To integrate Tenable Security Center with ARCON using Windows credentials:

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
Arcon Host	(Required) The Arcon IP address or DNS address. **Note:** If your Arcon installation is in a subdirectory, you must include the subdirectory path. For example, type *IP address or hostname/subdirectory path*.
Arcon Port	(Required) The port on which Arcon listens. By default, Tenable Security Center uses port 444.
API User	(Required) The API user provided by Arcon.
API Key	(Required) The API key provided by Arcon.
Authentication URL	(Required) The URL Tenable Security Center uses to access Arcon.
Password Engine URL	(Required) The URL Tenable Security Center uses to access the passwords in Arcon.
Username	(Required) The username to log in to the hosts you want to scan.
Checkout Duration	(Required) The length of time, in minutes, that you want to keep credentials checked out in Arcon. Configure the **Checkout Duration** to exceed the typical duration of your Tenable Security Center scans. If a password from a previous scan is still checked out when a new scan begins, the new scan fails. **Tip:** Configure the password change interval in Arcon so that password changes do not disrupt your Tenable Security Center scans. If Arcon changes a password during a scan, the scan fails.

Use SSL	When enabled, Tenable Security Center uses SSL through IIS for secure communications. You must configure SSL through IIS in Arcon before enabling this option.
Verify SSL Certificate	When enabled, Tenable Security Center validates the SSL certificate. You must configure SSL through IIS in Arcon before enabling this option.

9. Click **Submit**.

   Tenable Security Center saves your configuration.

Configure Tenable Security Center with ARCON (SSH)

In Tenable Security Center, you can integrate with Arcon using SSH credentials. Complete the following steps to configure Tenable Security Center with ARCON using SSH.

Required Tenable Security Center User Role: Any

To integrate Tenable Security Center with ARCON using SSH credentials:

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
Arcon Host	(Required) The Arcon IP address or DNS address. **Note:** If your Arcon installation is in a subdirectory, you must include the subdirectory path. For example, type *IP address or hostname/subdirectory path*.
Arcon Port	(Required) The port on which Arcon listens. By default, Tenable Security Center uses port 444.
API User	(Required) The API user provided by Arcon.
API Key	(Required) The API key provided by Arcon.
Authentication URL	(Required) The URL Tenable Security Center uses to access Arcon.
Password Engine URL	(Required) The URL Tenable Security Center uses to access the passwords in Arcon.
Username	(Required) The username to log in to the hosts you want to scan.
Checkout Duration	(Required) The length of time, in minutes, that you want to keep credentials checked out in Arcon. Configure the **Checkout Duration** to exceed the typical duration of your Tenable Security Center scans. If a password from a previous scan is still checked out when a new scan begins, the new scan fails. **Tip:** Configure the password change interval in Arcon so that password changes do not disrupt your Tenable Security Center scans. If Arcon changes a password

	during a scan, the scan fails.
Use SSL	When enabled, Tenable Security Center uses SSL through IIS for secure communications. You must configure SSL through IIS in Arcon before enabling this option.
Verify SSL Certificate	When enabled, Tenable Security Center validates the SSL certificate. You must configure SSL through IIS in Arcon before enabling this option.

9. Click **Submit**.

   Tenable Security Center saves your configuration.

Privilege Escalation with ARCON Credentials

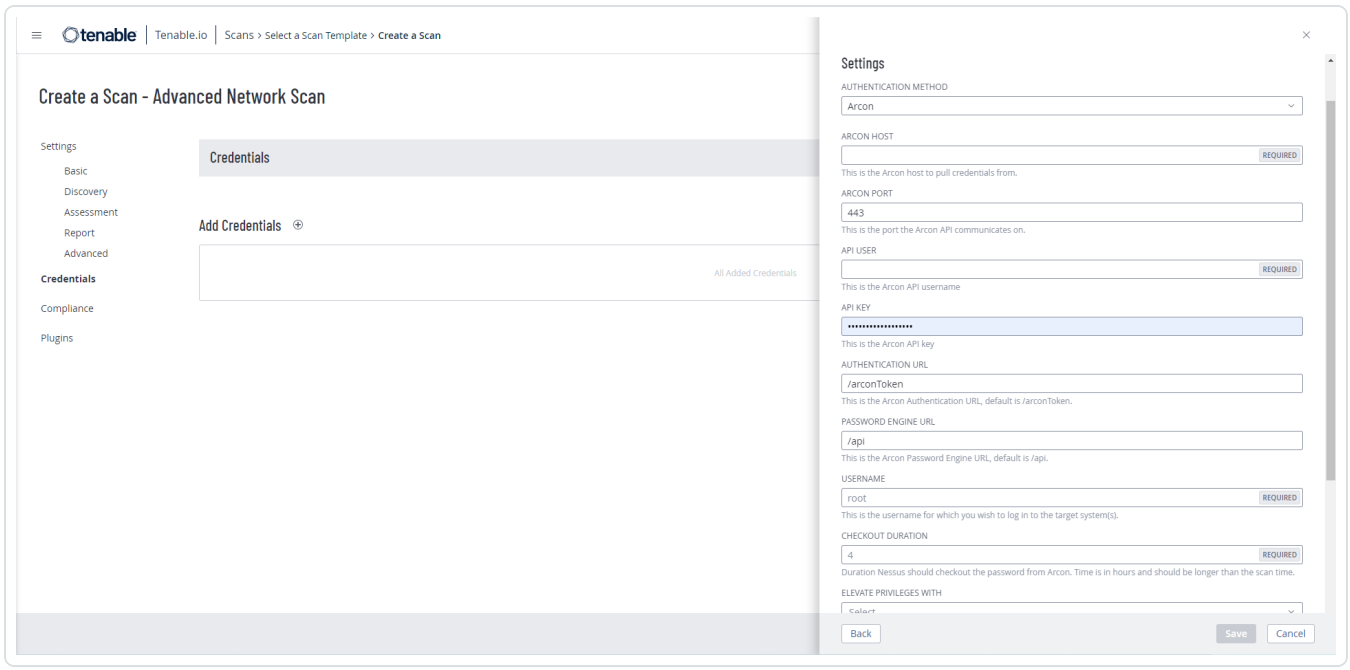
Tenable Vulnerability Management supports the use of privilege escalation, such as *su* and *sudo*, when using SSH through the ARCON authentication method. Arcon credential privilege escalation is available for Tenable Vulnerability Management, Tenable Nessus, and Tenable Security Center.

To configure SSH integration:

1. Log in to Tenable Vulnerability Management, Tenable Nessus, or Tenable Security Center.
2. Click **Scans**
3. Click **+ New Scan**.
4. Select a **Scan Template**.

   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** as the **Type** and ARCON as the **Authentication Method.**



11. Select an option for the **Elevate Privileges With** field.

> **Note:** Multiple options for privilege escalation are supported, including *su*, *su+sudo* and *sudo*. For example, if **sudo** is selected, additional fields for **Escalation Account Name**, **Escalation Username**, and **Location of Sudo (Directory)** are provided and can be completed to support authentication and privilege escalation through Arcon.

> **Note:** Additional information about all of the supported privilege escalation types and their accompanying fields can be found in the Tenable Security Center, Nessus, and Tenable Vulnerability Management user guides.