How-to Guide: Tenable for Arcon

Last Revised: November 19, 2019

Table of Contents

Welcome to Tenable for Arcon

This document provides information and steps for integrating Tenable applications with 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 Nessus Manageror Tenable.io.

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 life cycles of secrets making them easier to incorporate through various strategies

For additional information about Arcon, see the Arcon website.

Requirements

To properly 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.io or Nessus Manager.

Tenable User Role

You must have the appropriate role for your Tenable account as listed below.

Tenable.io - Standard, Scan Manager, Administrator, or System Administrator

Nessus Manager - Standard, Administrator, or System Administrator

Arcon Requirements

You must have an active Arcon account.

Nessus for Arcon Vault

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

Configure Nessus with Arcon (Windows)

Configure Nessus for Arcon (SSH)

Configure Nessus with Arcon (Windows)

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

Requirements

- Nessus Manager account
- Arcon account

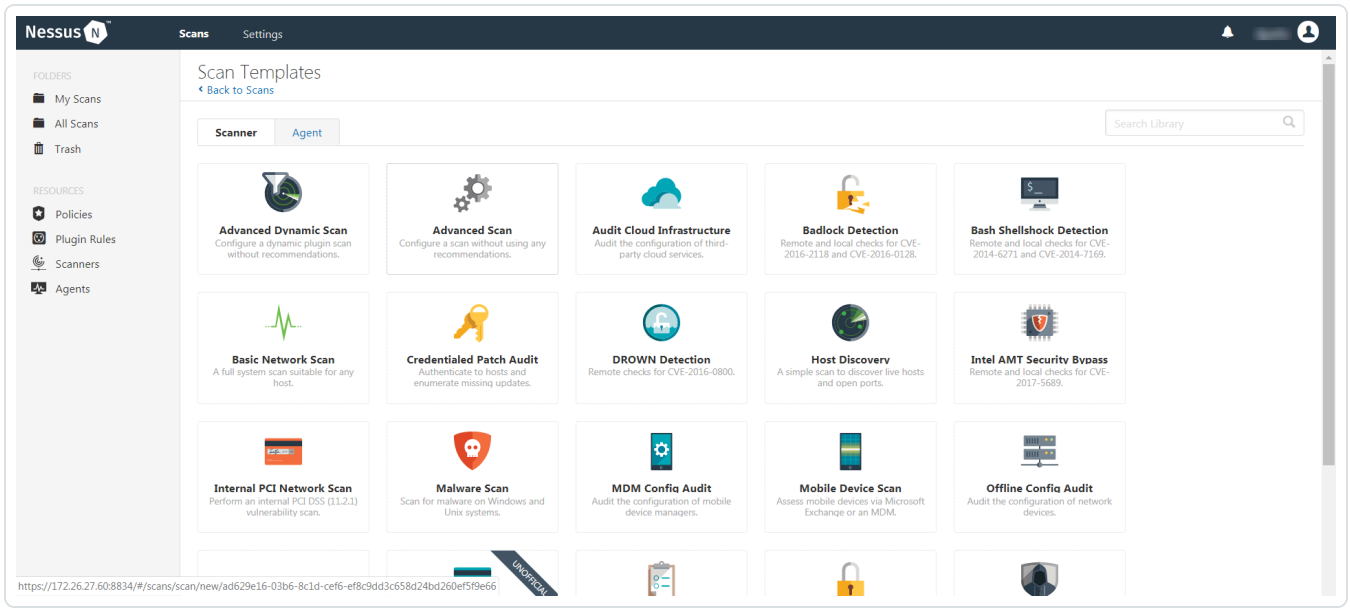
> **Required User Role:** Standard, Administrator, or System Administrator

To integrate Nessus with Arcon using Windows credentials:

1. Log in to Nessus Manager.
2. Click **Scans**.

   The **My Scans** page appears.
3. Click **+ New Scan**.

   The **Scan Templates** page appears.



4. Select a scan template.

   The selected scan template **Settings** 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.

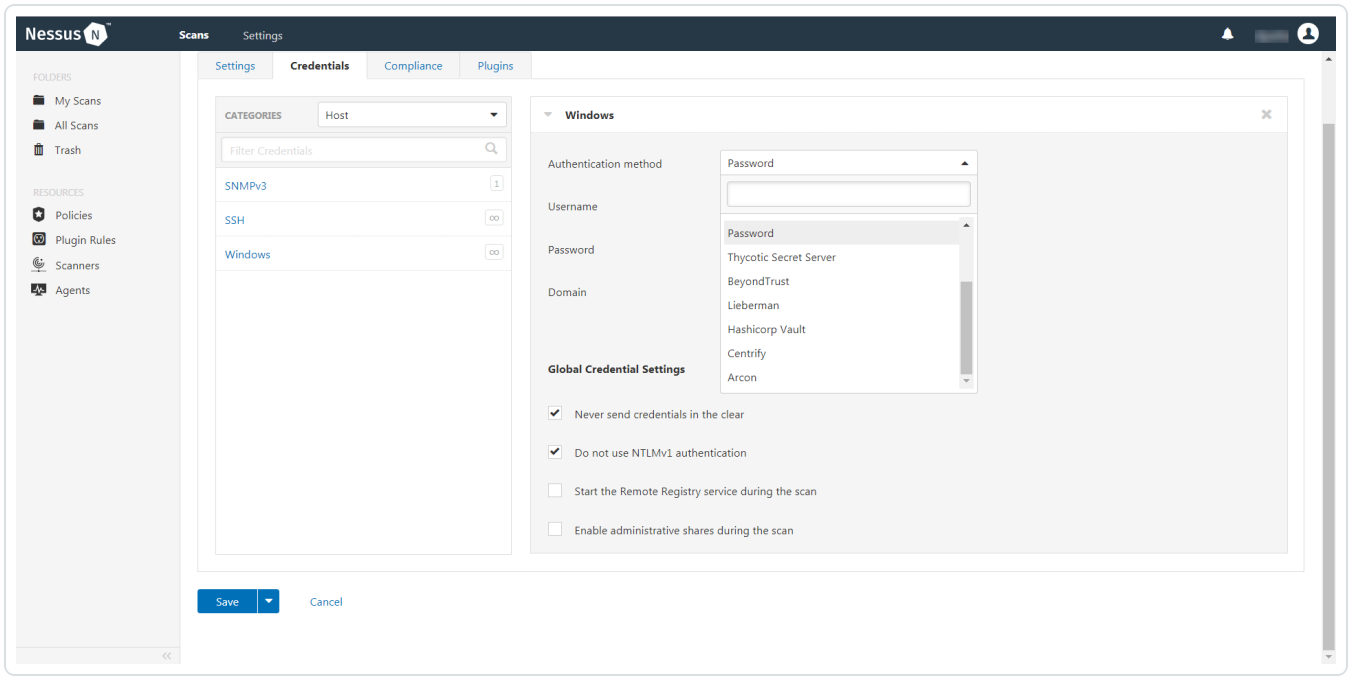
   The **Credentials** options appear. By default, the **Categories** drop-down box displays **Host**.

9. In the left menu, select **Windows**.

   The **Windows** settings appear.

10. In the **Windows** settings, click the **Authentication method** drop-down box.

    The **Authentication method** drop-down box options appear.



11. Select **Arcon**.

    The **Arcon** options appear.

12. Configure the Windows credentials.

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 Nessus Manager uses to access Arcon.
Password Engine URL	The URL Nessus Manager 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 hours, that you want to keep credentials checked out in Arcon. Configure the **Checkout Duration** to exceed the typical duration of your Tenable.io 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.io scans. If Arcon changes a password during a scan, the scan fails.
Use SSL	If enabled, Nessus Manager uses SSL through IIS for secure communications. You must configure SSL through IIS in Arcon before enabling this option.
Verify SSL	If enabled, Nessus Manager validates the SSL certificate. You must configure SSL through IIS in Arcon before

	enabling this option.

13. Click **Save**.

    The credential saves and the **My Scans** page appears.

What to do next:

To verify the integration is working:

1. On the **My 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.

Configure Nessus for Arcon (SSH)

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

Requirements

- Nessus Manager account
- Arcon account

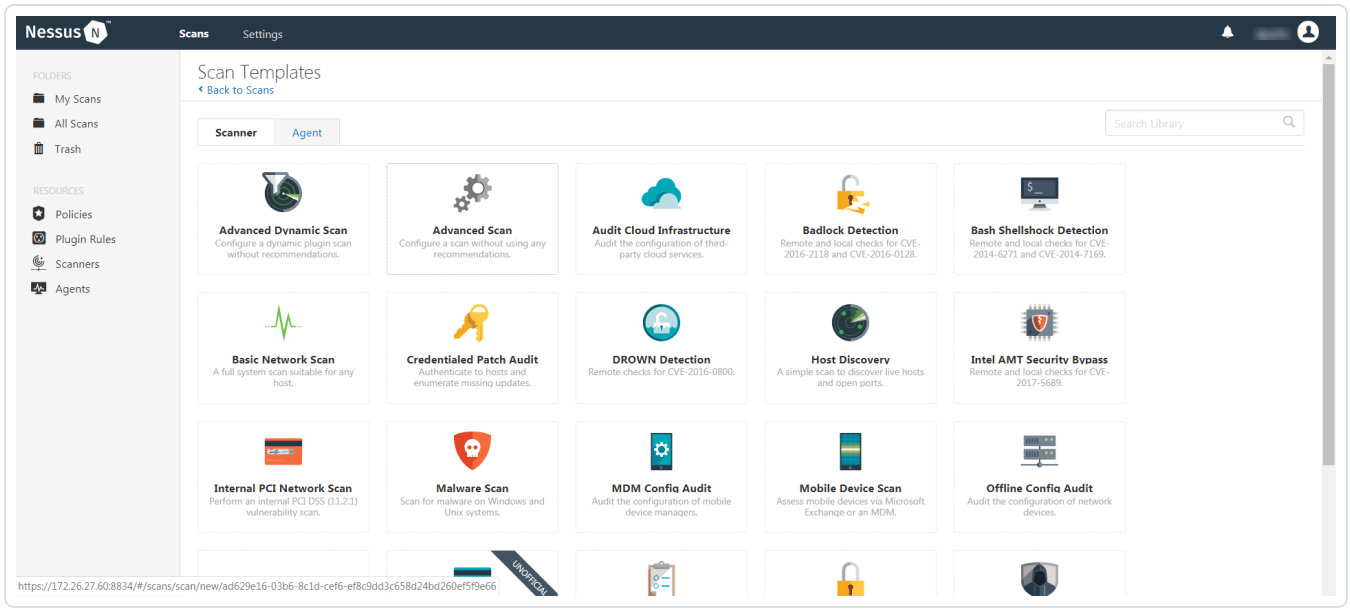
> **Required User Role:** Standard, Administrator, or System administrator

To integrate Nessus with Arcon using SSH credentials:

1. Log in to Nessus Manager.
2. Click **Scans**.

   The **My Scans** page appears.
3. Click **+ New Scan**.

   The **Scan Templates** page appears.



4. Select a scan template.

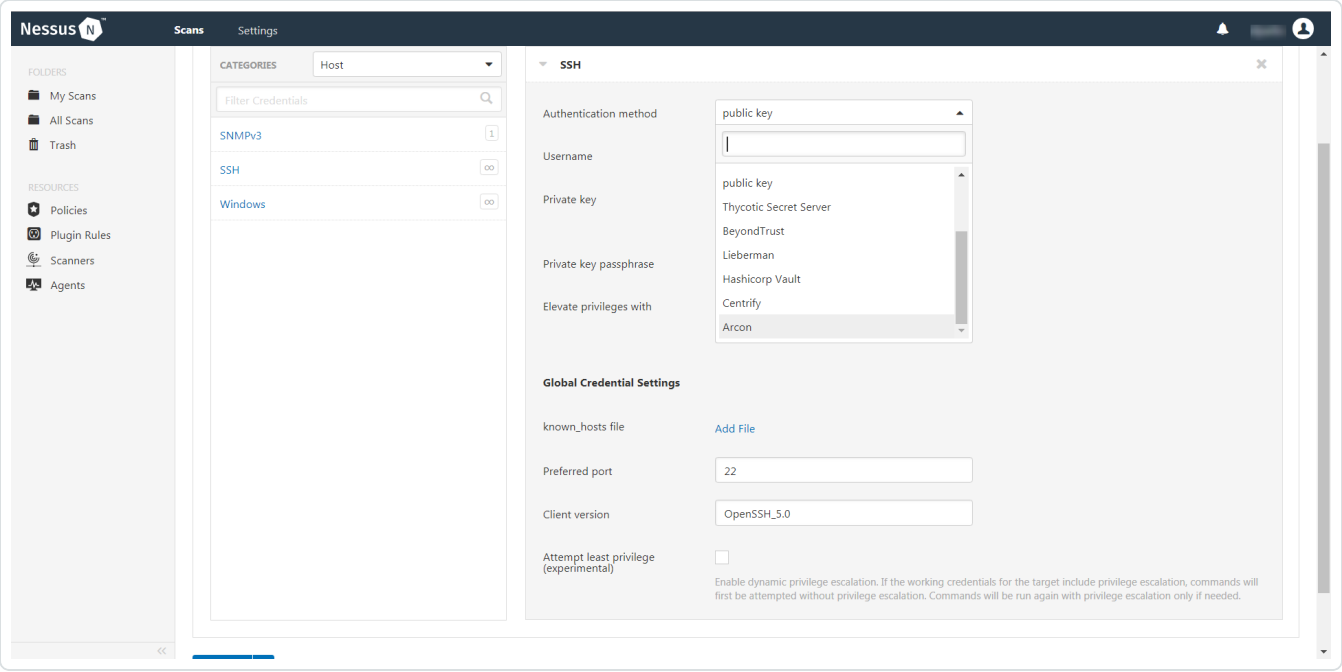
The selected scan template **Settings** page appears.

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. By default, the **Categories** drop-down box displays **Host**.
9. In the left menu, select **SSH**.

   The **SSH** settings appear.
10. In the **SSH** settings section, click the **Authentication method** drop-down box.

    The **Authentication method** drop-down box options appear.



11. Select **Arcon**.

    The **Arcon** options appear.
12. Configure the SSH credentials.

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 Nessus Manager uses to access Arcon.
Password Engine URL	The URL Nessus Manager 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 hours, that you want to keep credentials checked out in Arcon. Configure the **Checkout Duration** to exceed the typical duration of your Tenable.io 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.io scans. If Arcon changes a password during a scan, the scan fails.
Use SSL	If enabled, Nessus Manager uses SSL through IIS for secure communications. You must configure SSL through IIS in Arcon before enabling this option.
Verify SSL	If enabled, Nessus Manager validates the SSL certificate. You must configure SSL through IIS in Arcon before enabling this option.

13. Click **Save**.

What to do next:

To verify the integration is working:

1. On the **My 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.

Tenable.io for Arcon

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

Configure Tenable.io with Arcon (Windows)

Configure Tenable.io for Arcon (SSH)

Configure Tenable.io with Arcon (Windows)

In Tenable.io, you can integrate with Arcon using Windows credentials. Complete the following steps to configure Tenable.io with Arcon using Windows.

Requirements

- Tenable.io account
- Arcon account

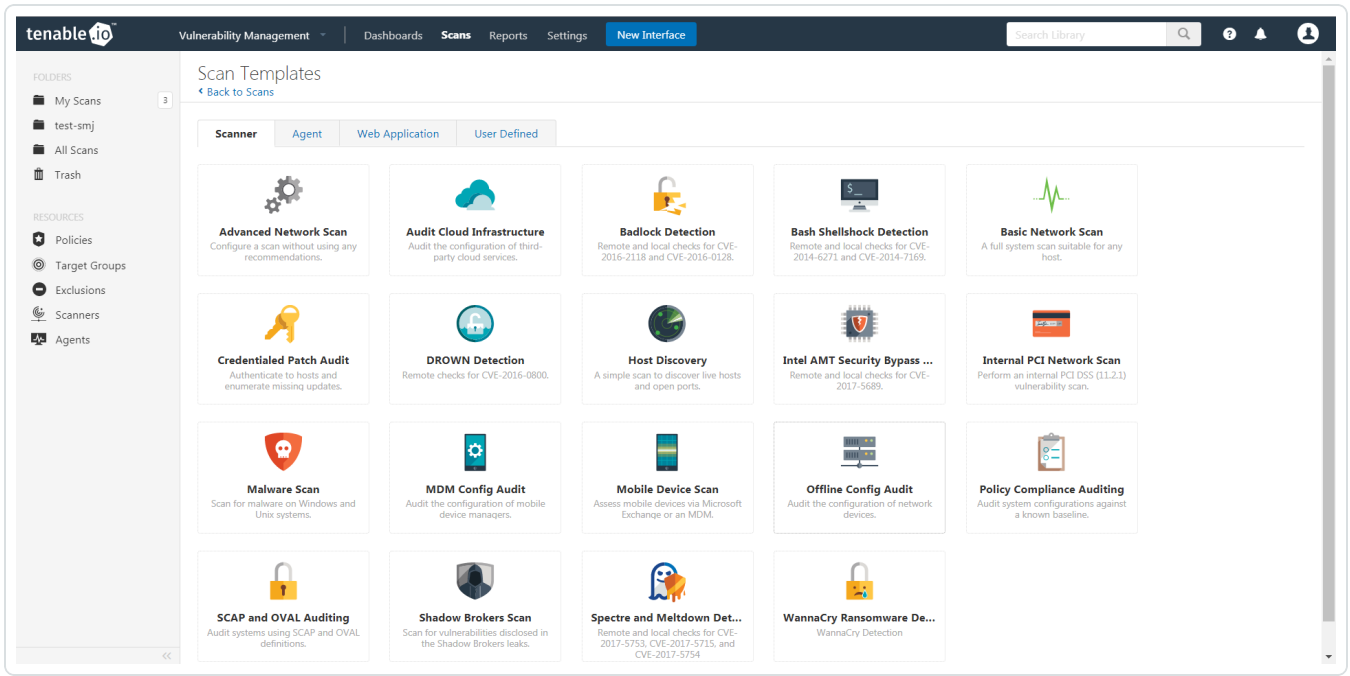
> **Required User Role:** Standard, Scan Manager, or Administrator

To integrate Tenable.io with Arcon using Windows credentials:

1. Log in to Tenable.io.
2. In the top navigation bar, click **Scans**.

   The **My Scans** page appears.
3. Click **+ New Scan**.

   The **Scan Templates** page appears.



4. Select a scan template.

   The selected scan template **Settings** 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. By default, the **Categories** drop-down box displays **Host**.

9. In the left menu, select **Windows**.

   The **Windows** settings appear.

10. In the **Windows** settings section, click the **Authentication method** drop-down box.

    The **Authentication method** drop-down box options appear.

11. Select **Arcon**.

    The **Arcon** options appear.

12. Configure the Windows credentials.

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.io uses to access Arcon.
Password Engine URL	The URL Tenable.io 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 hours, that you want to keep credentials checked out in Arcon. Configure the **Checkout Duration** to exceed the typical duration of your Tenable.io 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.io scans. If Arcon changes a password during a scan, the scan fails.
Use SSL	If enabled, Tenable.io uses SSL through IIS for secure communications. You must configure SSL through IIS in Arcon before enabling this option.
Verify SSL	If enabled, Tenable.io validates the SSL certificate. You must configure SSL through IIS in Arcon before enabling

	this option.

13. Click **Save**.

    The credential saves and the **My Scans** page appears.

What to do next:

Verify the integration is working.

1. On the **My 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.

Configure Tenable.io for Arcon (SSH)

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

Requirements

- Tenable.io account
- Arcon account

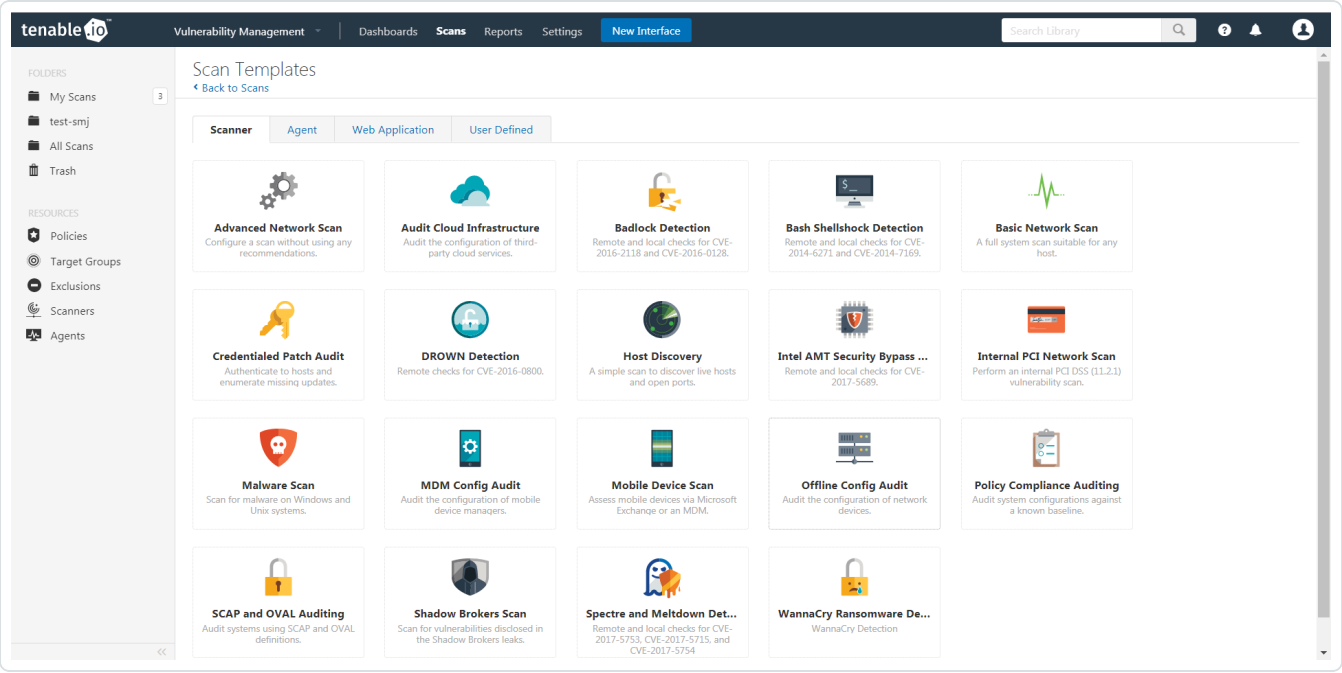
> **Required User Role:** Standard, Scan Manager, or Administrator

To integrate Tenable.io with Arcon using SSH credentials:

1. Log in to Tenable.io.
2. In the top navigation bar, click **Scans**.

   The **My Scans** page appears
3. Click **+ New Scan**.

   The **Scan Templates** page appears.



4. Select a scan template.

   The selected scan template **Settings** 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. By default, the **Categories** drop-down box displays **Host**.

9. In the left menu, select **SSH**.

   The **SSH** settings appear.

10. In the **SSH** settings section, click the **Authentication method** drop-down box.

    The **Authentication method** drop-down box options appear.

11. Select **Arcon**.

    The **Arcon** options appear.

12. Configure the SSH credentials.

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.io uses to access Arcon.
Password Engine URL	The URL Tenable.io 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 hours, that you want to keep credentials checked out in Arcon. Configure the **Checkout Duration** to exceed the typical duration of your Tenable.io 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.io scans. If Arcon changes a password during a scan, the scan fails.
Use SSL	If enabled, Tenable.io uses SSL through IIS for secure communications. You must configure SSL through IIS in Arcon before enabling this option.
Verify SSL	If enabled, Tenable.io validates the SSL certificate. You must configure SSL through IIS in Arcon before enabling this option.

13. Click **Save**.

What to do next:

To verify the integration is working:

1. On the **My 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.