Tenable.io for CyberArk

Introduction

This document describes how to configure Tenable.io for integration with CyberArk Enterprise Password Vault. Please email any comments and suggestions to support@tenable.com.

Security administrators know that conducting network vulnerability assessments means getting access to and navigating an ever-changing sea of usernames, passwords, and privileges. By integrating CyberArk Enterprise Password Vault with Tenable.io, customers now have even more choice and flexibility for reducing the credentials headache.

Benefits of integrating Tenable.io with CyberArk Enterprise Password Vault include:

- Credentials stored in CyberArk Enterprise Password Vault do not need to be managed and updated directly within Tenable.io
- Reduce the time and effort needed to document where credentials are stored within the entire organizational environment
- Automatically enforce security policies within specific departments or for specific business unit requirements, which simplifies compliance
- Reduce the risk of unsecured privileged accounts and credentials across the enterprise

Communication Architecture

The combined Tenable-CyberArk solution works when a Tenable.io scan policy is configured to query a CyberArk Enterprise Password Vault for privileged credentials. At the time of the scan, Tenable.io sends a request to CyberArk to request the privileged account credentials to be used. CyberArk then provides the privileged account credentials back to Tenable.io, and the provided credentials are then used to log in to the target system to identify vulnerabilities and misconfigurations.

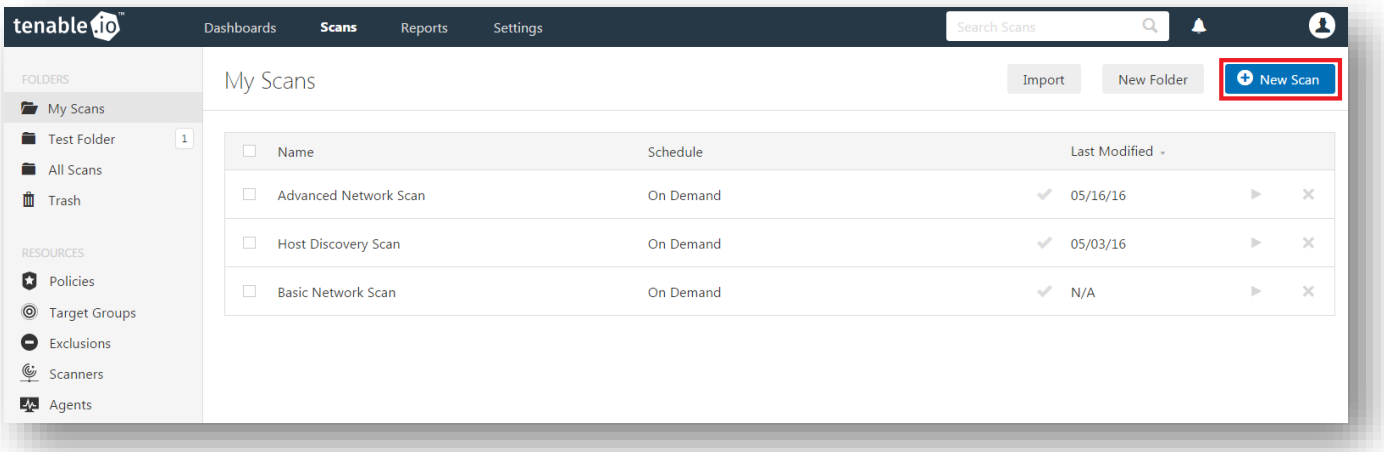
Tenable.io works with CyberArk Enterprise Password Vault version 7.x, 8.x, and 9.0.

Integrating with CyberArk Enterprise Password Vault

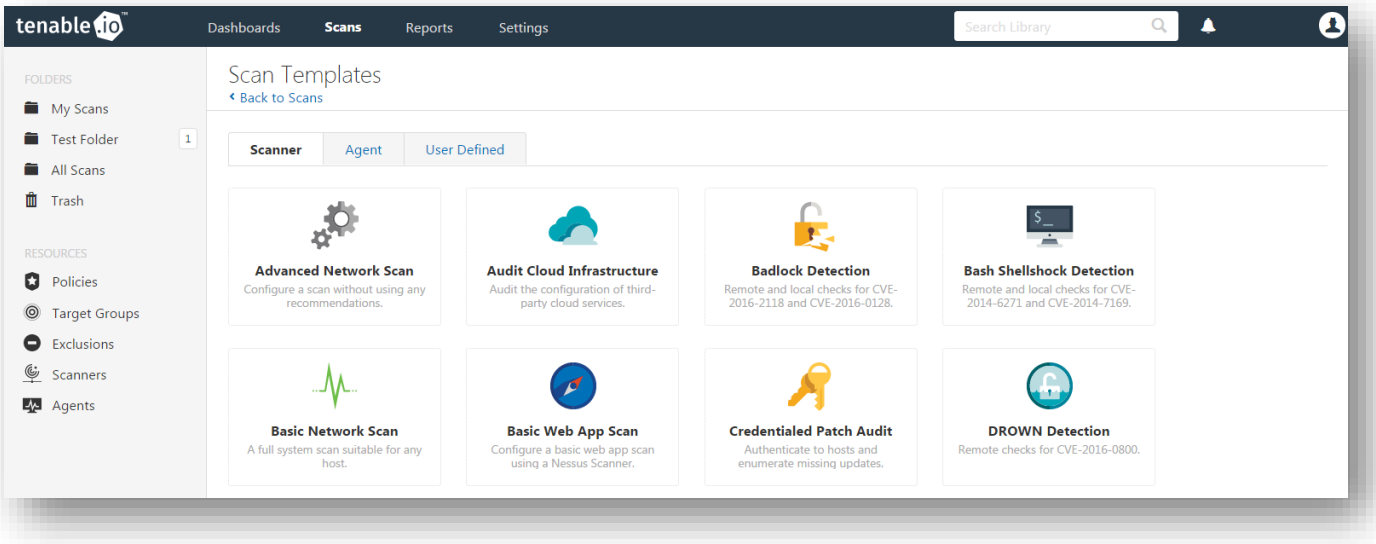
Configuring credentialed network scans using CyberArk's password management solution is a simple process. CyberArk integration with Tenable.io is seamless, so credentials are configured similarly to other credentialed network scans.

Configuring Windows Credentials

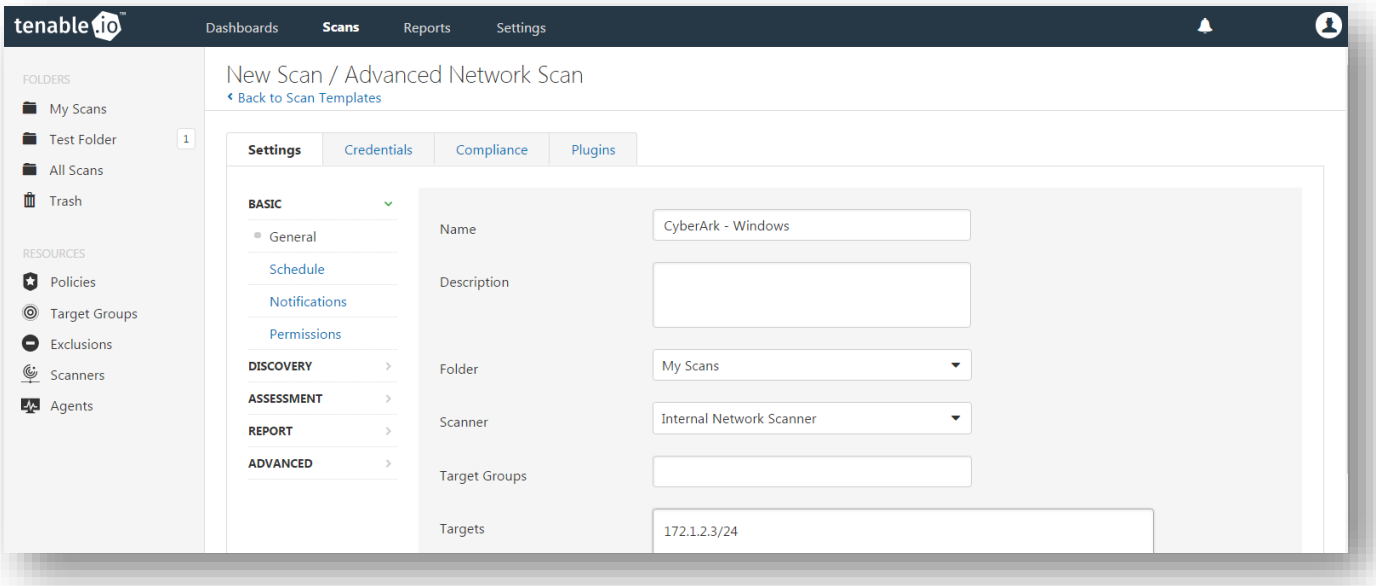
Log in to Tenable.io and click "**Scans**" and then "**+ New Scan**" to configure Tenable.io for credentialed scans of Windows systems using CyberArk's password management solution.



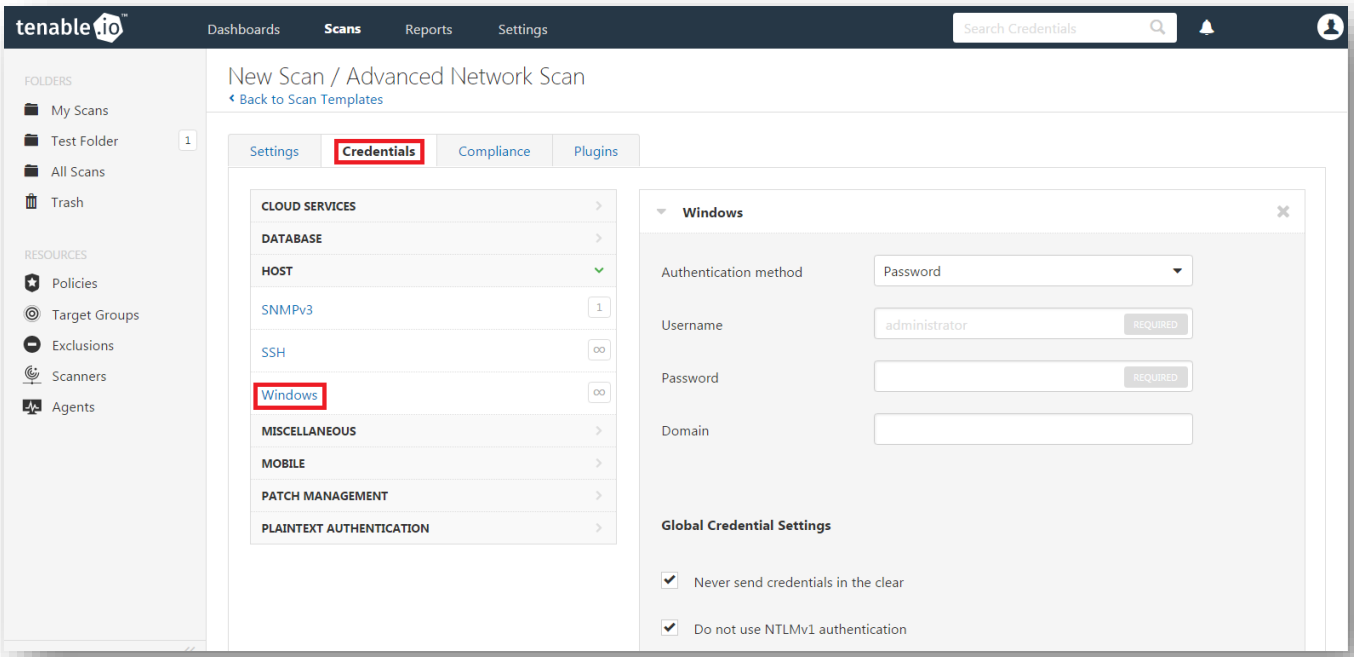
Select a “Scan Template” for the scan type required for your scan. For demonstration purposes, the “Advanced Network Scan” template will be used.



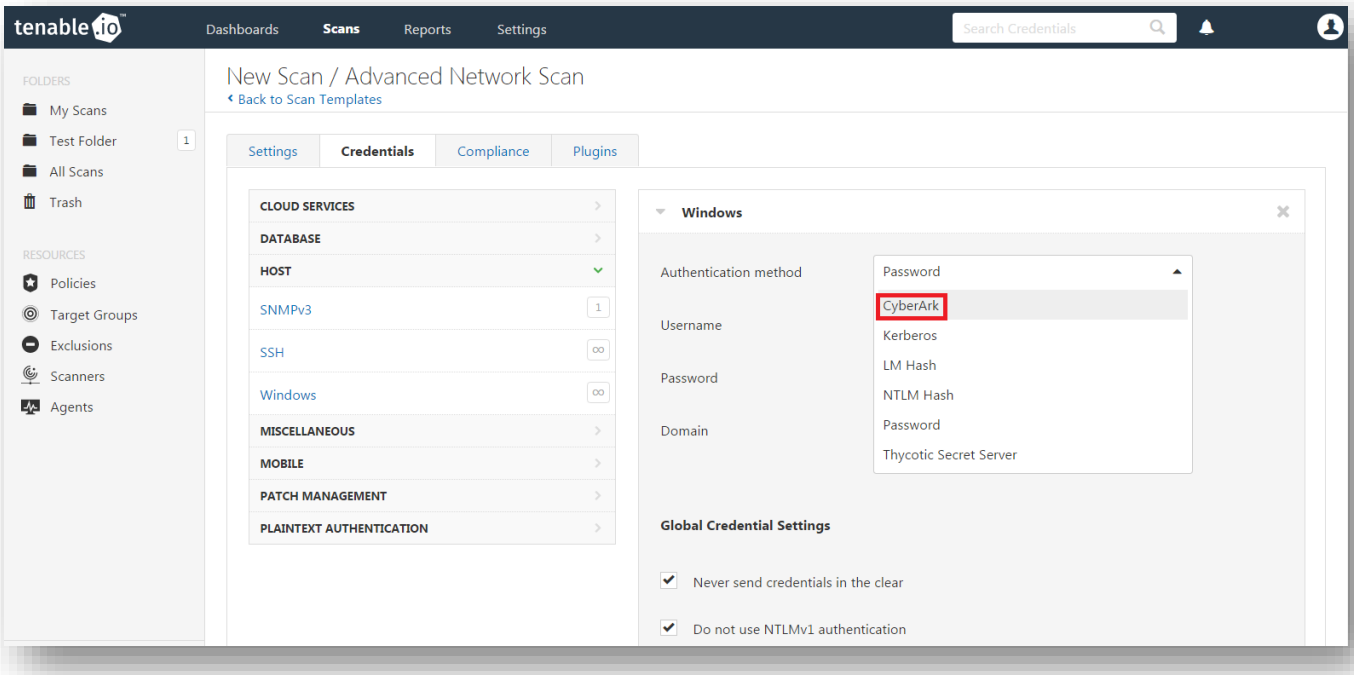
To configure a credentialed scan for Windows systems using CyberArk’s password management solution, enter a descriptive “**Name**” and enter the IP address(es) or hostname(s) of the scan “**Targets**”.



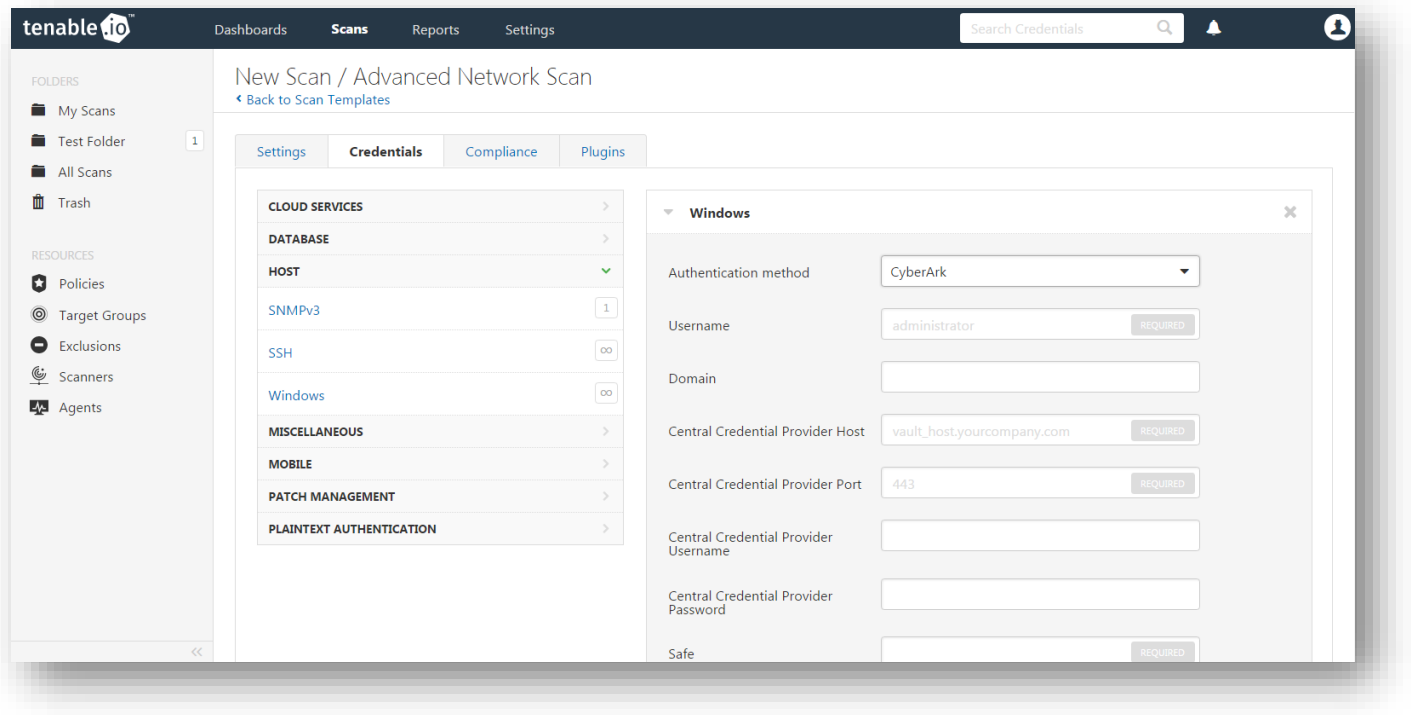
Once the "Name" and "Targets" have been configured, click "**Credentials**" (highlighted below) and then select "**Windows**" from the left-hand menu (highlighted below).



Click the "**Authentication method**" drop-down and select "**CyberArk**".



Configure each field for Windows authentication. Refer to the table below for a description of each field. Once the Windows credentials have been configured, click "**Save**" to finalize the changes.



The table below contains a description of each option:

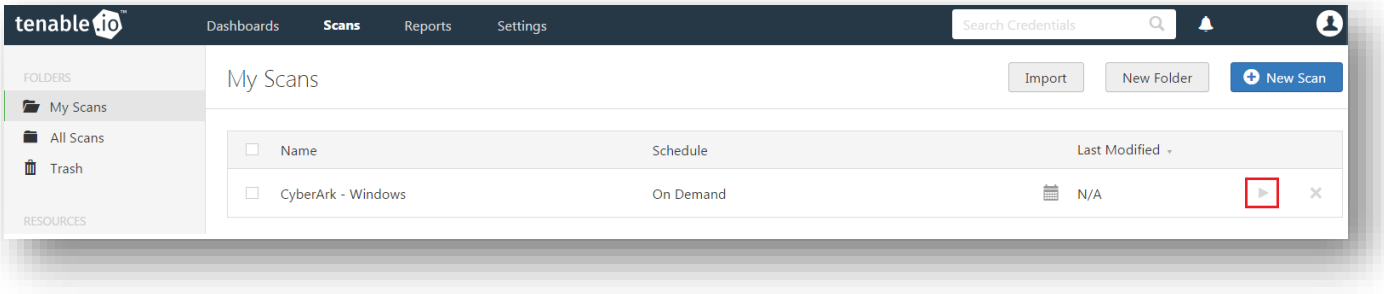
Option	Description
Username	The target system's username
Domain	This is an optional field if the supplied username is part of a domain
Central Credential Provider URL Host	The CyberArk Central Credential Provider IP/DNS address
Central Credential Provider URL Port	The port on which the CyberArk Central Credential Provider listens
Central Credential Provider Username	If the CyberArk Central Credential Provider is configured to use basic authentication, you can fill in this field for authentication.
Central Credential Provider Password	If the CyberArk Central Credential Provider is configured to use basic authentication, you can fill in this field for authentication.
Safe	The safe on the CyberArk Central Credential Provider server that contains the authentication information to be retrieved
AppID	The AppID that has been allocated permissions on the CyberArk Central Credential Provider to retrieve the target password

Folder	The folder on the CyberArk Central Credential Provider server that contains the authentication information to be retrieved
PolicyID	The PolicyID assigned to the credentials to be retrieved from the CyberArk Central Credential Provider
Use SSL	If CyberArk Central Credential Provider is configured to support SSL through IIS, select this option for secure communication. (Recommended)
Verify SSL Certificate	If CyberArk Central Credential Provider is configured to support SSL through IIS, select this option to validate the certificate. (Recommended)

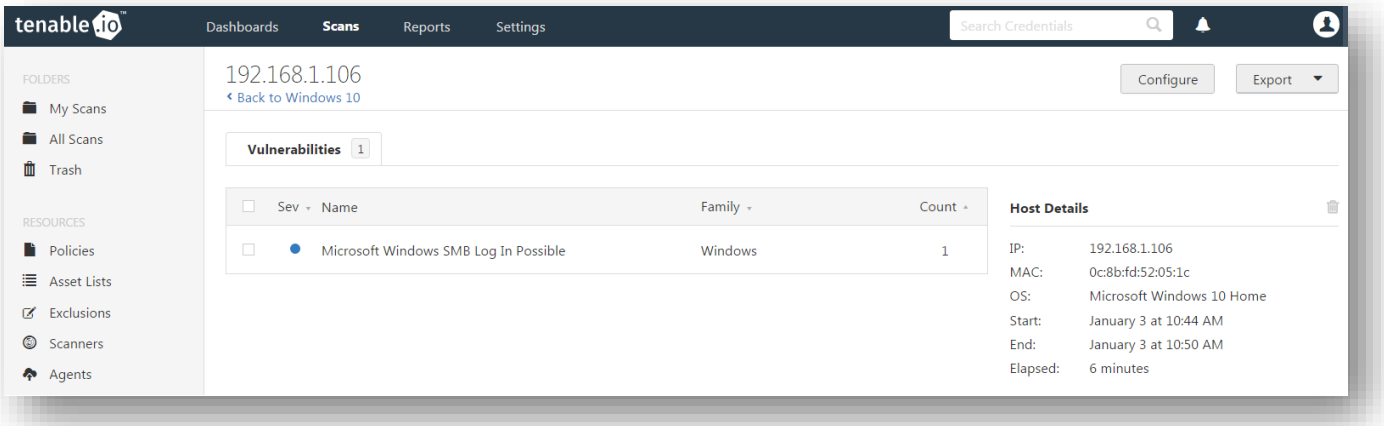
Tenable strongly recommends encrypting communication between Tenable.io and the CyberArk AIM gateway using HTTPS and/or client certificates. For information on securing the connection, refer to the "Tenable.io User Guide" and the "Central Credential Provider Implementation Guide" located at http://www.cyberark.com (login required).

Once the options to reach the CyberArk Enterprise Password Vault are set, click "**Save**" to save the changes.

To verify the integration is working, click the "**Launch**" button (highlighted below) to initiate an on-demand scan.



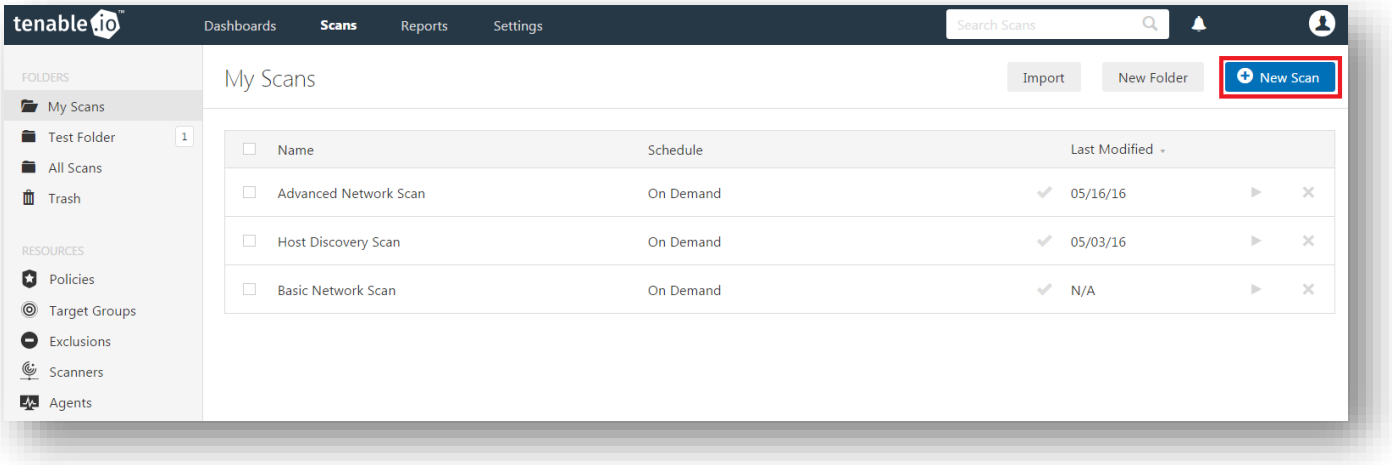
Once the scan has completed, select the completed scan and look for "Plugin ID 10394" (shown below), which validates that authentication was successful. If the authentication is not successful, refer to the "Debugging CyberArk Issues" section of this document.



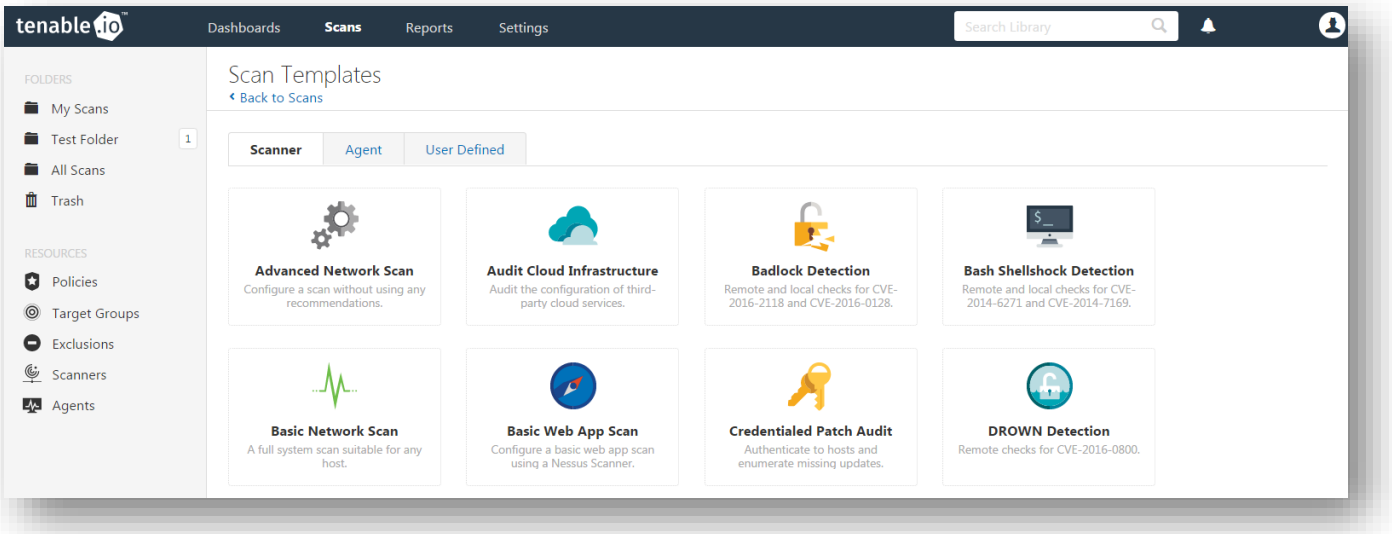
Configuring Linux Credentials

Configuring Linux credentialed scans follows the same basic steps as Windows credentialed scans with only a few minor differences.

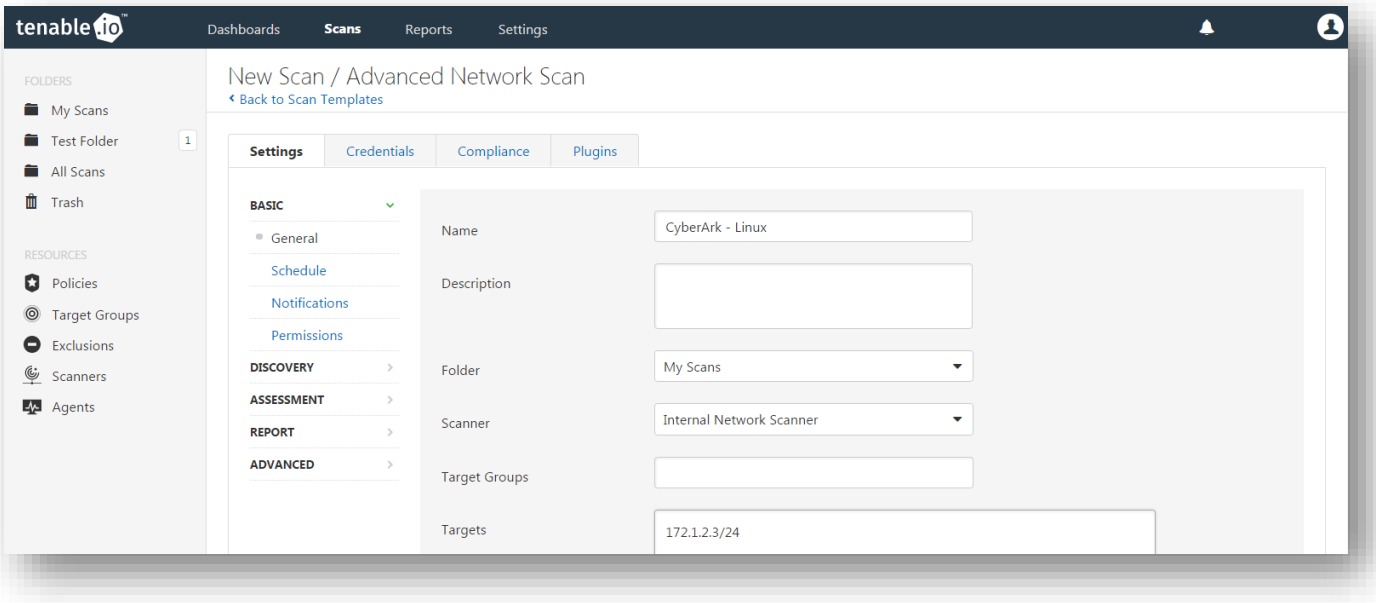
Log in to Tenable.io and click "**Scans**" and then "**+ New Scan**" to begin the Linux credentialed scan configuration.



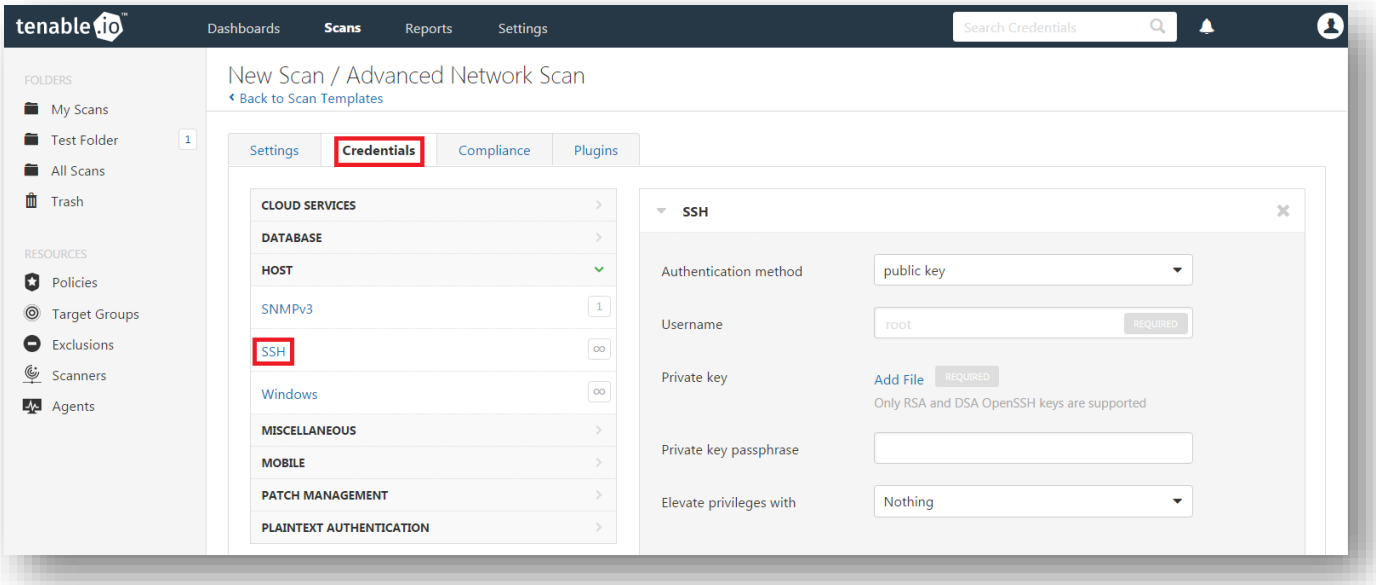
Select a "Scan Template" for the scan type required for your scan. For demonstration purposes, the "Advanced Network Scan" template will be used.



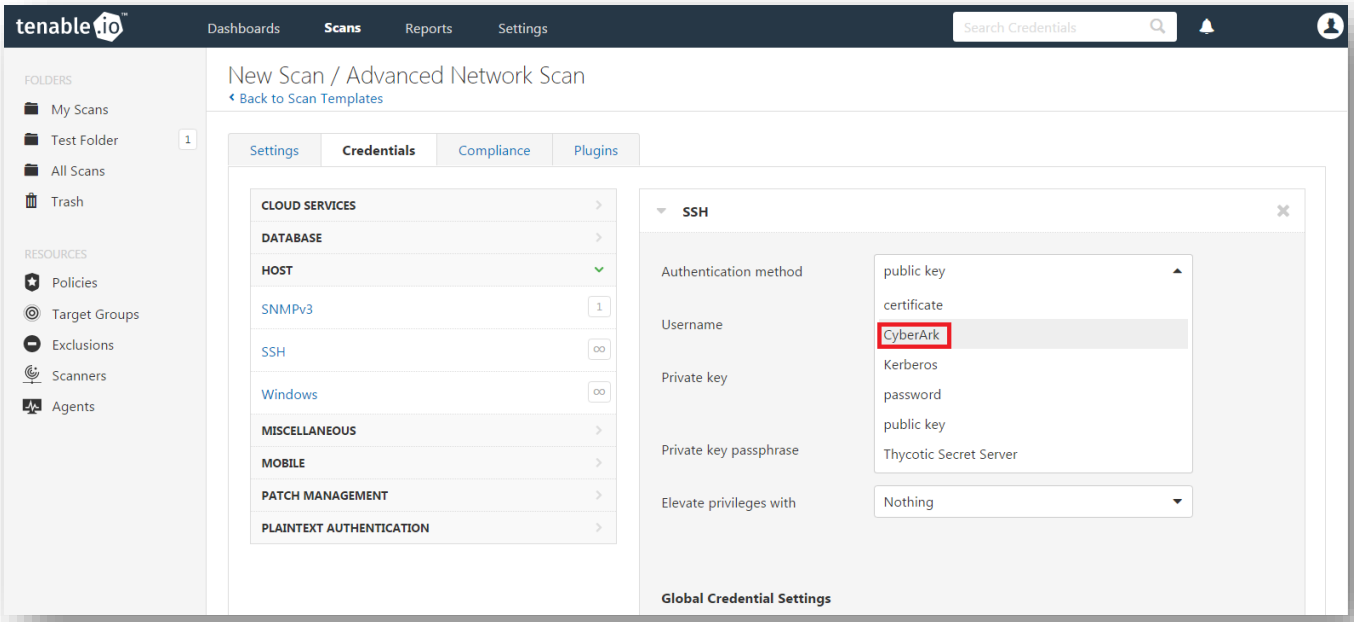
To configure a credentialed scan for Linux systems using CyberArk's password management solution, enter a descriptive "**Name**" and enter the IP address(es) or hostname(s) of the scan "**Targets**".



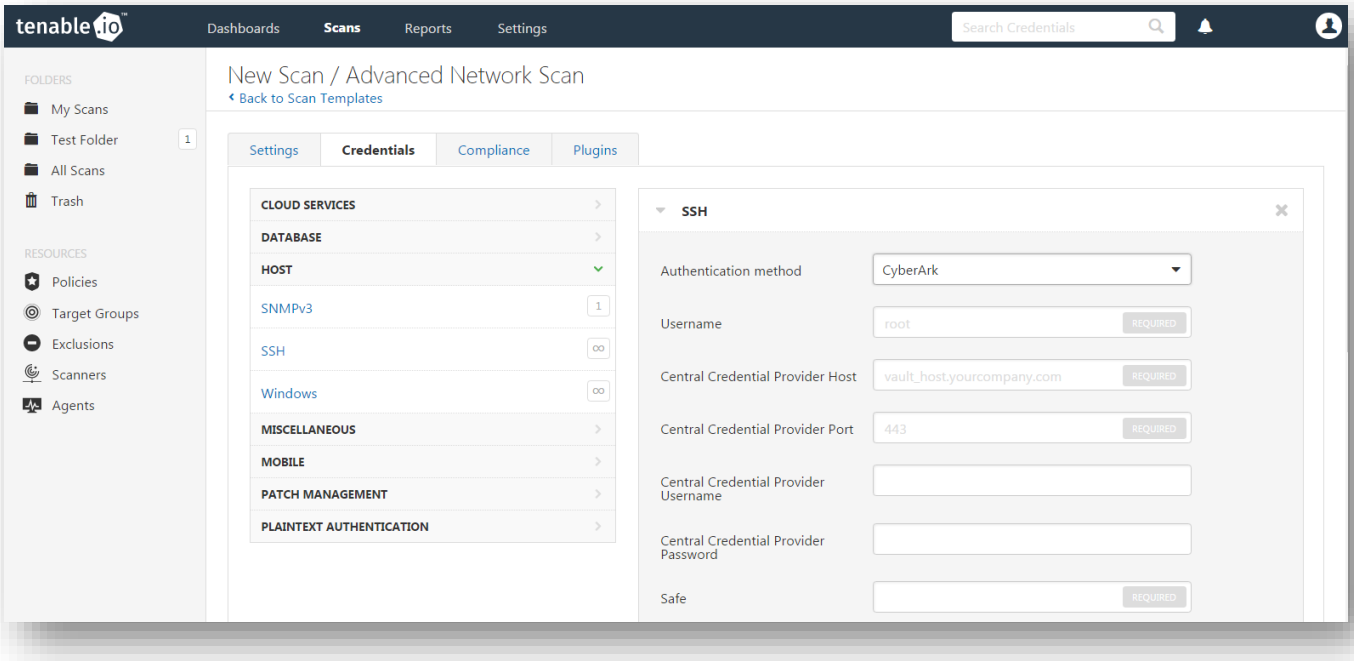
Once the "Name" and "Targets" have been configured, click "**Credentials**" (highlighted below) and then select "**SSH**" from the left-hand menu (highlighted below).



Click the "**Authentication method**" drop-down and select "**CyberArk**".



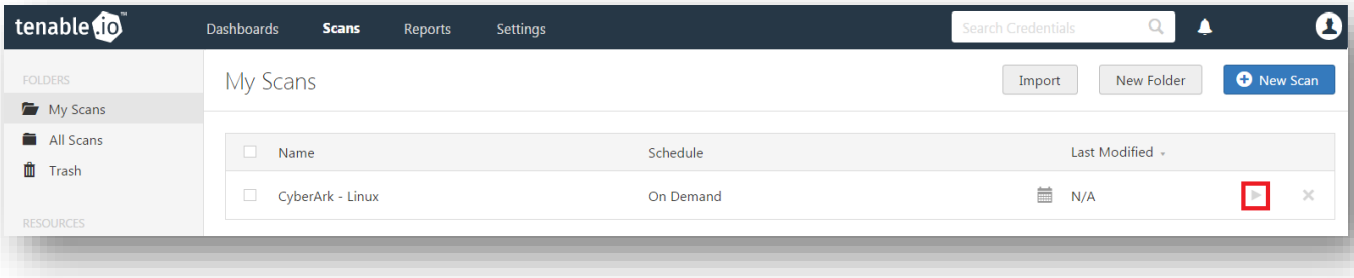
Configure each field for SSH authentication. Refer to the table below for a description of each field. Once the SSH credentials have been configured, click "**Save**" to finalize the changes.



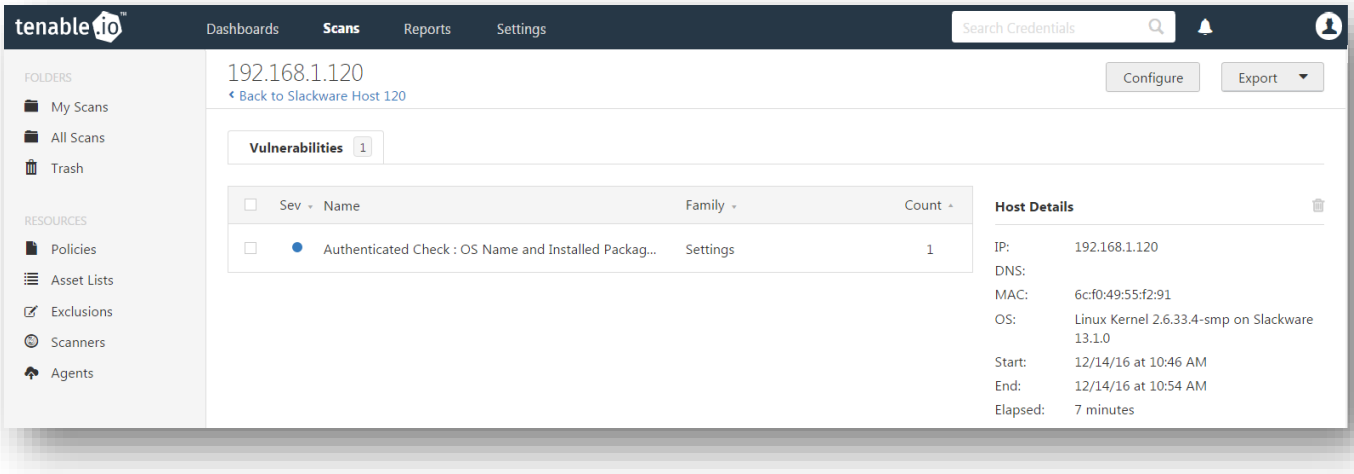
The table below contains a description of each option:

Option	Description
Username	The target system's username
Central Credential Provider URL Host	The CyberArk Central Credential Provider IP/DNS address
Central Credential Provider URL Port	The port on which the CyberArk Central Credential Provider listens
Central Credential Provider Username	If the CyberArk Central Credential Provider is configured to use basic authentication, you can fill in this field for authentication.
Central Credential Provider Password	If the CyberArk Central Credential Provider is configured to use basic authentication, you can fill in this field for authentication.
Safe	The safe on the CyberArk Central Credential Provider server that contains the authentication information to be retrieved
AppID	The AppID that has been allocated permissions on the CyberArk Central Credential Provider to retrieve the target password
Folder	The folder on the CyberArk Central Credential Provider server that contains the authentication information to be retrieved
PolicyID	The PolicyID assigned to the credentials to be retrieved from the CyberArk Central Credential Provider
Use SSL	If CyberArk Central Credential Provider is configured to support SSL through IIS, select this option for secure communication. (Recommended)
Verify SSL Certificate	If CyberArk Central Credential Provider is configured to support SSL through IIS, select this option to validate the certificate. (Recommended)
CyberArk elevate privileges with	Choose the method with which the user account specified in "username" will elevate privileges. If a method is chosen, additional fields will appear to configure the privilege escalation. Refer to the "Privilege Escalation with CyberArk Credentials" section of this document for additional details.

To verify the integration is working, click the "**Launch**" button (highlighted below) to initiate an on-demand scan.

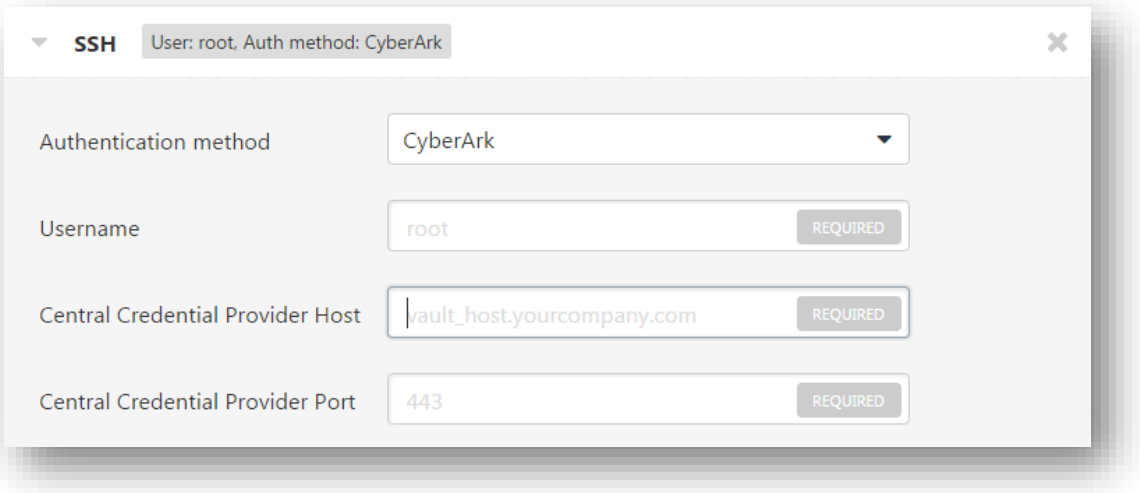


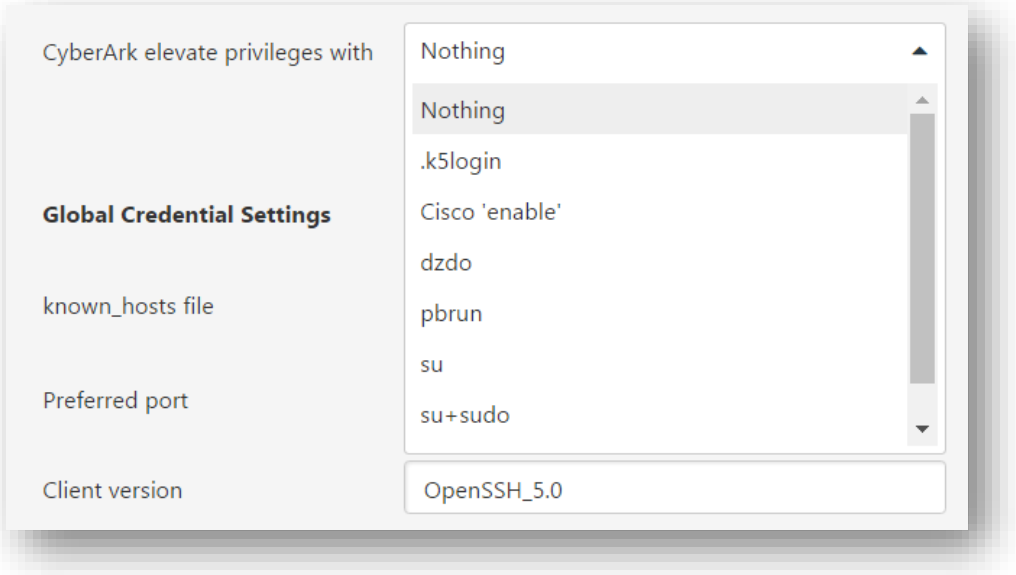
Once the scan has completed, select the completed scan and look for "Plugin ID 12634", which validates that authentication was successful. If the authentication is not successful, refer to the "Debugging CyberArk Issues" section of this document.



Privilege Escalation with CyberArk Credentials

Tenable.io supports the use of privilege escalation, such as “su” and “sudo”, when using SSH through the CyberArk authentication method. When adding a CyberArk Password Vault credential set, select “SSH” as the “Type” and “CyberArk” as the “Authentication Method”:

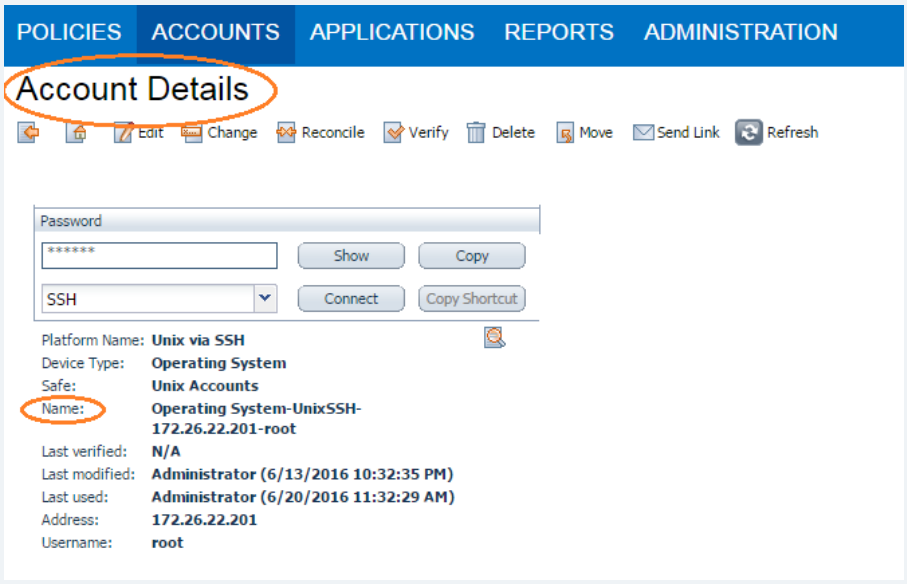




As shown above, an option for “CyberArk elevate privileges with” appears near the bottom of the configuration page. Multiple options for privilege escalation are supported, including “su”, “su+sudo”, and “sudo”. For example, if “sudo” is selected, additional fields for “sudo user”, “CyberArk Account Details Name”, and “Location of sudo (directory) are provided and can be completed to support authentication and privilege escalation through CyberArk Password Vault. Additional information about all of the supported privilege escalation types and their accompanying fields can be found in the “Tenable.io User Guide”.

When asked for a “CyberArk Account Details Name”, perform the following steps to obtain the correct value:

1. Log in to CyberArk Password Vault.
2. Choose the secret (password) you wish to use.
3. Look at the name parameter (such as in the image below) in the Account Details page; this is the value to supply in the “CyberArk Account Details Name” field.



Additional Information about CyberArk Enterprise Password Vault

CyberArk Domain and DNS Support

Tenable’s support for CyberArk allows Tenable.io to use its target list to query CyberArk Enterprise Password Vault for the target system’s credentials, and Tenable.io can use a flexible system to allow for DNS and domain support. Below is the explanation of the logic used by Tenable.io for scans using credentials from CyberArk Enterprise Password Vault.

Tenable.io Priority Scanning for CyberArk

Tenable.io sets a priority system that allows for flexible querying. The following is set out to describe the order Tenable.io tries values and the logic behind it.

1. Tenable.io will query CyberArk with the target value entered into the Tenable.io “Targets” configuration field. For example, if you put a FQDN in the target list, Tenable.io will query CyberArk with the address value of the FQDN. If you enter an IP address or range such as 192.168.1.1-20, Tenable.io will try to query using the IP address or IP range of the target system(s) in the CyberArk “Address” value. If the target system uses FQDN and can be resolved, then it will be contacted.

2. If the target value fails, Tenable.io will then look to see if there is a domain value (for a Windows system). If a domain value is present, Tenable.io will query CyberArk using the domain value for the address value to attempt to use domain credentials.

3. If the configured target value and the domain value both fail, Tenable.io will then pull the IP address of the system. If the IP address does not match one of the IP addresses supplied in the target list, Tenable.io will then query CyberArk using the IP address of the target itself. This is checked against the target value in the configuration to prevent querying CyberArk twice with the same value.

Retrieving Addresses to Scan from CyberArk

Tenable.io is able to use a feature in CyberArk to pull a list of targets to scan. Below is a description of how to pull the target system values and how to use them.

The following method of target address retrieval cannot be done from the default administrator account. You must create an account that is a member of the PVWAMonitor group to generate the following reports.

1. Click on Report at the top of the CyberArk Enterprise Password Vault web interface.
2. Click “Generate Report” at the top of the Report page.
3. Choose “Privileged Account Inventory”.
4. Click “Next”.
5. Specify the search parameters for the systems you want to scan.
6. Click “Next”.
7. Click “Finish”.
8. Download the CSV or XLS report.
9. Confirm the targets for Tenable.io to scan.
10. Confirm the values can all be resolved by Tenable.io.
11. Copy the values from the “Target system address” column.
12. Enter the values into Tenable.io. Either:
    a. Paste the values from addresses into the target list in Tenable.io.
    b. Paste the values into a file and use a file target list in Tenable.io.

Debugging CyberArk Issues

To enable debugging when you configure a scan in Tenable.io, go to Settings->Advanced->Debug Settings and Check “Enable plugin debugging”. If an issue is found, review the results of plugin “Debugging Log Report” (84239). If debug output for the system exists in the debug log, one or more of the following files will be present:

- logins.nasl: Used for Windows credentials. Shows higher level failures in Windows authentication
- logins.nasl~CyberArk: Used to output specific CyberArk- related debug information
- ssh_settings: Used for SSH credentials. Shows higher level failures in SSH authentication
- ssh_settings~CyberArk: Used to output specific CyberArk-related debug information

Example of output:

```
[2015-11-17 22:17:04] HTTP/1.1 500 Internal Server Error returned
[2015-11-17 22:17:04] HTTP 500 : Server was unable to process request. ---&gt;
      APPAP004E Password object matching query [Safe=Unix
      Accounts;UserName=credtester;Folder=Root;Address=172.26.22.26] was not found
      (Diagnostic Info: 5). Please check that there is a password object that answers
```

```
      your query in the Vault and that both the Provider and the application user
      have the appropriate permissions needed in order to use the password.
[2015-11-17 22:17:04] HTTP/1.1 500 Internal Server Error returned
[2015-11-17 22:17:04] HTTP 500 : Server was unable to process request. ---&gt;
      APPAP004E Password object matching query [Safe=Unix
      Accounts;UserName=admin;Folder=Root;Address=172.26.22.26] was not found
      (Diagnostic Info: 5). Please check that there is a password object that answers
      your query in the Vault and that both the Provider and the application user
      have the appropriate permissions needed in order to use the password.
[2015-11-17 22:17:04] HTTP/1.1 500 Internal Server Error returned
[2015-11-17 22:17:04] HTTP 500 : Server was unable to process request. ---&gt;
      APPAP229E Too many password objects matching query [Safe=Unix
      Accounts;UserName=admin;Folder=Root] were found: (Safe=Unix
      Accounts;Folder=Root;Object=Operating System-WinDesktopLocal-172.26.22.205-
      admin, Safe=Unix Accounts;Folder=Root;Object=Operating System-WinDesktopLocal-
      172.26.22.66-admin and more. See trace log for more information). (Diagnostic
      Info: 41)
```

The Tenable.io Priority Scanning for CyberArk section shows that a single system may send multiple requests that fail before finding a successful one. Because of this, the output to the debugging log may not show an issue with the scan, but it can be used as an audit trail if there is an issue. To address issues using the log, look for the parameters to match the intended query and see what error output was reported for that query. For example, if you intended to scan target 172.26.22.66 using parameters of (`Safe=Unix Accounts;UserName=admin;Folder=Root`), then you could discern from the log above that the reason the scan failed is because there were too many matching items to this query, and therefore no results were returned.

About Tenable Network Security

Tenable Network Security transforms security technology for the business needs of tomorrow through comprehensive solutions that provide continuous visibility and critical context, enabling decisive actions to protect your organization. Tenable eliminates blind spots, prioritizes threats, and reduces exposure and loss. With more than one million users and more than 20,000 enterprise customers worldwide, organizations trust Tenable for proven security innovation. Tenable's customers range from Fortune Global 500 companies, to the U.S. Department of Defense, to mid-sized and small businesses in all sectors, including finance, government, healthcare, higher education, retail, and energy. Transform security with Tenable, the creators of Nessus and leaders in continuous monitoring, by visiting tenable.com.