Tenable and Fudo Integration Guide

Last Revised: April 09, 2025

Table of Contents

Welcome to Fudo Enterprise

This document provides information and steps for integrating Tenable Vulnerability Management or Tenable Nessus Manager with the Fudo Privileged Access Management (PAM) System.

Fudo PAM is a privileged access management (PAM) software solution that stores, manages and monitors credentials. Tenable can integrate with Fudo PAM so that scans use credentials managed by the PAM. This results in better credential management and an improved view of cyber exposure.

Integration Tips

Fudo Enterprise is required

There are two Fudo PAM products, Fudo ONE (free version) and Fudo Enterprise (paid version). Currently, Fudo is only compatible with Fudo Enterprise, because the [secret checkout protocol](#) is required.

Target username is required

You have to specify the user to log into the target system. This is due to how Fudo's Secret Checkout API currently functions. The same is true for privilege escalation, if an escalation user is needed (i.e., user to escalate to) it must be entered.

API Authentication

The integration authenticates to the API using the specified API username and password. These should be the username and password of a user that has access to the Fudo PAM portal as well as to the desired target account(s). The integration first authenticates to the Fudo Access Gateway using the API username and password to retrieve a session ID, which is used to authenticate subsequent requests.

Account Name, Account ID, or Address

To check out the credential, you may enter the name of the account (Fudo Account Name) or an exact account ID (Fudo Account ID). When using the account name, the integration must make an additional HTTP request to list accounts, then it checks out the first one matching the name.

When checking out by **Account Name**, you may also optionally enter the associated address of the account (Fudo Account Address), or select **Use Target Address** to further limit credential queries to the target IP address or hostname. It is important to note that **Use Target Address** overrides anything specified as the Fudo Account Address.

It is also possible to query only by account address. For example, if you were to omit **account name** but specify an **Account Address**, the integration then lists accounts and uses the first one matching the specified address. This is also true for **Use Target Address**. It is important to note that when **Use Target Address** is given, the value of **Fudo Account Address** is ignored.

If you do not specify anything (i.e., Fudo Account Name, Fudo Account ID, or Fudo Account Address, and Use Target Address is unchecked), the Fudo integration does not return any credentials and logs an error in the debug logs.

Force and Check in Options: Not recommended

Fudo offers an option to check in passwords when the integration is done using them. Fudo also offers an ability to "force" checkout if another user has the password checked out. These options are available when configuring a credential using the integration, but they are not recommended.

Instead of using check in, Tenable recommends configuring a session timeout for secrets, so that secrets are automatically checked in after the scan is complete. Tenable recommends setting a checkout duration that matches or exceeds the estimated duration of the scan.

Privilege Escalation (SSH only)

Selecting a privilege escalation method that requires a password (for example, `sudo`) gives the same options for selecting an escalation account. In many cases, the escalation password is the same as the login password, and in these cases the escalation parameters may be left blank to default to that password.

Troubleshooting Debug Logs

The following section contains possible issues you may find in the Fudo **Debugging Log Report** log files and how to resolve them.

Server did not respond to request

If the Fudo server did not respond to a request, this is usually an issue of network connectivity or SSL. Verify the given host and port are accessible from the scanner. If the Fudo PAM server is using an SSL certificate not signed by a known CA, add the appropriate CA certificate to the scanner. Or, disable SSL verification.

Incorrect API username or password

The error "Failed to authenticate to Fudo API" may appear in the debug logs, and additionally the following HTTP response may be recorded in the logs:

```
"status": "failure", "data": {"message": "Incorrect username or password."}}
```

This is caused by an incorrect API username or API password.

No accounts found

When listing accounts, Fudo returns an empty list of accounts, and an "unable to obtain a credential ID" error appears in the debug logs. The following HTTP response may also be present:

```
{
    "items": [ ],
    "result": "success"
}
```

The API user must be added to the safe containing the desired account. Confirm by logging into the portal with the chosen API user. This user must have access to accounts.

Accounts found, but not a matching one

If the error "unable to obtain a credential ID" appears, but the HTTP response did not contain an empty list of items, the problem is most likely that the given username/ID/address does not match

accounts that the user has access to. Check the values of account name/address/ID and **Use Target Address**.

Object is not accessible

This HTTP response may appear in the debug logs, resulting in an error:

```
{"message": {"code": "NF", "data": [{"field": "Object is not accessible.", "message":
"Not Found", "code": "NF"}]}}
```

This is usually because the API user does not have appropriate permissions. In the safe, go to the **users** tab, select the checkbox next to the API user, and click the **manage options** button. This user needs the **reveal password** box checked.

Checkout error

```
{"result": {"error_code": 1001, "error": "Checkout error occurred"}}
```

Trying to check out a secret that is already checked out. Assign the account a session duration and retry.

Secret used by different user

```
{"result": {"error_code": 1003, "error": "Secret is used by different user"}}
```

This can be resolved with the "force" option.

Database Integration

To configure Database integration:

1. Log in to your Tenable user interface.

2. In the upper-left corner, click the **Menu** 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.

    The credentials options appear.

9. Click the **Credentials** tab.

    The **Credentials** 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 **Fudo**.

    The Fudo options appear.

13. Configure each option for the Database authentication.

Option	Description	Required
Username	The username to log in to the hosts to scan.	yes
Fudo Portal Host	The IP address or url for the Fudo portal.	yes
Fudo Port	The port on which the Fudo API communicates. The default value is 443.	yes
Fudo API Username	The username with which to connect to the Fudo API. This user should be able to log in to the Fudo portal and check out the target account credentials.	yes
Fudo API Password	The password for the Fudo API user.	yes
Get Credential By	Choose how to fetch the credential. Specify Account Name/Address to use the account's name and address, or Account ID to specify the exact identifier of the account.	yes
Fudo Account Name	The name of the account to fetch.	no
Fudo Account Address	When fetching an account by name/address, limit searches to accounts with the specified server address.	no
Use Target Address	When fetching an account by name/address, limit searches to accounts with the target server address. This overrides the value of **Fudo Account Address**.	no
Fudo Account ID	The exact ID of the account to fetch.	no
Use SSL	When enabled, Tenable uses SSL for secure communication. This is enabled by default.	no

Option	Description	Required
Verify SSL Certificate	When enabled, Tenable verifies that the SSL Certificate on the server is signed by a trusted CA.	no

SSH Integration

To configure SSH integration:

1. Log in to your Tenable user interface.

2. In the upper-left corner, click the **Menu** 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.

   The credentials options appear.

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 **Fudo**.

    The Fudo options appear.

13. Select **SSH**.

The **Settings** pane appears.

14. Configure each option for the SSH authentication.

Option	Description	Required
Username	The username to log in to the hosts to scan.	yes
Fudo Portal Host	The IP address or url for the Fudo portal.	yes
Fudo Port	The port on which the Fudo API communicates. The default value is 443.	yes
Fudo API Username	The username with which to connect to the Fudo API. This user should be able to log in to the Fudo portal and check out the target account credentials.	yes
Fudo API Password	The password for the Fudo API user.	yes
Get Credential By	Choose how to fetch the credential. Specify Account Name/Address to use the account's name and address, or Account ID to specify the exact identifier of the account.	yes
Fudo Account Name	The name of the account to fetch.	no
Fudo Account Address	When fetching an account by name/address, limit searches to accounts with the specified server address.	no
Use Target Address	When fetching an account by name/address, limit searches to accounts with the target server address. This overrides the value of **Fudo Account Address**.	no
Fudo Account ID	The exact ID of the account to fetch.	no

Option	Description	Required
Elevate privileges With	Use the drop-down menu to select the privilege elevation method, or select **Nothing** to skip privilege elevation. **Note:** Multiple options for privilege escalation are supported, including su, su+sudo and sudo. For example, if you select sudo, more fields for sudo appear, Escalation Account Name and Location of sudo (directory) are provided and can be completed to support authentication and privilege escalation. **Note:** Selecting a privilege escalation method offers the ability to fetch an escalation credential by Name/Address or by ID. This refers to the account containing the escalation password. In many cases (for example, sudo) this is the same password as the login password, and therefore these fields may be left blank.	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

Windows Integration

To configure Windows integration:

1. Log in to your Tenable user interface.

2. In the upper-left corner, click the **Menu** 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.

   The credentials options appear.

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 **Fudo**.

    The Fudo options appear.

13. Configure each option for Windows authentication.

Option	Description	Required
Username	The username to log in to the hosts to scan.	yes
Domain	The domain to use when logging in to the hosts to scan.	no
Fudo Portal Host	The IP address or url for the Fudo portal.	yes
Fudo Port	The port on which the Fudo API communicates. The default value is 443.	yes
Fudo API Username	The username with which to connect to the Fudo API. This user should be able to log in to the Fudo portal and check out the target account credentials.	yes
Fudo API Password	The password for the Fudo API user.	yes
Get Credential By	Choose how to fetch the credential. Specify Account Name/Address to use the account's name and address, or Account ID to specify the exact identifier of the account.	yes
Fudo Account Name	The name of the account to fetch.	no
Fudo Account Address	When fetching an account by name/address, limit searches to accounts with the specified server address.	no
Use Target Address	When fetching an account by name/address, limit searches to accounts with the target server address. This overrides the value of **Fudo Account Address**.	no
Fudo Account ID	The exact ID of the account to fetch.	no

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