Tenable and Akeyless PAM Integration Guide

Last Revised: July 13, 2026

Table of Contents

Welcome to Tenable for Akeyless PAM

This document provides information and steps for integrating Tenable Vulnerability Management or Tenable Nessus with Akeyless PAM.

The Tenable Akeyless PAM integration provides scans the ability to use credentials from the Akeyless Privileged Access Manager (PAM) platform in credentialed scans. This removes the need to store target credentials directly in Tenable, reduces secrets sprawl, and ensures that the latest credentials are used at scan time. You can integrate Akeyless PAM with Tenable Vulnerability Management or Tenable Nessus to perform credentialed scanning of SSH, Windows (SMB), and database targets.

The benefits of integrating Tenable with Akeyless PAM include:

- Centralized management of privileged credentials across your environment
- Support for multiple authentication methods including Access Key, Universal Identity (UID), and certificate-based (mTLS) authentication
- Support for both static secrets, and rotated secrets, allowing scans to always use current credentials
- Elimination of hardcoded credentials in scan policies

For more information, refer to the following product documentation:

- Tenable Vulnerability Management
- Tenable Nessus

What information does the Akeyless PAM integration collect?

The Akeyless PAM integration gathers target credentials for use in credentialed scans. Specifically, it collects:

- Username: The account name used to authenticate to the scan target.
- Password: The password for the account, retrieved from the Akeyless secret.
- Escalation Password: If privilege escalation is configured with a separate escalation credential, then an escalation password is collected. The integration does not collect escalation usernames. Enter escalation usernames manually.
- SSH private key: For SSH-based scans where the secret contains a private key instead of a password.
- Domain: Optionally retrieved from the secret or from the manually-entered values.

The integration does not collect or transmit vulnerability data. It only retrieves the credentials needed by the scanner to authenticate to the target system.

API requests per target

The integration makes two API requests to Akeyless per scan target: one request to authenticate and obtain an access token, and one request to retrieve the secret value. If privilege escalation is configured with a separate escalation credential, one additional secret retrieval request is made. The integration caches retrieved credentials for the duration of the scan to avoid repeated requests for the same secret.

Credentialed scans

Credentialed scans allow the Tenable scanner to log into the target system directly and perform a deeper assessment than is possible without credentials. This includes checking installed software versions, configuration settings, patch levels, and compliance status.

What the Akeyless PAM integration does not collect

The Akeyless PAM integration is not designed to collect vulnerability data, software inventory, or configuration details from target systems. It only retrieves credentials that the scanner then uses for target authentication. If privilege escalation is configured, the integration does not collect escalation usernames. Enter escalation usernames manually.

> Note: To perform compliance audits on target systems, configure additional audit files in your scan policy. The Akeyless PAM integration provides the credentials; compliance audit files define what is checked.

Akeyless PAM integration limitations

- The integration supports static, rotated and dynamic Akeyless secret types.
- Store other secrets as JSON objects containing at minimum a password field, an ssh_key field, or plain text. Secrets using other structures may not be parsed correctly.
- All scan targets using the same credential must share the same Akeyless secret path (Credential ID). To use different credentials for different targets, configure separate scan credentials.
- The Akeyless host must be network-accessible from the Tenable Nessus scanner.

Configure Akeyless PAM Integration for Tenable Vulnerability Management

Required User Role: Standard, Scan Manager, or Administrator

The Tenable Akeyless PAM integration is configured using the Akeyless PAM credential type, available under SSH settings, Windows credentials, and Database credentials in Tenable Vulnerability Management scan policies.

Required Permissions

The Akeyless PAM authentication method used by the integration must have read access to the secrets referenced in the scan credential.

To configure the required permissions in Akeyless PAM:

1. Log into your Akeyless PAM console.
2. Navigate to Auth Methods and create or identify the authentication method for Tenable to use (Access Key, Universal Identity, or Certificate).
3. Navigate to Access Roles and create a role that grants read access to the secret path(s) used for scanning (for example, /scan/credentials/*).
4. Attach the Access Role to the authentication method.

Note: For privilege escalation scans (SSH only), ensure the authentication method also has read access to the escalation credential path.

What to do next:

- Scan Configuration - Tenable Vulnerability Management

Scan Configuration

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

To configure an Akeyless PAM credential in a Tenable Vulnerability Management scan:

1. In Tenable Vulnerability Management, navigate to Scans.
2. Create, or edit, a scan.
3. Navigate to Credentials and select the appropriate credential type (SSH, Windows, or Database).
4. From the Authentication Method dropdown, select Akeyless.
5. Configure the options described in the following table.

Option	Description	Required
Akeyless Host	The hostname or IP address of your Akeyless instance. For the Akeyless SaaS platform, use api.akeyless.io.	Yes
Akeyless Port	The port on which the Akeyless API communicates. By default, Tenable uses 443.	Yes
Akeyless API URL	An optional base URL path appended to the host when constructing API requests. Leave blank for the default Akeyless SaaS or gateway API.	No
Access ID	The Access ID associated with your Akeyless authentication method. This	Yes

	value begins with p- for SaaS auth methods.	
Authentication Method	The method used to authenticate to Akeyless. Select Access Key, Universal Identity, or Certificate.	Yes
Access Key	The Access Key secret corresponding to the Access ID. Displayed when the Authentication Method is set to Access Key.	Yes (if using Access Key authentication)
UID Token Source	Whether to supply the Universal Identity token directly or read it from a file on the scanner. Possible options are Manual and File. Displayed when the Authentication Method is set to Universal Identity.	Yes (if using Universal ID authentication)
Universal Identity Token	The UID token used for Universal Identity authentication. Displayed when UID Token Source is set to Manual.	Yes (if using manual Universal ID entry)
Universal Identity Token File	The absolute path to a file on the Tenable Nessus scanner host that contains the UID token. Displayed when UID Token Source is set to File.	Yes (if using file-based Universal Identity)
Client Certificate	The PEM-format client certificate file used for certificate-based (mTLS) authentication. Displayed when the Authentication Method is set to	Yes (if using Certificate Authentication)

	Certificate.	
Private Key	The PEM-format private key file corresponding to the client certificate. Displayed when the Authentication Method is set to Certificate.	Yes (if using Certificate Authentication)
Passphrase For Private Key	The passphrase protecting the private key, if the key is encrypted. Displayed when the Authentication Method is set to Certificate.	No
Credential ID	The full path of the Akeyless secret that contains the target login credentials, for example /scan/linux/webserver.	Yes
Secret Type	The type of Akeyless secret to retrieve. Select Static for static secrets or Rotated for rotated secrets. Static by default.	Yes
Use SSL	Whether to use SSL/TLS when communicating with the Akeyless host. Enabled by default.	Yes
Verify SSL Certificate	Whether to verify the Akeyless host SSL certificate. Disable only in test environments.	Yes
Use Kerberos KDC	If enabled, Kerberos authentication is used to log in to the Windows target. Requires KDC host, port, transport, and	No

	domain. Applies to SSH and Windows credentials only.	
Elevate privileges with	The privilege escalation method to use after login (for example, sudo). Applies to SSH credentials only.	No
Escalation Credential ID	The Akeyless secret path for the escalation account credentials. If not specified, the primary Credential ID is used for both login and escalation. Applies to SSH credentials only.	No

6. Save the credential and launch the scan.

Configure the Akeyless PAM Integration for Tenable Nessus

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

The Tenable Akeyless PAM integration is configured using the Akeyless PAM credential type, available under SSH settings, Windows credentials, and Database credentials in Tenable Nessus scan policies.

Required Permissions

The Akeyless PAM authentication method used by the integration must have read access to the secrets referenced in the scan credential.

To configure the required permissions in Akeyless PAM:

1. Log into your Akeyless PAM console.
2. Navigate to Auth Methods and create or identify the authentication method for Tenable to use (Access Key, Universal Identity, or Certificate).
3. Navigate to Access Roles and create a role that grants read access to the secret path(s) used for scanning (for example, /scan/credentials/*).
4. Attach the Access Role to the authentication method.

> Note: For privilege escalation scans (SSH only), ensure the authentication method also has read access to the escalation credential path.

What to do next:

- Scan Configuration - Tenable Nessus

Scan Configuration

Required User Role: Standard, Scan Manager, or Administrator

To configure an Akeyless PAM credential in a Tenable Nessus scan:

1. In Tenable Nessus, navigate to Scans.
2. Create, or edit, a scan.
3. Navigate to Credentials and select the appropriate credential type (SSH, Windows, or Database).
4. From the Authentication Method dropdown, select Akeyless.
5. Configure the options described in the following table.

Option	Description	Required
Akeyless Host	The hostname or IP address of your Akeyless instance. For the Akeyless SaaS platform, use api.akeyless.io.	Yes
Akeyless Port	The port on which the Akeyless API communicates. By default, Tenable uses 443.	Yes
Akeyless API URL	An optional base URL path appended to the host when constructing API requests. Leave blank for the default Akeyless SaaS or gateway API.	No
Access ID	The Access ID associated with your Akeyless authentication method. This value begins with p- for SaaS auth methods.	Yes

Authentication Method	The method used to authenticate to Akeyless. Select Access Key, Universal Identity, or Certificate.	Yes
Access Key	The Access Key secret corresponding to the Access ID. Displayed when the Authentication Method is set to Access Key.	Yes (if using Access Key authentication)
UID Token Source	Whether to supply the Universal Identity token directly or read it from a file on the scanner. Possible options are Manual and File. Displayed when the Authentication Method is set to Universal Identity.	Yes (if using Universal ID authentication)
Universal Identity Token	The UID token used for Universal Identity authentication. Displayed when UID Token Source is set to Manual.	Yes (if using manual Universal ID entry)
Universal Identity Token File	The absolute path to a file on the Tenable Nessus scanner host that contains the UID token. Displayed when UID Token Source is set to File.	Yes (if using file-based Universal Identity)
Client Certificate	The PEM-format client certificate file used for certificate-based (mTLS) authentication. Displayed when the Authentication Method is set to Certificate.	Yes (if using Certificate Authentication)

Private Key	The PEM-format private key file corresponding to the client certificate. Displayed when the Authentication Method is set to Certificate.	Yes (if using Certificate Authentication)
Passphrase For Private Key	The passphrase protecting the private key, if the key is encrypted. Displayed when the Authentication Method is set to Certificate.	No
Credential ID	The full path of the Akeyless secret that contains the target login credentials, for example /scan/linux/webserver.	Yes
Secret Type	The type of Akeyless secret to retrieve. Select Static for static secrets or Rotated for rotated secrets. Static by default.	Yes
Use SSL	Whether to use SSL/TLS when communicating with the Akeyless host. Enabled by default.	Yes
Verify SSL Certificate	Whether to verify the Akeyless host SSL certificate. Disable only in test environments.	Yes
Use Kerberos KDC	If enabled, Kerberos authentication is used to log in to the Windows target. Requires KDC host, port, transport, and domain. Applies to SSH and Windows credentials only.	No

Elevate privileges with	The privilege escalation method to use after login (for example, sudo). Applies to SSH credentials only.	No
Escalation Credential ID	The Akeyless secret path for the escalation account credentials. If not specified, the primary Credential ID is used for both login and escalation. Applies to SSH credentials only.	No

6. Save the credential and launch the scan.

Scan Results Review

This section helps you interpret the results of scans that use the Akeyless PAM integration.

Plugin Families and Plugins

The following Tenable plugins are relevant to scans using the Akeyless PAM integration.

Settings plugin family:

- Integration Status (204872) Reports an overall success or failure of the Akeyless PAM integration.
- SSH settings (14273) Reads the SSH PAM credential configuration and calls the Akeyless PAM integration to retrieve credentials for SSH targets. This plugin is not indicative of authentication issues by itself; authentication failures are reported by the credential status plugins below.
- Login configurations (10870) Reads Windows (SMB) credential configuration and calls the Akeyless PAM integration to retrieve credentials for Windows targets.
- Database settings (33815) Reads database credential configuration and calls the Akeyless PAM integration to retrieve credentials for database targets.
- Nessus Scan Information (19506) Reports metadata about the scan including whether credentialed checks were successful. Check this plugin result first when investigating authentication issues.
- Target Credential Issues by Authentication Protocol - No Issues Found (110095) Indicates that credentials were provided and authentication succeeded for all targeted protocols. A result from this plugin confirms that the Akeyless integration returned credentials and the scanner successfully authenticated.

- Target Credential Status by Authentication Protocol - Failure for Provided Credentials (104410) Indicates that credentials were provided but authentication to the target failed. This may indicate that the credentials retrieved from Akeyless are incorrect or do not have sufficient permissions on the target host.
- Target Credential Status by Authentication Protocol - No Credentials Provided (110723) Indicates that no credentials were available for the targeted protocol. If this appears when an Akeyless credential is configured, the integration likely failed to retrieve the secret.
- Target Credential Issues by Authentication Protocol - Intermittent Authentication Failure (117885) Indicates that authentication succeeded for some targets but not others, which may point to per-target credential differences or intermittent Akeyless connectivity issues.
- Database Authentication Failure(s) for Provided Credentials (91822) Indicates that the database credentials retrieved from Akeyless could not authenticate to the target database. Check the Credential ID and that the secret contains a valid username and password for the target database.

Debug Log Reporting

Debug logs for the Akeyless PAM integration are written by the Tenable Nessus scanner during the scan. Log output is controlled by the debug logging settings in Tenable Nessus.

Log file names

The integration writes to log files named after the credential plugin that invoked it:

- SSH scans: ssh_settings.nasl~Akeyless
- Windows scans: logins.nasl~Akeyless
- Database scans: database_settings.nasl~Akeyless

Log files are attached to the Debugging Log Report (84239) plugin output.

What the logs contain

The debug logs record the full integration lifecycle for each scan, including:

- Configuration settings the integration loads from the scan policy (with sensitive values masked).
- The authentication method used and whether authentication succeeded.
- The Akeyless API endpoint called and the HTTP response status.
- Whether the secret was found and whether its value was parsed successfully.
- Cache hit/miss information for repeated credential retrievals.
- Any errors returned by the Akeyless API, including authentication failures and secret-not-found responses.

Common reasons for credentialed checks showing "no" status

- The Akeyless authentication method does not have an Access Role that grants read access to the configured Credential ID path.
- The Access Key, UID token, or client certificate provided is invalid or expired.
- The Akeyless host is unreachable from the scanner (firewall, incorrect hostname, or port).
- The Credential ID path does not exist in Akeyless or is misspelled.
- The secret value is not valid JSON or does not contain a password or ssh_key field.
- For rotated secrets, the Secret Type is set to static (or vice versa), causing the wrong API endpoint to be called.
- SSL certificate verification fails because the Akeyless gateway uses a self-signed certificate and Verify SSL Certificate is enabled.

Additional Information

Helpful Tips

The overall process of the Akeyless PAM integration is like other Privileged Access Manager (PAM) integrations, as follows:

- Tenable Vulnerability Management passes the scan policy and credential settings down to Tenable Nessus. This includes the Akeyless host, port, authentication credentials, and the Credential ID of the secret to retrieve.
- The Tenable Nessus scanner communicates with the Akeyless API. The scanner first authenticates to Akeyless using the configured authentication method (Access Key, Universal Identity, or Certificate) to obtain an access token. It then calls the appropriate secret retrieval endpoint to obtain the username, password, and/or SSH key required for target authentication.
- The scanner uses the retrieved values to authenticate to the scan targets.

Testing Integration Connectivity

You can use curl to verify connectivity between the scanner host and the Akeyless API before running a scan.

Test Akeyless API reachability:

```
curl -s -o /dev/null -w "%{http_code}" \
  https://api.akeyless.io/auth \
  -X POST \
  -H "Content-Type: application/json" \
  -d '{"access-type":"access_key","access-id":"<your-access-id>","access-key":"<your-access-key>"}'
```

A response of 200 confirms the Akeyless API is reachable and the access key credentials are valid. A response of 401 confirms reachability but indicates invalid credentials.

Test secret retrieval (using the token from the auth response above):

```
curl -s \
  https://api.akeyless.io/get-secret-value \
  -X POST \
  -H "Content-Type: application/json" \
  -d '{"names":["/path/to/your/secret"],"token":"<token-from-auth-response>"}'
```

A successful response returns the secret value. A 403 response indicates the authentication method does not have an Access Role granting read access to that path.

Test certificate authentication:

```
curl -s \
  https://api.akeyless.io/auth \
  -X POST \
  -H "Content-Type: application/json" \
  --cert /path/to/client.crt \
  --key /path/to/client.key \
  -d '{"access-type":"certificate","access-id":"<your-access-id>"}'
```

FAQs

> Credentialed checks show "no" even though an Akeyless credential is configured.

Check the integration debug log (see Debug Log Reporting) for the specific error. Common causes are:

- The Access Role is not attached to the authentication method, or does not include the secret path in its permissions.
- The Credential ID is incorrect. Verify the exact path in the Akeyless console — paths are case-sensitive.
- The Akeyless host field points to the wrong endpoint. For SaaS, use api.akeyless.io. For a self-hosted gateway, use the gateway's hostname.

> Authentication fails with a certificate error.

- Ensure the certificate has been registered as an allowed certificate in the Akeyless Certificate Auth Method, and that an Access Role is attached to that method.
- If using a passphrase-protected key, confirm the passphrase is entered correctly in the Passphrase For Private Key field.
- If using a self-hosted gateway, verify the SSL certificate of the gateway is trusted by the scanner, or consider testing with "Verify SSL" disabled.

> HTTP 401: Authentication fails or the token is rejected.

- UID tokens have a limited lifetime. If storing the token directly, verify it has not expired. Consider using the Universal Identity Token File option so the token can be rotated on disk without updating the scan credential.

- Verify the `uid-token` value does not contain trailing whitespace or newline characters. The integration strips trailing whitespace from file-based tokens automatically.

The scan returns the wrong credentials or stale passwords.

- If using a rotated secret, confirm that Secret Type is set to rotated in the scan credential. Using the static endpoint against a rotated secret does not return the current rotation values.
- Credential values are cached for the duration of a single scan run. If credentials were rotated mid-scan, restart the scan to pick up the new values.