



Protegrity Insight Discovery 3.0.0

Created on: Jun 30, 2020

Notice

Copyright

Copyright © 2004-2020 Protegrity Corporation. All rights reserved.

Protegrity products are protected by and subject to patent protections; Patent: <https://support.protegrity.com/patents/>

Protegrity logo is the trademark of Protegrity Corporation.

NOTICE TO ALL PERSONS RECEIVING THIS DOCUMENT

Some of the product names mentioned herein are used for identification purposes only and may be trade marks and/or registered trademarks of their respective owners.

Table of Contents

Copyright..... ii

Chapter 1 Appendix C: Scan Task Advanced Configuration Settings..... 4

Chapter 2 Appendix I: Integrating Insight Discovery with CyberArk..... 6

2.1 Setting up Custom Authentication Using CyberArk..... 7

Chapter 1

Appendix C: Scan Task Advanced Configuration Settings

This section describes the advanced configuration settings that you can set while creating or editing a task.

Each configuration setting is a key-value pair setting in JSON format. You can separate multiple key-value pairs using a comma separator. You can override the default values of the configuration settings from the **Config** field, which is visible if you click the **Advanced Settings** link on the *Add Discovery Job* or *Edit Discovery Job* dialog box.

The configuration settings that are displayed depend on the selected datastore.

The following table describes the advanced configuration settings and lists the datastores for which each setting is applicable. The table also lists the default values for each configuration setting.

Table 1-1: Insight - Advanced Configuration Settings

Configuration Setting	Description	Syntax	Applicable Datastores	Default Value
custom_auth	Specify the configuration for connecting to a third-party authentication system, such as CyberArk, for retrieving the password of the datastore that you want to scan. You can specify the following parameters: <i>name</i> - Specifies the name of the CyberArk configuration that determines the CyberArk system with which you want to communicate. For example, specify the value as <i>cyberark</i>. For more information about the CyberArk configuration name, refer to the <i>CyberArk configuration name</i> entry in the table in step 2d of the section Setting up Custom Authentication Using CyberArk. <i>Object</i> - Specifies the unique name of the account created in the CyberArk system	<pre>{ "custom_auth": { "name": "cyberark", "params": { "Object": "<Unique account name>" } } }</pre>	For more information about the datastores supported by CyberArk, refer to the CyberArk documentation .	Not applicable

Configuration Setting	Description	Syntax	Applicable Datastores	Default Value
	for storing the password of the required datastore. For more information about the <i>Object</i> parameter, refer to the section Call the Web Service using REST in the CyberArk documentation.			

Chapter 2

Appendix I: Integrating Insight Discovery with CyberArk

2.1 Setting up Custom Authentication Using CyberArk

CyberArk Application Access Manager (AAM) provides custom authentication to access datastores that are scanned by Insight. This enables Insight Discovery to connect to the datastores without requiring to store the password.



The CyberArk Application Access Manager is deployed using an agentless configuration.

For more information about the CyberArk Application Access Manager, refer to the [CyberArk documentation](#).

The following figure illustrates the communication flow between Insight Discovery and CyberArk for retrieving the password for the datastore that needs to be scanned.

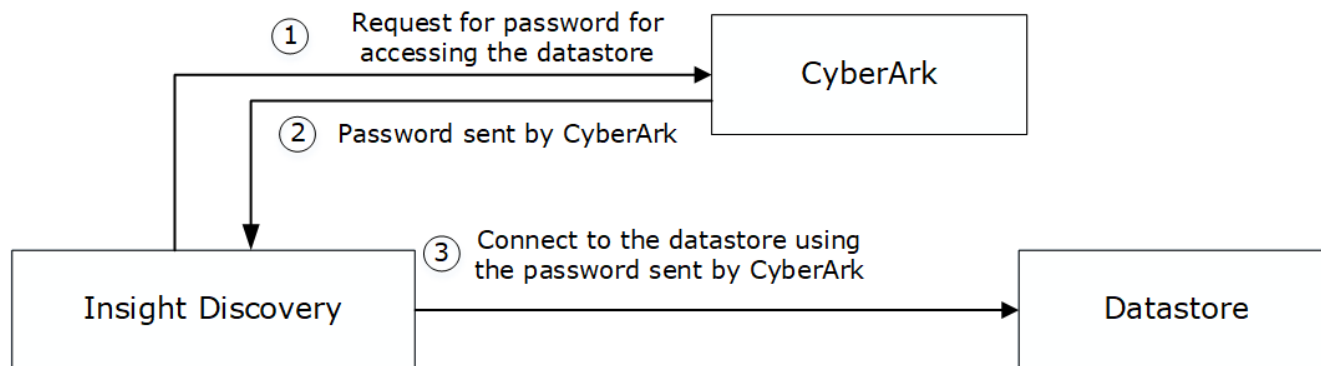


Figure 2-1: Communication Flow Between Insight Discovery and CyberArk

The CyberArk system has been configured to store the password for the datastore that needs to be scanned using Insight Discovery. The following steps specify the sequence that is followed for requesting a password from the CyberArk system.

1. Insight Discovery sends a request to the CyberArk system for retrieving the password to connect to the datastore.

2. CyberArk authenticates the request from Insight Discovery and returns the password for connecting to the datastore.
3. Insight Discovery uses the password obtained from the CyberArk system to connect to the datastore.

Important:

Insight Discovery does not save the password that is obtained from CyberArk.

2.1 Setting up Custom Authentication Using CyberArk

The following sections describe the prerequisites and tasks for setting up custom authentication for Insight Discovery using CyberArk.

Before you begin

- Ensure that you define the Insight Discovery application in the Password Vault Web Access (PVWA) Applications Management UI in the CyberArk system.
For more information about defining an application, refer to the section [Add applications](#) in the CyberArk documentation.
- Ensure that you have created a self-signed or a trusted client certificate for the CyberArk system. You need to copy this certificate to the machine on which Insight Discovery has been installed. This certificate is used to authenticate the Insight Discovery application, when it sends a request to the CyberArk system for obtaining the password of the datastore that you want to scan.

Important:

Protegrity recommends that you use a certificate-based authentication method for authenticating the Insight Discovery application to the CyberArk system.

To set up custom authentication using CyberArk:

1. Perform the following steps to upload the client certificate to the certificate repository.
 - a. Login to the Appliance Management Web UI and navigate to **Settings > Network Settings > Certificate Repository**.
The Certificate Repository screen appears.
 - b. Click **Upload new files** to upload the CyberArk client certificate to the certificate repository.
When Insight sends a request to the CyberArk system for retrieving the passwords for a specific datastore, CyberArk uses the uploaded certificate to authenticate Insight.

For more information about uploading a certificate, refer to the section [Uploading Certificates or CRL](#) in the [Certificate Management Guide](#).

2. Perform the following steps to modify the *sureloc.json* file.
 - a. On the Appliance Management Web UI, navigate to **Settings > System > Files**.
The List of Product Files screen appears.
 - b. In the **Insight - Settings** section, edit the *sureloc.json* file.
 - c. Edit the following code block in the *sureloc.json* file.

```
"custom_auth": {
```

```
"<CyberArk configuration name>": {
  "type": "CyberArk",
  "url": "https://services-uscentral.skytap.com:16945/AIMWebService/api/Accounts",
  "cert": "<ID of the client certificate used by the CyberArk to authenticate Insight>",
  "verify": "<Value for verifying the client certificate>",
  "params": {
    "AppId": "<Application ID defined in CyberArk>",
    "Safe": "<Safe name defined in CyberArk>"
  }
}
```

d. Modify the following fields in the custom authentication.

Field	Description
CyberArk configuration name	Specify a name for the CyberArk configuration. If you have multiple CyberArk systems, then you can create separate configurations for each of the systems. For example, if you have separate CyberArk systems for the development and testing environments, then you can create two entries for each configuration. You can specify the names for the individual configurations as <i>cyberark_dev</i> and <i>cyberark_qa</i>. In this example, you can add the following code block in the <i>sureloc.json</i> file: <pre>"custom_auth": { "cyberark_dev": { "type": "CyberArk", "url": "<value>", "cert": "<value>", "verify": "<value>", "params": { "AppId": "<value>", "Safe": "<value>" } }, "cyberark_qa": { "type": "CyberArk", "url": "<value>", "cert": "<value>", "verify": "<value>", "params": { "AppId": "<value>", "Safe": "<value>" } } }</pre> When you are creating a data discovery task, you need to specify the name of the CyberArk configuration as the value of the <i>name</i> parameter in the <i>custom_auth</i> configuration setting in the advanced configuration settings for that task.

Field	Description
	For more information about the <i>custom_auth</i> configuration setting, refer to the Scan Task Advanced Configuration Settings section.
type	Specifies the type of authentication. For example, specify the value as <i>CyberArk</i> .
url	Specify the URL of the Central Credential Provider Web Service, which is used by Insight Discovery to retrieve the password of the datastore that you want to scan. For example, specify the value of the URL as <i>https://<host:port>/AIMWebService/api/Accounts</i> The following parameters are specified in the URL: • <i>host</i> - IP address or host name of the machine where the Central Credential Provider Web Service has been installed. • <i>port</i> - Port number that is used to access the Central Credential Provider Web Service AIMWebService is the name of the Central Credential Provider Web Service. For more information about the Central Credential Provider and the Central Credential Provider Web Service, refer to the section Central Credential Provider in the CyberArk documentation.
cert	Specify the ID of the client certificate, which is mentioned on the Certificate Repository screen, used by the CyberArk system to authenticate Insight. If the CyberArk server is not using a certificate-based authentication method, then you need to specify the value of the <i>cert</i> parameter as <i>null</i> .
verify	Specify whether the self-signed or trusted client certificate that you have uploaded to establish a secure communication between the CyberArk system and Insight, needs to be verified. You can either specify a boolean value or a string value for this parameter.

Field	Description
	If you specify a boolean value, then this parameter determines whether the client certificate is verified by the CyberArk system. In this case, you can specify one of the following values for this parameter: <i>true</i> - The client certificate is verified. <i>false</i> - The client certificate is not verified. You can also specify the ID of the CA certificate. Insight uses this value to internally identify the path where the Certificate Authority bundle is stored. The Certificate Authority bundle is used to verify the client certificate. For more information about the <i>verify</i> parameter, refer to the SSL Cert Verification section in the <i>Python Requests</i> module.
params/appID	Specifies the unique ID of the Insight Discovery application that has been defined in the PVWA Applications Management UI.
params/Safe	Specifies the name of the safe where the password of the datastore to be scanned is stored.

For more information about the parameters defined in the CyberArk system, refer to the section [Call the Web Service Using REST](#) in the CyberArk documentation.

- Perform the following steps to modify the advanced configurations while creating a data discovery task.

For more information about creating a data discovery task, refer to the section [Creating a Data Discovery Task](#).

- In the **Add Discovery Job** dialog box, click **Advanced Settings** to display the **Config** text area.
- Specify the following advanced configuration settings for using the custom authentication.

```
{"custom_auth":{"name":"cyberark","params":{"Object":"<Unique account name>"}}
```

- Modify the following fields in the custom authentication.

Field	Description
name	Specifies the name of the CyberArk configuration that you want to use for connecting to the CyberArk system. For example, specify the value as <i>cyberark</i>. For more information about the CyberArk configuration name, refer to the CyberArk configuration name

Field	Description
	entry in the table in step 2d of the section Setting up Custom Authentication Using CyberArk .
params/Object	Specifies the unique name of the account created for storing the password of the required datastore.

For more information about the parameters defined in the CyberArk system, refer to the [Central Credential Provider Implementation Guide](#).

You can use this configuration to connect to a CyberArk system for retrieving the password for the datastore that you want to scan.