CYBERARK SECRETS MANAGER

(Agent Based Credential Provider CP)

SECRETS MANAGER INTEGRATION - TECHNICAL DOCUMENTATION

Name of Company: Eracent

Website: www.eracent.com

Name of Product: ITMC Discovery

Version: 10.1.96

Date: 21 April 2017 (26 November 2020)

ITMC DISCOVERY OVERVIEW

Eracent's automated bot-driven IT Asset Management (ITAM) and Software Asset Management (SAM) solutions help to maximize the use of IT assets and licenses, minimize expenditures, and reduce audit risk. Benefits are achieved through discovery and application utilization reporting for cloud, mobile, data center and desktop platforms, comprehensive lifecycle management, software license optimization, and flexible process automation.

Eracent's ITMC Discovery™ and Eracent Network Probe (ENP) are two foundational modules that underpin all the company's other solutions, and they are the two key components that interact with CyberArk. ITMC Discovery and ENP provide full network visibility, showing an updated view of all devices and installed applications at any point in time. This enables reconciliation to verify that all relevant items are protected via CyberArk functionality.

Version: 10.1.96

KEY BENEFITS

ITMC Discovery and the Eracent Network Probe provide full network visibility, showing an updated view of all devices and installed applications at any point in time. This enables reconciliation to verify that all relevant items are protected via CyberArk functionality.

ITMC Discovery provides deep-dive discovery of software and hardware attributes that may drive and support key decisions.

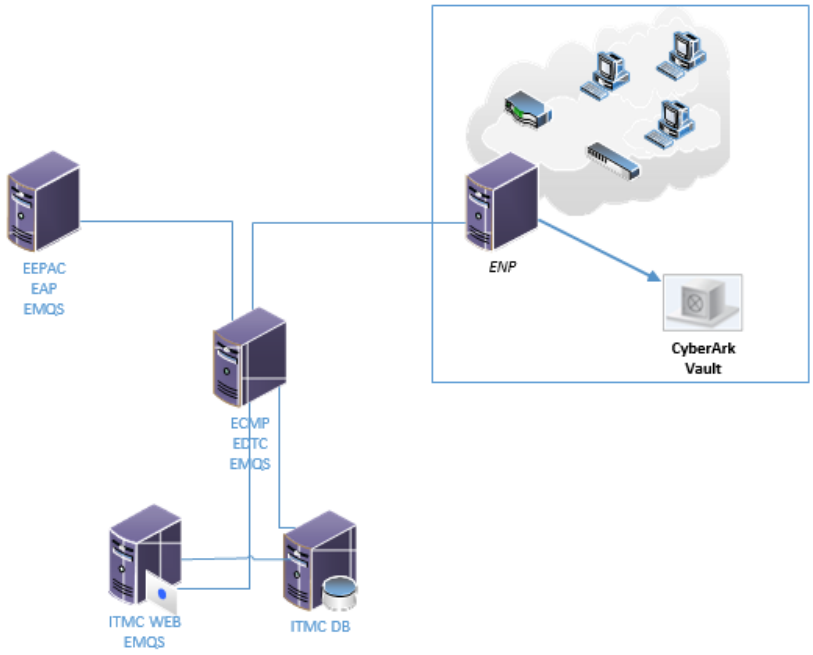
Eracent's Application Dependency Mapping detects and visually depicts all relationships between hardware, databases, and software that comprise application systems. This includes protocols and dependencies. This data can also drive and support key decisions.

Integration between the Eracent Network Probe and other aspects of ITMC Discovery with CyberArk provides a highly automated and accurate method for verifying that all networked and non-networked machines and applications are fully accounted for. This ensures that any items that should be covered by CyberArk functionality will be included.

PRODUCT DIAGRAM & DESCRIPTION OF PRODUCT INTEGRATION

The Eracent Network Probe (ENP) is an agentless remote data collector service. The aim of the ENP service is to provide as much identification information about all devices connected to a corporate network as possible. The resulting data provides basic information for the identifying and tracking devices. The data obtained can be used directly for tracking assets attached to the network, and for

targeting devices for deployment of more complex device-specific asset management agents.



SECRETS MANAGER INTEGRATION

The Eracent Network Probe uses encrypted lookup tables (LUTs) to store credentials for discovery probes. ENP's probes use LUTs to retrieve matching credentials for a given IP address. For each credential configured with CyberArk method, ENP will trigger a password request from the Digital Vault. ENP uses a C/C++ Application Password SDK to communicate with a local Provider to retrieve passwords and password properties.

Each Eracent Network Probe service is installed on separate server and needs its own instance of CyberArk Secrets Manager Credential Provider installed. A typical installation consists of a single Eracent Network Probe, thus only one CyberArk Credential Provider is required.

CREDENTIAL RETRIEVAL

The Eracent Network Probe supports CyberArk stored passwords for Windows and Unix credentials.

1. CyberArk password properties used for performing a query:

Property name	Mandatory
UserName	True
Address	False

2. CyberArk password properties retrieved from CyberArk Vault

Property name	Mandatory
Password	True
PolicyId	False
LogonDomain (Windows only)	False

SECRETS MANAGER INSTALLATION

Secrets Manager Installation - https://docs.cyberark.com/Product-Doc/OnlineHelp/AAM-CP/Latest/en/Content/CP%20and%20ASCP/installing-the-Credential-Provider.htm?tocpath=Installation%7CCredential%20Provider%7CInstall%20the%20Credential%20Provider%7C____0

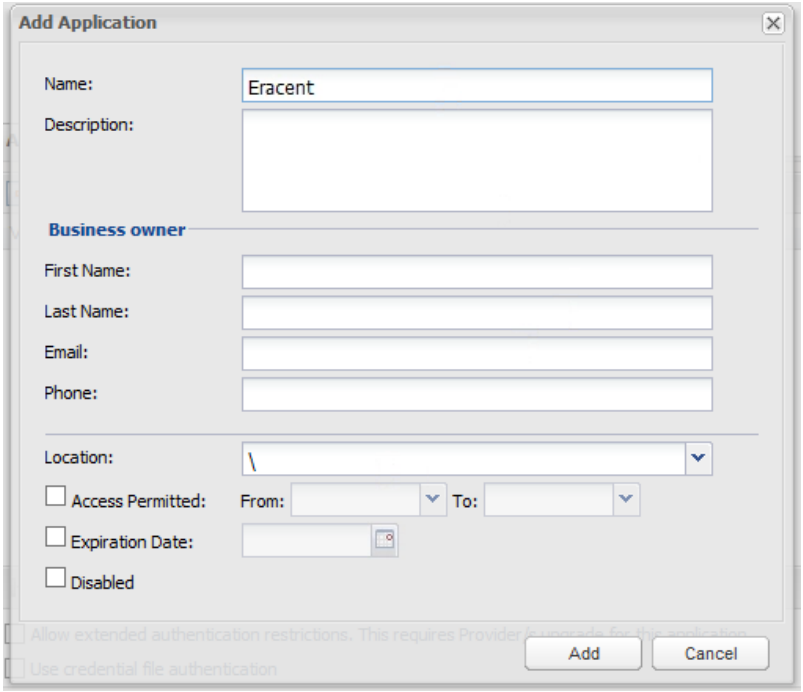
SECRETS MANAGER CONFIGURATION

The following sections provide details on ITMC Discovery configuration with CyberArk Secrets Manager.

DEFINING THE APPLICATION ID (APPID) AND AUTHENTICATION DETAILS

To define the application, define it manually through the CyberArk Password Vault Web Access (PVWA) interface:

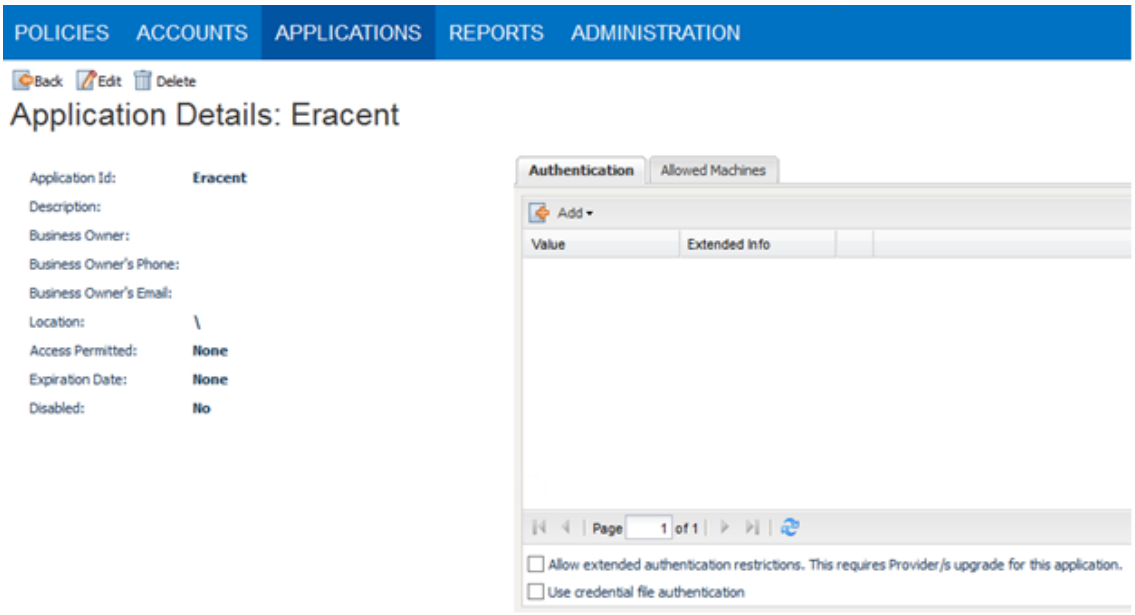
- ☐ Log in as user allowed to manage applications (it requires Manage Users authorization)
- ☐ In the Applications tab, click **Add Application**. The Add Application page appears.



☐ Specify the following information:

- In the **Name** box, specify the unique name (ID) of the application. The recommended Application ID for this integration is: Eracent
- In the **Description** box, specify a short description of the application that will help you identify it.
- In the **Business owner** section, specify contact information about the application's business owner.
- In the **Location** box, specify the location of the application in the Vault hierarchy. If a location is not selected, the application will be added in the same location as the user who is creating this application.

☐ Click **Add**. The application is added and is displayed in the Application Details page.



☐ Check the **Allowing extended authentication restrictions** box. This enables you to specify an unlimited number of machines and Windows domain OS users for a single application.

☐ Specify the application's **Authentication** details. This information enables the Credential Provider to check certain application characteristics before retrieving the application password. Partner should suggest the authentication details to secure the access by the partner's application.

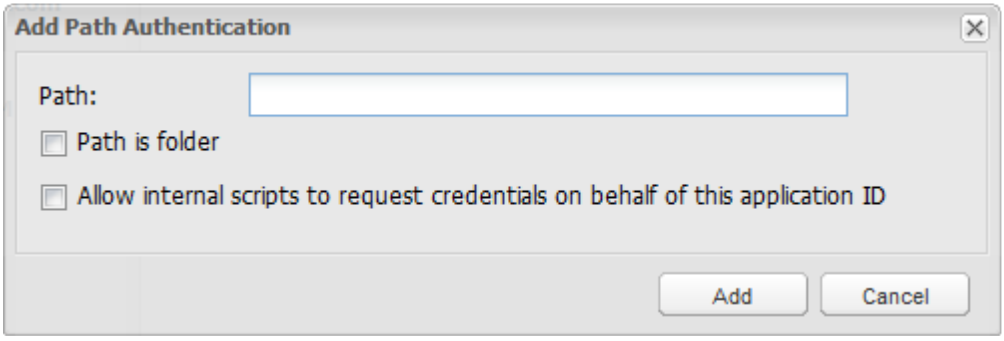
☐ In the Authentication tab, click **Add**. A drop-down list of authentication characteristics is displayed.

☐ Select the authentication characteristic to specify.

☐ Select **OS user**. The Add Operating System User Authentication window appears.

☐ Specify the name of the OS user who will run the application, then click **Add. T**he OS user is listed in the Authentication tab.

☐ Select **Path**. The Add Path Authentication window appears.



☐ In the **Path** box, specify the path where the application will run. To indicate that the specified path is a folder, select **Path is folder**. To allow internal scripts to retrieve the application password for this application, select **Allow internal scripts to request credentials on behalf of this application ID**.

☐ Click **Add**. The Path is added as an authentication characteristic with the information that you specified.

☐ Specify a hash:

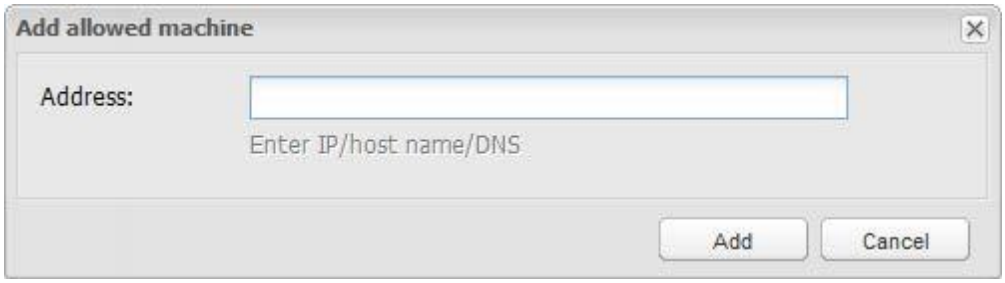
- Run the AIMGetAppInfo utility to calculate the application's unique hash. Copy the hash value that is returned by the utility.
- In the PVWA, select **Hash**. The Add Hash window appears.

- In the Hash edit box, paste the application's unique hash value, or secify multiple hash values with a semi-colon. You can add additional information in a comment after each hash value specified for an application by specifying '#' after the hash value, followed by the comment.
  For example, OE883B7OD5B6E3EE37D37198049C9507C8383DB6 **#app2**
  Note: The comment must not include a colon or a semicolon.

- Click **Add**. The Hash is added as an authentication characteristic with the information that you specified.

☐ Specify the application's Allowed Machines. This information enables the Credential Provider to make sure that only applications that run from specified machines can access their passwords.

- In the Allowed Machines tab, click **Add**. The Add allowed machine window is displayed.



- In the **Address** box, specify the IP/hostname/DNS of the machine where the application will run and will request passwords, then click **Add**. The IP address is listed in the Allowed Machines tab.

  Make sure the servers allowed include all mid-tier servers or all endpoints where the Secrets Manager Credential Providers were installed.

PROVISIONING ACCOUNTS AND SETTING PERMISSIONS FOR APPLICATION ACCESS

For the application to perform its functionality or tasks, the application must have access to particular existing accounts, or new accounts to be provisioned in CyberArk Vault.

In the Password Safe, provision the privileged accounts that will be required by the application. You can do this in either of the following ways:

- **Manually** – Add accounts manually one at a time, and specify all the account details.
- **Automatically** – Add multiple accounts automatically using the Password Upload feature.

  For this step, you require the **Add accounts** authorization in the Password Safe.

For more information about adding and managing privileged accounts, refer to **the Privileged Access Security Implementation Guide.**

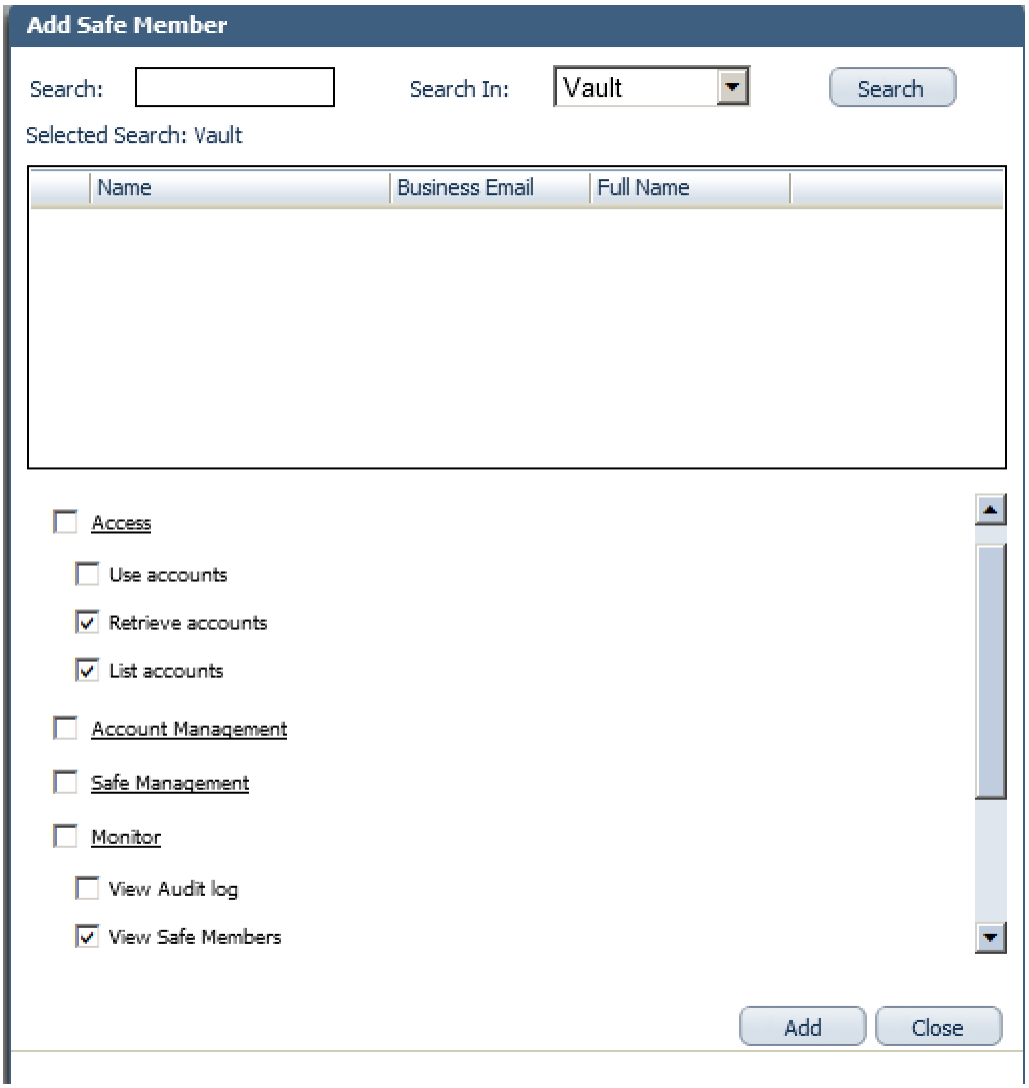
Once the accounts are managed by CyberArk, make sure to setup the access to both the application and CyberArk Application Password Providers serving the Application.

Add the Credential Provider and application users as members of the Password Safes where the application passwords are stored. This can either be done manually in the Safes tab, or by specifying the Safe names in the CSV file for adding multiple applications.

☐ Add the Provider user as a Safe Member with the following authorizations:

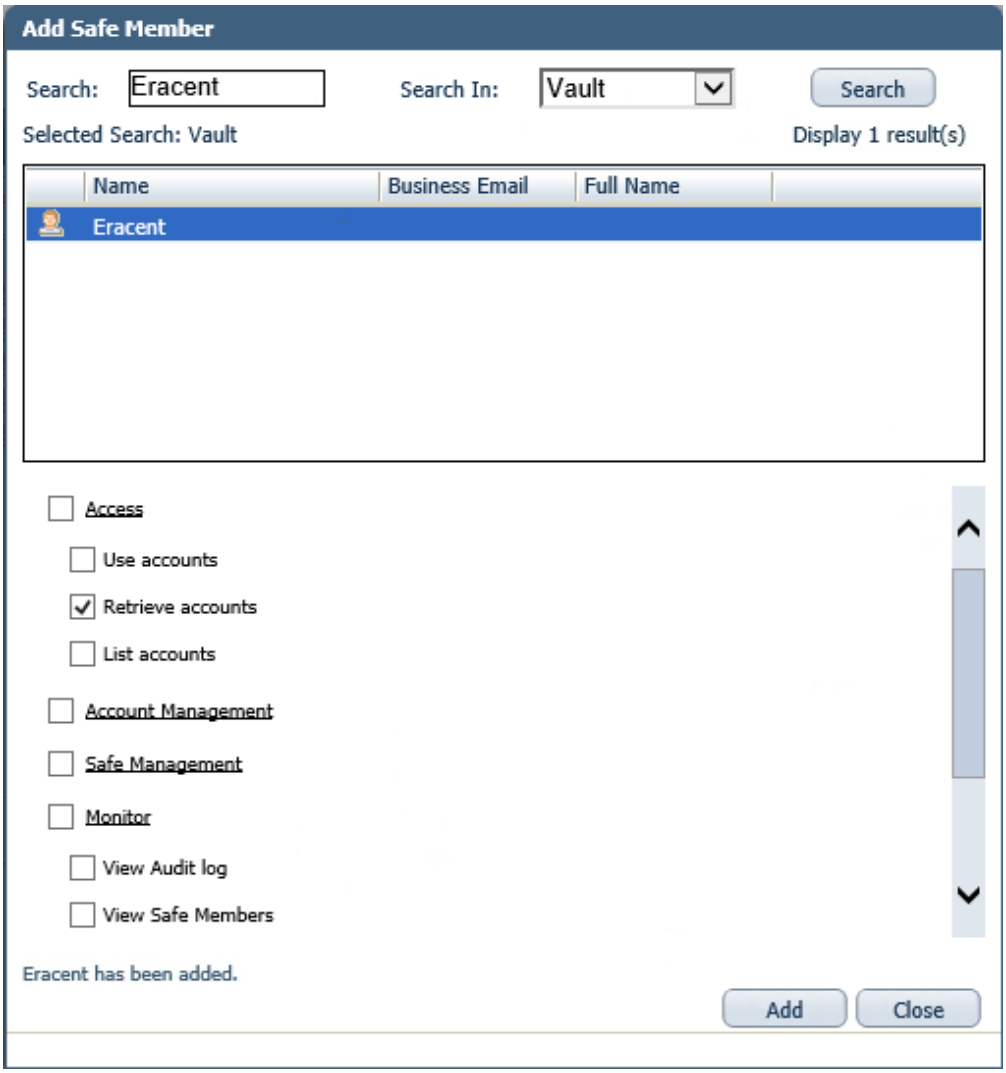
- List accounts
- Retrieve accounts
- View Safe Members

Note: When installing multiple Providers for this integration, it is recommended to create a group for them, and add the group to the Safe once with the above authorization.



☐ Add the application (the APPID) as a Safe Member with the following authorizations:

- Retrieve accounts



☐ If the Safe is configured for object level access, make sure that both the Provider user and the application have access to the password(s) to retrieve.

For more information about configuring Safe Members, refer to the **Privileged Access Security Implementation Guide.**

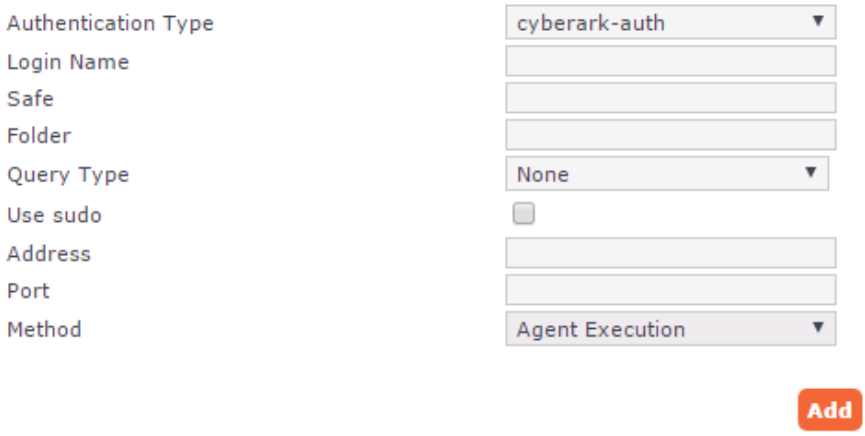
ITMC DISCOVERY INSTALLATION & INTEGRATION CONFIGURATION

Refer to ITMC_InstallGuide_10_1 for ITMC Discovery installation.

EracentNetworkProbe requires Secrets Manager to be installed. CPasswordSDK.dll needs to be added to PATH environment variable and needs to be accessible by ENP. EracentNetworkProbe automatically detects CyberArk support and logs it in logs\AgentDeployment.log file.

All devices scheduled and eligible for Eracent Network Probe processing will be matched against credentials LUTs. Credentials with 'cyberark-auth' authentication method will use CyberArk Vault to retrieve passwords before further processing.

Both Windows and Unix targets can be configured to utilize CyberArk for password retrieval.



Unix credentials configuration screen.

Name	Required	Description
Login Name	Yes	User to logon as
Safe	Yes	CyberArk Safe
Folder	Yes	CyberArk Folder
Query Type	Yes	None – no IP address is used (login, safe and folder) IP Address – login, IP, safe and folder are used to query CyberArk FQDN – revDNS is used to translate IP Address (fqdn is used) Hostname – revDNS is used to translate IP Address (host part is used) Domain Query – required Login Name in format domain\user. Domain is used in Address field
Use sudo	No	Enables Eracent Network Probe sudo mode
Address	No	Address for which given credentials are valid
Port	No	SSH service port number

Windows credentials configuration screen.

Name	Required	Description
User Name	Yes	User to logon as
Domain	No	Domain name to use for login
Safe	Yes	CyberArk Safe
Folder	Yes	CyberArk Folder
Query Type	Yes	None – no IP address is used (login, safe and folder) IP Address – login, IP, safe and folder are used to query CyberArk FQDN – revDNS is used to translate IP Address (fqdn is used) Hostname – revDNS is used to translate IP Address (host part is used) Domain Query – required Login Name in format domain\user. Domain is used in Address field
Network Address	No	Address for which given credentials are valid

List specific steps to configuring Partner Product to work with Secrets Manager, including:

1. Any special configurations within or outside the product
2. How to specify credentials for scanning, that are stored in the Vault (instead of providing usernames and passwords) – include screenshots and description of steps

PARTNER CONTACT INFO

Business Contact	Name	Terry Divelbliss
	Email	terryd@eracent.com
	Tel	+1 (724) 942-2481
Technical Contact	Name	Marek Checinski
	Email	marek.checinski@eracent.com
	Tel	+48 696 069 653
Support Contact	Name	Krzysztof Matyskiel
	Email	krzysztof.matyskiel@eracent.com
	Tel	+48 500 115 020