



APPLICATION ACCESS MANAGER

(Agentless Central Credential Provider CCP)

AAM INTEGRATION - TECHNICAL DOCUMENTATION TEMPLATE

DOCUMENT PURPOSE: THIS TEMPLATE IS TO BE COMPLETED BY PARTNER AND IS REQUIRED FOR CYBERARK SECURED CERTIFICATION. THE AAM INTEGRATION TECHNICAL DOCUMENTATION WILL BE MADE AVAILABLE TO PARTNERS, CUSTOMERS AND PROSPECTS.

Name of Company: Eaton

Website: <https://www.eaton.com>

Name of Product: IED Manager Suite

Version: 7.6

Date: 2021-11-22

PARTNER SOLUTION OVERVIEW

Eaton's IED Manager Suite (IMS) software provides reliability, security and compliance for utility automation systems. It helps utilities manage configuration settings, passwords and firmware of the intelligent electronic devices (IEDs) used in substation and distribution automation systems. It reduces maintenance costs through secure remote access and helps comply with NERC CIP. IMS software is one of Eaton's grid automation system solutions.

IMS supports IEDs from most vendors, including Eaton, SEL, GE and others.

Devices are deployed in widely distributed geographical areas and maintenance often requires expensive truck rolls. Operations need to be performed simultaneously on a large number of devices to change seasonal settings and perform firmware updates to address security or operational issues. Communications are often slow and failure prone, requiring multiple retries. IMS provides distribution operators with tools to automate the most time-consuming maintenance operations

Version: 7.6

Platform components:

- Security Server
- Passthrough Manager
- Event Manager
- Configuration Manager
- Password Manager
- Update Manager
- Enterprise Gateway
- Enterprise Gateway Services
- Data Bridge
- Web application server

Most server components are typically deployed on the same server. However, they are designed for the most part for possible deployment on different machines.

KEY BENEFITS

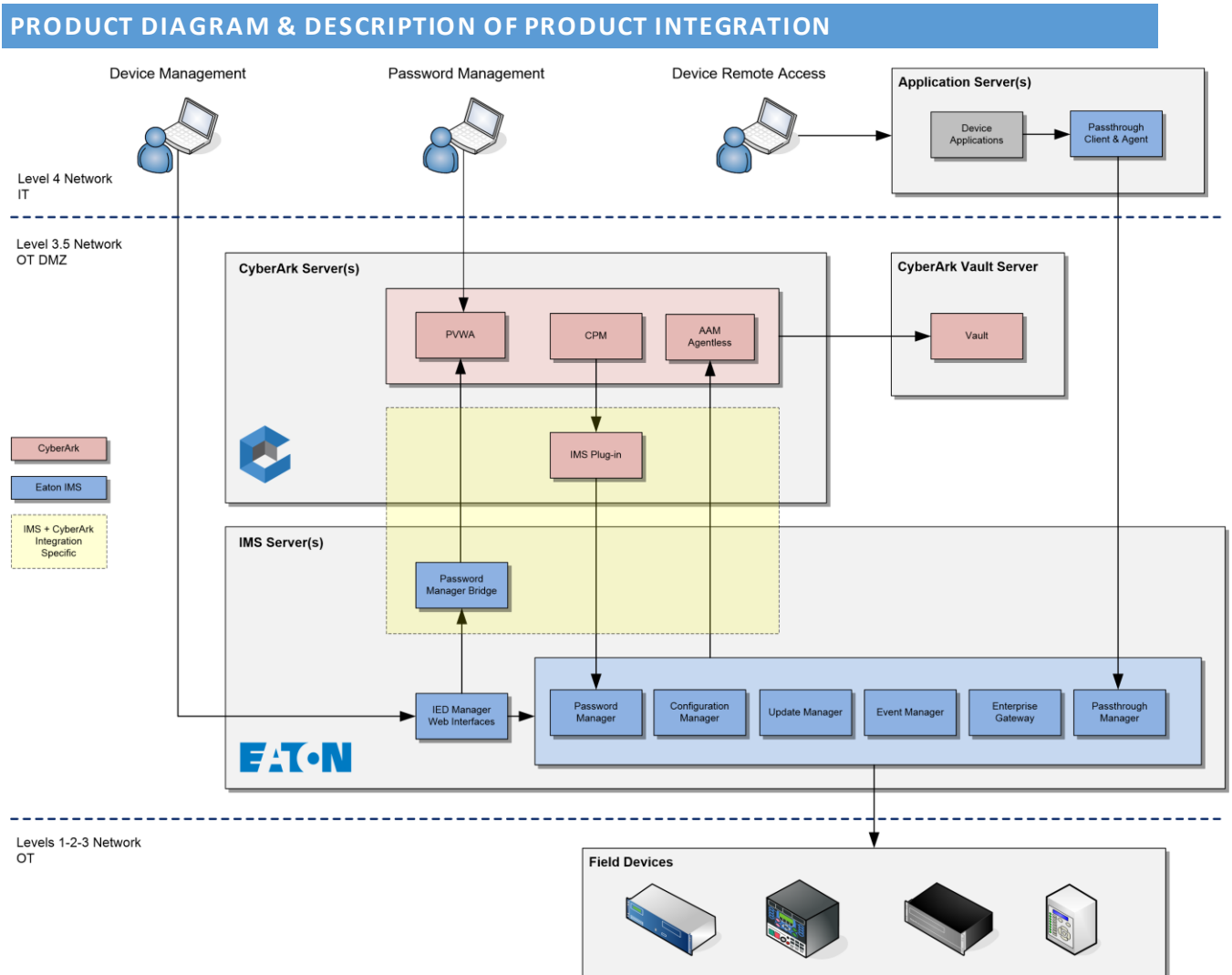
Benefits of IED Manager Suite:

- Track IED inventory and log all changes
- Easily access compliance reports and auditable logs
- Securely access remote IEDs
- Role-based access control to IEDs
- Enterprise single sign-on capability to IEDs. Users no longer need to know IED passwords and can connect to devices using their standard corporate credentials
- Manage and update device configuration settings, passwords and firmware

- Retrieve, store and manage power system events, fault records, SOE and oscillography from protection relays and DFRs
- Retrieve and publish real-time operational data for asset monitoring and business intelligence

Benefits of integrating IED Manager Suite with CyberArk AAM:

- Store IED passwords in centralized Enterprise vault
- Audit IED password access and history using CyberArk solutions
- Use CPM to automate password rotation on IEDs in a seamless manner to IMS systems and users. This is a separate integration (Refer to the IED Manager Suite CPM Implementation Guide).



AAM INTEGRATION

Typical integration of AAM is done at two locations:

- IMS Central Server
- Internet Information Services (IIS) hosting IMS web applications

Typical implementations are hosting web applications on the Central Server, therefore there is only one machine involved.

Optionally one or more Enterprise Gateway Services can be installed on the Central Server or on different endpoints. This is when IMS is used to implement real-time data acquisition of devices.

The following components are integrated with AAM:

- Passthrough Manager†
- Configuration Manager
- Password Manager
- Update Manager
- Enterprise Gateway
- Enterprise Gateway Services
- Web application server†

Components with † are those that can access AAM to retrieve IED passwords on behalf of a user.

CREDENTIAL RETRIEVAL

1) Credential retrieval is done whenever a system component needs to log on to an IED to accomplish a maintenance task. Those tasks are:

- Event retrieval
- Configuration retrieval
- Configuration/firmware update
- Password update/verification

The frequency of such tasks is subject to maintenance schedules configured inside IMS according to customer desires. Some typical scenarios are to perform event retrieval twice per day and configuration retrieval once per week, on each IED that supports those features. Each of these tasks can also be performed on a one-off basis by special request triggered from a Web user interface.

The tasks are shared among different Windows services all running on the same Central Server. The Enterprise Gateway will usually need to retrieve credentials only once during initial startup, or upon the first connection attempt, and then whenever login fails (e.g., if the password has been changed).

2) Another system task performed by the Enterprise Gateway Services will require credential retrieval upon initial startup:

- Real-time operational data acquisition

As with other tasks, retrieval is performed only for IEDs that are actively acquired. For this task, however, the Services can be scattered among different endpoints.

- 3) Credential retrieval can also occur when the following user task is performed on IEDs that support automatic login by IMS:
 - Remote access to IED
- 4) Whenever one of the tasks previously described is performed on an IED with serial connection, or an IED isolated from the IMS network, credential retrieval also occurs for accounts of Gateway systems that accomplish the following:
 - Passthrough access to IED

This is because IMS needs to log on to one or more Gateways for initiating the passthrough access.

- 5) Credential retrieval can also occur upon specific user requests:
 - View a password in the Password Manager Web application
 - View a password in the Passthrough Client application.

The user needs to have the appropriate permissions in IMS to perform this action. For the Web application, the action is analogous to a similar action in the Password Vault Web Access. It is performed by the IIS application pool. For the Passthrough Client application, the action is performed by the Central Server. It is typically requested when a user wants to perform remote access on an IED for which IMS does not support automatic login. For both actions, IMS keeps an audit log of which users have accessed the password. IMS will also mention which user performed the access in the “reason” provided in the query to CyberArk.

In all scenarios, accounts to query are identified by IMS by the safe name and the full account name (or object name). There are no specific properties required. Account names have the following format, which is guaranteed to be unique for one IMS server:

`<SubstationName>@<IEDName>@<UserName>`

REQUIREMENTS

The IED Manager Suite system is compatible with virtual environments (VMWare, Hyper-V and others).

Minimum system requirements for IMS Server:

- Intel Xeon or an equivalent
- Intel Core 2 or an equivalent
- Operating System, the following versions are supported:
 - Microsoft Windows Server 2012 R2
 - Microsoft Windows Server 2016
 - Microsoft Windows Server 2019

- Database Engine. IMS databases are stored in a Microsoft SQL Server instance. The following versions are supported:
 - SQL Server 2012
 - SQL Server 2014
 - SQL Server 2016 SP1
 - SQL Server 2017
 - SQL Server 2019
- X.509 Server certificate for server authentication and TLS

Requirements for AAM integration:

- X.509 Client certificate for each IMS endpoint, signed by same authority

AAM INSTALLATION

Refer to the “Credential Provider Implementation Guide” for CyberArk Agentless installation and configuration.

AAM CONFIGURATION

The following sections provide details on IED Manager Suite configuration with CyberArk AAM.

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.

Add Application

Name: Eaton-IMS

Description: All services from IED Manager Suite

Business owner

First Name:

Last Name:

Email:

Phone:

Location: \

☒ Access Permitted: From: To:

☐ Expiration Date:

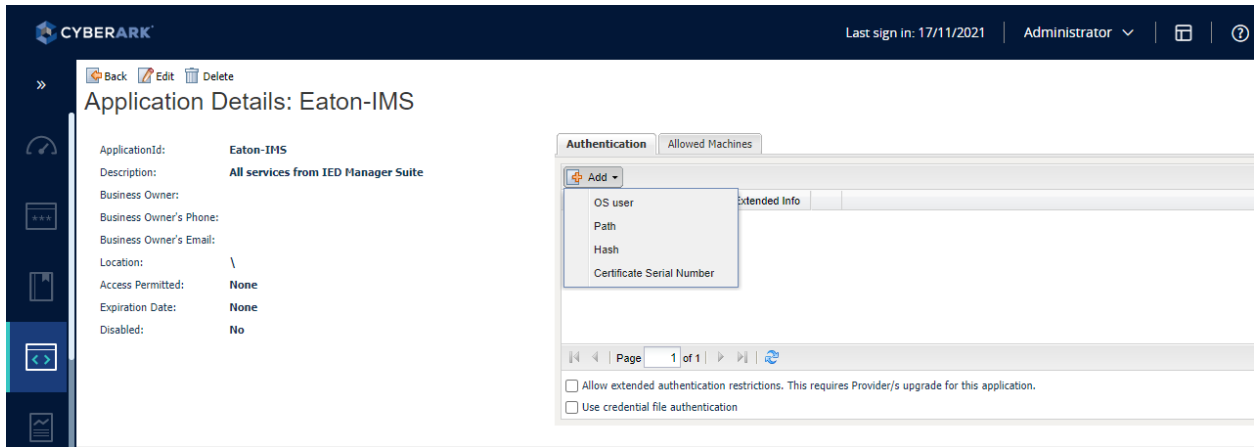
☐ Disabled

Add Cancel

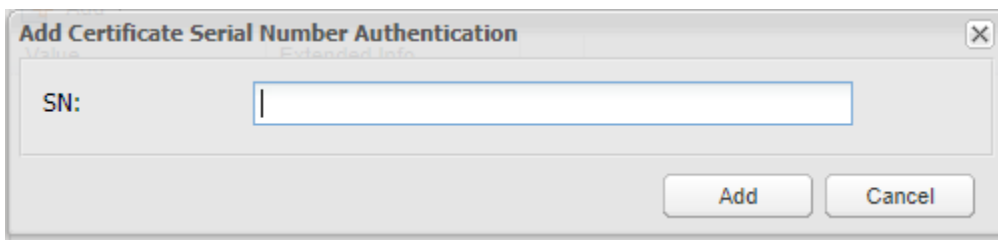
☐ Specify the following information:

- In the **Name** box, specify the unique name (ID) of the application. The recommended Application ID for this integration is: APP ID = Eaton-IMS
- 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.

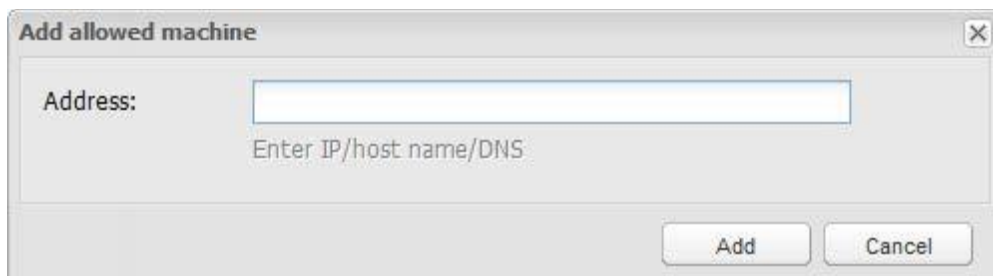
☐ Click **Add**. The application is added and is displayed in the Application Details page.



- ☐ Specify the application's **Authentication** details. This information enables the Credential Provider to check certain application characteristics before retrieving the application password.
- ☐ In the Authentication tab, click **Add**. A drop-down list of authentication characteristics is displayed.
- ☐ Select **Certificate Serial Number**. The Add Certificate Serial Number Authentication window appears.



- ☐ Specify the serial number (SN) of the client certificate that will be provided by the application, then click **Add**. The Certificate Serial Number is listed in the Authentication tab.
- ☐ Add the Certificate Serial Number used by each machine that will run the Enterprise Gateway Services, if any.
- ☐ Specify the application's Allowed Machines. This information enables AAM 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.

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.

- **Automatically with IMS** – Synchronize all accounts from IMS automatically using the IMS Password Manager Bridge service.

For this step, you require to install the IMS Password Manager Bridge on the IMSCentral Server. You also require a user with the **Access** and **Account Management** authorizations in the Password Safe. This user will be used by the IMS Password Manager Bridge for provisioning accounts. The user must be using the “Password” (a.k.a. cyberark) authentication method.

The IMS Password Manager Bridge is the recommended approach, as it will synchronize all IED accounts from an existing IMS system along with their current or default passwords, as well as their custom properties, including IDs which are required by the CPM for password change/verification. It will also synchronize all changes made to the IMS configuration automatically with the Password Safe, live, including deleting accounts. Note that synchronization only occurs one-way from IMS to the Password Safe.

Automatic provisioning by IMS also requires that certain account properties be defined in the platform(s) configured for the accounts. These properties are already pre-defined in the IED Manager Suite Platform available on the Marketplace. Before importing the platform, you need to create the corresponding custom File Categories in the Server Vault (where the Vault is installed).

☐ Add the following File Categories to the Vault:

- ResourceID (numeric)
- UserProfileID (numeric)
- Region
- Substation
- DeviceName
- Gateway
- PassthroughName
- IMSAddress

For more information about installing and configuring the IMS Password Manager Bridge, refer to the next section.

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

Before 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 provider user (where the Central Credential Provider is installed) 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 Safe Member

Search:

Search In:

Vault

Search

Selected Search: Vault

Name	Business Email	Full Name
------	----------------	-----------

☐ Access

☐ Use accounts

☒ Retrieve accounts

☒ List accounts

☐ Account Management

☐ Safe Management

☐ Monitor

☐ View Audit log

☒ View Safe Members

Add

Close

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

- Retrieve accounts

11

☐ 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.

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

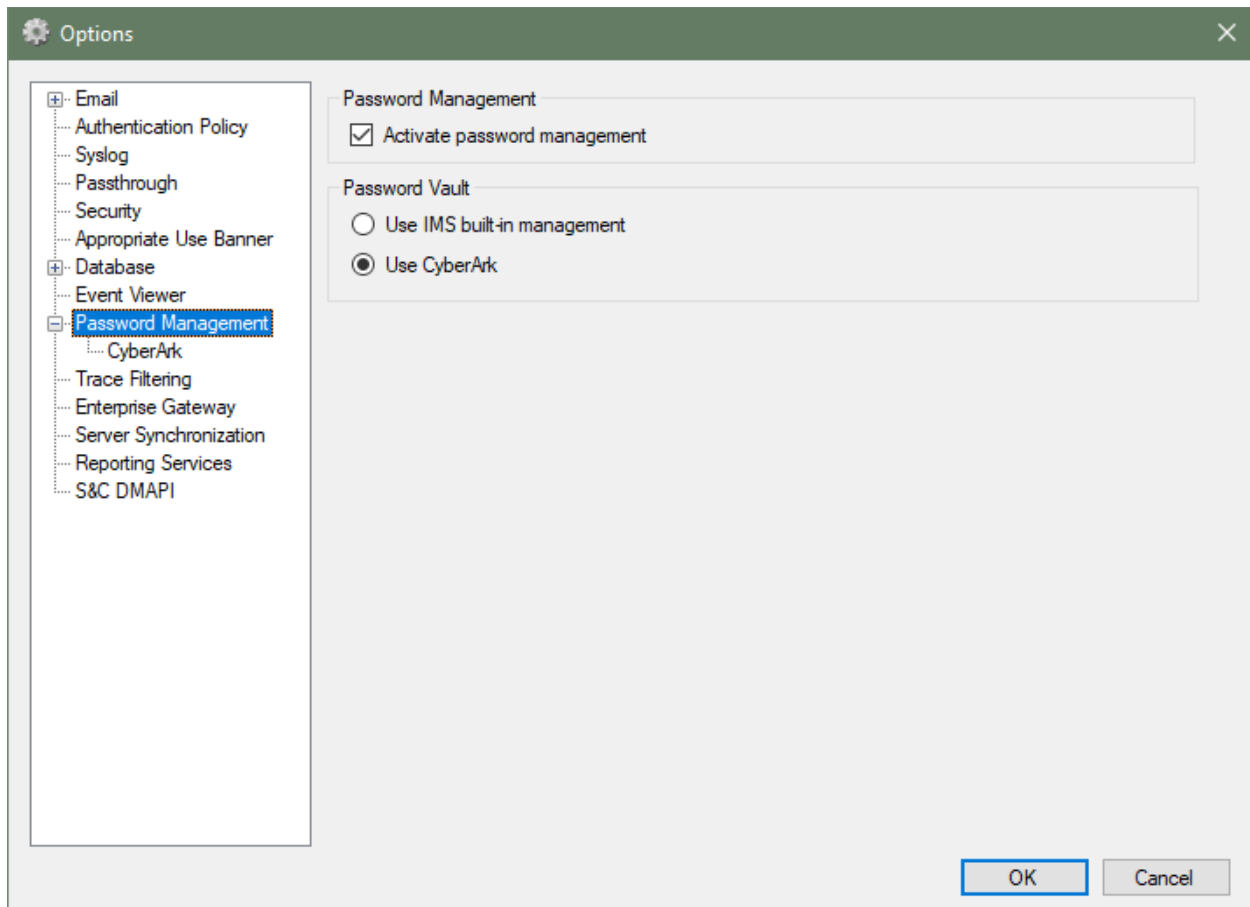
- 12

PARTNER PRODUCT INSTALLATION & INTEGRATION CONFIGURATION

Refer to the **IMS – Installation Guide** for Partner Product installation.

To configure IMS to use AAM, do the following:

- ☐ Open the Enterprise Management Console application on the IMS Central Server and log in.
- ☐ Go to Tools | Options menu.
- ☐ In the Options dialog window, select the Password Management section.
- ☐ Under Password Vault, select “Use CyberArk”.



This option is only available if you have a proper IMS license with the option included.

Next, configure IMS to query its dedicated Password Safe.

- ☐ In the Options dialog window, expand the Password Management section.
- ☐ Select the CyberArk section in the tree.
- ☐ Specify the following information:
 - In the **Safe Name** box, specify the name of the Password Safe where IED accounts are stored.

- In the **Web Service URL** box, specify the URL to access the AIM Web Service REST API.
- In the **App ID** box, specify the unique name (ID) of the application. The recommended Application ID for this integration is: APP ID = Eaton-IMS
- In the **Certificate Issuer Name** box, specify the name of the Certificate Authority that is used to sign the client certificate used by IMS to authenticate to AAM. You can also specify only part of the name, as it will be used to match any certificate whose issuer's name contains the string provided.

Options

General Details

Safe name:

Credential Provider

Web Service URL:

App ID:

Certificate Issuer Name:

Password Vault Web Access

Rest API URL:

☐ Create accounts in the safe only for IEDs "In Service"

IMS Services credentials

	IMS Service	Account	Password
▶	Password Bridge	IMSBridge	

OK Cancel

The Certificate Issuer Name is used by IMS to identify the client certificate to provide in its HTTPS requests to AAM. Such a certificate must be signed by the designated issuer and installed in the Local Machine certificate store of each IMS server endpoint.

The folder name is not provided. IMS always specifies the root folder in its requests, for all IED accounts. It also specifies the Safe and object name.

Next, you can configure IMS Password Manage Bridge for automatic provisioning of accounts in the Password Safe.

- ☐ In the Options dialog window, expand the Password Management section.

- ☐ Select the CyberArk section in the tree.
- ☐ Specify the following information:
 - In the **Rest API URL** box, specify the URL to access the Password Vault Web Access REST API.
 - In the **Account** box, specify the cyberark user that IMS Password Manager Bridge will use to authenticate to the PVWA.
 - In the **Password** box, specify the password for the cyberark user account provided.

The password is encrypted by IMS using RSA before it is stored in the options file.

One last step required for automatic provisioning is to specify the Policy ID(s) to assign to the accounts created by the IMS Password Manager Bridge.

- ☐ Open the Enterprise Management Console application on the IMS Central Server and log in.
- ☐ Select the Password Policies section in the tree.
- ☐ Specify the following information:
 - In the **External Vault Policy ID** column, specify the Policy ID of the platform to associate with each IMS password policy.

Configure: \ Password Policies					
Define password management policies.					
	Name	Min Length	Max Length	Generator	External Vault Policy ID
	ABB Default Policy	8	64	Complex 4: [A-Z][a-z][0-9][0~!@%*+= {}<>:;?_#&-/.~]	
	ABB WHMI Policy	9	20	Complex 4: [A-Z][a-z][0-9][0~!@%*+= {}<>:;?_#&-/.~]	
	AMETEK Default Policy	6	8	Complex 3: [A-Z][a-z][0-9][0~!@%*+= {}<>:;?_#&-/.~]	
	Arteche Default Policy	4	10	Complex 2: [A-Z][a-z][0-9][0~!@%*+= {}<>:;?_#&-/.~]	
	Arteche Shared Key Policy	12	50	Alphanumeric	
	Beckwith Default Policy	4	4	Numeric	
	Beckwith Standard Security Policy	6	6	Alphanumeric	
	Cooper Controls and Relays Default Policy	4	64	Complex 3: [A-Z][a-z][0-9][0~!@%*+= {}<>:;?_#&-/.~]	
	Cooper Controls and Relays MMI Policy	4	4	Numeric	
	Cooper Controls and Relays NXG CL-7 Policy	8	20	ProView NXG Complex	
	Cooper Controls and Relays NXG Policy	6	10	ProView NXG	
	DNP3 Update Key	32	32	Hexadecimal	
	Eaton Secondary Network Default Policy	8	15	Complex 3: [A-Z][a-z][0-9][0~!@%*+= {}<>:;?_#&-/.~]	
	GE UR Series 7.x+ Default Policy	6	20	Complex 3: [A-Z][a-z][0-9][0~!@%*+= {}<>:;?_#&-/.~]	
▶	GE UR Series Default Policy	8	8	Numeric	
	ION Power Meters Default Policy	8	8	Numeric	
	MiCOM Relays Default Policy	4	4	Alphabetic	
	NovaTech Orion Default Policy	8	20	Complex 3: [A-Z][a-z][0-9][0~!@%*+= {}<>:;?_#&-/.~]	
	RFL Default Policy	5	64	Complex 5: [A-Z][a-z][0-9][0~!@%*+= {}<>:;?_#&-/.~]	
	RuggedCom Switches Advanced Policy	12	64	Complex 4: [A-Z][a-z][0-9][0~!@%*+= {}<>:;?_#&-/.~]	
	RuggedCom Switches Default Policy	10	15	Alphanumeric	
	S&C Default Policy	8	12	Complex 6: [A-Z][a-z][0-9][0~!@%*+= {}<>:;?_#&-/.~]	
	SEL Relays Advanced Policy	8	63	Complex 3: [A-Z][a-z][0-9][0~!@%*+= {}<>:;?_#&-/.~]	IEDManagerSuite
	SEL Relays Default Policy	5	6	Alphanumeric	SELviaIMS
	Siemens Confirmation ID Policy	6	10	Numeric	
	SMP Computing Platform Default Policy	8	63	Complex 3: [A-Z][a-z][0-9][0~!@%*+= {}<>:;?_#&-/.~]	
	SMP Device Default Policy	6	16	Complex 3: [A-Z][a-z][0-9][0~!@%*+= {}<>:;?_#&-/.~]	IEDManagerSuite
	User Defined Default Policy	1	32	Complex 3: [A-Z][a-z][0-9][0~!@%*+= {}<>:;?_#&-/.~]	
	Windows Default Policy	8	63	Complex 3: [A-Z][a-z][0-9][0~!@%*+= {}<>:;?_#&-/.~]	

The default Policy ID for the Marketplace platform is IEDManagerSuite. However, if using password management, you will probably need to create more platforms by duplicating the original one.

Automatic provisioning is only effective for IED accounts that are using a password policy that is mapped to a valid existing Policy ID.

For more information about installing and configuring the IMS Password Manager Bridge, refer to the **IMS with CyberArk – Integration Guide** in the Partner Product documentation.

PARTNER CONTACT INFO

Business Contact	Name	Patrick Cossette
	Email	patrickcossette@eaton.com
	Tel	+1.514.502.2213
Technical Contact	Name	Eaton Support
	Email	eas-support@eaton.com
	Tel	(800) 815-2258
Support Contact	Name	Eaton Support
	Email	eas-support@eaton.com
	Tel	(800) 815-2258