INTEGRATION GUIDE

Automation Systems Manager (ASM) Integration with CyberArk Application Access Manager (AAM)

Advanced Services Appliance (ASA) Integration with AAM

INDUSTRIAL DEFENDER®

Solution Overview

Multiple vendor systems, geographically dispersed plants and hard-to-reach endpoints make it difficult to effectively monitor, manage and protect industrial control system (ICS) networks. Traditional IT enterprise solutions can be demanding of already limited computing resources and often fail to fully address the cybersecurity needs of operational environments. Industrial Defender ASM is an industry leading solution for security, compliance and operations of control systems environments.

By combining multiple applications on a single platform, it provides a consolidated real-time view to secure and manage your control systems environment. From ultra-low bandwidth requirements to proprietary protocols, Industrial Defender ASM was designed and built from the ground up to ensure security, safety and reliability of your control systems. Certified to maintain performance standards by multiple control systems vendors, Industrial Defender ASM is the only platform to offer applications specifically engineered to address the overlapping requirements of cybersecurity, compliance, and change management.

1.1 Key Benefits

The security, reliability, and availability of the automation control systems—at the heart of critical infrastructure—are of paramount importance. They have spawned stringent requirements to meet both internal quality of service goals as well as external government standards and regulations, which bring potentially significant fines for non-compliance. To add to this challenge, industrial control systems are typically quite complex with a plethora of asset and data types.

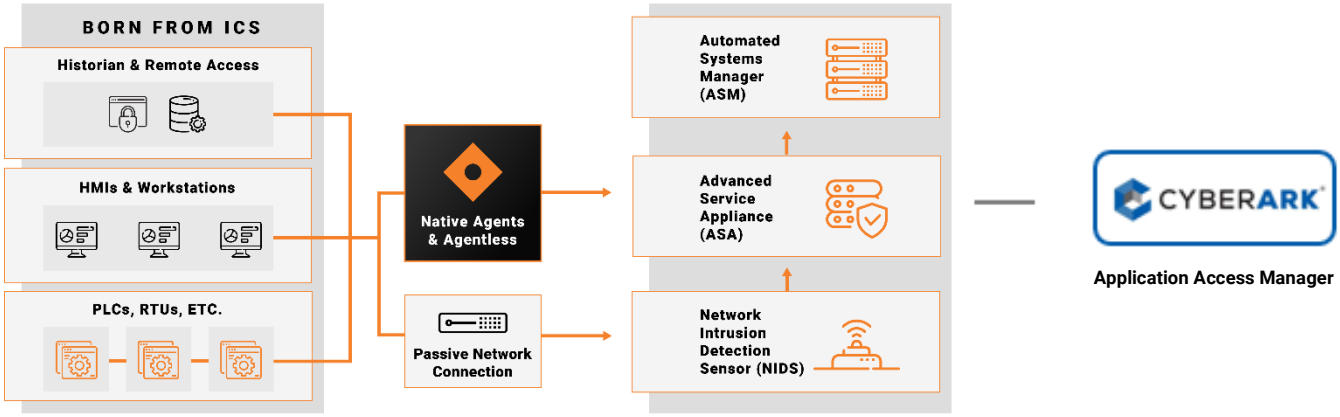
To maximize security, reliability, and availability of control systems, Industrial Defender's ASM technology solution gives critical infrastructure owners the tools necessary to safely collect, monitor, and manage OT asset data at scale, while providing cross-functional teams with a unified view of security. The ASM infrastructure consists of three interrelated components:

- Automation Systems Manager (ASM)
- Advanced Services Appliance (ASA)
- Network Intrusion Detection System (NIDS)

This infrastructure can be deployed at your locations with no disruption to operations and no reboot required. The vendor-agnostic solution is tuned to collect data from 100+ types of industrial endpoints – including those hard to reach RTUs, IEDs, and PLCs – and report on baseline deviations, alert on priority security events and flag policy violations. With up-to-date information operators can confidently manage users, compliance reporting, patches, security events and incident response from a single, unified view.

By leveraging the customer's existing CyberArk vault, the task of maintaining continually updating passwords at the ASA is eliminated, drastically reducing administrative overhead.

1.2. Product Diagram



In a traditional Industrial Defender ASM solution, endpoint credentials are entered and stored on the ASA, which can also support external credential stores, including CyberArk AAM. Polling from the ASA for agentless devices remains the same, the ASA retrieves the end point credentials from AAM, then uses those credentials to connect directly to the end point for state data collection.

2. Installation

2.1. AAM Installation

The agent based AAM (Credential Provider) software package and dependencies are not installed on the ASA from the factory. Follow your installation guide to install and configure it.

NOTE: Contact Industrial Defender support for a dependency package if the ASA does not have access to a CentOS repository.

2.1.1. Enabling CyberArk on the ASA

Once the CyberArk AAM has been installed and configured on the ASA, the ASA must have the password manager enabled. Logon to the ASA and run the following command.

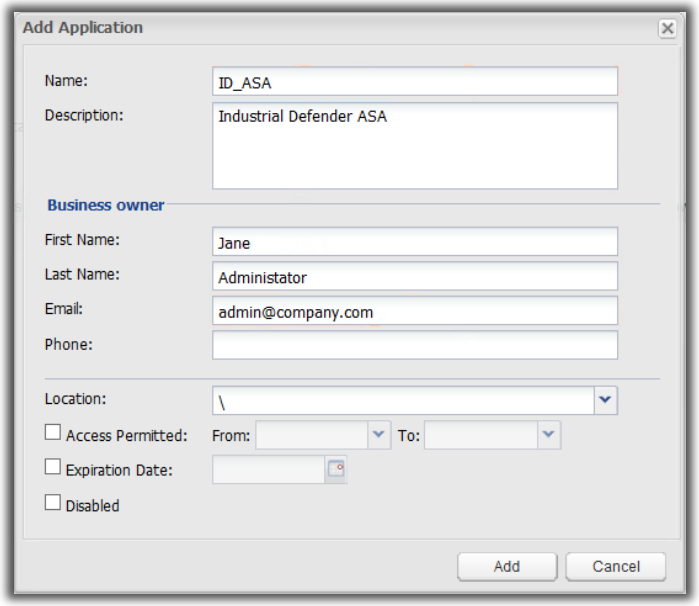
```
ASA> set passwordmanager cyberark
passwordmanager cyberark
```

2.2. AAM Configuration

2.2.1. Defining the Application ID and Authentication Details

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

Log in as a user allowed to manage applications (Manage Users authorization required)
In the **Applications** tab, click **Add Application**.



Specify the following information:

- In the **Name** field, specify the unique name (ID) of the application. The default

Application ID for ASM is **ID_ASA**.
    - Note: Application ID can be modified by editing the *CyberArk.properties* file located in */var$IDROOT/password-managers.d on the ASA*.
- In the **Description** field, 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** field, specify the location of the application in the Vault hierarchy. If a location is not specified, 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.

Select the **Allowed Machines** tab, then click the **Add** button.

In the **Add allowed machine** dialog, enter the IP address, hostname, DNS name of the ASA and click **Add**.

2.2.2. Provisioning Accounts and Setting Permissions for Application Access

For the ASA to be able to retrieve credentials for the assets, the ASA must have access to the asset accounts provisioned in the CyberArk Vault.

In the Password Safe, provision the end point accounts that will be required by the ASA. 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 asset accounts, refer to the **Privileged Access Security Implementation Guide**.

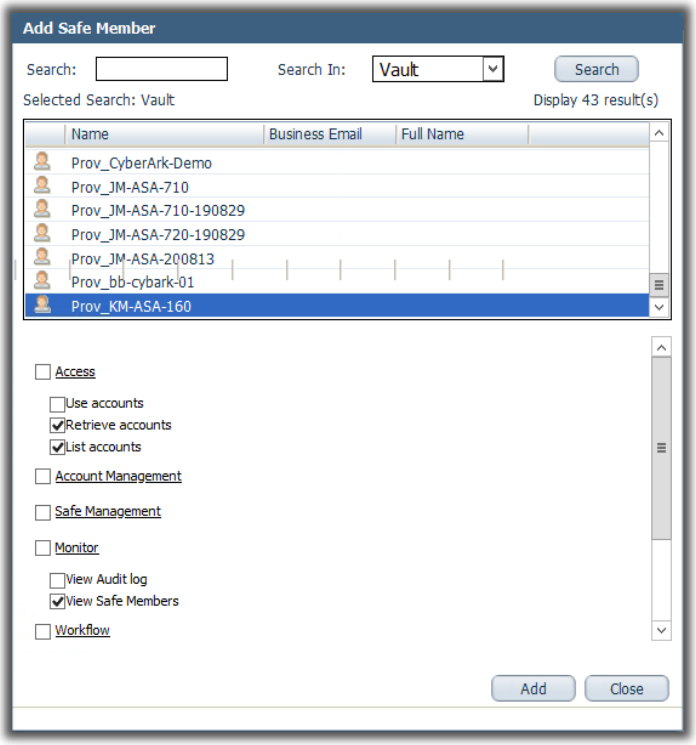
Once the accounts are managed by CyberArk, make sure to setup the access to both the ASA and CyberArk Application Password Providers serving the ASA.

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

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

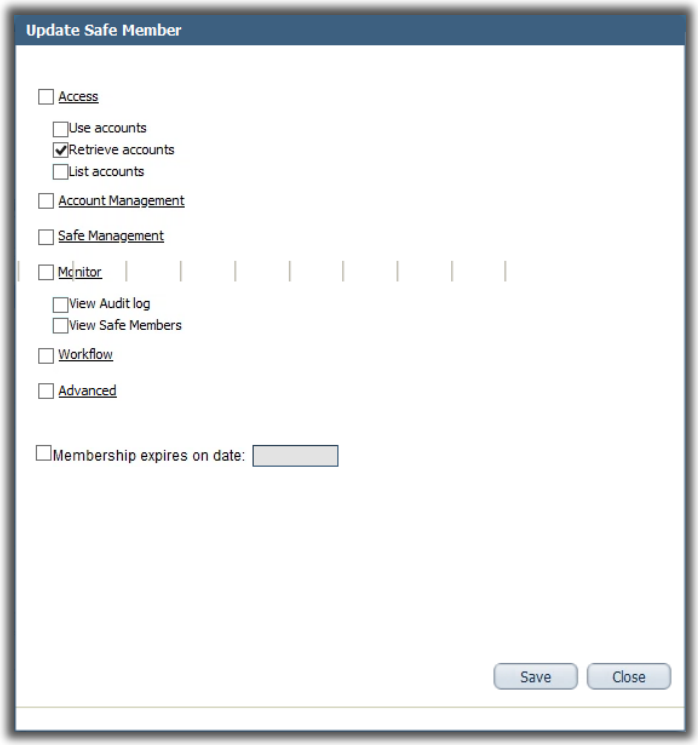
- List accounts
- Retrieve accounts

- 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 that both the Provider user and the ASA have access to the password(s) to retrieve.

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

2.3. Configuring Assets to use CyberArk

2.3.1. Agentless

For state data collection to work on agentless assets with credentials stored in the CyberArk vault, an existing or new account needs to be provisioned in the vault. Once the accounts are managed by CyberArk, make sure you have access to both the application and the CyberArk Application Password Providers serving the Application.

Add Asset to the ASM (ASM 7.3 and later)

Create a new agentless asset in the ASM using the steps found in the *Manually Creating an Asset* section of the **ASM User Guide**.

However, rather than assigning a collection profile via the ASM user interface, refer to the

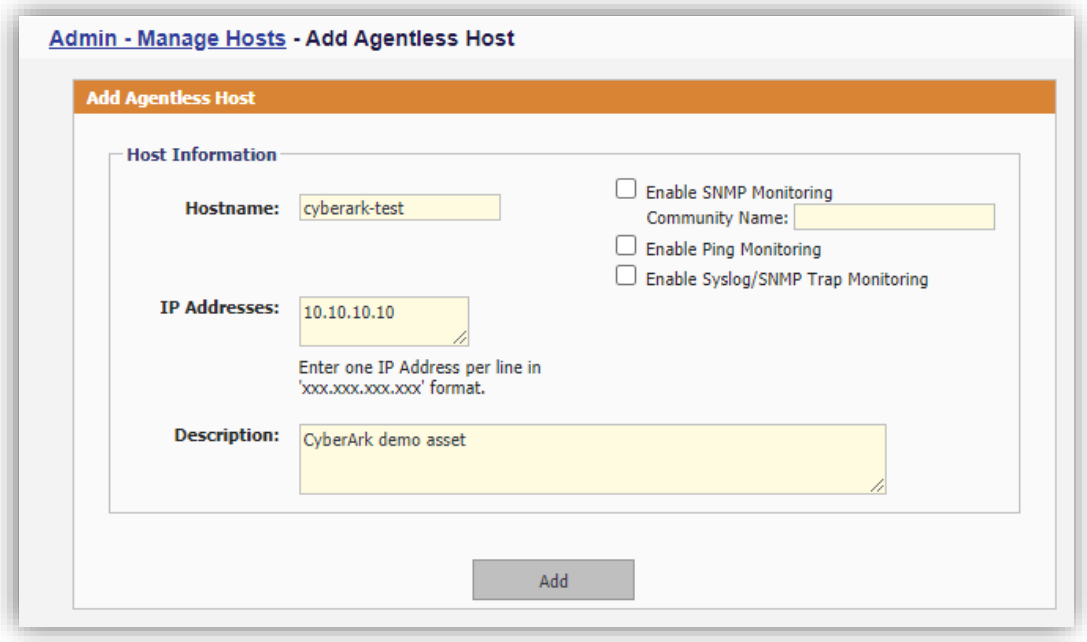
instructions below in the **Configure Asset Credentials on the ASA Command Line** section below.

Add Asset to the ASA (ASM 7.2 and earlier)

As would normally happen when adding a new agentless asset to the environment, open the ASA web user interface and click the **Add Host** link.

In the *Add Host* dialog, select either **Agentless Host** or **Windows Agentless (WMI) Host** and click **Next**.

In the *Admin - Manage Hosts - Add Agentless Host* screen, fill out the **Hostname, IP Addresses,** and **Description** fields, then select any additional options required and click **Add**.



For additional information, refer to the Industrial Defender Advanced Services Appliance (ASA) Administration Guide.

Configure Asset Credentials on the ASA Command Line

Using the collection-utility, configure the asset for polling. In this example, we are configuring a Linux asset.

Login to the ASA and run the collection utility, select option 1 to Manage Devices, then option 3 to configure a device for polling. Select the asset you wish to configure.

```
ASA> exec collection-utility

    ######################
    # Manage Collectors #
```

```
    ######################

    1. Manage Devices
    2. Manage Profiles
    3. Manage Profile Groups
    Q. Quit

    Enter selection 1

    ##################
    # Manage Devices #
    ##################

    1. List Polled Devices
    2. Manage Polled Device
    3. Configure Device for Polling
    4. Remove Device from Polling
    Q. Quit

    Enter selection [q] 3

    ################################
    # Configure Device for Polling #
    ################################

    1. cyberark-test
    Q. Quit

    Enter selection [q] 1
```

Select the profile for the asset.

```
    Enter profile search pattern [all] centos

    ######################################
    # Select Profile for 'cyberark-test' #
    ######################################

    1. RHEL6 privileged [Red Hat Enterprise/CentOS v6 privileged user]
    2. RHEL6 unprivileged [Red Hat Enterprise/CentOS v6 unprivileged]
    3. RHEL7 privileged [Red Hat Enterprise/CentOS v7 privileged]
    4. RHEL7 unprivileged [Red Hat Enterprise/CentOS v7 unprivileged]
    5. Red Hat [Red Hat Enterprise/CentOS Linux 5]
    6. Red Hat unprivileged [Red Hat Enterprise/CentOS Linux 5
unprivileged]
    Q. Quit

    Enter selection [q] 3

        Device : cyberark-test
        IP     : 55.55.55.55
```

```
Profile: RHEL7 privileged

Save this configuration? (y/n) [n] y
```

If you have enabled the CyberArk password manager on the ASA, you will be prompted to select either the local password store or use an external password manager. Select Password Manager in the Setup Credentials menu and select CyberArk in the list of password managers.

```
####################
# Setup Credentials #
####################

1. Local Store
2. Password Manager
Q. Quit

Enter selection [q] 2

####################
# Password Managers #
####################

1. CyberArk
Q. Quit

Enter selection [q] 1
```

Enter the Vault information at the prompts.

```
What is the Vault's Safe value for the credentials related to this
asset(or quit):test
What is the Vault's Folder value for the credentials related to this
asset(or quit):root
What is the Vault's Object value for the credentials related to this
asset(or quit):CyberArk-test-root
```

Note: The Object value is either the auto-generated name pattern or the custom name set in the Account in the vault

The asset is now configured.

Verify Authentication Is Working

The configuration can be validated using the Check Asset function at the ASM and confirming new state data has been collected from the newly configured asset.

THE INDUSTRIAL DEFENDER DIFFERENCE

Since 2006, Industrial Defender has been solving the challenge of safely collecting, monitoring, and managing OT asset data at scale, while providing cross-functional teams with a unified view of security. Their specialized solution is tailored to complex industrial control system environments by engineers with decades of hands-on OT experience. Easy integrations into the broader security and enterprise ecosystem empower IT teams with the same visibility, access, and situational awareness that they're accustomed to on corporate networks. They secure some of the largest critical control system deployments with vendors such as GE, Honeywell, ABB, Siemens, Schneider Electric, Yokogawa and others to protect the availability and safety of these systems, simplify standards and regulatory requirements, and unite OT and IT teams.

1 (877) 943-3363 • (617) 675-4206 • info@industrialdefender.com

225 Foxborough Blvd, Foxborough, MA 02035

industrialdefender.com