



CYBERARK SECRETS MANAGER

(Agent Based Credential Provider CP)

SECRETS MANAGER INTEGRATION - TECHNICAL DOCUMENTATION

Name of Company: AlgoSec

Website: www.algosec.com

Name of Product: AlgoSec Security Management Suite (ASMS)

Version: 2018.2

Date: November 2018 (Revised 17 October 2020)

ALGOSEC SECURITY MANAGEMENT SUITE OVERVIEW

The AlgoSec Security Management Suite (ASMS) delivers a complete, integrated solution for managing complex network security policies — from the business application layer to the network infrastructure. With powerful visibility across virtual, public and hybrid cloud and physical environments, the AlgoSec suite automates and simplifies the entire security change management process to accelerate application delivery while ensuring security and compliance.

The AlgoSec suite can be deployed as a VM, a dedicated hardware appliance or as an AWS AMI.

Version: 2018.2

KEY BENEFITS

Application Connectivity Management

- Automated discovery and mapping of business connectivity
- Translation of business requirements into networking terms
- Impact assessment to avoid outages
- Rapid datacenter and cloud migration
- Business-centric risk analysis
- Secure application decommissioning

Security Policy Change Automation

- Security policy workflow automation
- Topology analysis and optimal rule design
- Proactive risk and compliance verification
- Automated policy push
- Change validation and reconciliation
- SLA tracking and complete audit trail
- Integration with ticketing systems

Network Abstraction & Policy Analysis

- Topology map and traffic simulation
- Firewall rule optimization and cleanup
- Audit-ready compliance reports
- Risk assessment
- Baseline configuration compliance
- Network segmentation enforcement

Key Benefits of Integrating ASMS with Secrets Manager

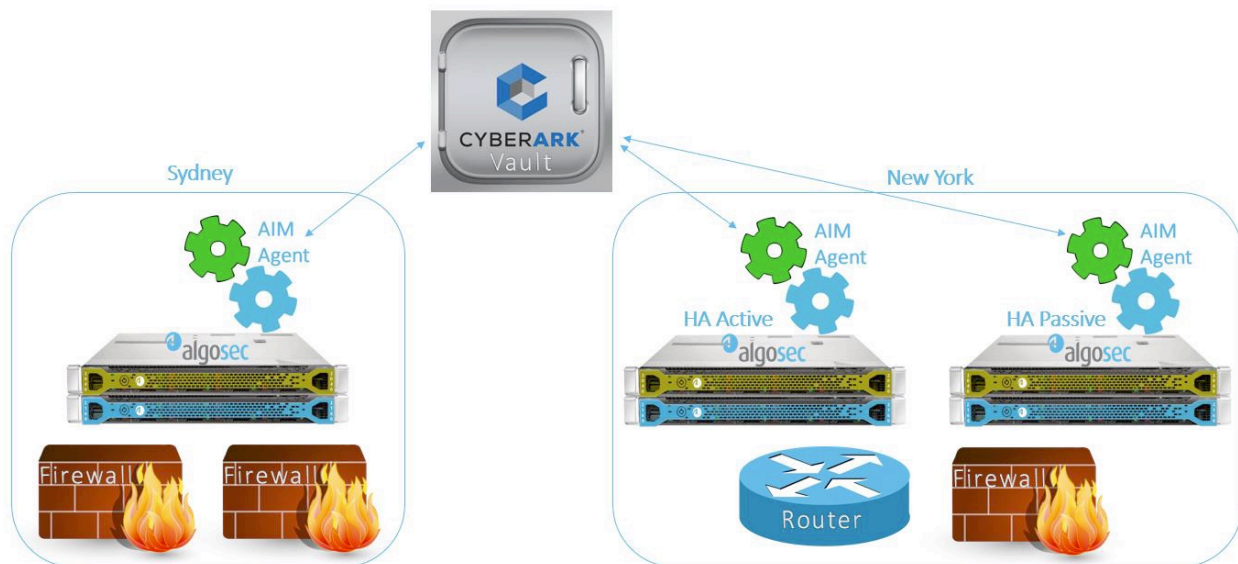
- ASMS allows users to manage large and complex networks, which can scale up to 10,000s of security devices, including routers, firewalls, load-balancers, web proxies, and more.
- Some customers prefer to keep credentials to their strategic security devices in dedicated vault systems such as CyberArk.
- Integrating ASMS with CyberArk allows the customer to enjoy the ASMS benefits while making sure that the ASMS-managed security devices credentials are kept in CyberArk vault, enjoying all the benefits the CyberArk vault presents.
- Once the relevant CyberArk configuration has been set on ASMS, the credentials retrieval from CyberArk is transparent to the user.
- ASMS allows the user to set the required CyberArk configuration to a bulk of devices rather than doing that for each device individually.
- The above is especially important for customers having an existing ASMS setup with multitude of devices.

PRODUCT DIAGRAM & DESCRIPTION OF PRODUCT INTEGRATION

An AlgoSec end-customer can install one or more ASMS hosts based on the environment requirements. The installation options are:

1. A single host
2. Two hosts, serving for High Availability (HA) or Disaster Recovery (DR) purposes
3. A Central Manager host and one or more hosts in different geographical locations near the target security devices
4. Any combination of the second and third option.

The second and third option are illustrated in the diagram below.



SECRETS MANAGER INTEGRATION

A customer may install one or more ASMS hosts based on their environment requirements, setup, and physical location. For example, an environment may require ASMS high availability setup, in which there

are typically 2 ASMS hosts. Or, it may require ASMS Geographical distribution setup, in which the number of ASMS hosts depends on the number of physical locations.

The CyberArk Secrets Manager agent must be installed on each of the ASMS hosts, as each of them will need to connect to the security devices they manage, thus requiring credentials.

ASMS allows several recurrent processes and ad-hoc actions requiring connecting to the managed security devices, and in turn requiring credentials retrieval from CyberArk.

Recurrent processes:

- Monitor cycle: Typically a monitor cycle runs every 5 minutes for each managed device
- Analysis report: Typically an analysis (report) once a day for each managed device

Ad-hoc action:

- ActiveChange: Pushes policy changes towards a security device. There is no static frequency for this action. It happens according to the customer usage of the ASMS suite. A large enterprise can run around 100 ActiveChange actions daily.

CREDENTIAL RETRIEVAL

When credentials retrieval from a CyberArk vault is required and configured so in ASMS, ASMS assumes the customer has installed the CyberArk Secrets Manager Agent SDK on each of the ASMS hosts.

The ASMS software uses the Secrets Manager Agent SDK to retrieve credentials from a target security device.

SECRETS MANAGER INSTALLATION

Refer to the “Credential Provider and ASCP Implementation Guide” for CyberArk Agent based installation and configuration.

This functionality is solely under the responsibility of the end customer. ASMS does not serve any part in the CyberArk software installation and configuration. In case the customer encounters issues installing the Secrets Manager software and/or validating that it communicates properly with the matching vault, the customer should approach CyberArk TAC to troubleshoot this issue.

SECRETS MANAGER CONFIGURATION

The following sections provide details on AlgoSec Security Management Suite 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.

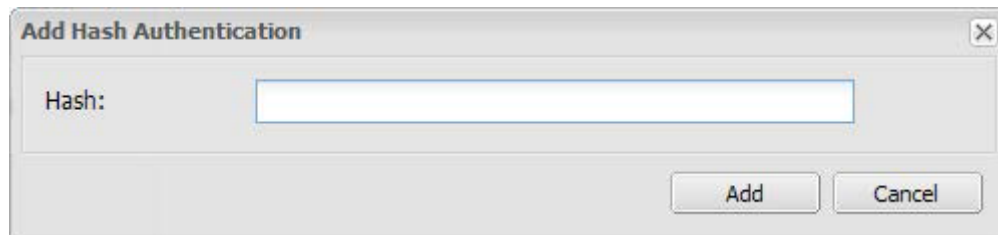
The screenshot shows the 'Add Application' dialog box. It has a title bar with a close button. The main area contains several input fields and checkboxes. The 'Name' field is filled with 'Algosec'. The 'Description' field is empty. Below a horizontal line is the 'Business owner' section, which includes fields for 'First Name', 'Last Name', 'Email', and 'Phone', all of which are empty. Below this is the 'Location' field, which is a dropdown menu showing a backslash character. Below the 'Location' field are three checkboxes: 'Access Permitted', 'Expiration Date', and 'Disabled', all of which are unchecked. The 'Access Permitted' checkbox has 'From' and 'To' dropdown menus. The 'Expiration Date' checkbox has a date picker. At the bottom right are 'Add' and 'Cancel' buttons.

- ☐ Specify the following information:
- In the **Name** box, specify the unique name (ID) of the application. The recommended Application ID for this integration is: Algosec
 - 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.

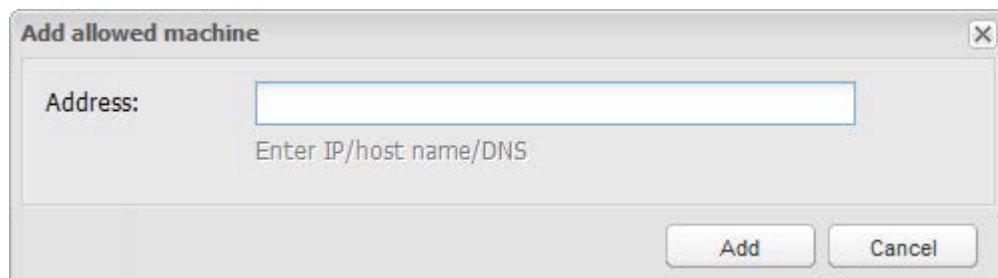
- ☐ Check the **Allowing extended authentication restrictions** box. This enables you to specify an unlimited number of machines and Windows domain OS users for a single application.
- ☐ Specify the application's **Authentication** details. This information enables the Credential Provider to check certain application characteristics before retrieving the application password.
- ☐ 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**. The 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.


 A dialog box titled "Add Hash Authentication" with a close button (X) in the top right corner. It contains a label "Hash:" followed by a text input field. At the bottom right, there are two buttons: "Add" and "Cancel".

- In the Hash edit box, paste the application's unique hash value, or specify 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.


 A dialog box titled "Add allowed machine" with a close button (X) in the top right corner. It contains a label "Address:" followed by a text input field. Below the input field, there is a hint text "Enter IP/host name/DNS". At the bottom right, there are two buttons: "Add" and "Cancel".

- 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 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

Add Safe Member

Search: Search In:

Selected Search: Vault Display 5 result(s)

	Name	Business Email	Full Name
	Algosec_AFA		
	Algosec_test		
	Algosec_QA		
	Algosec		
	Prov_algosec		

☐ Access

- ☐ Use accounts
- ☒ Retrieve accounts
- ☐ List accounts

☐ Account Management
☐ Safe Management
☐ Monitor

- ☐ View Audit log
- ☐ View Safe Members

Algosec has been added.

- ☐ 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**.

ALGOSEC SECURITY MANAGEMENT SUITE INSTALLATION & INTEGRATION CONFIGURATION

Refer to AlgoSec Firewall Analyzer Administrator Guide for AlgoSec Security Management Suite installation.

AFA provides the option to integrate with CyberArk, allowing AFA to access devices without saving the device credentials on the AlgoSec Security Management Suite server. ASMS will connect to CyberArk

vault to fetch the device credentials analysis, real-time change monitoring, and implementing changes with ActiveChange.

Once CyberArk integration is configured, when setting up a device (add or edit), you will have the option to specify the parameters that AFA should use to connect to the CyberArk vault in order to fetch the device credentials. CyberArk integration is supported for the following device brands:

- Fortinet FortiManager
- Juniper Netscreen
- Cisco ASA/PIX/FWSM
- Cisco Nexus
- Cisco IOS
- F5 BIG-IP
- Blue Coat

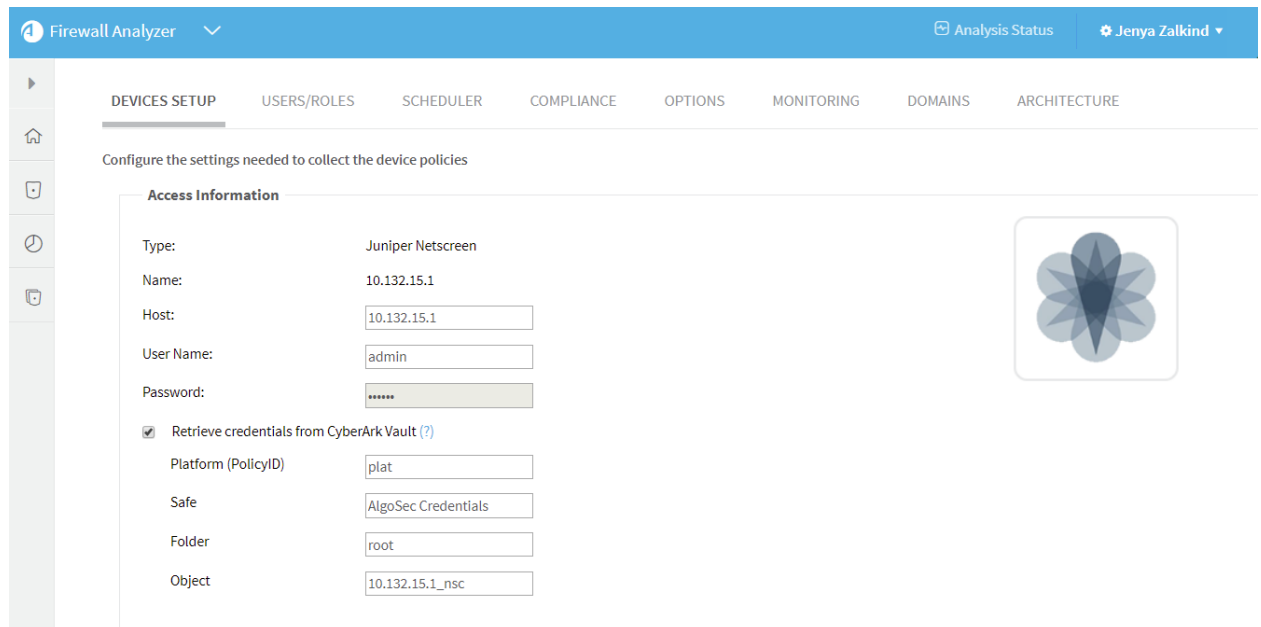
Important: Prior to configuring CyberArk integration in the AFA Web Interface, you must configure the CyberArk Secrets Manager agent on all AlgoSec hosts (Central Manager, Remote Agents, secondary nodes of HA/DR clusters, etc.). You must install the Secrets Manager agent on all hosts and configure it to communicate with the CyberArk vault.

To configure CyberArk integration:

1. In the toolbar, click your username.
2. In the drop-down menu, select **Administration**. The **Administration** page appears.
3. In the **Options** tab of the **Administration** page, click the **Authentication** sub-tab. The **Authentication** page appears.

The screenshot shows the 'Administration' page in the Firewall Analyzer web interface. The top navigation bar includes 'Firewall Analyzer', 'Analysis Status', and a user dropdown menu showing 'admin'. The left sidebar contains navigation icons. The main content area is titled 'Administration' and has tabs for 'DEVICES SETUP', 'USERS/ROLES', 'SCHEDULER', 'COMPLIANCE', 'OPTIONS' (selected), 'MONITORING', 'DOMAINS', and 'ARCHITECTURE'. Under the 'OPTIONS' tab, there are sub-tabs: 'General', 'Language', 'Display', 'Log analysis', 'Proxy', 'Mail', 'Storage', 'Workflow', 'Authentication' (selected), 'Backup/Restore', and 'Advanced Configuration'. The 'Authentication' sub-tab is active, showing 'User Authentication' settings. It includes radio buttons for 'Authentication Server' (selected) and 'Single Sign On'. Under 'Authentication Server', there are checkboxes for 'Local', 'RADIUS', and 'LDAP'. A checkbox for 'The Authentication server is case-sensitive' is also present. Below this, there are radio buttons for 'Default for new users: Local', 'Radius', and 'LDAP'. A text field for 'Default Mail Domain:' is shown with an example: 'For example: "AlgoSec.com"'. The bottom section is titled 'CyberArk' and includes a checkbox 'Allow to setup devices with CyberArk credentials management (?)'. Below this, there are input fields for 'Platform (Policy ID):' (containing 'Platform_NG'), 'Safe:' (containing 'Web'), and 'Folder:' (containing 'Root'). The CyberArk logo is visible in the bottom right corner of the section.

4. In the CyberArk area, select the **Allow to setup devices with CyberArk credentials management** check box to enable the CyberArk fields.
5. If desired, specify default values for all devices that will be authenticated via CyberArk using the Default CyberArk Fields. Any default values you specify will appear pre-populated when defining a new device in AFA.
6. Click **OK** to finish configuring CyberArk. Once configured, CyberArk will appear as an option for authenticating all supported device brands.



The screenshot shows the 'Firewall Analyzer' web interface. The top navigation bar includes 'Analysis Status' and the user 'Jenya Zalkind'. The main menu has tabs for 'DEVICES SETUP', 'USERS/ROLES', 'SCHEDULER', 'COMPLIANCE', 'OPTIONS', 'MONITORING', 'DOMAINS', and 'ARCHITECTURE'. The 'DEVICES SETUP' tab is active, showing a configuration page for a device. The page title is 'Configure the settings needed to collect the device policies'. The 'Access Information' section contains the following fields:

- Type: Juniper Netscreen
- Name: 10.132.15.1
- Host: 10.132.15.1
- User Name: admin
- Password: (masked with asterisks)
- ☒ Retrieve credentials from CyberArk Vault (?)
- Platform (PolicyID): plat
- Safe: AlgoSec Credentials
- Folder: root
- Object: 10.132.15.1_nsc

A Juniper logo is visible on the right side of the configuration area.

PARTNER CONTACT INFO

Business Contact	Name	Omer Ganot
	Email	Omer.Ganot@algosec.com
	Tel	
Technical Contact	Name	Nechami Ofek
	Email	Nechami.Ofek@algosec.com
	Tel	
Support Contact	Name	AlgoSec Support
	Email	support@algosec.com
	Tel	