



APPLICATION IDENTITY MANAGER

AIM INTEGRATION - TECHNICAL DOCUMENTATION TEMPLATE

Name of Company STEALTHbits Technologies Inc.

Website www.STEALTHbits.com

Name of Product StealthAUDIT

Version 8.0

Date 11/30/16

PARTNER SOLUTION OVERVIEW

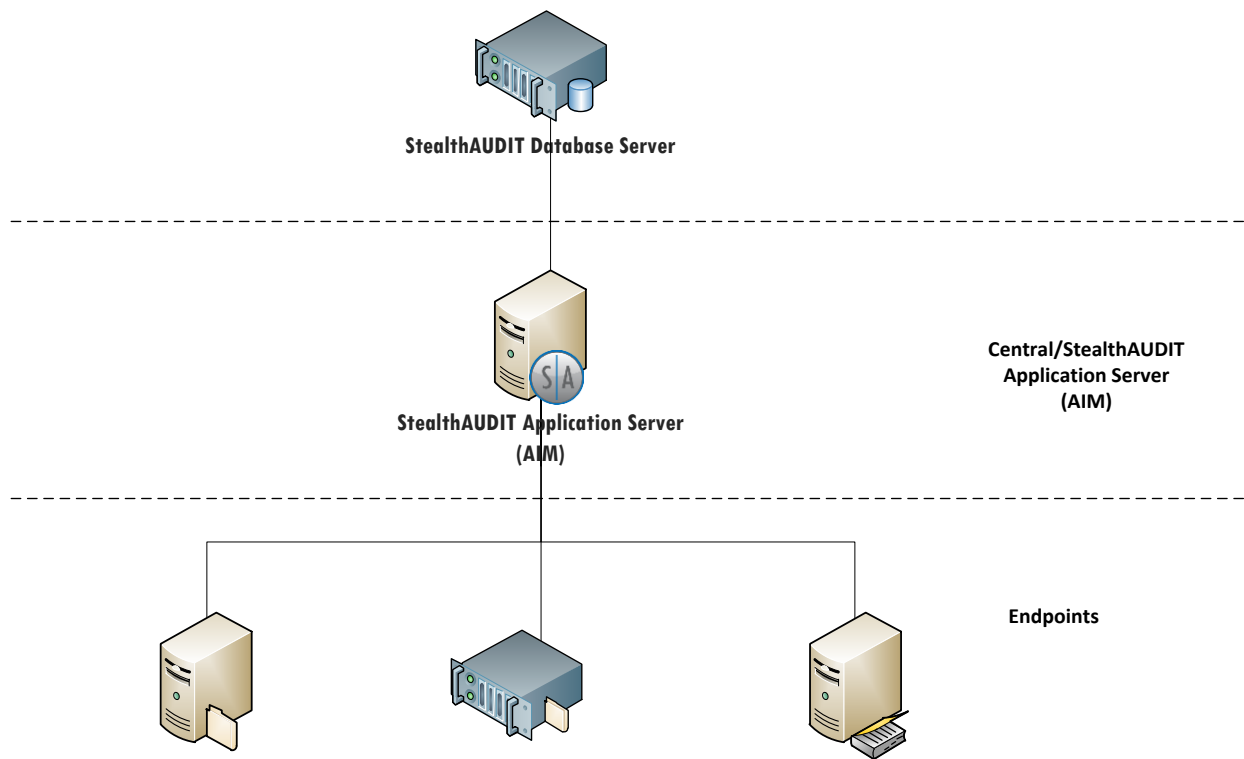
StealthAUDIT 8.0 is a Windows Server based application, capable of being installed on Windows 2008+. The StealthAUDIT Management Platform is the backbone of the STEALTHbits product line. It is composed of various built in modules with the capabilities of performing data collection, data analysis, reporting, and remediation in order to secure our customers' network infrastructure. The open architecture, and powerful collection capabilities gives our customers' the ability to have unprecedented control over their Microsoft connected infrastructure.

KEY BENEFITS

StealthAUDIT helps our customers to reduce risk, fulfill and enforce compliance requirements, and reduce operational costs associated with the management and security of their critical systems and applications. It does so by helping collect and analyze the data our customers need to answer the most difficult questions across their most important IT assets such as their File Systems, Active Directory, Exchange, cloud based technologies, and various other solutions. . Unlike other products on the market, StealthAUDIT is a true platform and not a point solution. Its flexibility and open architecture allow our customers to automate manual tasks, and allows us to establish interoperability between technologies and process, creating efficiencies to afford organizations the time to be visionary.

CyberArk Privileged Account Security Solution offers components designed to discover, secure, rotate, and control access to privileged account passwords used to access systems throughout the enterprise IT environment. This solution is being deployed at many of our customers, and will require their service accounts used to run StealthAUDIT to have passwords that are stored and managed through CyberArk Enterprise Password Vault. The objective of this integration is to allow StealthAUDIT end users the ability to leverage service accounts for StealthAUDIT jobs whose passwords are stored in the CyberArk Password Vault. By doing so, an extra layer of security will be provided over the service accounts used to collect our customer's most important data.

PRODUCT DIAGRAM & DESCRIPTION OF PRODUCT INTEGRATION



StealthAUDIT is a Windows Server based application, and is required to be installed on a dedicated console. There are specific configurations depending on the solution being used, but typically, customers use a single StealthAUDIT instance to scan their entire infrastructure. For the integration with CyberArk, the Application Identity Manager needs to be installed on the StealthAUDIT Application server.

StealthAUDIT requires elevated access for the collection of data from various endpoint systems, including File Systems (Windows, NAS, Unix\Linux), SharePoint, Exchange, Active Directory, and various other platforms including cloud services. The necessary level of access is required on each of the target endpoints. These elevated credentials are retrieved during various phases of the data collection process

- To identify target endpoints and retrieve/refresh relevant information necessary to connect and collect data from these hosts. This information is often retrieved once, and only refreshed as required by the customer. In some cases, the refreshing of host information could be as often as daily or weekly.
- To collect specific data from target endpoints. This is done on a scheduled basis, with the interval based on the solution being leveraged. Customers are encouraged to run daily collections against their Active Directory environment, which is the fundamental collection

required to correlate AD objects with metadata, activity information, and permissions from the target hosts. For our other solutions, such as Data Access and Governance, the collections may run once a week, or even once a month, depending on the size and use case for the customer.

- To collect data on a scheduled basis. When collections and reports are scheduled within StealthAUDIT, they leverage a specific set of Windows Credentials (domain or local). This credential must be configured within StealthAUDIT, and will be called each time a scheduled task is executed. This will typically occur multiple times a day.

The initial integration built between StealthAUDIT and CyberArk will include support for retrieving passwords for Windows Domain and Local accounts. The required fields to be able to retrieve the password are:

- Safe
- Folder
- Address
 - o This must translate to the domain name in the case of a domain account, or the server name in the case of a local account
- Username

AIM INSTALLATION

Refer to “Credential Provider and ASCP Implementation Guide” for CyberArk Credential Provider installation.

In order for StealthAUDIT to query CyberArk for service account passwords, the Application Identity Manager must be installed on the StealthAUDIT console. The following steps are necessary for the complete setup:

1. An application must be defined in the Vault corresponding to StealthAUDIT. The ApplicationID accepted by StealthAUDIT by default will be StealthAUDIT, but can be configured by end users if necessary within the console if necessary. The user created by the application created must be given the appropriate rights on each Safe which contains service account credentials that will be used within StealthAUDIT.
2. Prior to installation of the CyberArk AIM package, make sure that the appropriate network access exists between the SA console and both the Vault and Components consoles.
3. Install the proper version of the Credential Provider/AIM. For StealthAUDIT, this will be the Windows (AIM only) package. Do so by copying the Windows (AIM Only) folder to your StealthAUDIT console and run the Setup file
4. During installation, you will be prompted for the following information
 - a. Server Address and Port for the CyberArk Vault server:
 - b. Vault Administrator Credentials.
5. Once the installation has completed, you will find the necessary binaries, the Credential Manager service, and the necessary application password SDKs which will be leveraged by StealthAUDIT to query the Vault. Additionally, a user will be created in the vault correlating back to the machine on which AIM was

installed. This user must be added as a member to each safe that contains service account credentials that will be used within StealthAUDIT. Give this user the following rights on each Safe:

- a. Retrieve Accounts
 - b. List Accounts
 - c. View Member Safe
6. Once the necessary access has been provisioned within CyberArk, the service account credentials can be configured for use within StealthAUDIT

AIM CONFIGURATION

DEFINING THE APPLICATION ID (APPID) AND AUTHENTICATION DETAILS

To define the Application, here are the instructions to define it manually via CyberArk's PVWA (Password Vault Web Access) Interface:

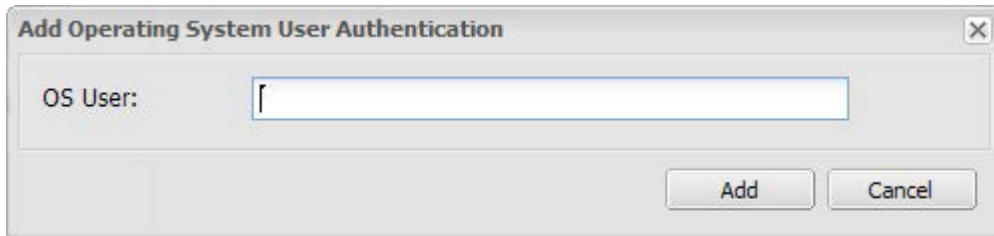
1. Logged in as user allowed to managed applications (it requires Manage Users authorization), in the Applications tab, click **Add Application**; the Add Application page appears.

>>Replace this screenshot with data filled in (i.e. with the pre-defined APPID the customer should use, specified in the "Name" field)

The screenshot shows the 'Add Application' dialog box. The 'Name' field contains 'StealthAUDIT'. The 'Description' field is empty. The 'Business owner' section has fields for 'First Name', 'Last Name', 'Email', and 'Phone', all of which are empty. The 'Location' field is a dropdown menu showing a backslash character. Below this are checkboxes for 'Access Permitted', 'Expiration Date', and 'Disabled', each followed by a date selection field. The 'Access Permitted' checkbox is checked. The 'Add' and 'Cancel' buttons are at the bottom right.

2. Specify the following information:
 - In the Name edit box, specify **StealthAUDIT**
 - In the Description, 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 lowest section, 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.
3. Click **Add**; the application is added and is displayed in the Application Details page.

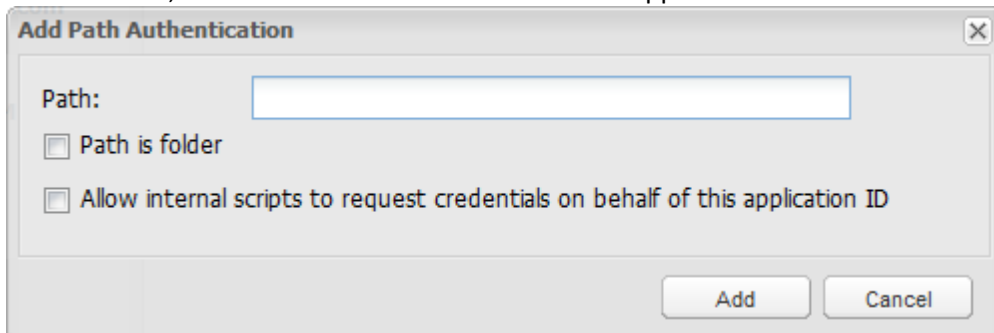
- **Allowing extended authentication restrictions.** This enables you to specify an unlimited number of machines and Windows domain OS users for a single application. Please check this box.
4. Specify the application's **Authentication** details. This information enables the Credential Provider to check certain application characteristics before retrieving the application password. Customers can further lock down StealthAUDIT access to the vault by specifying a particular OS User, Path, or Allowed Machine.
 - In the Authentication tab, click **Add**; a drop-down list of authentication characteristics is displayed.
 - Select the authentication characteristic to specify.
 5. Specify the OS user:
 - a. Select **OS user**; the Add Operating System User Authentication window appears.



b. Specify the name of the OS user who will run stealthAUDIT, then click **Add**; the OS user is listed in the Authentication tab.

6. Specify the application path:

a. Select **Path**; the Add Path Authentication window appears.



b. Specify the StealthAUDIT path:

C:\Program Files (X86)\STEALTHbits\StealthAUDIT\StealthAUDIT.exe.

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

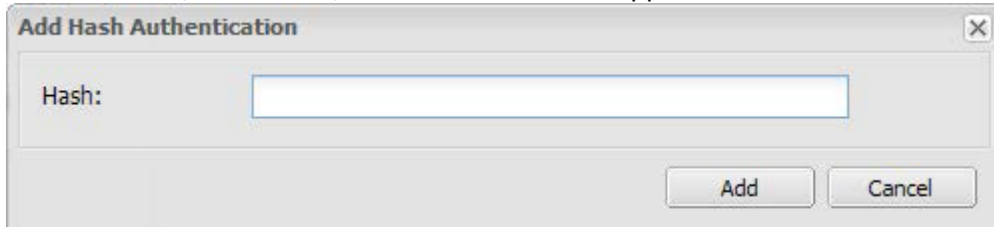
7. Specify a hash:

a. Run the AIMGetAppInfo utility to calculate the application's unique hash on StealthAUDIT:

C:\Program Files (X86)\STEALTHbits\StealthAUDIT\StealthAUDIT.exe.

b. Copy the hash value that is returned by the utility.

c. In the PVWA, select **Hash**; the Add Hash window appears.



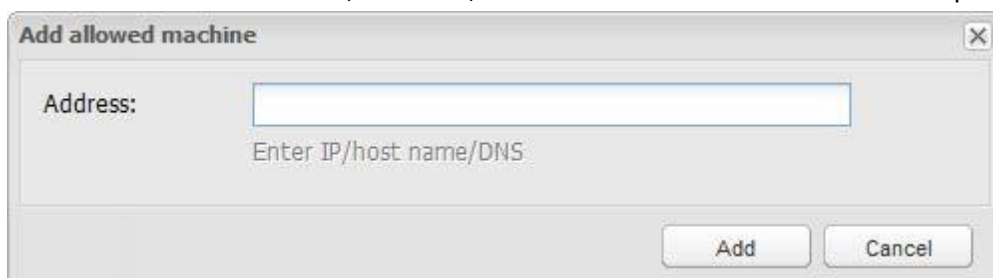
d. In the Hash edit box, paste the application's unique hash value, or specify multiple hash values with a semi-colon. You can add additional information in a comment after each hash value specified for an application by specifying '#' after the hash value, followed by the comment.

For example, OE883B70D5B6E3EE37D37198049C9507C8383DB6 #app2

Note: The comment must not include a colon or a semicolon.

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

8. 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.



- 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 AIM 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 (Step 1). 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 (Step 2).

1. In the Password Safe, provision the privileged accounts that will be required by the applications. You can either 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 Account Security Implementation Guide**.

2. 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.
 - i. 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

- ii. 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 1 result(s)

Name	Business Email	Full Name
StealthAUDIT		

☐ Access
☐ Use accounts
☒ Retrieve accounts
☐ List accounts
☐ Account Management
☐ Safe Management
☐ Monitor
☐ View Audit log

StealthAUDIT has been added.

-
- iii. If your environment is configured for dual control:
 - In PIM-PSM environments (v7.2 and lower), if the Safe is configured to require confirmation from authorized users before passwords can be retrieved, give the Provider user and the application the following permission:
 - Access Safe without Confirmation
 - In Privileged Account Security solutions (v8.0 and higher), when working with dual control, the Provider user can always access without confirmation, thus, it is not necessary to set this permission.
- iv. 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.

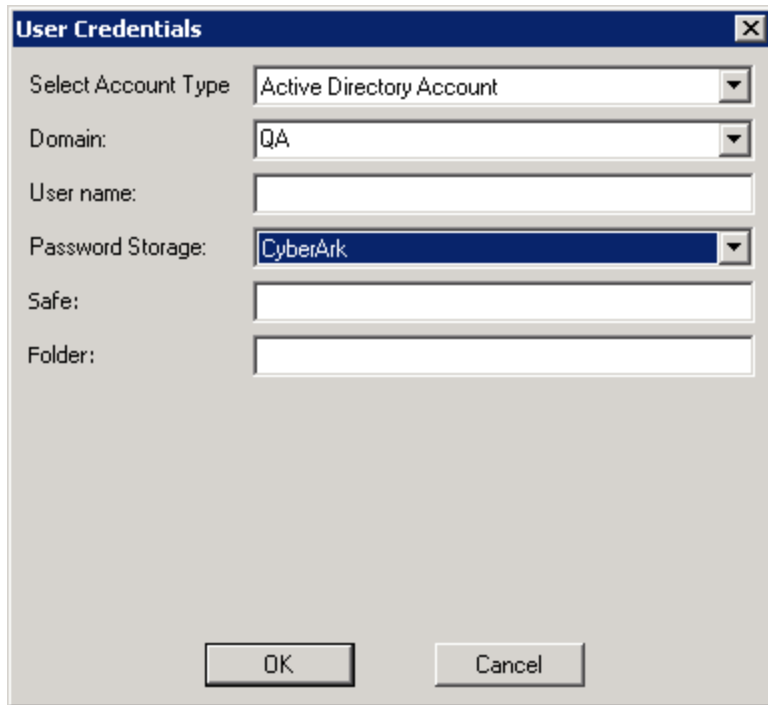
For more information about configuring Safe Members, refer to the **Privileged Account Security Implementation Guide**.

STEALTHAUDIT INSTALLATION & CONFIGURATION

Refer to STEALTHbits_SMP_InstallationGuide.pdf for Partner Product installation.

Once AIM has been installed on the CyberArk console, the necessary service accounts can be configured for use within StealthAUDIT by following the steps below:

1. After starting StealthAUDIT, you can configure credentials on the following Settings nodes:
 - a. Connection Profile:
 - i. Click Add Connection Profile
 - ii. Once a new profile has been added, click Add User Credential
 - iii. The CyberArk Password Storage option will only be available for the following Account Types:
 1. Active Directory
 2. Local Windows Account
 - iv. Select one of these account types along with the CyberArk Password Storage option
 1. If Active Directory is shown, fill in the appropriate Domain and User Name. The address field configured for this account in CyberArk should match the Domain value filled in here. This must be an actual domain, as opposed to the fqdn of the domain controller
 2. If Local Windows Account is chosen, the domain field will be autopopulated with a value that will be filled in dynamically at the time of data collection or job execution. The address field configured for this account in CyberArk should match the Name field in Host Management of the host being targeted.
 - v. Specify the Safe and Folder in which the credential is stored in CyberArk
 - b. Schedule
 - i. Click Add User Credential. If a user credential already exists, click Edit
 - ii. Choose whether you will be using a 'Local Account for this system' or 'Account for the following domain'
 1. If the first option is chosen, enter the username, and corresponding safe and folder. The domain field will be autopopulated with a value that will be filled in dynamically at the time of task creation or execution.
 2. If the second option is chosen, fill in the appropriate domain and user name. The address field configured for this account in CyberArk should match the domain value filled in here. This must be an actual domain, as opposed to the fqdn of the domain controller.
2. Once configured, the credentials can now be used within StealthAUDIT, and the password will be retrieved from CyberArk when needed:



The image shows a Windows-style dialog box titled "User Credentials" with a close button (X) in the top right corner. The dialog contains several input fields and dropdown menus. The "Select Account Type" dropdown is set to "Active Directory Account". The "Domain:" dropdown is set to "QA". The "User name:" field is empty. The "Password Storage:" dropdown is set to "CyberArk". The "Safe:" field is empty. The "Folder:" field is empty. At the bottom of the dialog are two buttons: "OK" and "Cancel".

Select Account Type	Active Directory Account
Domain:	QA
User name:	
Password Storage:	CyberArk
Safe:	
Folder:	

OK Cancel

Common use cases:

1. Active Directory Account
 - a. The user will specify: Domain (Address), Username, address, Safe, and Folder
2. Local Windows Account
 - a. The user will specify: Username, Safe, and Folder

PARTNER CONTACT INFO

Business Contact	Name	Bob Stanton
	Email	Bob.Stanton@STEALTHbits.com
	Tel	(201) 447-9304
Technical Contact	Name	Farrah Vijayan
	Email	Farrah.Vijayan@STEALTHbits.com
	Tel	201.301.1825
Support Contact	Name	John Albanese
	Email	John.Albanese@STEALTHbits.com
	Tel	201-857-5311