



APPLICATION ACCESS MANAGER

(Agent Based Credential Provider CP)

AAM INTEGRATION - TECHNICAL DOCUMENTATION

Name of Company: NetSol Technologies Europe Ltd.

Website: netsoltech.com

Name of Product: LeaseSoft

Version: 1.0 (Issued)

Date: 23 March 2021

PARTNER SOLUTION OVERVIEW

LeaseSoft is a Loan and Leasing Administration System.

It is used by Independent Finance Companies and Asset Finance subsidiaries of larger Banks to administer portfolios of Instalment Credit contracts.

It administers the full Contract lifecycle from origination, in-life management, to end-of-term processing.

It integrates with various 3rd party systems, such as:

- Proposal origination/import
- Websites / online Portal
- Credit Reference Agencies
- Banking, for Payout and Direct Debit Collections
- Document generation systems
- Accounting Packages

Version: TBD

Platform components:

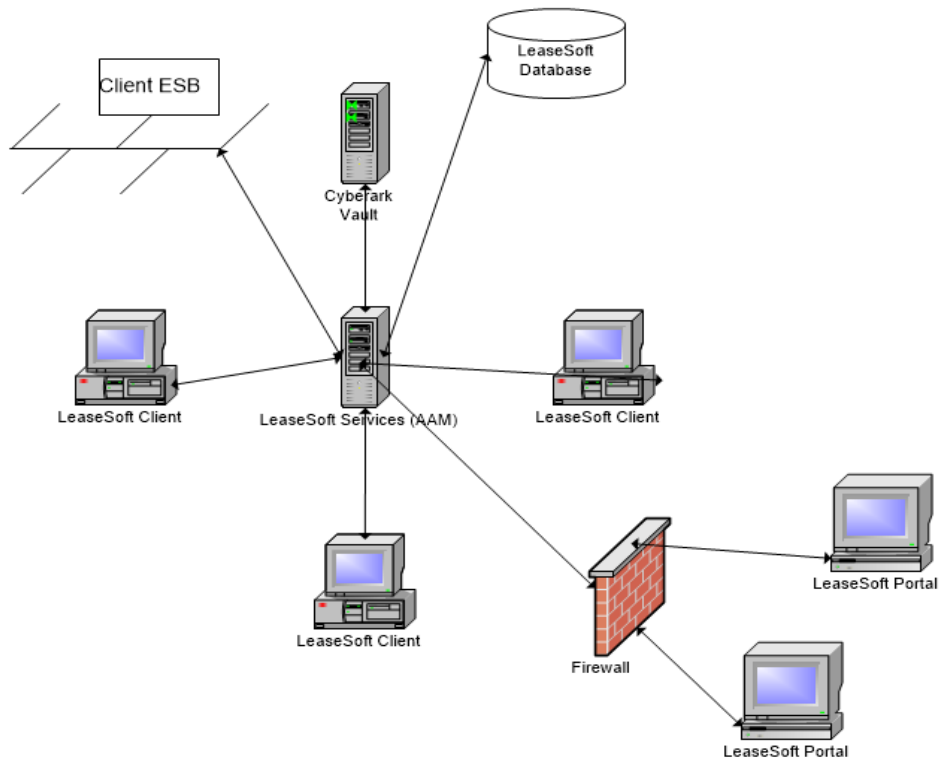
- LeaseSoft Client
- LeaseSoft Portal
- LeaseSoft Services

KEY BENEFITS

LeaseSoft provides a full lifecycle management of Instalment Credit Contract portfolios with process automation. The benefits of LeaseSoft also include a proven track record and domain expertise along with ensured service levels.

Integrating LeaseSoft with CyberArk AAM provides enhanced Security and Secret Management by eliminating hard coded credentials with the ability to centrally manage credentials for human and non-human identities. Operations become more efficient as the management and rotation of credentials can be automated. Development is simplified for applications that need to securely access sensitive resources. Compliance and Audit benefits include the enforcing of internal and regulatory requirements around the management and monitoring of application credentials with detailed audit trails.

PRODUCT DIAGRAM & DESCRIPTION OF PRODUCT INTEGRATION



AAM INTEGRATION

AAM has been integrated into the LeaseSoft Services layer and this sits on a Central Server. A typical installation would consist of 1 mid-tier server with several endpoints on a local network with external users connecting from a portal via the Internet. The number of endpoints would depend on the client and how many instances of LeaseSoft are used.

LeaseSoft uses the AAM to store and provide connection details and passwords for other required services such as Database connections, Enterprise Service Bus along with any other details that are deemed sensitive.

CREDENTIAL RETRIEVAL

On startup of LeaseSoft Services, credential retrieval from the Cyberark Vault is triggered. These credentials are then used to connect to external services such as the LeaseSoft Database and the Client Enterprise Service Bus as required to process Client requests or automated/scheduled tasks.

LeaseSoft Services runs on the Windows platform and the following properties are required to access a credential from the Vault - Application ID, Safe and Object name.

REQUIREMENTS

Client has an existing 'On-Prem' Vault and all software, network, and hardware requirements have been satisfied. The client also has in-house technical expertise.

AAM INSTALLATION

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

AAM CONFIGURATION

The following sections provide details on LeaseSoft 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: NetSolTech-LeaseSoft

Description: Loan and Leasing Administration System, including Premium Finance Contracts.

Business owner

First Name:

Last Name:

Email:

Phone:

Location: \

☒ Access Permitted: From: To:

☐ Expiration Date:

☐ Disabled

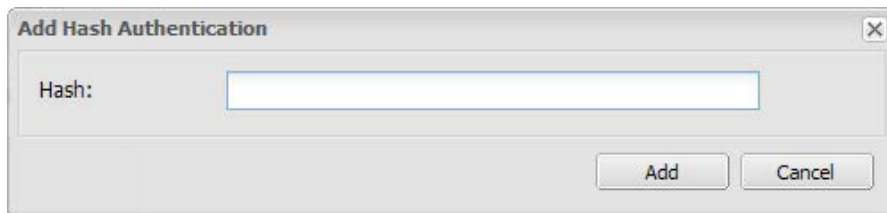
Add Cancel

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

Client to fill this in

The screenshot shows the CyberArk Application Details page. The top navigation bar includes the CyberArk logo, the user's last sign-in time (7/11/2019), and the user's role (Administrator). The page title is 'Application Details: PartnerName-ApplicationName'. The left sidebar contains navigation icons. The main content area has two tabs: 'Authentication' and 'Allowed Machines'. The 'Authentication' tab is active, showing an 'Add' button and a list of authentication methods: OS user, Path, Hash, and Certificate Serial Number. The 'Allowed Machines' tab is also visible. The page footer indicates 'No authentications to display' and 'Page 1 of 1'.

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



The image shows a dialog box titled "Add Hash Authentication". It has a close button (X) in the top right corner. Inside the dialog, there is a label "Hash:" followed by a text input field. At the bottom right of the dialog, 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.

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

Display 5 result(s)

	Name	Business Email	Full Name
	Prov		
	Prov		
	Prov		
	Prov		
	Prov		

☐ Access

☐ Use accounts
 ☒ Retrieve accounts
 ☒ List accounts

☐ Account Management

☐ Safe Management

☐ Monitor

☐ View Audit log
 ☒ View Safe Members

☐ Workflow

Add

Close

- ☐ Add the application (the APPID - **NetSolTech-LeaseSoft**) as a Safe Member with the following authorizations:
- Retrieve accounts

Add Safe Member

Search:
Search In:

Selected Search: Vault
Display 4 result(s)

	Name	Business Email	Full Name
	NetSolTech-LeaseSoft		

☐ Access

☐ Use accounts
☒ Retrieve accounts
☐ List accounts

☐ Account Management
☐ Safe Management
☐ Monitor

☐ View Audit log
☐ View Safe Members

☐ Workflow

- ☐ 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**.

Client will be provided with Partner Product installation services.

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

1. Client to add section in appSettings.json file as demonstrated below

```
"CyberarkConfiguration": {  
  "Name": "NetSol Cyberark Config",  
  "Application": {  
    "AppID": " NetSolTech-LeaseSoft ",  
    "Safe": [  
      {  
        "Name": "test",  
        "CyberarkObjects": [  
          {  
            "Name": "testobject",  
            "Replaces": "ConnectionStrings:LeaseSoftDb",  
            "Value": ""  
          }  
        ]  
      }  
    ]  
  }  
},
```

Section above will use the following to request a value from the Vault.

ApplicationID : **NetSolTech-LeaseSoft**

Safe: test

Object Name: testobject

The value retrieved from the safe will be used in the LeaseSoft application and overwrite or add the Value to the application configuration using the key provided in the Replaces part of the CyberarkObjects.

PARTNER CONTACT INFO

Business Contact	Name	Phillip Ring
	Email	phillip.ring@netsoltech.com
	Tel	+44 (0) 1403 282 300
Technical Contact	Name	David Salako
	Email	David.salako@netsoltech.com
	Tel	+44 (0) 1403 282 300
Support Contact	Name	NetSol Support
	Email	ipfsupport@netsoltech.com
	Tel	+44 (0) 1403 282 300