

Account Lifecycle Manager

Administrator Guide

Version: 2023.x

Publication Date: 3/14/2024

Account Lifecycle Manager Administrator Guide

Version: 2023.x, Publication Date: 3/14/2024

© Delinea, 2024

Warranty Disclaimer

DELINEA AND ITS AFFILIATES, AND/OR ITS AND THEIR RESPECTIVE SUPPLIERS, MAKE NO REPRESENTATIONS ABOUT THE SUITABILITY OF THE INFORMATION CONTAINED IN THE DOCUMENTS AND RELATED GRAPHICS, THE SOFTWARE AND SERVICES, AND OTHER MATERIAL PUBLISHED ON OR ACCESSIBLE THROUGH THIS SITE FOR ANY PURPOSE. ALL SUCH MATERIAL IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND. DELINEA AND ITS AFFILIATES, AND/OR ITS AND THEIR RESPECTIVE SUPPLIERS, HEREBY DISCLAIM ALL WARRANTIES AND CONDITIONS WITH REGARD TO SUCH MATERIAL, INCLUDING ALL IMPLIED WARRANTIES AND CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT.

THE MATERIAL PUBLISHED ON THIS SITE COULD INCLUDE TECHNICAL INACCURACIES OR TYPOGRAPHICAL ERRORS. CHANGES ARE PERIODICALLY ADDED TO THE INFORMATION HEREIN. DELINEA AND ITS AFFILIATES, AND/OR ITS AND THEIR RESPECTIVE SUPPLIERS, MAY MAKE IMPROVEMENTS AND/OR CHANGES IN THE MATERIAL DESCRIBED HEREIN AT ANY TIME.

Disclaimer of Liability

IN NO EVENT SHALL DELINEA AND ITS AFFILIATES, AND/OR ITS AND THEIR RESPECTIVE SUPPLIERS, BE LIABLE FOR ANY SPECIAL, INDIRECT, OR CONSEQUENTIAL DAMAGES (INCLUDING LOSS OF USE, DATA, PROFITS OR OTHER ECONOMIC ADVANTAGE) OR ANY DAMAGES WHATSOEVER, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE, OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF SOFTWARE, DOCUMENTS, PROVISION OF OR FAILURE TO PROVIDE SERVICES, OR MATERIAL AVAILABLE FROM THIS SITE.

Table of Contents

Administrator Guide	i
Introduction to Account Lifecycle Manager	1
Key Features	1
Role-Based Access Controls	1
Workflow Templates	1
Service Account Discovery	1
Example Workflow	1
ALM Initial Setup Task List	2
Step 1 - Verify System Requirements	2
Thycotic One accounts	2
Browser Compatibility	2
Vault Types	3
Domain Types	3
ALM Engine Windows Service	3
Step 2 - Setup the ALM Engine Service	3
ALM Engine Service Requirements	3
Required Ports	4
ALM Engine Installation	4
ALM Engine Logon Account Configuration in AD	5
Additional ALM Engine Logon Account Information	6
ALM Engine Logs	6
View Full Versions of ALM Engine Logs	6
LDAPS	7
ALM Engine: Troubleshooting	7
See Also	7
Step 3 - Create a Domain	7
View Existing Domains	8
Integrate ALM with Active Directory	9
Domain Synchronization	9
Sync Users	10
Active Directory Account Discovery Tool	10
Integrate ALM with Amazon Web Services (AWS)	11
Setting Permissions for AWS	11
Integrate ALM with Azure Active Directory	13
Optional: Use these steps to enable Sync:	18
Integrate Google Cloud Platform	18
Integrate Group Managed Service Accounts	20
Overview	20
Requirements:	21
Parameters:	21
Step 4 - Create a Vault	21

Table of Contents

Integrate with AWS Secrets Manager	22
Integrate with HashiCorp Vault	22
Integrate ALM with Secret Server	22
Integrate ALM with DevOps Secrets Vault	24
Integrate with Azure Key Vault	25
Integrate with HashiCorp Vault	25
Integrate with AWS Secrets Manager	26
Self-Hosted ALM Installation Steps	26
Prerequisites	26
Additional Requirements	27
Docker Configuration	27
Supported Authentication Methods	27
Azure AD Open ID Connect	28
Configure Auth0 Open ID Connect (OIDC)	36
Thycotic One Open ID Connect (OIDC) Configuration	39
Installation	42
Change to that directory.	42
Download and Install the Script:	42
Domain name	42
SSL/TLS Configuration	43
Database Configuration	43
Admin User	43
Authentication Configuration	43
Email Configuration	44
Finishing Setup and Adding Licenses	44
Navigate to Licensing page	44
Understanding ALM Objects	44
Users	44
Roles	45
Account Owner	45
Requestor	45
Approver	45
System Administrator	45
Custom Roles	45
Groups	46
Workflow Templates	46
Custom Roles	46
Permissions	46
Features to Which Permissions Apply	47
Example Custom Roles Setup	48
Events, Notifications, and Recipients	53
At End of Lifecycle (AEOL) Actions	55
Review	55
Disable	56

Table of Contents

Expire	56
Delete	57
ALM End-of-Lifecycle Account Disposition Logic for Option Availability, Account Status, and User Review	
Actions	57
Account Status when EOL Reached Systematically	58
User Actions on Review EOL	59
User Actions on Disable EOL	60
User Actions on Delete EOL	61
User Actions on Expire EOL	62
AD Account Expiration Dates	62
Computing's Midnight Conundrum	63
ALM Storage of Dates	64
Using ALM	64
Navigating ALM	65
Customizing the UI	66
Accounts Home	67
Viewing and Cloning Accounts	67
Viewing the Account Summary	68
Viewing Account Details	68
Cloning a New Account	69
Discovering Accounts	69
Account Migration	71
Bulk Renew	74
Viewing and Creating New Requests	76
Review New Requests	76
Creating New Requests	77
Viewing Request Details	79
Approving Requests	79
Alerts	80
Workflows	81
Overview	81
Workflow Template Fields	82
Building Workflow Templates	82
Create a Workflow	83
Managing Workflow Templates	86
Workflow Template Versioning	87
Managing Integrations	88
Managing Domains	89
Viewing Domains	89
Creating a Domain	90
Viewing Domain Details	90

Table of Contents

Editing Domains	90
Deleting Domains	91
Managing Engines	91
Viewing Engines	91
Downloading an Engine	92
Reviewing Activation Tokens	92
Viewing, Enabling/Disabling and Reassigning Engines	93
Managing Engine Pools	94
Viewing Engine Pools	94
Creating an Engine Pool	94
Viewing and Editing Engine Pool Details	95
Managing Vaults	95
Viewing Vaults	95
Creating a Vault	96
Viewing and Editing Vault Details	96
Working with Personnel	96
Users	96
Thycotic One accounts	96
Creating ALM Users	96
Managing Users	98
Change Display Name	98
Enable/Disable User	99
Add User email	99
Add/Remove User Groups	99
Add/Remove User Roles	99
Link an Active Directory Account	100
Groups	100
Creating Groups	101
Managing Groups	101
Enable/Disable Group	102
Add/Remove Users	103
Add/Remove Roles	104
Create and Manage Roles	105
Default Roles Provided by ALM	106
Create Custom Roles	106
Manage Roles	107
Edit Role Permissions	108
Enable/Disable Role	108
Edit Users	108
Edit Groups	108
Audits	108
User Logs	108
ALM Engine Logs	109

Table of Contents

Configuration	109
Integrate with Other Applications	110
SIEM Integration	110
Creating a SIEM Integration	111
Deleting a SIEM Integration	112
ServiceNow Integration	113
Alert Settings	113
Alerts for Email Templates	114
Alerts for Webhooks	115
Creating a Webhook	115
Alerts for Webhook Authorization	116
ALM Administration	117
Calibrating the ALM Engine	118
Service Account Discovery Tool	118
Prerequisites	118
Ports	121
Walkthrough	121
Domain Credentials	121
Scan Settings	123
Discovering Accounts	123
Results	124
FAQ	125
Reports	125
Release Notes	126
Account Lifecycle Manager: Change Log	126
References	137
SLAs and Related Operational Considerations	137
Business Continuity	137
Disaster Recovery	138
Confidentiality	138
Data-at-rest	138
Data-in-Transit	138
Client Authentication	138
Integrity: Code Signing	138
General Data Protection Rule (GDPR)	138
SOC II	139
New This Month: November	139
New Account Notifications	139
ALM Engine Calibration	139
Tabbed Interface for Vault Detail Pages	139
Beta Feature Release: ALM Engine Configuration Website Tool	139

Introduction to Account Lifecycle Manager

Account Lifecycle Manager (ALM) controls the creation, management, and decommissioning of Active Directory Service Accounts running on your organization's network. ALM reduces Service Account sprawl and increases security by enforcing governance and creating accountability using role-based permissions. Depending on a user's role, they can request, approve, provision, manage, and retire service accounts.

Key Features

Role-Based Access Controls

ALM manages Service Accounts by assigning each account to a User within your organization. ALM uses four **Roles** to define User permissions and determine accountability. A User's Role determines how they interact with ALM and Service Accounts.

- **Account Owner**- All ALM Users are given the Account Owner Role. Account Owners can read and update managed accounts assigned to them.
- **System Administrator**- A System Administrator has full access to ALM's configuration and management. They can create and manage Users, Roles, Groups, and Workflows.
- **Requestor**- Requestors can request the provisioning of new service accounts.
- **Approver**- Approvers review requests for new service accounts and approve or deny their provisioning.



Note: ALM roles are distinct from Active Directory Roles. They do not overlap.

Workflow Templates

The **System Administrator** can create templates that guide how Service Accounts in your organization are approved and monitored. Templates determine the approval process, review intervals, notification options, and end-of-lifecycle action for Service Accounts.

Service Account Discovery

ALM protects your network by controlling newly created privileged accounts. However, you may already have unmanaged Service Accounts running on your network. Using **Service Account Discovery**, you can scan your network to identify Service Accounts that are active and unmanaged. Using ALM, you can then assign these accounts to Users within your organization or remove the accounts entirely.

Example Workflow

1. The **System Administrator** installs ALM on your network according to your organization's policies.
 - They create users and assign them Roles.
 - They create a **workflow template** that determines the provisioning process.
2. A User with the **Requester** Role logs into ALM and asks that a Service Account be created.
3. ALM notifies a User with the **Approver** Role that a request has been made.

ALM Initial Setup Task List

4. The **Approver** logs into ALM and approves or denies the request.
 - If the request is denied, the **Approver** provides a reason for the denial. ALM notifies the **Requester** of the denial and the reason.
 - If the request is approved, ALM creates a proxy for the requested Service Account within Active Directory. The ALM proxy and the Active Directory account will share the same name. ALM will then notify the **Requester** that the account has been approved and provisioned.
5. Once a service account has been provisioned, ALM monitors the account throughout its lifecycle.
 - The **workflow template** determines the renewal and retirement timeline for the account.
 - ALM will send notifications for upcoming lifecycle events to the selected Users.
 - ALM logs each step for easy auditing.

ALM Initial Setup Task List

Getting started with ALM requires these tasks:

- **Step 1** Make sure your network meets the [System Requirements](#).
- **Step 2** [Set up an ALM Engine](#).
- **Step 3** [Create a Domain](#) and Integrate with Active Directory and/or Azure Active Directory or a supported directory service, and assign the Domain to a Pool.
- **Step 4** [Create a Vault that](#) integrates with Other Applications such as Secret Server and/or DevOps Secrets Vault.
- **Step 5** Integrate with Other Applications, for example, [ServiceNow](#) and [SIEM](#).

Step 1 - Verify System Requirements

Successful use of ALM requires that your organization's IT infrastructure meet several criteria.

Thycotic One accounts

Each member of your organization who will use ALM must have a **Thycotic One** account. These free accounts provide authentication to Delinea's cloud services, including ALM.

To open a Thycotic One account, visit [Thycotic One](#).

The email a User submits when signing up for Thycotic One will be the email they must provide later when obtaining an ALM User account.

Browser Compatibility

- Google Chrome
- Mozilla Firefox

Vault Types

- Delinea Secret Server ALM uses Secret Server to store credentials for the accounts it creates in Active Directory. This removes security risks long associated with storage of the temporary credentials for new AD accounts.

If you are not using Secret Server Cloud, your Secret Server version must be Version 10.2.000018 or later with the Secret Server Platinum or Pro license. Secret Server's web services must be running.

Instructions related to Secret Server requirements appear in [Integrate ALM with Secret Server](#).

- Delinea DevOps Secrets Vault
- Azure Key Vault
- AWS Secrets Manager
- HashiCorp Vault

Domain Types

The following domain types are supported:

- An Active Directory Domain Controller on Windows Server 2012 or later
- Azure AD Domain Services
- Amazon Web Services Identity and Access Management
- Google Cloud Platform Identity and Access Management.

Note: A User account privileged to create Active Directory accounts can authenticate into AD to create other AD accounts.

For details on integration with Active Directory, see [Integrate ALM with Active Directory](#).

ALM Engine Windows Service

The ALM Engine is a Windows Service that runs on a machine in your organization's environment.

The ALM Engine Windows Service runs on your organization's hardware. It manages interactions between the ALM cloud service and your Active Directory installation. It also supports ALM's integration with your organization's Secret Server instance.

See [Setup the ALM Engine Service](#) for details.

Step 2 - Setup the ALM Engine Service

The ALM Engine is a Windows Service that runs on your organization's hardware. It manages interactions between the ALM cloud service and your Active Directory installation. It also supports ALM's integration with your organization's Secret Server instance.

ALM Engine Service Requirements

The ALM Engine Windows service must:

ALM Initial Setup Task List

- be able to reach your domain controller over LDAPS
- run on a domain controller or domain-joined machine, with
 - Windows Server 2012 or later, and
 - Microsoft .NET 4.7.1 or later installed
- run as a non-domain joined computers automatically using Network Service as the service account, *OR* as an AD account with AD permissions to:
 - create, delete, and manage User accounts
 - reset User passwords and force next-logon password changes
 - read all User information
 - modify the membership of a Group

Required Ports

The ALM Engine will communicate to *.accountlifecyclecloud.com over port 443



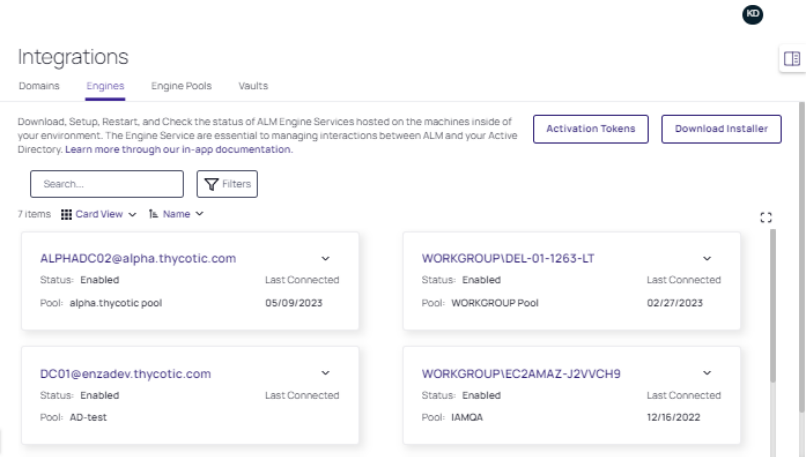
Note: ALM Engine will communicate through port 5671 to the below Urls for each region

Region	URL	Port
US East	thycotic-enza-prod-eastus-sb01.servicebus.windows.net	5671
AU Cen	thycotic-enza-prod-auscen-sb01.servicebus.windows.net	5671
CAN Cen	thycotic-enza-prod-cac-sb01.servicebus.windows.net	5671
EU West	thycotic-enza-prod-westeuro-sb01.servicebus.windows.net	5671

ALM Engine Installation

To install a new ALM Engine, select **Integrations** in the left navigation panel. On the **Engines** tab, click **Download Installer** to obtain the installer files.

ALM Initial Setup Task List



Copy the installer to the computer that will host the ALM Engine. Unzip the file and run:

`install.cmd`

Follow the prompts until the installation finishes.



Note: The activation token for the ALM Engine will last **8 hours**. If the engine needs to be reinstalled, a new token will need to be obtained.

ALM Engine Logon Account Configuration in AD

Change the logon account for the Delinea ALM Engine to an AD account with the following AD permissions.

Table:*ALM Engine AD Service Account Permissions*

AD Object	Permissions for ALM Engine
Organizational Unit	list contents
	read all properties
	create User objects
	delete User objects
User	list contents
	read all properties
	change password
	reset password
	write all properties

ALM Initial Setup Task List

AD Object	Permissions for ALM Engine
Groups	list contents
	read all properties
	write member

To change the logon account:

1. Run **services.msc** to open the **Services Control Manager**.
2. Find **Thycotic ALM Engine**, right-click, and select **Properties**.
3. In the Properties panel, select **Log On**.
4. Select **This account**:
5. Supply the AD account name for the ALM Engine service and the account credentials. Click **OK**.
6. Restart the ALM Engine service by right clicking **Thycotic ALM Engine** and selecting **Restart**.
7. Back in ALM, the new ALM Engine will appear in the **Unassigned ALM Engines** section.
8. Click the ALM Engine, assign it to a pool, and click **Activate**.

Additional ALM Engine Logon Account Information

The ALM Engine's AD Service Account requires several machine-specific permissions. The installer sets these permissions, so you will not need to perform these steps as part of your initial ALM setup. However, take note that if the service account changes, you may need to reapply these permissions:

- Local Security or Domain Policy: "Log on as a service"
- Registry: Full Control on Computer\HKLM\SOFTWARE\Thycotic Software Ltd
- File System: C:\ProgramData\Thycotic Software Ltd

ALM Engine Logs

Admins can view ALM Engine error messages and sync information in the **ALM Engine Log**, available in ALM under **Audit > ALM Engine Logs**. This is an abbreviated log; the ALM Engine does not send all log messages back to ALM.

View Full Versions of ALM Engine Logs

Use these steps to view the full logs on the machine hosting the ALM Engine service:

1. Log into the machine where the ALM Engine is located.
2. From root, navigate to: ProgramData > Thycotic Software Ltd > ALMEngine > packages > Thycotic Provision
3. Locate the appsettings.json file.
4. Open appsettings.json with Notepad or other suitable text editor.

ALM Initial Setup Task List

5. Under the **Serilog** section, you will see **MinimumLevel**, and below that, **Default : Information**
6. Change that to **Default : Verbose**
7. Save the file.
8. Open **Services**
9. Restart the ALM Engine service.

LDAPS

ALM requires LDAPS for AD integration, with reliance on port 636; the port number is not configurable.

ALM Engine: Troubleshooting

If the ALM Engine does not run properly, review its operation logs for clues. If you cannot resolve the problem, [contact Delinea for support](#).

See Also

See Also the *ALM Engine Calibration Tool* section of the [ALM Administration](#) article.

Step 3 - Create a Domain

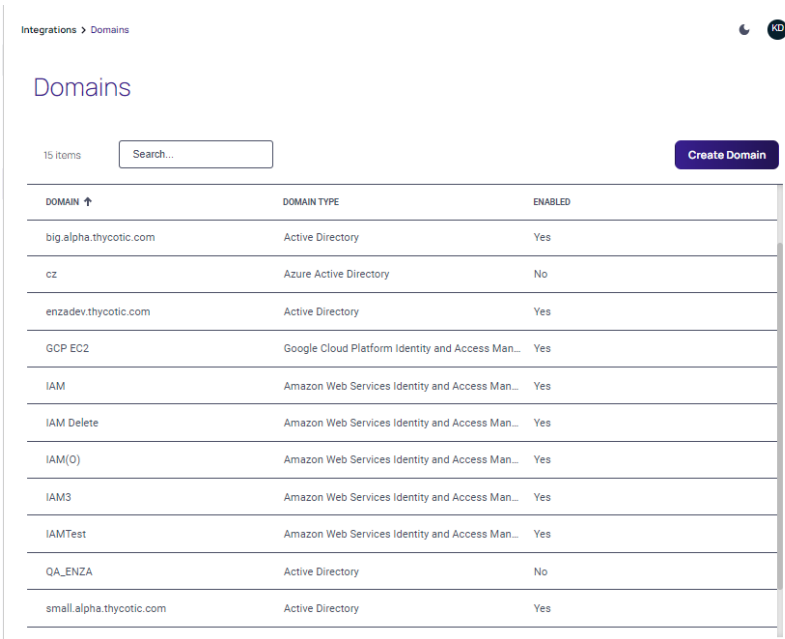
ALM uses domain integration to automatically provision accounts for use.

Click **Integrations** in the left navigation panel and select the **Domains** tab to view the domains currently integrated into ALM.

Supported domains include;

- [Active Directory](#)
- [Azure Active Directory](#)
- [Amazon Web Services](#)
- [Google Cloud Platform](#)

ALM Initial Setup Task List



Click **Create Domain**.

View Existing Domains

Click any domain to view the identifiers that characterize the domain. Use **Search** to quickly identify a domain for display.

The **DOMAIN TYPE** is displayed, along with whether the domain is enabled or disabled. Supported domain types include: Active Directory, Azure Active Directory, Google Cloud Platform Identity and Access Management, and Amazon Web Services Identity and Access Management.

Other features for a domain include: **Delete** in the top right of the page to delete the domain and **Sync** to sync the domain manually. To set up or edit a scheduled sync, click **Edit** under **Sync Schedule**.

Identifiers vary depending on the domain type and include:

Attribute	Definition	Features
General	domain details and sync features	Edit is available for both the Domain details and the Sync Schedule.
Users	users granted access to the domain	Search by DISPLAY NAME is available. Filters are available for enabled and disabled users.
Groups	groups granted access to the domain	Search by group NAME is available. Filters are available for enabled and disabled groups.
Roles	roles defined for use in the domain	Search by group DISPLAY NAME is available. Filters are available for enabled and disabled roles.

ALM Initial Setup Task List

Attribute	Definition	Features
Organizational Units	organizational units granted access to the domain	Both the NAME and DISTINGUISHED NAME are displayed for a unit.
Resources	users, groups, and policies associated with the domain	The resource NAME , TYPE , and ENABLED status are displayed.
Attributes	values assigned to the domain for management and tracking	The NAME and DESCRIPTION of each attribute is listed.
Managed Accounts	Active Directory accounts with privileges to run services and tasks for the domain	The DISPLAY NAME , SAM ACCOUNT NAME , DISTINGUISHED NAME , ENABLED status, and MANAGED STATE are shown. Filters are available to reach of these fields.

Integrate ALM with Active Directory

Use these steps to integrate ALM with Active Directory.

- Navigate to **External Domains > Add Domain**.
- Enter the **Name** of your Active Directory domain.
- **Add** the domain to ALM.

After you create the Active Directory domain in ALM, you must assign it to an ALM Engine Pool:

- Browse to the **ALM Engine Pools** section.
- Select the intended ALM Engine Pool and choose **Manage Pool**.
- Use **Assign** and select the Active Directory domain to assign to the pool.

Once you assign the AD domain to an ALM Engine Pool, you start synchronization by managing the External Domain.

To perform an ad-hoc synchronization of a specific Domain, go to the **Manage** tab of the Domain, use the **Actions** button, and select **Sync**.

The Users, Groups, Organizational Units, Attributes, and Managed Accounts of the Domain will all be synced. Depending on the Domain size, synchronizing may take up to 15 minutes

Domain Synchronization

You can set the interval that ALM automatically syncs and schedule on-demand syncs.



Note: ALM checks for synchronization requests at the top of each hour. Syncs should be scheduled for the start of the next hour or they will not start until the following day. *Example: If it is 9:30, the soonest a sync can be scheduled is 10:00. If a sync were scheduled at 9:30 for 9:45, ALM Would not sync until 9:45 the following day.*

Sync Users

Within a Domain, you can identify to ALM selected AD Groups and their Child Groups that should have their Users synced to ALM and then kept in sync. This tool directly applies to the task of importing existing AD user accounts into ALM for governance.

Users within selected Groups and Child Groups will automatically receive the Account Owner Role because like all Users in ALM they will belong to the Everyone Group. Once initially synced, Users may be added to other ALM Groups and assigned additional Roles.

Use these steps to enable **Sync Users**.

1. Navigate to the **Domains** page.
2. Select the **Domain** to **Sync Users**.
3. On the **Manage** tab of the **Domains** detail page:
 - a. Click **Actions**.
 - b. Select **Edit**.
 - c. In the lower half of the **Manage** tab, locate the **Sync Users** tool.
4. Set the **Enable Sync** toggle to **Yes**.
5. Scroll or search from the **Available Groups** table to locate the Domain's Groups to sync with ALM.
6. Click the green + (plus) icon to the right of the Group to place it in the **Synchronized Groups** table on the right.
7. To finalize the configuration, return to **Actions** at the top of the page and click **Save**.

Notes

- You can disable this sync at any time.
- You can control the sync schedule using the **Sync this domain** feature on the **Manage** tab of the **Domains** detail page.
- Be mindful of the number of users your selections will cause to be synced into ALM, as subscription limits apply to how many users come into ALM via this feature.
 - Navigate to the **Subscription** page of ALM to view subscription consumption figures.

Active Directory Account Discovery Tool

The AD Account Discovery Tool allows System Administrators to select any or all service Accounts within a specific domain and import them to ALM, where they can be managed by associating them with Workflow Templates and assigning Owners.

Located under Administration > Account Discovery, the tool presents a simple four-step process for bringing AD service Accounts under ALM management.

Be sure to familiarize yourself with the limitations on these steps before you begin this process.

ALM Initial Setup Task List

- select the domain
 - limit: you can select only **one** domain at a time; to analyze multiple domains, you must separately apply the Discovery Tool to each domain
- select Accounts within the domain
 - note: Accounts must be selected from Organizational Units; you *can* select Accounts from multiple OUs
- assign the selected Accounts to a Workflow Template
 - limit: you will only have the option to assign **all** of the selected Accounts to **one** Workflow Template
- assign Users and Groups as Owners of the Accounts
 - limit: in assigning Users and Groups to be the Account Owners, you will be assigning **all** of the Accounts you selected to be owned by **each** User and Group you select here

Integrate ALM with Amazon Web Services (AWS)

Use these steps to integrate ALM with AWS Directory.

- Navigate to **External Domains > Add Domain**.
- Enter the **Name** of your AWS domain.
- **Add** the domain to ALM.

After you create the AWS domain in ALM, you must assign it to an ALM Engine Pool.

- Browse to the **ALM Engine Pools** section.
- Select the intended ALM Engine Pool and choose **Manage Pool**.
- Use **Assign** and select the AWS domain to assign to the pool.

Once you assign the AWS domain to an ALM Engine Pool, you start synchronization by managing the External Domain.

To perform an ad-hoc synchronization of a specific Domain, go to the **Manage** tab of the Domain, use the **Actions** button, and select **Sync**.

Setting Permissions for AWS

Use these steps to integrate ALM with Amazon Web Services Identity and Access Management.

1. Launch a Windows EC2 instance in AWS.
2. Create a new IAM Role with the permissions shown on the **Permissions** tab below, or use JSON as shown. Note that the **Resources** can be set to all (*).
3. Assign the new role to the EC2 instance.
4. Install the ALM Engine on the EC2 instance.

ALM Initial Setup Task List

5. Assign the ALM Engine to a domain and pool in ALM.

PermissionsPolicy usageTagsPolicy versionsAccess Advisor

< BackIAM

Policy summary{} JSONEdit policy

Q Filter

Action (20 of 159) Show remaining 139	Resource
List (8 of 36 actions)	
GetLoginProfile	All resources
ListAccessKeys	All resources
ListAttachedGroupPolicies	All resources
ListAttachedUserPolicies	All resources
ListGroups	All resources
ListGroupsForUser	All resources
ListPolicies	All resources
ListUsers	All resources
Read (1 of 28 actions)	
GetUser	All resources
Tagging (1 of 16 actions)	
TagUser	All resources
Write (8 of 56 actions)	
AddUserToGroup	All resources
CreateAccessKey	All resources
CreateLoginProfile	All resources
CreateUser	All resources
DeleteAccessKey	All resources
DeleteLoginProfile	All resources
DeleteUser	All resources
RemoveUserFromGroup	All resources
Permissions management (2 of 23 actions)	
AttachUserPolicy	All resources
DetachUserPolicy	All resources

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "visualEditor0",
      "Effect": "Allow",
      "Action": [
        "iam:ListPolicies",
```

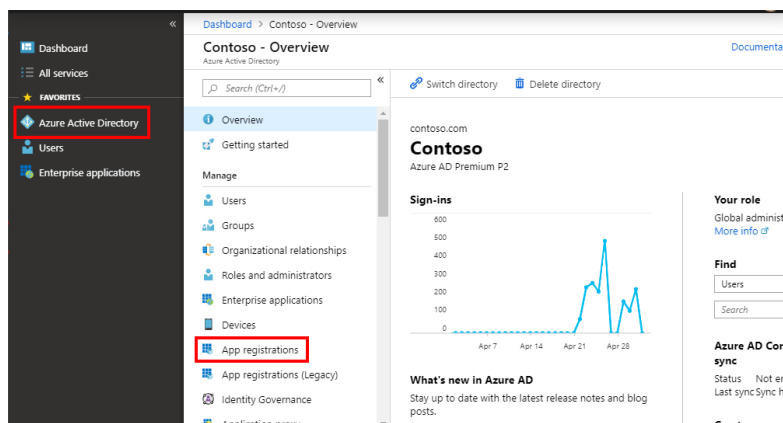
ALM Initial Setup Task List

```
        "iam:DeleteAccessKey",
        "iam:AttachUserPolicy",
        "iam:DeleteUser",
        "iam:CreateUser",
        "iam:TagUser",
        "iam:CreateAccessKey",
        "iam:CreateLoginProfile",
        "iam:RemoveUserFromGroup",
        "iam:AddUserToGroup",
        "iam:ListGroupsForUser",
        "iam:ListAttachedUserPolicies",
        "iam:ListUsers",
        "iam:ListAttachedGroupPolicies",
        "iam:ListGroups",
        "iam:GetUser",
        "iam:DetachUserPolicy",
        "iam:GetLoginProfile",
        "iam:DeleteLoginProfile",
        "iam:ListAccessKeys"
    ],
    "Resource": "*"
}
]
```

Integrate ALM with Azure Active Directory

Use these steps to integrate ALM with Azure Active Directory.

1. Open a browser and navigate to the Azure Active Directory admin center.
2. Select Azure Active Directory in the left-hand navigation, then select App registrations under Manage.



3. Select New registration. On the Register an application page, set the values as follows.
 - Set Name: (Delinea ALM)
 - Set Supported account types to: Accounts in this organizational directory only - (Single tenant)

ALM Initial Setup Task List

- Leave Redirect URI empty.

The screenshot shows the 'Register an application' page in the Azure portal. The 'Name' field is filled with 'Thyctic ALM'. Under 'Supported account types', the first option 'Accounts in this organizational directory only (Thyctic Dev ALM1 only - Single tenant)' is selected. The 'Redirect URI (optional)' section has a dropdown menu set to 'Web' and a text input field containing 'e.g. https://myapp.com/auth'.

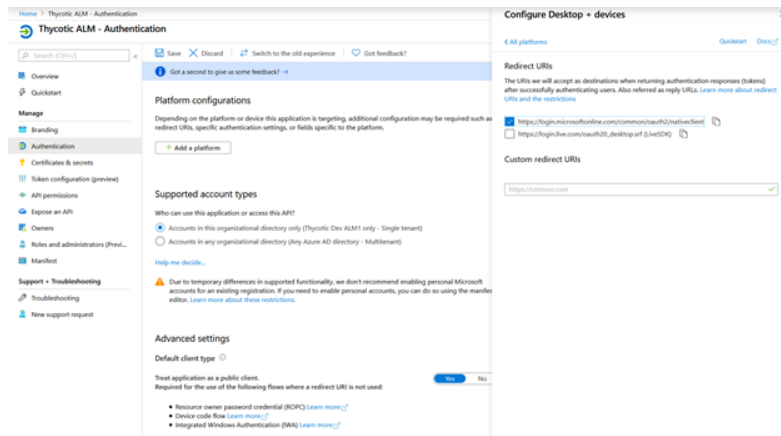
4. Select Register. On the Delinea ALM App Registration page, copy the value of the Application (client) ID and (tenant) ID.

The screenshot shows the 'Thyctic ALM' app registration page. The 'Overview' tab is selected. The 'Application (client) ID' is 'f5c330d-8809-4807-8403-03a680e3e3b8' and the 'Directory (tenant) ID' is '1818c8e-8312-4613-96f9-879a22d9ff63'. The 'Object ID' is '0e95f02b-ba5d-4826-831f-39248524f272'.

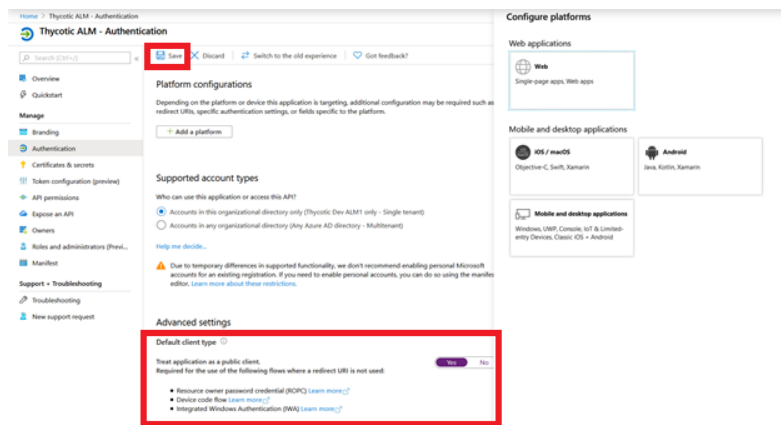
5. Select the Add a Redirect URI link. On the Redirect URIs page, locate the Add Platform and select (Mobile and desktop applications) section. Select the https://login.microsoftonline.com/common/oauth2/nativeclient URI. Click **Configure**.

The screenshot shows the 'Configure platforms' page in the Azure portal. The 'Web applications' section is expanded, showing 'Web' and 'Mobile and desktop applications'. The 'Mobile and desktop applications' section is selected, showing 'iOS / macOS' and 'Android'. The 'Supported account types' section is also visible, showing the same options as in the previous screenshot.

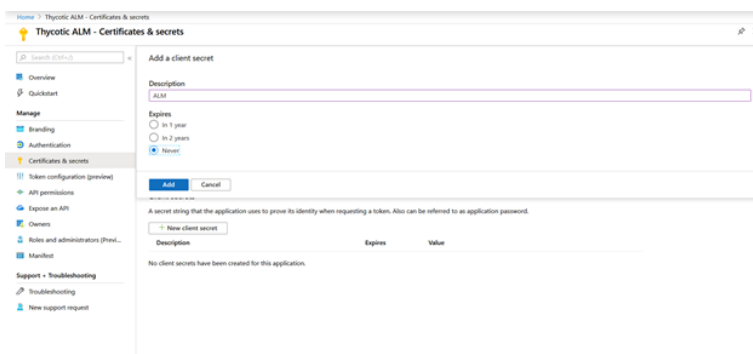
ALM Initial Setup Task List



- Locate the Default client type section and change the Treat application as a public client toggle to **Yes**, then choose **Save**.



- Select Certificates and secrets.
 - Click new client secret and name (ALM).
 - Copy the client secret for later.



- Select API Permissions in the left navigation panel.

ALM Initial Setup Task List

- Select Add Permissions.
- Select Microsoft Graph.
- Add the following permission options:
 - Delegated Permissions
 - Directory.AccessAsuser.All
 - Application Permissions
 - Group.Read.All
 - Group.ReadWrite.All
 - Group.Selected
 - User.Read.All
 - User.ReadWrite.All
 - RoleManagement.Read.All
 - RoleManagement.Read.Directory
 - RoleManagement.ReadWrite.Directory

ALM Initial Setup Task List

API permissions

Refresh

Configured permissions

Applications are authorized to call APIs when they are granted perm all the permissions the application needs. [Learn more about permis](#)

+ Add a permission Grant admin consent for Thycoti

API / Permissions name	Type	Desc
Microsoft Graph (7)		
Directory.AccessAsUser.All	Delegated	Acces
Domain.ReadWrite.All	Application	Read
Group.Read.All	Application	Read
Group.ReadWrite.All	Application	Read
Group.Selected	Application	Acces
User.Read.All	Application	Read
User.ReadWrite.All	Application	Read

< All APIs

Microsoft Graph
https://graph.microsoft.com/ Docs

What type of permissions does your application require?

Delegated permissions
Your application needs to access the API as the signed-in user.

Application permissions
Your application runs as a background service or daemon without a signed-in user.

Select permissions [expand all](#)

Type to search

Permission	Admin Consent Required
> AccessReview	
> AdministrativeUnit	
> Application	
> AppRoleAssignment	
> ApprovalRequest	
> AuditLog	
> BitlockerKey	
> Calendars	
> CallRecords	
> Calls	
> ChannelMessage	
> Chat	
> Contacts	
> DelegatedPermissionGrant	
> Device	
> DeviceManagementApps	
> DeviceManagementConfiguration	
> DeviceManagementManagedDevices	
> DeviceManagementRBAC	
> DeviceManagementServiceConfig	
> Directory	
Domain (1)	
☒ Domain.ReadWrite.All Read and write domains ⓘ	Yes
> EduAdministration	
> EduAssignments	
> EduRoster	
> ExternalItem	
> Files	
Group (3)	
☐ Group.Create Create groups ⓘ	Yes
☒ Group.Read.All Read all groups ⓘ	Yes
☒ Group.ReadWrite.All Read and write all groups ⓘ	Yes
☒ Group.Selected Access selected groups ⓘ	Yes

Add permissions Discard

9. Select Grant admin consent.
10. Switch over to ALM.
 - Navigate to **Integrations**
 - Select **Domains** from list.
 - Select **Add Domain**.

ALM Initial Setup Task List

- Enter a **Name** for the Domain.
- From the **Domain Type** dropdown, select **Azure Active Directory**.
- Select **Edit** from the **Actions** menu.
- *Optional* Enable and configure domain synchronization.
- Enter the client, secret, and tenant ID in the created Azure AD Domain.
- Select **Save** from the **Actions** menu.

The screenshot shows the 'Thycotic ALM' domain configuration page in the ALM interface. The breadcrumb trail is 'Integrations > Domains > Thycotic ALM'. The 'Manage' tab is active, showing a sidebar with 'Users', 'Groups', 'Attributes', and 'Managed Accounts'. The main content area has a 'Name' field with 'Thycotic ALM'. The 'Domain Type' is set to 'Azure Active Directory'. The 'Enabled' toggle is turned on. The 'Sync this domain' section shows 'Enable sync' turned on, with a frequency of 'Every 1' day, starting on '1 - First' day of the month at '7:00 PM'. At the bottom, there are fields for 'Client ID', 'Client Secret', and 'Azure Tenant ID' under the 'Azure AD Connection' section.

Optional: Use these steps to enable Sync:

1. In ALM, navigate to the Domains page.
2. Select a **Domain** you want **Sync** enabled.
3. On the **Manage** tab of the **Domains** detail page,
 - select **Edit**,
 - and locate the **Sync** tool (in the lower half of the **Manage** tab).
4. Set the **Enable Sync** toggle to **Yes**.
5. Set the desired sync frequency.

Review your work. To commit the configuration, return to the **Actions** button at the top of the page and select **Save**.

Integrate Google Cloud Platform

Use these steps to integrate the Google Cloud Platform.

ALM Initial Setup Task List

1. Launch a Windows Google Compute Instance in GCP and note the Service Account associated with the instance.
2. Create a new IAM Role for ALM Provisioning. The role needs to be created at the organization level if multiple projects will be used for provisioning accounts. If not, then the role can be created in a single project. Define the following permissions on the Permissions tab:
 - iam.roles.list
 - iam.serviceAccountKeys.create
 - iam.serviceAccountKeys.delete
 - iam.serviceAccountKeys.get
 - iam.serviceAccountKeys.list
 - iam.serviceAccounts.create
 - iam.serviceAccounts.delete
 - iam.serviceAccounts.disable
 - iam.serviceAccounts.enable
 - iam.serviceAccounts.get
 - iam.serviceAccounts.getIamPolicy
 - iam.serviceAccounts.list
 - iam.serviceAccounts.setIamPolicy
 - iam.serviceAccounts undelete
 - iam.serviceAccounts.update
 - resourceManager.organizations.get
 - resourceManager.organizations.getIamPolicy
 - resourceManager.organizations.setIamPolicy
 - resourceManager.projects.get
 - resourceManager.projects.getIamPolicy
 - resourceManager.projects.list
 - resourceManager.projects.setIamPolicy
3. At the Organization or Project level, assign the Google Compute Instance Service Account to the ALM Provisioning role created.

ALM will sync all Service Accounts, Roles, Organizations, and Projects that it has access to. To exclude certain Organizations and Projects from sync, explicitly deny the ALM Role access to them.
4. Install a certificate on the Windows Google Compute Instance for the Service Account.
 - a. Find the Service Account for the engine machine and generate a PK12 access key.
 - b. Install the access key on the Windows Google Compute Instance in the Trusted Root Certificate folder.

ALM Initial Setup Task List

- c. The Service Account (Active Directory Account or Network Service) used to run the ALM Engine Service needs to be able to access the certificate locally.
5. Enable Domain Wide Delegation for the Service Account used by the ALM Engine to perform requests:
 - a. The scopes required are:
<https://www.googleapis.com/auth/admin.directory.domain.readonly>
<https://www.googleapis.com/auth/admin.directory.group.readonly>
<https://www.googleapis.com/auth/admin.directory.user.readonly>
 - b. Enable Admin SDK API (https://developers.google.com/admin-sdk/?hl=en_US).
 - c. When creating the GCP IAM Domain in the ALM UI, specify the email of the GCP Admin user to impersonate. The Admin user must have logged into GCP at least one time and accepted the terms and conditions.
6. Install the ALM Engine on the Google Compute Instance.
7. Assign the ALM Engine to a Google Cloud Domain and pool in ALM.
8. Set the Admin email account on the ALM Domain.
9. Sync the ALM Domain.

Integrate Group Managed Service Accounts

Overview

Group Managed Service Accounts (gMSAs) provide automatic password and simplified service principal name (SPN) management to multiple servers.

ALM supports the provisioning and lifecycle management of gMSAs. This is achieved when **Group Managed Service Account** is selected as the **Account Type** when the System Administrator is creating a Workflow Template.



Note: ALM Active Directory domains do not sync gMSA accounts by default. To sync gMSA accounts, select **Sync Group Managed Service Accounts** prior to performing a sync.

ALM Initial Setup Task List

Account Lifecycle Manager

Workflow Templates >

New Template

1 Setup 2 Vault 3 Directory Services 4 Ownership 5 Lifecycle Next

Template Details
This tool will guide you through the process of creating and publishing a Workflow Template to use for creating managed accounts.

Template Name: gMSA Account Managmeent

Account Type: Active Directory

End of Lifecycle Action: Review

Service Account: ☒

Terms of Service: [Empty text area]

Purpose: [Empty text area]

Delinea

Requirements:

- RSAT needs to be installed on the engine machine
 - Use Powershell and run script: Install-WindowsFeature RSAT-AD-PowerShell
 - Use GUI and Enable RSAT through Turn Windows Features on or off
- Microsoft Active Directory prerequisites and one-time preparation, [see Microsoft documentation](#)

Parameters:

Certain Parameters are set by default and others by the attributes list in a workflow template.

- **PrincipalsAllowedToDelegateToAccount** - Set by the Users and Groups selected in the template.
- **KerberosEncryptionType** - Accepted values (None, DES, RC4, AES128, AES256). Only one is allowed.
- **ServicePrincipalNames** - Accepts a comma-separated list of service principal names. This has to be unique for each request.

Step 4 - Create a Vault

ALM integrates with the following vaults for storage and management of account credentials:

- [Secret Server](#)
- [DevOps Secrets Vault](#).
- [Azure Key Vault](#)
- [AWS Secrets Manager](#)
- [Hashicorp](#)

Integrate with AWS Secrets Manager

Use these steps to integrate ALM with AWS Secrets Manager.

- In ALM, navigate to **Integrations** on the left-hand menu and click **Vaults**.
- Click **Create Vault** in the upper right-hand corner.
- On the Add Vault Modal, select **AWS Secrets Manager** from the Template drop-down menu. Click **Next**.
- Fill in the required fields:
 - **AWS Secrets Manager Display Name** is the name that will display for the vault in ALM.
 - **AWS Secrets Manager URL** is the location of the vault.
 - **Access Key ID** is the login name for the vault.
 - **Secret Access Key** is the password for the vault.
- Click **Save**.

Once added, you can select AWS Secrets Manager as a vault option when creating Workflow Templates. Accounts created from that template will use AWS Secrets Manager for the storage and management of account credentials.

Integrate with HashiCorp Vault

ALM currently supports HashiCorp Vault with token-based authentication and the key/value Secrets Engine.

Use these steps to integrate ALM with HashiCorp Vault:

- In ALM, navigate to **Integrations** on the left-hand menu and click **Vaults**.
- Click **Create Vault** in the upper right-hand corner.
- On the Add Vault Modal, select **HashiCorp Vault** from the Template drop-down menu. Click **Next**.
- Fill in the required fields:
 - **HashiCorp Vault Display Name** is the name that will display for the vault in ALM.
 - **HashiCorp Vault URL** is the location of the vault.
 - **Vault Connection Token** is the authentication token provided in the HashiCorp UI.
- Click **Save**.

Once added, you can select HashiCorp Vault as a vault option when creating Workflow Templates. Accounts created from that template will use HashiCorp Vault for the storage and management of account credentials.

Integrate ALM with Secret Server

ALM integrates with Secret Server for storage and management of account credentials, connecting to Secret Server through the ALM Engine service, which uses the Secret Server Rest API. If you use an on-premises installation of Secret Server, the version must be **10.2.000018** or later.

Because Account Lifecycle Manager works with Secret Server through Secret Server's web services, you must enable those services on your Secret Server instance.

Use these steps to enable the Secret Server web services:

ALM Initial Setup Task List

1. Log in to Secret Server as an Administrator and navigate to **Admin > Configuration**.
2. On the **General** tab, under **Application Settings**, find the entry for **Enable Webservice**.
3. If the entry displays as **No**, you must change it.
 - Use the **Edit** button found below the settings to reveal controls for making changes.
 - Set the toggle box for **Enable Webservice** to active.
 - Use the **Save** button below the settings to save the change.

You must also set up a Secret Server account for ALM that has privileges to:

- view folders accessible to ALM Users
- create Secrets in those folders
- view Secret Template permissions

To integrate ALM with Secret Server, use these steps:

1. Select **Integrations** in the left navigation panel, then select the **Vaults** tab.
2. Click **Create Vault**.
3. At the **Template** drop-down, select **Delinea Secret Server**.
4. Provide the following information: **_Secret Server Display Name**, **Secret Server URL**, and the **Username** and **Password** for the Secret Server account that will run this integration.



Note: Delinea recommends creating a Secret Server Application Account with the minimum permissions.

Role

Role Name	ALM Users
Enabled	Yes
Created	8/23/2019

< 1 to 3 of 3 >

PERMISSIONS

Add Secret

View Folders

View Secret Templates

Back
Edit

You must use a template with the following fields, and you must not add new required fields to the template:

- domain
- Username
- password
- notes

Integrate ALM with DevOps Secrets Vault

ALM integrates with Delinea's DevOps Secrets Vault (DSV) for storage and management of Account credentials. Use these steps to integrate ALM with DevOps Secrets Vault.

1. In the left navigation panel, select **Integrations** and navigate to the **Vaults** tab. Select **Create Vault**.
2. At the **Template** drop-down and select **Delinea DevOps Secrets Vault**.
3. Click **Next** to confirm that selection, and fill in the required information:
 - **DevOps Secrets Vault Display Name** entry is the vault label in ALM that distinguishes it from other vaults
 - **DevOps Secrets Vault URL** specifies the URL of your DevOps Secrets Vault instance

ALM Initial Setup Task List

- **ClientID** records the Client ID of your DevOps Secrets Vault instance
- **ClientSecret** is the password for your ClientID

4. Click **Create Vault** to confirm your entries

Once you have added it, you can select **Delinea DevOps Secrets Vault** as a vault option when creating Workflow Templates.

Requests made based on Workflow Templates that have a DevOps Secrets Vault will use DevOps Secrets Vault for the storage and management of Account credentials.

Integrate with Azure Key Vault

Use these steps to integrate ALM with Azure Key Vault.

1. In ALM, navigate to **Integrations** on the left-hand menu and click **Vaults**.
2. Click **Create Vault** in the upper right-hand corner.
3. On the Add Vault Modal, select **Azure Key Vault** from the Template drop-down menu. Click **Next**.
4. Fill in the required fields:
 - **Azure Key Vault Display Name** is the name that will display for the vault in ALM.
 - **Azure Key Vault URL** is the location of the vault.
 - **ClientID** is the login name for the vault.
 - **ClientSecret** is the password for the vault.
 - **TenantID** is the tenant name of your Azure account.
5. Click **Save**.

Once added, you can select Azure Key Vault as a vault option when creating Workflow Templates. Accounts created from that template will use Azure Key Vault for the storage and management of account credentials.

Integrate with HashiCorp Vault

ALM currently supports HashiCorp Vault with token-based authentication and the key/value Secrets Engine.

Use these steps to integrate ALM with HashiCorp Vault.

- In ALM, navigate to **Integrations** on the left-hand menu and click **Vaults**.
- Click **Create Vault** in the upper right-hand corner.
- On the Add Vault Modal, select **HashiCorp Vault** from the Template drop-down menu. Click **Next**.
- Fill in the required fields:
 - **HashiCorp Vault Display Name** is the name that will display for the vault in ALM.
 - **HashiCorp Vault URL** is the location of the vault.
 - **Vault Connection Token** is the authentication token provided in the HashiCorp UI.
- Click **Save**.

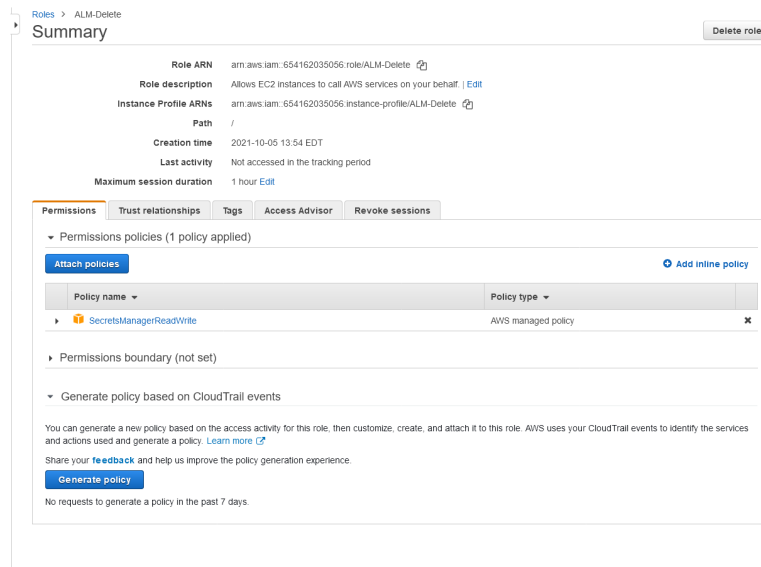
ALM Initial Setup Task List

Once added, you can select HashiCorp Vault as a vault option when creating Workflow Templates. Accounts created from that template will use HashiCorp Vault for the storage and management of account credentials.

Integrate with AWS Secrets Manager

Integration with AWS Secrets Manager requires running an ALM Engine on an EC2 instance.

1. Launch a Windows EC2 instance in AWS.
2. Create a new IAM Role and attach the policy SecretsManagerReadWrite.
3. Assign the new role to the EC2 instance.
4. Install the ALM Engine on the EC2 instance.



Self-Hosted ALM Installation Steps

1. Make sure that you meet the System Requirements listed below.
2. [Configure Docker](#).
3. [Install ALM](#).
4. [Finish and Add Licenses](#).

Prerequisites

The following are required to install the self-hosted version of ALM:

1. Linux Machine

 **Note:** Tested against the following - Ubuntu 16.04, Ubuntu 18.04, Debian 9, Debian 10, CentOS 8.2, Fedora 32.

2. Docker

ALM Initial Setup Task List

- Manages the images and containers used by ALM.
- Installation Instructions : <https://docs.docker.com/get-docker/>

3. Docker Compose

- This is required for ALM's installation script to manage the local orchestration of services.
- Installation instructions: <https://docs.docker.com/compose/install/>

4. Port Configuration

- After installation, the docker containers will require the following ports to be available on the host system:
 - TCP/80, if LetsEncrypt certificate management is enabled.
 - TCP/443 for the web UI.

Additional Requirements

During installation and configuration, you will need to know the following ahead of time:

- **Domain** (Example: alm.thycotic.com)
 - Site where ALM will be accessible to users through a web browser.
- **SSL/TLS Certificate for the domain**
 - Can be managed automatically using LetsEncrypt, as an option.
 - Or a certificate and chain can be provided manually during setup.
- **Open ID Connect (OIDC) credentials**
 - ALM uses OIDC for user authentication.
 - This can be configured through Azure Active Directory or Thycotic One.
- **SMTP credentials** (*optional*) - Allows ALM to send email notifications to users. If you choose to not use SMTP, put in any values for the questions and please understand email notifications will not be sent in ALM. This can be re-configured in the future by running `./alm.sh install`, this will initiate the install process again but exclude initial user configuration.

Docker Configuration

Once Docker has been installed, add your user to the docker group. This allows the ALM setup script to run docker commands without sudo:

```
sudo groupadd docker
sudo gpasswd -a $USER docker
sudo service docker restart
```



Note: Log out and back in for the change to take effect.

Supported Authentication Methods

ALM on-prem currently supports authentication through:

ALM Initial Setup Task List

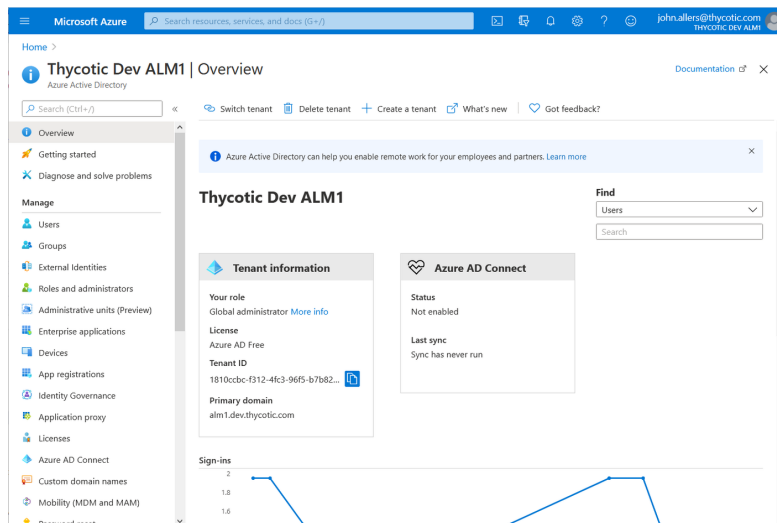
- [Auth0](#)
- [Azure AD Open ID Connect](#)
- [Thycotic One Open ID Connect](#)

Azure AD Open ID Connect

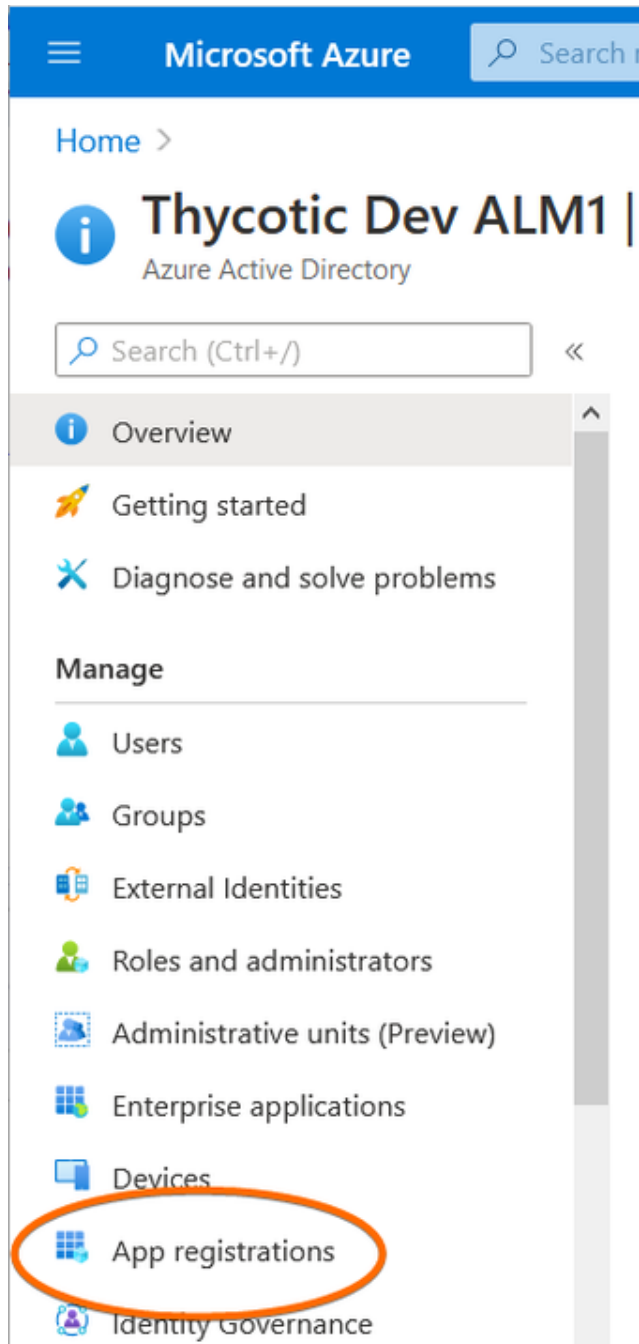
To configure Azure AD OIDC with ALM:

Create a New App Registration

1. Navigate to portal.azure.com and then **Azure Active Directory**.

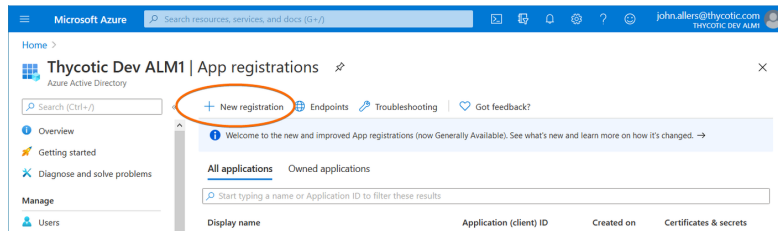


2. In the left-hand navigation panel, select **App registrations**.



3. On the top of the App registration page, click **+New registration**.

ALM Initial Setup Task List



4. On the **Register an application** page, provide:
 - a. Name- the name you would like for ALM. (*Example: ALM On-Prem*)
 - b. Supported account types- choose single tenant (default).
 - c. Redirect URI- set the drop-down to **Web** and provide the sign-in URL for your ALM instance.
5. Click **register**. You will be taken to the newly created App registration page.

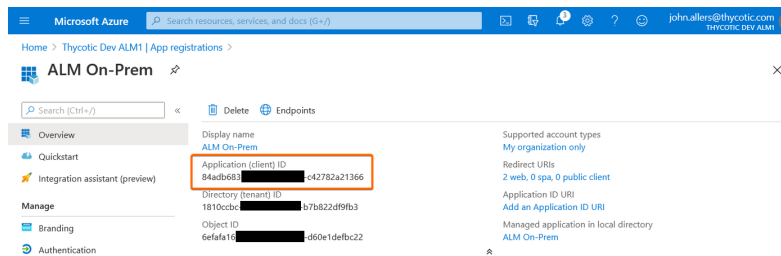
A screenshot of the 'Register an application' page in the Microsoft Azure portal. The page has a blue header with 'Microsoft Azure' and a search bar. The user is logged in as 'john.allers@thycotic.com'. The main content area is titled 'Register an application'. It contains several sections:

- Name**: A text input field with the value 'ALM On-Prem' and a green checkmark icon.
- Supported account types**: A section titled 'Who can use this application or access this API?' with three radio button options:
 - ☒ Accounts in this organizational directory only (Thycotic Dev ALM1 only - Single tenant)
 - ☐ Accounts in any organizational directory (Any Azure AD directory - Multitenant)
 - ☐ Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
- Redirect URI (optional)**: A section with a text input field containing 'https://instance01.john.enzadev.com/signin-oidc' and a green checkmark icon.

At the bottom, there is a blue button labeled 'Register'.

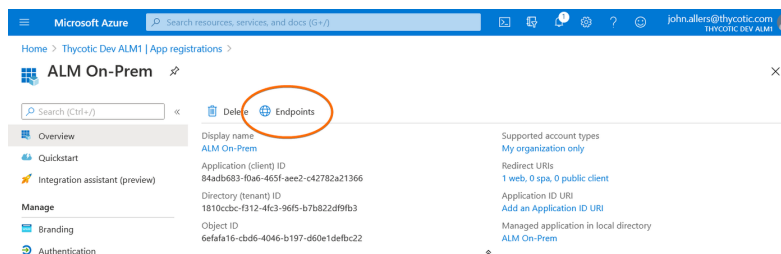
6. On the registration page, take note of the **Application (client) ID value**. This will be used for the **OIDC Client ID** value during ALM setup.

ALM Initial Setup Task List

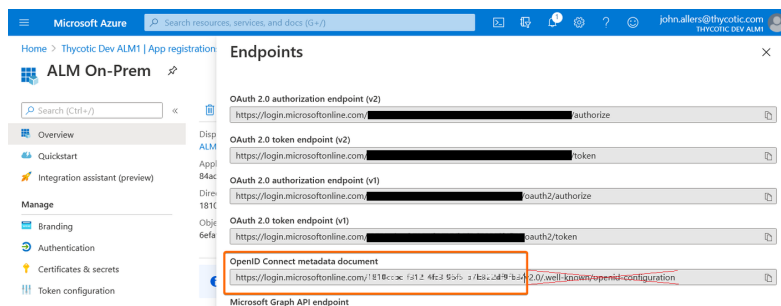


Configure OIDC URLs

1. On the top of the registration page, click **Endpoints**. The endpoints dialogue will open.

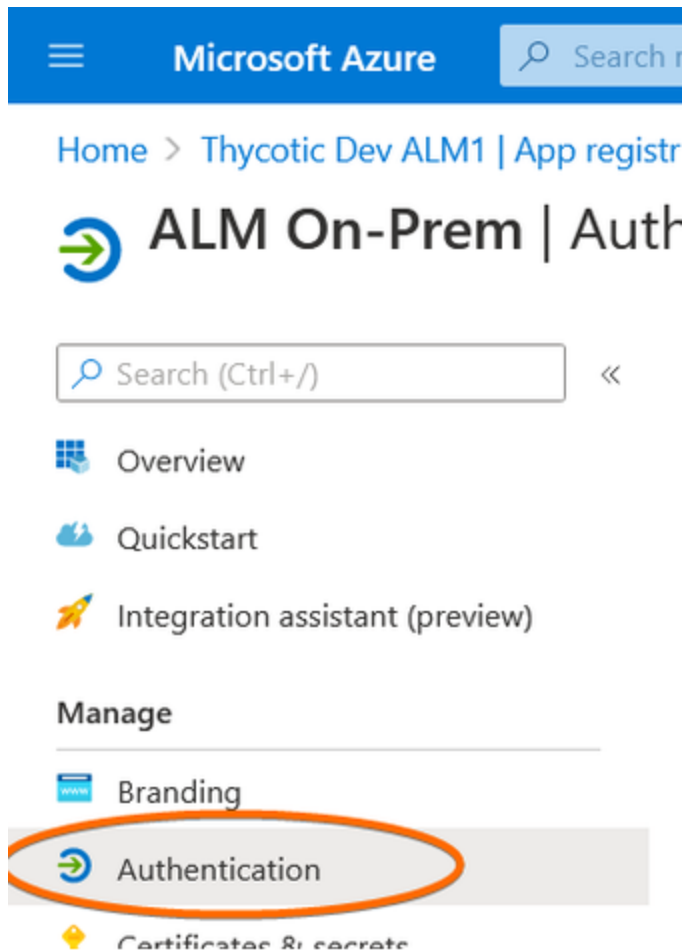


2. Copy the **OpenID Connect metadata document** value, but omit the *v2.0/well-known/openid-configuration* portion of the URL. This will be the **OIDC Authority URL**.

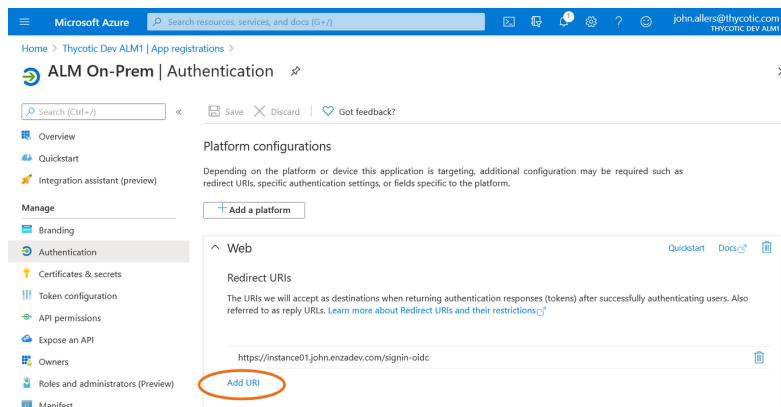


3. Close the Endpoints dialogue.
4. On the left-hand navigation menu, click **Authentication**. The Platform configurations panel will open.

ALM Initial Setup Task List



5. Under Web, click **Add URI**.



6. Enter `https://YOUR_ALM_DOMAIN/signout-callback-oidc`.

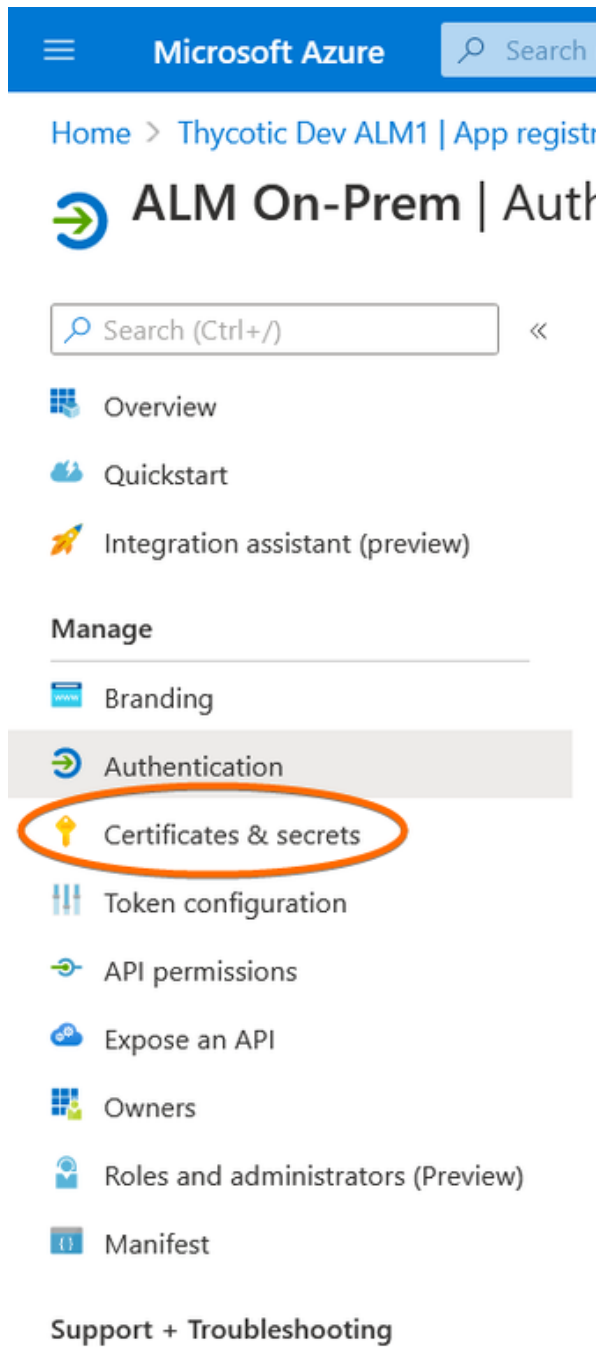
ALM Initial Setup Task List

The screenshot shows the Microsoft Azure portal interface for configuring an application. The top navigation bar includes the Microsoft Azure logo, a search bar, and user information. The breadcrumb trail indicates the path: Home > Thycotic Dev ALM1 | App registrations > ALM On-Prem | Authentication. The left sidebar contains a 'Manage' section with links to Overview, Quickstart, Integration assistant (preview), Branding, Authentication (selected), Certificates & secrets, Token configuration, API permissions, Expose an API, Owners, Roles and administrators (Preview), and Manifest. The main content area is titled 'Platform configurations' and includes a description of platform-specific configurations and an 'Add a platform' button. A 'Web' configuration panel is expanded, showing 'Redirect URIs' with a list of two URIs: 'https://instance01.john.enzadev.com/signin-oidc' and 'https://instance01.john.enzadev.com/signout-callback-oidc'. The second URI is highlighted with a green checkmark. An orange arrow points from the 'Roles and administrators (Preview)' link in the sidebar to the 'Add URI' button in the 'Web' panel.

7. On the top of the panel, click **Save**.

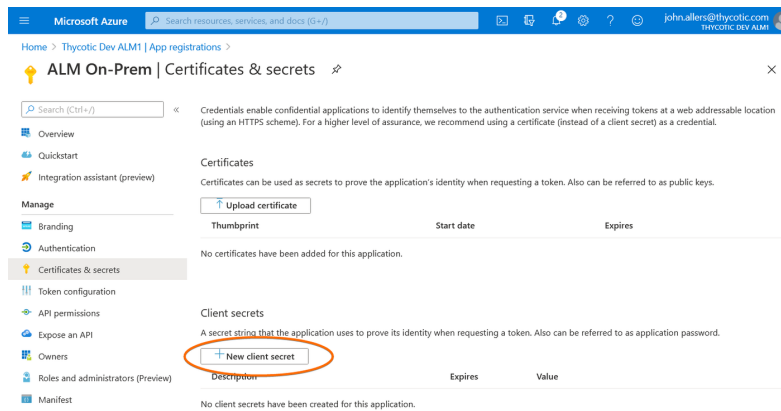
Create Client Secret

1. In the left-hand navigation menu, click **Certificates & secrets**. The Certificates & secrets panel will open.

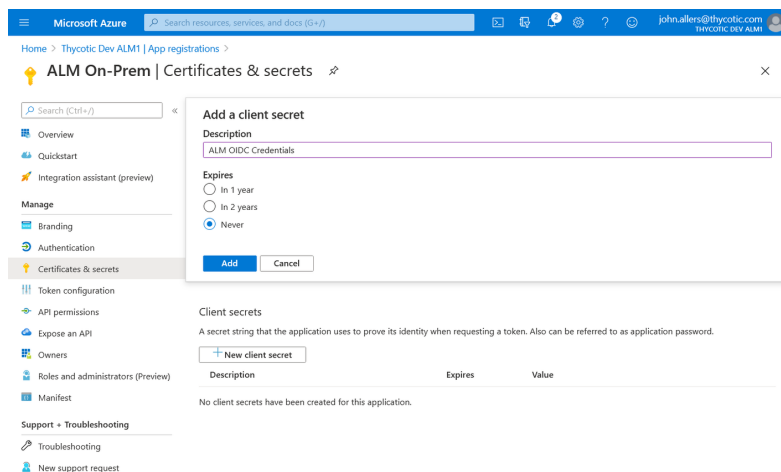


2. Under Client secrets, click **New client secret**.

ALM Initial Setup Task List



3. On the **Add a client secret** dialog, choose:
 - a. A description. (*Example: ALM OIDC Credentials*)
 - b. An expiration date. **When this secret expires, ALM will need to be reconfigured with manually with a new secret.**
4. Click **Add** to save the new client secret.



5. The new secret will now be displayed in the Client secrets section of the Certificates & secrets page.
6. Click the **Copy to clipboard icon** and store the secret value. It will be used as the OIDC Client Secret during ALM setup.

ALM Initial Setup Task List

Microsoft Azure Search resources, services, and docs (G+)

Home > Thycotic Dev ALM1 | App registrations >

ALM On-Prem | Certificates & secrets

Search (Ctrl+/) «

Copy the new client secret value. You won't be able to retrieve it after you perform another operation or leave this blade.

Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Certificates

Certificates can be used as secrets to prove the application's identity when requesting a token. Also can be referred to as public keys.

Upload certificate

Thumbprint	Start date	Expires
No certificates have been added for this application.		

Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

New client secret

Description	Expires	Value
ALM OIDC Credentials	12/31/2299	F4K5-...-...

Copy icon highlighted with a red arrow.

7. The OpenID connect configuration for Azure AD is now ready for use with ALM.

Configure Auth0 Open ID Connect (OIDC)

Create An Application in Auth0

The Auth0 application will allow for authentication with ALM.

1. Sign into [Auth0](#) or create an account.
2. Navigate to **Applications**

Auth0 Search for users or applications Help & Support Docs Discuss Your Needs

Thank you for purchasing the Free Auth0 plan. You have 5 days left in your trial to experiment with features that are not in the Free plan. Like what you're seeing? Please enter your billing information here. BILLING

Getting Started

Try your Login box

With Auth0 your authentication experience is ready to go. Customize it to match your brand identity and try it now to see how it works.

Try it out Customize

Default App

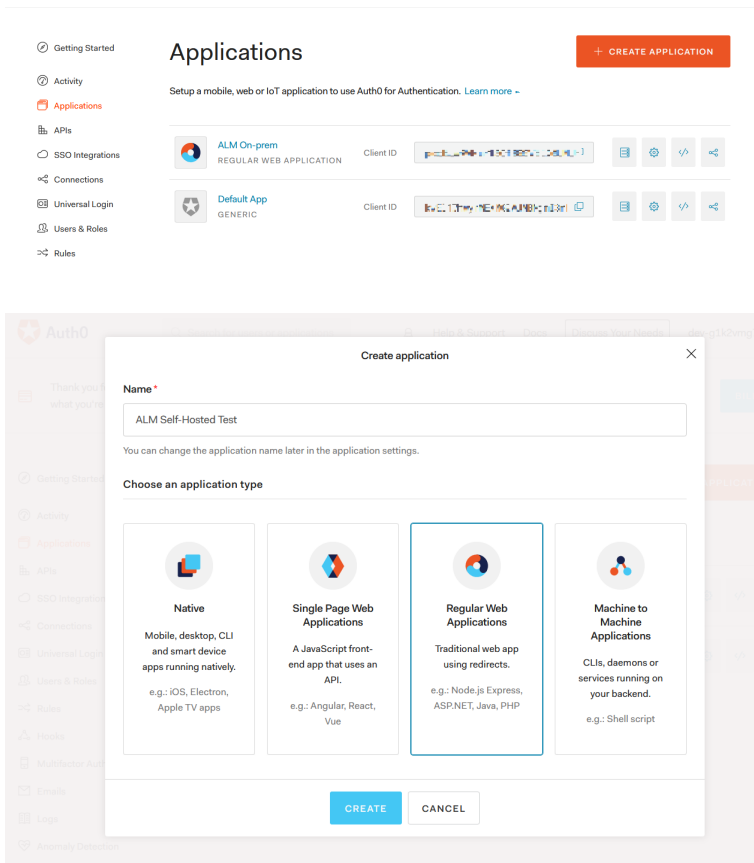
Login Sign Up

non@gmail.com

3. Click **Create Application**.

ALM Initial Setup Task List

- Provide a **Name**.
- Under **Choose an application type** select **Regular Web**.
- Click **Create**.



Copy Domain/Client ID/Client Secret

After the application is created, find and copy the values that will be needed during the ALM setup.

1. Select the **Settings** tab.
2. Under **Basic Information**, make note of the following:
 - **Domain**- This will be the OIDC Authority URL value during setup.
 - **Client ID**
 - **Client Secret**

ALM Initial Setup Task List

Getting Started

Activity

Applications

APIs

SSO Integrations

Connections

Universal Login

Users & Roles

Rules

Hooks

Multifactor Auth

Emails

Logs

Anomaly Detection

Extensions

Back to Applications

ALM Self-Hosted Test

REGULAR WEB APPLICATION

Client ID

Dt0rZRjIquLo92QA9N66osRBRm0sN0Ui

Quick Start

Settings

Addons

Connections

Basic Information

Name *

ALM Self-Hosted Test

Domain

oewg.ub2unq.us.auth0.com

Client ID

Dt0rZRjIquLo92QA9N66osRBRm0sN0Ui

Client Secret

.....

Getting Started

Activity

Applications

APIs

SSO Integrations

Connections

Universal Login

Users & Roles

Rules

Hooks

Multifactor Auth

Emails

Logs

Anomaly Detection

Extensions

Get Support

Back to Applications

ALM Self-Hosted Test

REGULAR WEB APPLICATION

Client ID

Dt0rZRjIquLo92QA9N66osRBRm0sN0Ui

Quick Start

Settings

Addons

Connections

Basic Information

Name *

ALM Self-Hosted Test

Domain

oewg.ub2unq.us.auth0.com

Client ID

Dt0rZRjIquLo92QA9N66osRBRm0sN0Ui

Client Secret

.....

The Client Secret is not base64 encoded.

Configure Settings

While in the Settings section, configure the settings that are specific to your self-hosted instance.

ALM Initial Setup Task List

1. Scroll down to the **Applications URIs** section and fill out the following fields

- **Application Login URI** - `https://{your ALM Domain}`
- **Allowed Callback URLs** - `https://{your ALM Domain}/signin-oidc,https://{your ALM Domain}/signout-callback-oidc`
- **Allowed Logout URLs** - `https://{your ALM Domain}/authentication/logout`

Application URIs

Application Login URI `https://selfhosted.john.enzadev.com`

In some scenarios, Auth0 will need to redirect to your application's login page. This URI needs to point to a route in your application that should redirect to your tenant's `/authorize` endpoint. [Learn more](#)

Allowed Callback URLs `https://selfhosted.john.enzadev.com/signin-oidc, https://selfhosted.john.enzadev.com/signout-callback-oidc`

After the user authenticates we will only call back to any of these URLs. You can specify multiple valid URLs by comma-separating them (typically to handle different environments like QA or testing). Make sure to specify the protocol (`https://`) otherwise the callback may fail in some cases. With the exception of custom URI schemes for native clients, all callbacks should use protocol `https://`.

Allowed Logout URLs `https://selfhosted.john.enzadev.com/authentication/logout`

A set of URLs that are valid to redirect to after logout from Auth0. After a user logs out from Auth0 you can redirect them with the `returnTo` query parameter. The URL that you use in `returnTo` must be listed here. You can specify multiple valid URLs by comma-separating them. You can use the star symbol as a wildcard for subdomains (`*.google.com`). Query strings and hash information are not taken into account when validating these URLs. Read more about this at <https://auth0.com/docs/logout>

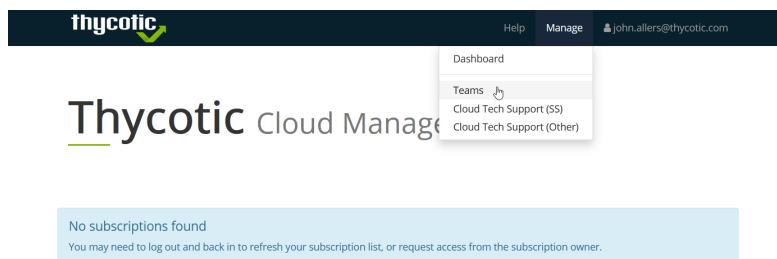
2. Scroll to the bottom of the page and click **Save Changes**.

Thycotic One Open ID Connect (OIDC) Configuration

To configure Thycotic One OIDC authentication for use with ALM:

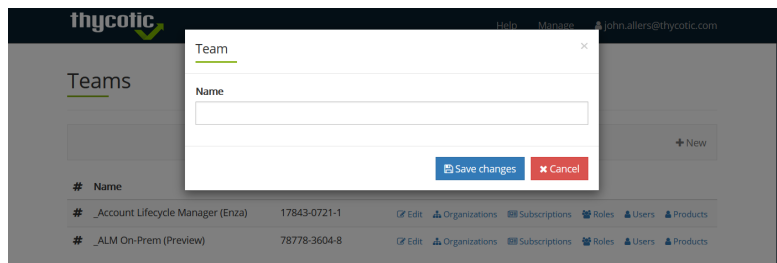
Select a Team

1. Navigate to portal.thycotic.com
2. On the top menu, click **Manage** and then **Teams**.



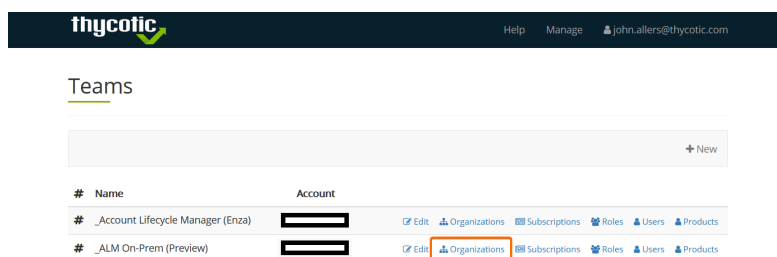
ALM Initial Setup Task List

3. If there are no existing teams, create one by clicking **+New**. Give the Team a name and click **Save Changes**.

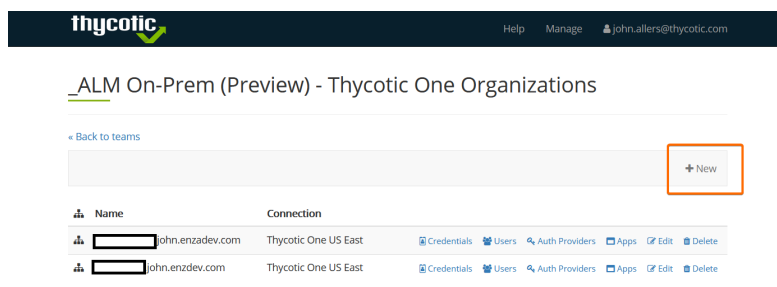


Create a New Organization

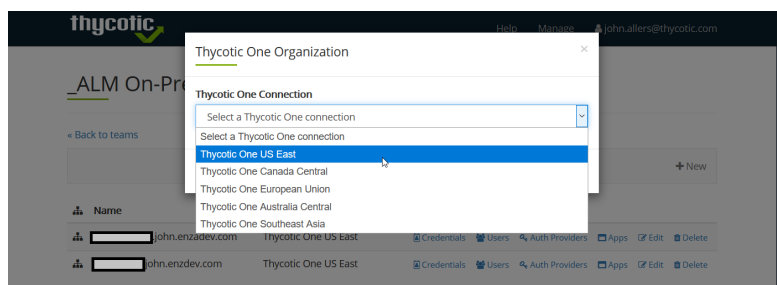
1. To the right of the team name, click **Organizations**.



2. On the organizations page click **+New**.



3. From the drop-down, select the Thycotic One region that you would like to use.



4. On the organization preferences page, you can configure the following options:

ALM Initial Setup Task List

- The **Name** of the organization.
- The **Thycotic One Connection Region**.
- The **lockout attempt count**. This will determine the number of failed logins before a user is locked out.
- The **minimum password strength**. This will determine the complexity of passwords that users must use for logging in.
- The **Two-Factor Login Policies**. Leaving the drop-downs at **No Preference** will allow users to choose their two-factor method.

The screenshot shows the 'Thycotic One Organization' configuration form. The form includes the following fields and options:

- Name:** On Prem Testing
- Thycotic One Connection:** Thycotic One US East
- Security Policy:**
 - Lockout Attempt Count:** 7
 - Minimum Password Strength:** Safely Unguessable
- Two-Factor Login Policy:** No Preference
- SMS Two Factor Policy:** No Preference
- TOTP Two Factor Policy:** No Preference

At the bottom of the form are 'Save' and 'Cancel' buttons. A green arrow points from the bottom right of the form towards the right side of the page.

- Once your configuration is complete, click **Save**.

Configure OIDC Credentials

- On the organizations page, click **Credentials** next to the organization you created.

The screenshot shows the 'Thycotic One Organizations' page. It features a table with the following columns: Name, Connection, and a row of action links. The 'Credentials' link for the 'On Prem Testing' organization is highlighted with a red box.

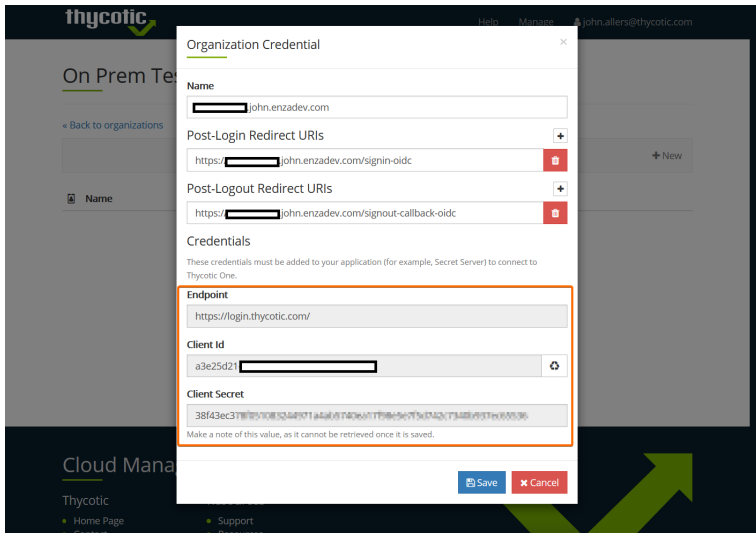
Name	Connection	
On Prem Testing	Thycotic One US East	Credentials Users Auth Providers Apps Edit Delete
john.enzadev.com	Thycotic One US East	Credentials Users Auth Providers Apps Edit Delete
john.enzdev.com	Thycotic One US East	Credentials Users Auth Providers Apps Edit Delete

- Click **+New**.
- Complete the **Organization Credential** form:

ALM Initial Setup Task List

- a. Give the credential a name.
- b. The **Post-Login redirect URIs** should be: `https://YOUR_ALM_DOMAIN/signin-oidc`
- c. The **Post-Logout Redirect URIs** should be: `https://YOUR_ALM_DOMAIN/signout-callback-oidc`

 **Note:** Be sure to save the **Endpoint**, **Client Id**, and **Client Secret**. You will need these values when performing ALM Self-Hosted setup.



- d. Click **Save**.
4. OpenID Connect configuration for Thycotic One is now complete and ready for use with ALM.

Installation

Create a directory to store the ALM data.

```
mkdir ~/alm
```

 **Note:** This directory will contain configuration files for ALM. Permissions should be set to only necessary users. (e.g. the account that installed ALM, an account used for running backups, etc.)

Change to that directory.

```
cd ~/alm
```

Download and Install the Script:

```
curl https://alc-cdn01.azureedge.net/scripts/alm.sh -o alm.sh && chmod +x alm.sh && ./alm.sh install
```

Domain name

what domain name will users use to access ALM?

To use LetsEncrypt, you'll need a domain name that points to your public IP, and ports 80 and 443 forwarded from your router to the local IP of the machine that is running ALM.

ALM Initial Setup Task List

SSL/TLS Configuration

--- SSL/TLS Configuration ---

ALM requires a SSL/TLS certificate to ensure that all web communication is secure. ALM can be configured to use LetsEncrypt to automatically create and manage the certificate. Or you may provide your own.

would you like to use LetsEncrypt to generate an SSL/TLS certificate for docker.enzadev.com? [y/n]:

y will pull the certbot container and attempt to get a certificate for the domain entered in the previous step. The acquired certificates will be under ./alldata/letsencrypt

n will wait for you to copy the certificate (named <DOMAIN>.crt, e.g.example.alm.com.crt) and private key (named <DOMAIN>.key, e.g.example.alm.com.key) to the same folder as the install script. It will move them to the ./alldata/ssl directory as part of the install.

Database Configuration

--- Database Configuration ---

ALM needs to set up a SQL Server database to store its data. You can use your own SQL Server instance to host the database, or you may choose to have a SQL Server Express instance set up automatically as a container.

Do you want to automatically set up your database in a SQL Express container? [y/n]:

y will generate credentials and move on to the next step

n will prompt you for the connection info for SQL Server.

Enter the connection info for your SQL Server:

Server:

Database:

User ID:

Password:

Admin User

--- Admin User ---

ALM requires at least one admin user. We will configure the first admin user as part of the installation process. This admin user will also receive email alerts regarding LetsEncrypt certificate expirations.

Initial User Display Name:

Initial User Email:

These are the values that will be used for the initial admin account. Make sure you use an account that can log into the OIDC instance below.

Authentication Configuration

--- Authentication Configuration ---

ALM requires an OpenID Connect (OIDC) provider for user authentication. Please provide the credentials to your preferred OIDC provider.

OIDC Authority URL:

OIDC Client ID:

OIDC Client Secret:



Note: The domain you use will need to be configured as a reply url in whatever OIDC provider you use, or you will get an “invalid reply url” error when you try to log in.

Email Configuration

--- Email Configuration ---

ALM uses SMTP to send email notifications to users. Please provide the SMTP credentials to your preferred provider.

Server:

Port:

Use SSL?:

Use Credentials?:

(If yes, then:)

Domain:

User Name:

Password:



Note: Use these settings to connect to an SMTP server. These do not need to be valid to complete the install.

Finishing Setup and Adding Licenses

Once the setup is complete, browse to your ALM instance using the chosen domain name.

When running in Self Hosted mode, ALM requires license keys to add more than one user and one ALM Engine.

Navigate to Licensing page

1. Open **Administration > Configuration** in the left navigation menu
2. Click the **License** tab
3. Enter the license **Name** and **Key**



Note: Users and engines are licensed separately, so two licenses will need to be entered.

4. Once this step setup is complete, you will now have ability to add multiple users and ALM Engines depending on the allowances of the license.

Understanding ALM Objects

ALM relies on four objects to govern Service Accounts: Users, Roles, Groups, and Workflow Templates.

Users

An ALM **User** object is a proxy for either a **User account** or a **service account** that is **stored in Active Directory**.

- When the ALM User object is a proxy for an Active Directory **User account**, you will perform ALM operations on the ALM proxy purely to control what a person authenticated as that AD User account can do within ALM.
- When the ALM User object is a proxy for an Active Directory **service account**, you will perform ALM operations on the ALM proxy to deliver lifecycle management of the proxied AD service account.

- When you use ALM to create an ALM User object as a proxy for an Active Directory service account that **does not yet exist** in Active Directory, **ALM will create the service account in Active Directory**.
- **After this initial creation** of a service account in Active Directory, ALM operations performed on ALM proxies for AD accounts usually do not directly affect the AD accounts as stored in Active Directory, although there are obvious exceptions such as when an account is disabled.

Roles

An ALM **Role** defines the privileges that the User has in ALM and the tasks that the User can perform.

- ALM Roles have **nothing to do** with Active Directory Roles and should not be confused with them.

Delinea provisions ALM with several Roles already set up—Account Owner, Requester, Approver, and System Administrator—and for most organizations these will suffice for initial operations.

Account Owner

All users automatically have the Account Owner Role. The Account Owner Role is also fixed to the built-in Everyone Group that contains all users in ALM.

This Role provides entry level features and permissions sufficient for a User to read and update managed accounts assigned to them.

Requestor

Users with the Requestor Role can request the provisioning of new service accounts. Requestors begin each Request by selecting a Workflow Template which determines the lifecycle of the account and the approval process.

Approver

ALM delivers Requests to Approvers according to the workflow and approval steps specified by the template. An Approver receives notices of account Requests and approves or denies each Request according to the chosen workflow. Some workflows will require multiple Approvers.

On approval, ALM provisions the account and designates the Requestor as the first owner.

System Administrator

This Role holds all privileges. Organizations use this all-powerful Role to perform initial customer configurations of Account Lifecycle Manager. A System Administrator can provision Users, integrate ALM with external systems, set up ALM Engines, and create Workflow Templates.

Because the System Administrator Role is so highly privileged, its use carries risk of accidental macro-scale changes to your ALM configuration. As a best practice, use the System Administrator Role only for tasks that require its privileges, and when done with those tasks, log out and resume use of less privileged Roles.

Custom Roles

Once familiar with ALM, you may decide to use the [Custom Roles](#) feature to create Roles that support specific business needs.

- Example: A custom Auditor Role configured with privileges required to view ALM's Audit Logs but otherwise lacking the full range of privileges given to a System Administrator.

Groups

An ALM **Group** object defines Groups of ALM User objects that have something in common with each other, such as access to a resource.

- ALM Groups have **nothing to do** with Active Directory Groups and should not be confused with them.

Workflow Templates

An ALM **Workflow Template** defines a workflow applicable to Requests **made in ALM** for provisioning in **Active Directory** of a service account of a particular type.

- The Workflow Template defines the information that must be provided with the Request, the approval steps that must be completed for the Request to be granted, and who has approval authority at each step.
- Requests for some kinds of service accounts may require just one step, approved by only one person. Requests for other kinds of service accounts may require multiple steps and Approvals by more than one person at some or all of the approval steps.
- Workflow templates also control the selection of BEOL (before end of lifecycle) and AEOL (at end of lifecycle) Notifications ALM sends, when it sends them, and to whom, plus what options the Notifications will offer for managing the service account.

Custom Roles

ALM System Administrators can create Custom Roles. To define Custom Roles, you review a list of ALM features paired with the permissions potentially applicable to each feature.

- Roles differ from one another in the specific permissions assigned to them in relation to each ALM feature.
- A Custom Role is a Role you create to meet your specific business needs when the built-in Roles will not suffice.

Once you have set the per-feature permissions for a Role, you add Users or Groups (or both) to the Role, thereby granting the Role's permissions to those Users, and to Users who belong to those Groups.

As with the built-in Roles, you can:

- edit the name of the Custom Role
- enable or disable the Custom Role
- enable or disable automatic addition of new Users to the Custom Role
- add or remove Users from the Custom Role
- add or remove Groups from the Custom Role

Permissions

Permissions control what actions Users can take within ALM. Distinct permissions within ALM include:

Create allows creation of the object for which you grant the permission

Understanding ALM Objects

Read allows passive use of a feature, such as to read (view) a list of objects or view an object's details

Update: allows changes to the object for which you grant the permission, for example, update a Managed Account

Delete: allows a User to delete the object for which you grant the permission

Manage: gives additional, administrative access to the object to which it applies, for which the User must already have non-administrative privileges

- As an example, Users with Manage permission on Managed Account feature would give access to all the Managed Accounts.

Features to Which Permissions Apply

In defining a Custom Role, you specify the permissions the Custom Role holds in relation to specific ALM features. The features subject to access control via permissions include:

API Token: Access to the API Token feature allows a User to view, create, and manage API Tokens. These enable the User to obtain Bearer tokens, required by ALM for further processing.

Audit: ALM logs most events, including User actions, system events, and remote worker activity. Audit permissions allow a User to view these logs.

Configuration: A User with Configuration permissions can define the System Administrator's email address.

Directory-Service: With Directory Service permissions, a User can configure ALM's integration with the organization's directory services provider—its **External Domain**:

- Presently ALM supports only one External Domain, that being Active Directory.
- For Active Directory, additional settings include AD Groups, Users, Group Mappings, and OUs.

Email Notification: ALM provides several broadly applicable Email Notification Categories. Email Notifications inform Users and Groups of Users about events affecting objects with which they have a connection—for example, the User is named in the governing Workflow Template as the Approver for a step in the workflow.

Group: Groups are collections of Users. You use Groups to more efficiently apply the same management activities to more than one User at once. You can assign Groups to Approval Steps just as you would an individual User; likewise, you can assign Account Ownership to a Group.

Managed Account: A Managed Account is an AD Service Account created and managed through ALM.



Note: Read permission provides visibility to only accounts owned by the User. The Manage permission provides visibility of all managed accounts. In order to see all accounts the Read and Manage permission must be applied to the same Custom Role.

Provision Template: With Provision Template permissions, Users can create Workflow Templates to govern the approval process for AD service accounts.

Provision Template Workflow: Provision Template Workflow permissions allow a User to set a Workflow Template's Approval Steps. Setting Approval Steps involves designating which Users and Groups must approve the provisioning of a requested service account, and in what order—the workflow.

Provision Approval: To be designated as an Approver for Approval Steps set in a Workflow Template, a User must have permissions for Provision Approval. This gives access to ALM's Approvals section, which lists Requests waiting for an Approver's review and gives access to all Request details.

ALM Engine: A User must have ALM Engine permissions to download the installer for the ALM Engine Windows Service. This permission also enables the User to view in ALM the list of installed ALM Engines and assign ALM Engines to ALM Engine Pools.

Role: The Roles permission enables a User to create Custom Roles and assign Users to them. It also allows the User to add Users to the standard Account Owner, Requester, Approver, and System Administrator Roles.

User: Users with permissions to the User feature can add, remove, or update User accounts, including to designate whether a User is an Approver or Requester.

Vault: With Vault permissions, a User can configure and manage ALM's connection to your organization's Delinea Secret Server.

Webhook: Webhooks provide a framework for connecting ALM to external services. With Webhooks permissions, a User can create custom webhooks.

The [Example Custom Roles Setup](#) article details permissions for a broadly useful Custom Roles setup.

Example Custom Roles Setup

Table: *Permissions for an Example Custom Roles Setup*

Features	Description	Read	Create	Update	Delete	Manage
provision-request	access to Account Requests	Provision	Provision	Provision	visibility and access to all Requests (used in conjunction with Read, Create, Update, Delete permissions)	same as for Delete
		Provision States	Provision State			
		Provision Tags				
		access to Request area in UI				

Understanding ALM Objects

Features	Description	Read	Create	Update	Delete	Manage
managed-account	access to Managed Accounts (accounts provisioned through the product)	Managed Accounts	Managed Accounts	Managed Accounts	visibility and access to all Managed Accounts (used in conjunction with Read, Create, Update, Delete permissions)	<i>same as for Delete</i>
		access to Managed Accounts area in UI				
provision-approval	access to Request Approvals	Provision Approval	Provision Approval	Provision Approval	visibility and access to all Approvals (used in conjunction with Read, Create, Update, Delete permissions)	<i>same as for Delete</i>
		access to Approval area in UI				
provision-template	access to Account Templates	Template	Template	Template	access to Template Workflow area in UI	<i>same as for Delete</i>
					allows Approval of Template Workflows	

Understanding ALM Objects

Features	Description	Read	Create	Update	Delete	Manage
provision-template-workflow	access to Account Template Workflows	Template Workflow	Template Workflow	Template Workflow	access to Template Workflow area in UI	<i>same as for Delete</i>
					allows Approval of Templates	
group	access to Groups	Groups	Groups	Groups	access to Groups area in UI	<i>same as for Delete</i>
					manage Group Users (used in conjunction with Read, Create, Update, Delete permissions)	
					manage Group Roles (used in conjunction with Read, Create, Update, Delete permissions)	
user	access to Users	Users	Users	Users	access to Users area in UI	<i>same as for Delete</i>
		User Emails	User Emails	User Emails	Trigger verification email	

Understanding ALM Objects

Features	Description	Read	Create	Update	Delete	Manage
					manage User Groups (used in conjunction with Read, Create, Update, Delete permissions)	
					manage User Roles (used in conjunction with Read, Create, Update, Delete permissions)	
role	access to Roles	Roles	Roles	Roles	access to Roles area in UI	<i>same as for Delete</i>
		Role Permissions	Role Permissions	Role Permissions	manage Role Permissions (used in conjunction with Read, Create, Update, Delete permissions)	
					manage Role Users (used in conjunction with Read, Create, Update, Delete permissions)	

Understanding ALM Objects

Features	Description	Read	Create	Update	Delete	Manage
					manage Role Groups (used in conjunction with Read, Create, Update, Delete permissions)	
alm-engine	access to ALM Engines	ALM Engine	ALM Engine	ALM Engine	access to ALM Engine area in UI	<i>same as for Delete</i>
		ALM Engine Pools	ALM Engine Pools	ALM Engine Pools	test connectivity to ALM Engines and Pools	
audit	access to Audits	Audits	n/a	n/a	n/a	n/a
		access to Audits area in UI				
directory-service	access to all things related to LDAP/AD/Directory Services	External Domain	<i>same as for Read</i>	<i>same as for Read</i>	access to Directory Services areas in UI	<i>same as for Delete</i>
		External Groups				
		External Users				
		External User Group Mapping				
		External OUs				

Features	Description	Read	Create	Update	Delete	Manage
vault	access to Vaults	Integrations (Secret Server)	Integrations (Secret Server)	Integrations (Secret Server)	access to Integrations area in UI	<i>same as for Delete</i>
		Integration Templates				
api-token	access to API Tokens	API Tokens	API Tokens	API Tokens (only updates to the description and enable/disable allowed)	API Tokens	n/a
configuration	access to system configuration settings	n/a	Configuration	Configuration	Configuration	n/a
	settings currently available:					
	AdminEmail - (For SAP) Email address for the Send Feedback link					
email-notification	access to Email Notification Templates	Email Notification	n/a	Email Notification	n/a	n/a
webhook	access to Webhooks	Webhooks	Webhooks	Webhooks	Webhooks	n/a

Events, Notifications, and Recipients

To request that a new AD service account be provisioned, a Requester selects the Workflow Template applicable to the type of service account being requested, provides the information required by that Workflow Template, and submits the Request.

From there, the Request must pass through each of the Approval Steps specified by the Workflow Template. As this happens, ALM keeps process participants informed by sending Notifications. If the Request wins approval, the service account will be provisioned.

Understanding ALM Objects

Provisioning marks the beginning of the account's lifecycle—the period of time it remains active, during which it will be tracked according to the specifications in the Workflow Template against which it was provisioned.

- For example, the template might specify that the account should expire in one year; or, that it requires renewal after six months. ALM sends notifications timed in relation to these settings—if an account requires renewal at six months, ALM notifies the account owner in advance of the six-month mark. Within ALM, the account owner has the option to approve or deny account renewal.

ALM provides for varied and strongly granular lifecycle event tracking and notification activities, as in the following table.

Table: *Account Lifecycle Manager Events, Notifications, and Recipients*

Object	Event	Description	Email Notification Recipients
Template	Workflow needs approval	The template's workflow needs approval.	System Administrators
	Published	A template has been published.	None, by default; Allow for System Administrators
	Unpublished	A template has been unpublished	None, by default; Allow for System Administrators
	De-activated	A template has been de-activated.	None, by default; Allow for System Administrators
Request	Submitted	A Requester asks that an account be provisioned.	None
	Step requires approval	Kick off a step of approval	Approvers for step
	Approved	All the approval steps have been approved	Requester
	Rejected		Requester
	Queued for provisioning		None
	Provisioned		Requester
	Provisioning failed		Requester

Object	Event	Description	Email Notification Recipients
Managed Account	Ownership Changed		Account Owners
	Requires Renewal		Account Owners



Tip: Closely related to these notifications, ALM [At End of Lifecycle Actions \(EOLAs\)](#) define the actions Account Owners can take when an account expires, for example, they can renew the account. Similarly, **BEOLs** refers to Before End of Lifecycle Actions, the steps Account Owners can take when an account nears its expiration date.

At End of Lifecycle (AEOL) Actions

Account Lifecycle Manager allows a System Administrator to define in a Workflow Template the At End of Lifecycle actions (AEOLs) that will apply to accounts provisioned against that Workflow Template. The Template also controls the schedule and pacing of Notifications to be sent by ALM as the End of Lifecycle date approaches, and the parties who will receive the Notifications.

When an account comes up for review at or near the end of its lifecycle, ALM sends Notifications to the Users or Groups designated in the Workflow Template and as scheduled in that Template.

The actions ALM allows reviewers to take correspond to the At End of Lifecycle actions specified by the Workflow Template. These may include:

- Review
- Disable
- Expire
- Delete

Review

An account provisioned with an AEOL action of Review will not be curtailed in any way with passage of the End of Lifecycle date. The Review action serves simply to document a User's acknowledgement that the account remains necessary.

Reviewers of an account that has Review as the AEOL action have three choices:

- Renew

Before the Renewal Date set in the applicable Workflow Template, the **Renew** option is unavailable. Beginning on the Renewal Date, the Renew option is available.

Selecting Renew extends the account's lifecycle until the next Review, based on the Review Interval set in the Workflow Template. The renewal period will start at UTC 00:00. On renewal of the Account, the Renew option will become unavailable until the next review date.

- Disable

The **Disable** option will disable the account in ALM **and** in Active Directory. Once selected, this option is replaced by a choice to **Enable**, allowing the User to re-enable the account as needed.

- Delete Account and Secret

The **Delete Account and Secret** option will delete the account and any associated secrets. Selecting this option requires the User to confirm (or cancel) the action.

Disable

An account provisioned with an AEOL action of **Disable** will be disabled in Active Directory at the End of Lifecycle, unless the Account Owner Renews the account prior to the End of Lifecycle date.

Reviewers of an account that has Disable as the AEOL action have three choices:

- Renew

Before the Renewal Date set in the applicable Workflow Template, the **Renew** option is unavailable. Beginning on the Renewal Date, the Renew options is available.

Selecting Renew will extend the account's lifecycle until the next Review, based on the Review Interval set in the Workflow Template. The renewal period will start at UTC 00:00. On renewal of the account, the Renew option will again be unavailable until the next Review Date.

- Disable

The **Disable** option will disable the account in ALM **and** in Active Directory. Once selected, this option is replaced by a choice to **Enable**, allowing the User to re-enable the account as needed.

- Delete Account and Secret

The **Delete Account and Secret** option will delete the account and any associated secrets. Selecting this option requires the User to confirm (or cancel) the action.

Expire

For an account provisioned with an AEOL action of **Expire**, ALM sets the Expiration Date in Active Directory such that AD will disable the account at the End of Lifecycle date unless the Account Owner renews the account prior to that date.

Accordingly, the first option likely to become available to the Account Owner who will review the Account is the option to **Submit for Approval to Renew**, offered by a Notification sometime in advance of the End of Lifecycle date so that the Account can be renewed before it would otherwise expire.

- A System Administrator who configures a Workflow Template with Expire as the End of Lifecycle Action must decide how far in advance of the End of Lifecycle date to set the Renewal Date, bearing in mind that the Approval to Renew process duplicates the entire original approval process.
- The Renewal Date set by the Administrator controls the timing of initial Notifications to the Account Owner.

Account Owners reviewing an account that has Expire as the AEOL action have three choices:

■ Submit for Approval to Renew

Before the Renewal Date set in the applicable Workflow Template, this choice will not be available. Beginning on the Renewal Date, this action is available to the Account Owner.

Choosing to renew initiates the Approval Steps specified in the associated Workflow Template and replaces the selection to *Submit for Approval to Renew* with an *Approvals in Process* notation.

- If Approval is denied, the notation switches back to Submit for Approval to Renew and remains that way until and after the Account expires.
- If the Approval is granted, the *Approvals in Process* notation is removed, and the account is renewed for the renewal period defined at UTC 00:00. The Submit for Approval to Renew option remains unavailable until the next Renewal Date.

■ Disable

The **Disable** option will disable the account in ALM **and** in Active Directory. Once selected, this option is replaced by a choice to **Enable**, allowing the User to re-enable the account as needed.

■ Delete Account and Secret

The **Delete Account and Secret** option will delete the account and any associated secrets. Selecting this option requires the User to confirm (or cancel) the action.

Delete

An account provisioned with an AEOL action of **Delete** will be disabled (not actually deleted) at the End of Lifecycle date, unless the Account Owner renews the account prior to that date.

Reviewers of an account that has Delete as the AEOL action have three (sometimes four) choices:

■ Disable

The **Disable** option will disable the account in ALM **and** in Active Directory. Once selected, this option is replaced by a choice to **Enable**, allowing the User to re-enable the account as needed.

■ Delete Account and Secret

The **Delete Account and Secret** option will delete the account and any associated secrets. Selecting this option requires the User to confirm (or cancel) the action.

■ Clone As New Request

Option for bringing a Deleted account back online and active. Performing this option generates a new Request that goes through the Approval process in accordance with the Workflow Template the account was provisioned against.

See the [End-of-Lifecycle Account Disposition Logic](#) article for details on the logic of options availability vs. account status and review actions.

ALM End-of-Lifecycle Account Disposition Logic for Option Availability, Account Status, and User Review Actions

Table: *ALM End-of-Lifecycle Account Disposition Logic*

S. No.	Options to be Available	Review BEOL	Review AEOL	Disable BEOL	Disable AEOL	Delete BEOL	Delete AEOL	Expire BEOL	Expire AEOL
1	Renew	nonfunctional or Yes (based on the Notifications set in the Workflow Template)	Yes	Yes (based on the Notifications set in the Workflow Template)	Yes				
2	Disable	Yes	Yes	Yes		Yes		Yes	
3	Enable				Yes				
4	Delete Account & Secret	Yes	Yes	Yes	Yes	Yes		Yes	Yes
5	Submit for Approval to Renew							Yes (based on the Notifications set in the Workflow Template)	Yes
6	Clone as New Request	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Account Status when EOL Reached Systematically

S. No.	Account Status	Review BEOL	Review AEOL	Disable BEOL	Disable AEOL	Delete BEOL	Delete AEOL	Expire BEOL	Expire AEOL
1	Active	Yes	Yes	Yes		Yes		Yes	
2	Disabled				Yes				
3	Deleted						Yes		
4	Expired								Yes

S. No.	Account Status	Review BEOL	Review AEOL	Disable BEOL	Disable AEOL	Delete BEOL	Delete AEOL	Expire BEOL	Expire AEOL
5	Renewing						<i>applies on use of the Clone as New Request option</i>		<i>applies on use of the Submit for Approval to Renew option</i>

User Actions on Review EOL

S. No.	options to be Displayed	Review BEOL	Account Status	Review AEOL	Account Status
1	Renew	a. unavailable b. Yes (based on the Notifications set in the Workflow Template)	Active	Enabled	Active
2	Disable	a. Yes b. on use, makes Enable option available	a. Active b. using the Disable option changes the Status to Disabled c. using the Enable option changes the Status to Active	a. Yes b. on use, enables the Enable option	a. Active b. using the _Enable or Renew option changes the Status to Active c. using the Enable option changes the Status to Active
3	Delete Account & Secret	a. Yes b. on use, requires Clone as New Request option to reinstate account	a. Active	a. Yes	a. Active

User Actions on Disable EOL

S. No.	options to be Displayed	Review BEOL	Account Status	Review AEOL	Account Status
1	Renew	unavailable	Active	a. Yes b. on use, updates EOL based on lifecycle duration and makes option unavailable	Active
2	Disable	a. unavailable b. Yes (<i>based on the Notifications set in the Workflow Template</i>)	a. Active b. using the Disable option changes the Status to Disabled	No	
3	Delete Account & Secret	a. Yes b. on use, enables the Clone as New Request option to reinstate account	a. Active b. using the Delete Account & Secret option changes the status to Deleted	a. Yes b. on use, requires Clone as New Request option to reinstate account	a. Active b. using the Delete Account & Secret option changes the status to Deleted

User Actions on Delete EOL

S. No.	options to be Displayed	Review BEOL	Account Status	Review AEOL	Account Status
1	Disable	a. Yes b. on use, enables the Enable option	a. Active b. using the Disable option changes the Status to Disabled c. using the Enable option changes the Status to Active	No	Deleted
2	Delete Account & Secret	on use, enables the Clone as New Request option	a. Deleted b. using the Delete Account & Secret option changes the Status to Deleted	No	Deleted
3	Clone as New Request			Yes	a. Deleted b. Using the Clone as New Request generates a new Request for Approval in a Submitted Status c. No other requests with the same name on the same domain can be submitted until the submitted request is rejected or the account created from an approved request is deleted.

User Actions on Expire EOL

S. No.	options to be Displayed	Review BEOL	Account Status	Review AEOL	Account Status
1	Disable	a. Yes b. on use, enables the Enable option	a. Active b. using the Disable option changes the Status to Disabled c. using the Enable option changes the Status to Active	a. Yes b. on use, enables the Enable option	Expired
2	Delete Account & Secret	Yes	a. Active b. using the Delete Account & Secret option changes the Status to Deleted	No	Expired
3	Submit for Approval to Renew			Yes	a. Expired b. using the Submit for Approval to Renew option changes the Status to Renewing c. on provisioning of the account, the Status changes to Active

AD Account Expiration Dates

When working with account expiration dates in Active Directory, you may notice that Active Directory accounts do not always expire when it seems they should. This issue, which is external to ALM, traces back to a purely abstract linguistics problem that has confounded the software industry from its earliest days.

In the case of Active Directory, the problem shows up in the convoluted relationship between Active Directory's **Account expires** entry (on the Account tab of AD's Account Properties dialog) and its **accountExpires** attribute (visible on the Attribute Editor tab).

Understanding ALM Objects

oneday-1 Properties

Published Certificates Member Of Password Replication Dial-in Object
Security Environment Sessions Remote control
Remote Desktop Services Profile CDM+ Attribute Editor
General Address Account Profile Telephones Organization

User login name:
User login name (pre-Windows 2000): ENZADEV\ oneday-1
Logon Hours... Log On To...
☐ Unlock account
Account options:
☐ User must change password at next login
☐ User cannot change password
☐ Password never expires
☐ Store password using reversible encryption
Account expires:
☐ Never
☒ End of: Sunday, June 30, 2019
OK Cancel Apply Help

oneday-1 Properties

Published Certificates Member Of Password Replication Dial-in Object
Security Environment Sessions Remote control
Remote Desktop Services Profile CDM+ Attribute Editor

Attributes:

Attribute	Value
accountExpires	7/1/2019 8:00:00 PM Eastern Daylight Time
badPasswordTime	(never)
badPwdCount	0
cn	oneday-1
codePage	0
countryCode	0
distinguishedName	CN=oneday-1,OU=QA Testing,DC=enzaDEV
dSCorePropagationD...	(0x0 = (WRITE)
instanceType	(never)
lastLogoff	(never)
lastLogon	7/1/2019 11:08:15 AM Eastern Daylight Tim
lastLogonTimestamp	7/1/2019 11:08:15 AM Eastern Daylight Tim
logonCount	1
name	oneday-1

Edit Filter
OK Cancel Apply Help

In a typical environment, **Account expires** and **accountExpires** may appear to be out of sync. As an example, in the illustration above The **Account expires** entry indicates that the account should expire at the “End of” the day entered on the Account tab, while **accountExpires** shows the account expiring at 8:00 PM the following day.

Computing’s Midnight Conundrum

As a representation of time, the word “midnight” denotes the instant marking the end of one day and the beginning of the next. Conceptually, an instant has a duration of zero, but our time keeping systems depend on units defined as intervals of time: seconds, minutes, and hours.

- We can tidily represent the instant that **begins** a new day as 00:00, or more traditionally, as 12:00 AM, but we have no similarly tidy way to represent the instant that **ends** a day.
- The time of 11:59:59 leaves one second on the clock, so it cannot be used to denote the end of a day. Using 12:00 to denote the end of the day and 00:00 to denote the beginning would be sensible, but culture is not always sensible; by tradition, 12:00 belongs to the new day it begins, hence the notation 12:00 AM.

This leaves no commonly recognized way for software to symbolically represent the instant (“the time of day”) that marks the end of a day. With no other option, Active Directory encodes the “End of” day entry as 12:00 AM the next

Using ALM

day. While logically equivalent to the end of the day, by formal definition 12:00 AM is no part of the day just ended; it is part of the morning of the day just beginning. If you set the “End of” day entry to a Wednesday, the time value recorded, when strictly interpreted, evaluates as Thursday.

In Active Directory, the **accountExpires** attribute is defined as 12:00 AM UTC of the day **after** the **last full day** that the account was active. When Active Directory applies this definition to the incorrect, already-one-day-forward entry in the **Account expires** field, it kicks the value of the **accountExpires** attribute out 24 hours past what would be correct. Finally, in rendering that 12:00 AM UTC value in the UI, Active Directory considers the local time zone.

In the illustrated example, it works out like this:

- The **Account expires** field’s “End of” day entry shows June 30. For want of a way to denote the last instant of June 30, this records as 12:00 AM UTC July 1.
- The **accountExpires** attribute, being defined as 12:00 AM UTC of the day after the last full day the account was active, accordingly calculates to 12:00 AM UTC July 2.
- In displaying 12:00 AM UTC July 2 as the **accountExpires** attribute value, Active Directory adjusts for the time zone context; in the example, with the context being Eastern Daylight Time, this works out to 8:00 PM July 1.

In the final outcome, the entries do not align, creating a substantial time window for an account to remain active beyond the end of the day it is supposed to expire.

Efforts by Microsoft to fix this issue face challenges having nothing to do with the technical aspects, such as the imperative to remain interoperable with the world’s installed base of software, and the risk that by correcting a problem you will break all the workarounds to the problem, causing widespread problems for your customers and other software vendors. For these and many other reasons, peculiarities related to account expiration persist in Active Directory.

If you would like to learn more about this longstanding, solutions-resistant issue, visit Richard Mueller’s classic treatment of the topic:

[Account Expiration Article by Richard Mueller](#)

ALM Storage of Dates

Dates and times at rest in the cloud (that is, in ALM storage) are UTC time.

When you work within the ALM UI, ALM handles the interpretation of UTC to local time for display in the ALM UI, and back to UTC for storage when you update a date and time via the ALM UI.

If you should happen to work directly with the API, note that a call that returns a date and time will return it in UTC.

Likewise, when working directly with the API, any date and time information you provide should be in UTC.

Using ALM

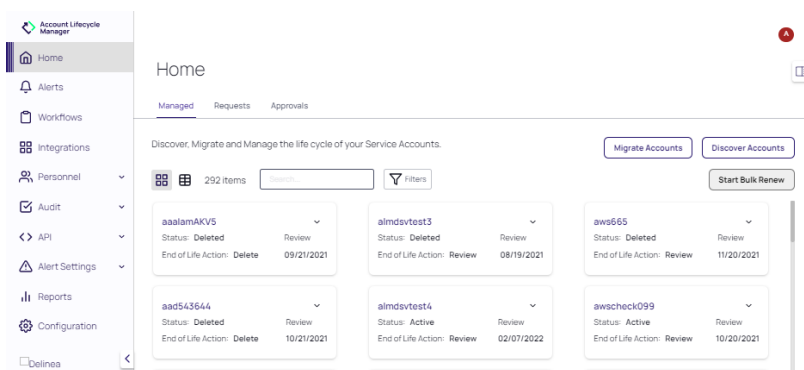
Once you have installed the [ALM engine](#) and integrated with both Secret Server and Active Directory, you are ready to begin using ALM. Refer to [Navigating ALM](#).

The selections on the left navigation panel access the following functionality that governs the discovery, provisioning and decommissioning of accounts:

Using ALM

 **Note:** Certain features (as noted in the documentation) are only available when the appropriate permissions are configured for the user account.

- [Home](#) provides the view of existing accounts and allows management of accounts and account requests.
- [Workflow](#) accesses functionality for creating and managing workflows for the management of accounts.
- [Integrations](#) after initial setup, provides tools for configuring or modifying Domains and Pools, Engines, and Vaults.
- [Personnel](#) will walk you through creating users, groups, and workflows in ALM.
- [Audits](#) provides insights into user activity and Engine Logs.
- [Alerts](#) can be configured for email templates, webhooks, and webhook authorization
- [API](#) accesses API documentation and allows for the creation of API tokens.

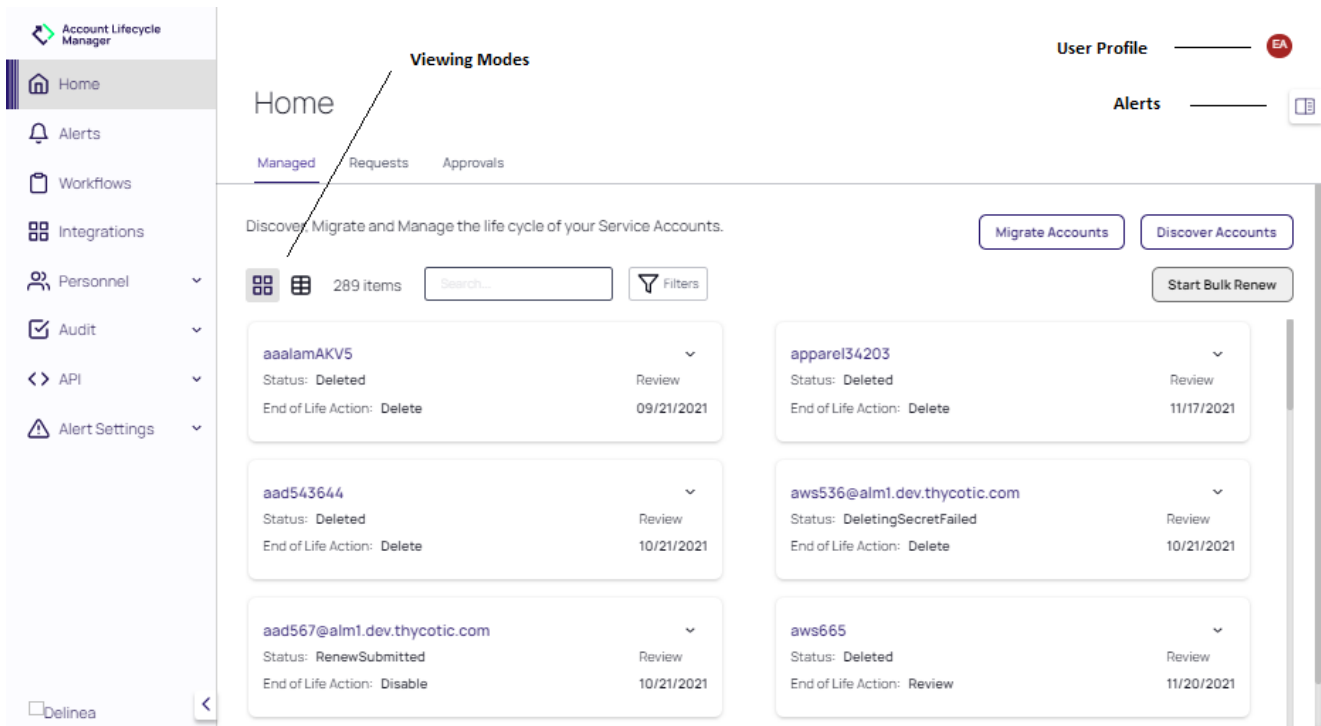


Navigating ALM

Account Lifecycle Manager provides a user interface (UI) for discovering, provisioning, and decommissioning user accounts.

The ALM UI has been refreshed with a new design and navigation to enhance user experience. Learn more about the Delinea experience [here](#).

Using ALM



The UI consists of the following functional areas:

- Left Navigation Panel - provides a fixed reference for accessing DSV functionality. Click Administration to manage DSV users, user groups, and roles. Secrets are managed in either a Shared Vault (team access) or a Home Vault (private access).
- Content Container - this main central area of the page updates with details for the selected feature. When applicable, certain pages allow the view to toggle between card and list mode. Click the Viewing Mode icons to toggle between these modes.
- User Profile - accesses general information for your user that includes assigned groups and roles, a link to ALM documentation, and logout.
- Alerts - Click the Alert icon to alternately open and close the Alerts panel.

Customizing the UI

To adjust the look and feel of the UI:

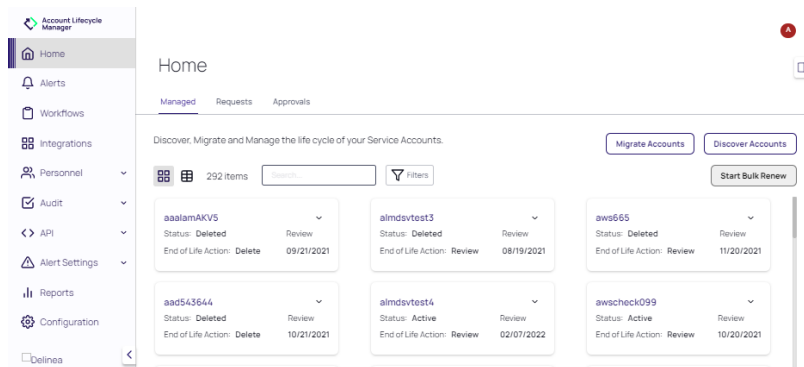
Click your User Profile. Selections for theme appear as **Toggle Theme to Dark**, **Toggle Theme to Light**, or **Toggle Theme to OS**. Click an option to toggle between light and dark modes, or default to the current OS settings for Windows clients.



Note: If **Toggle Theme to OS** is selected, the UI will follow the Windows selection made in Settings > Personalization > Colors.

Accounts Home

Click **Home** to view the Managed Accounts, requests for Managed Accounts, and their approval status in the application. The tabs on the **Home** page, access the following areas of functionality for Managed Accounts: **Accounts**, **Requests**, and **Approvals**.



Account features on the Home page include:

- **Account Discovery**, where administrators can import accounts using predefined workflow templates
- **Account Migration**, where administrators can move existing accounts to different workflow templates or between different versions of a template
- **Bulk Renew**, that allows updating of Managed Accounts that are within their review period

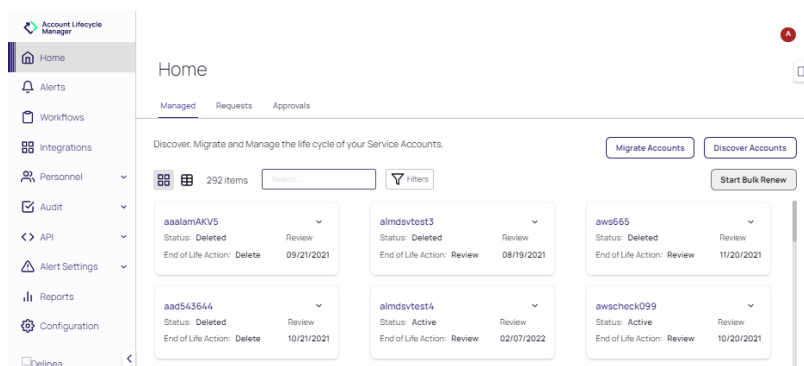
The tabs on the Home page include:

- **Managed** viewing and cloning existing Managed Accounts
- **Requests** provisioning of accounts and management of existing provisioned accounts
- **Approval** process for management of pending service account provisioning Requests

Viewing and Cloning Accounts

Accounts are used to run all services across your network. ALM helps to managed those accounts.

Click **Home** in the left navigation bar to view all accounts currently managed by ALM.



Viewing the Account Summary

Managed accounts can be viewed as cards or viewed as a list, using the Viewing Mode icons. When viewing a card, click the down arrow on a card to expand the card and view its summary fields. When viewing an account in list mode, column headers represent summary fields.

The following summary fields are provided for each account.

Field	Description
Name	The title used to identify the account in the user interface.
Status	Indicates the state of an account. Status indicators that may appear include: Deleted , Active , Expired , or Review Submitted , as well as Retrying . Failure indicators that may appear may include account actions such as expiring, enabling, or when disabling has failed, as well as if a renewal was rejected.
Review	The date the account is eligible for review as defined on the Workflow Template. The default is 15 days prior to the end of lifecycle date (expiration on). See End-of-Lifecycle Account Disposition Logic .
End of Lifecycle Action	The disposition defined for the account at its end of lifecycle. See End-of-Lifecycle Account Disposition Logic .
Workflow	The name of the Workflow Template assigned to the account. Refer to Building Workflow Templates for information regarding Workflow Templates.
Expires	The date when the account reaches its end of lifecycle and will be moved to the disposition defined by the end of lifecycle action.
Life Duration	The length of time that the workflow is actionable.
Description	The purpose, objective, and any descriptors that identify the account.

Viewing Account Details

In either Card mode or List mode, click the name of the account to access account details. The associated Account page is displayed.

The tabs on the Account page access the following details regarding the account:



Note: Certain fields in the account details are editable, indicated by an **Edit** link, when available.

- General
- Configuration
- Lifecycle
- Remote Account

Accounts Home

- Management
- History

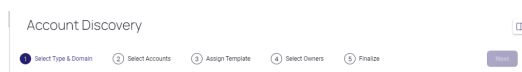
Cloning a New Account

When viewing account details, the **Actions** drop-down provides a **Clone as a New Request** option. Click **Clone as a New Request** to automatically recreate a request for a new account using the metadata from the current account. Refer to [Viewing and Creating Requests](#).

Discovering Accounts

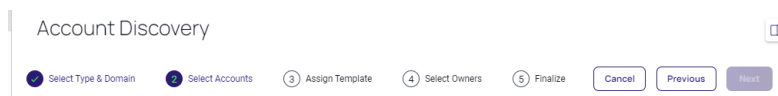
Using the **Account Discovery** wizard, administrators can import accounts using predefined workflow templates. Owners and attributes are specified during the discovery process. Administrators can specify attribute values to update in Active Directory/Azure AD or leave the values blank so they inherit the values present in Active Directory/Azure AD.

1. At the Home page, select the **Managed** tab. Then, click **Discover Accounts**.
2. **Select Type & Domain.**

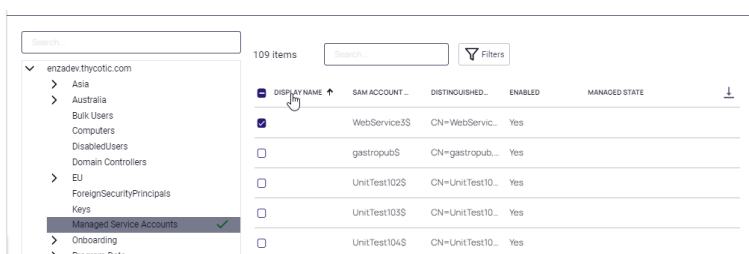


- a. From the **Account Type** drop-down menu, choose from Active Directory, Azure Active Directory, or Group Managed Service Account.
- b. From the **Domain** drop-down menu, select the Domain accounts will be migrated from. Accounts cannot be migrated between domains.
- c. Click **Next** in the upper right-hand corner.

3. **Select Accounts.**



- a. Choose the accounts to be migrated by clicking the check box to the left of the account name, or enable the check box next to the Search bar to select all accounts.



- b. Use the Search field to display all accounts that match the search criteria. Use the **Filter** drop-down to restrict the list of accounts to specific End of Lifecycle account types, Workflows, or accounts created on a

specific date.

- c. Click **Next** in the upper right-hand corner.

4. Assign Workflow Template.

- a. Select the workflow, review interval, review date, and owners for the accounts being imported. Click **Next**.

5. Select Owners.

- a. Next, assign owners for each account. You can set the owners for each individual account, or assign the same group of owners to all accounts.

NAME	Remove
Administrator	Remove
Alex Z	Remove
Alex Kaluski	Remove

- b. Click **Remove** next to a user or group in the list to remove the user or group from the account.

To add a user or group, click **Add** and select either **Add Users** or **Add Groups**. When prompted, select the users or groups to add as owners and click **Add**.

- a. Click **Next** in the upper right-hand corner.

6. Finalize.

Finalize

Review all the import information prior to confirming the import of the selected accounts.

Domain Name	enzadev.thycotic.com
Template Name	AD SS Connector Test
Review Interval	30x Days

1 item

- a. Review the domain name, workflow template, review interval, lifecycle end date, accounts, and owners. Change information by clicking on the previous steps. Make sure to click **Next** on any updated fields.

- b. Once you have verified that the information is correct, click **Complete** to finalize the wizard and move the accounts.

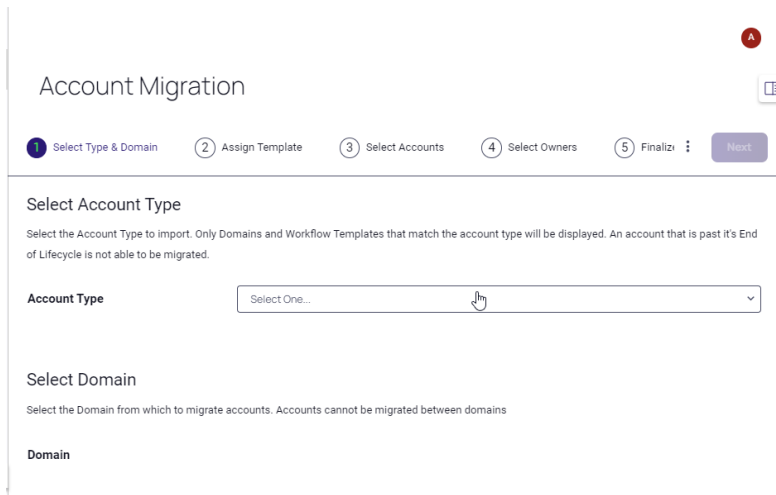
Account Migration

Using the **Account Migration Wizard**, administrators can move existing accounts to different workflow templates or between different versions of a template.

Migrating accounts from one workflow template to another may be desired when workflow templates have a version change. Administrators can also add additional attributes to be updated in Active Directory/Azure AD during this migration. Administrators can specify attribute values to update in Active Directory/Azure AD or leave the values blank so they inherit the values present in Active Directory/Azure AD.

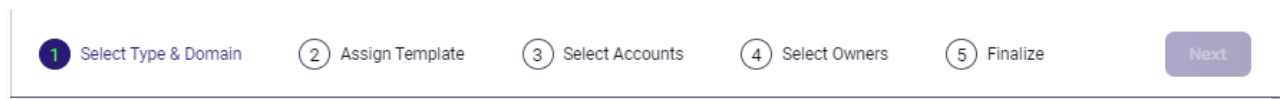
 **Note:** Only accounts that are *active* and *before* their end-of-lifecycle can be migrated.

1. At the Home page, select **Migrate Accounts**.



The screenshot shows the 'Account Migration' wizard interface. At the top, there is a progress bar with five steps: 1. Select Type & Domain (active), 2. Assign Template, 3. Select Accounts, 4. Select Owners, and 5. Finalize. A 'Next' button is located to the right of the progress bar. Below the progress bar, the main content area is titled 'Select Account Type'. It contains a text box with the placeholder 'Select One...' and a dropdown arrow. Below this, there is a section titled 'Select Domain' with a text box and a dropdown arrow. The text 'Select the Domain from which to migrate accounts. Accounts cannot be migrated between domains' is displayed above the domain selection area.

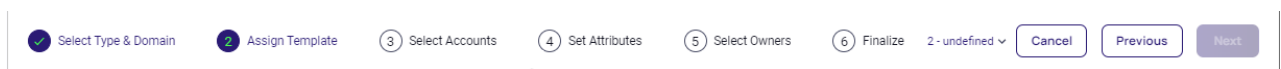
2. **Select Type & Domain.**



The screenshot shows the 'Account Migration' wizard interface at step 2: Assign Template. The progress bar now shows step 1 as completed and step 2 as active. The 'Next' button is still present. The main content area is titled 'Assign Template' and contains a text box with the placeholder 'Select One...' and a dropdown arrow. Below this, there is a section titled 'Select Domain' with a text box and a dropdown arrow. The text 'Select the Domain from which to migrate accounts. Accounts cannot be migrated between domains' is displayed above the domain selection area.

- a. From the **Account Type** drop-down menu, choose from Active Directory, Azure Active Directory, or Group Managed Service Account.
- b. From the **Domain** drop-down menu, select the Domain accounts will be migrated from. Accounts cannot be migrated between domains.
- c. Click **Next** in the upper right-hand corner.

3. **Assign Template.**



The screenshot shows the 'Account Migration' wizard interface at step 3: Select Accounts. The progress bar now shows steps 1 and 2 as completed and step 3 as active. The 'Next' button is still present. The main content area is titled 'Select Accounts' and contains a text box with the placeholder 'Select One...' and a dropdown arrow. Below this, there is a section titled 'Select Domain' with a text box and a dropdown arrow. The text 'Select the Domain from which to migrate accounts. Accounts cannot be migrated between domains' is displayed above the domain selection area.

- a. At the **Workflow** drop-down, select the available accounts to be migrated from. If the workflow is associated with a vault, only managed accounts with secrets in the same vault can be migrated to the selected template.

Assign Workflow Template

Pick the workflow, review interval, lifecycle end date, and owners for the accounts being migrated.

The selected workflow will dictate the accounts available to migrate. If the workflow is associated with a vault, only managed accounts with secrets in the same vault can be migrated to the selected template.

If you choose to **Reassign OU**, any account you select will be moved from their currently assigned OU to the OU specified by the selected workflow. If the workflow allows for child OUs to be selected, you can pick a specific child OU as the new OU for the accounts chosen in the next step.

Workflow

Review Interval

Lifecycle End Date

Keep Current Date ☐

Reassign OU ☐

- b. The selection for **Review Interval** determines when an accounts end of lifecycle will occur. Choosing a date in the past will cause the accounts to expire as of midnight (00:00) UTC.
- c. Enable **Keep Current Date** to leave each migrated account with it's current End of Life date.
- d. Enabling **Reassign OU** moves any selected account from its currently assigned Organizational Unit (OU) to the OU specified by the selected workflow. If the workflow allows for child OUs to be selected, a specific child OU can be selected as the new OU for the accounts to be migrated.
- e. Choose **Reassign Secret Folder** to limit the selection of accounts in the next step to only those accounts that have a secret associated with them. (This option is only available when Secret Server is used as the vault.)
- f. Click **Next** in the upper right-hand corner.

4. Select Accounts.

☒ Select Type & Domain
 ☒ Assign Template
 ☒ **Select Accounts**
☐ Set Attributes
 ☐ Select Owners
 ☐ Finalize

- a. Choose the accounts to be migrated by clicking the check box to the left of the account name, or enable the check box next to the Search bar to select all accounts.

Account Migration

☒ Select Type & Domain
 ☒ Assign Template
 ☒ **Select Accounts**
☐ Set Attributes
 ☐ Select Owners
 ☐ Finalize

13 Items

NAME	STATUS	WORKFLOW TEMPLATE	END OF LIFECYCLE ACTION	CREATED ON
☐ AADRAWSS3@almf.de...	Active	AADRAWSS3@almf V1.0	Review	03/28/2022
☒ AzKVSpace@almf.de...	Active	Rob-Az-KV-Test-000 V1...	Review	11/05/2021
☐ CheckID@almf.dew.thy...	Active	AADN5333 V1.0	Review	10/05/2021
☒ D187993@almf.dew.th...	Active	AAD/89@ V1.0	Disable	10/05/2021
☒ ERAZIAMTest@almf.de...	Active	ER-AZ-IAF V1.0	Review	09/01/2021

- b. Use the Search field to display all accounts that match the search criteria. Use the **Filter** drop-down to restrict the list of accounts to specific End of Lifecycle account types, Workflows, or accounts created on a specific date.
- c. Click **Next** in the upper right-hand corner.

5. **Set Attributes.**

Account Discovery

1 Select Type & Domain 2 Select Accounts 3 Assign Template 4 Select Owners 5 Finalize

Cancel Previous Next

- a. The list of available accounts are displayed in the **Accounts** panel on the left of the page. Select an account to populate its associated attributes. Select **Update All** to display attributes from all accounts.

 **Note:** For **Update All** operations, any attributes shared between accounts will be updated in bulk for all accounts. Additionally, attributes not present in an account will be added; attributes no longer defined in the migrated template will no longer appear.

Accounts ☒ Update All **Add Attributes**

2 Items

NAME	VALUE
MailNickname (MailN...	new server 903
UserPrincipalName (... Empty fields will use exists	

- b. If needed, edit the current value for an attribute. Blank values are supported. Blank values will be pulled in from Active Directory with bulk refresh.

 **Note:** Use blank fields to support unique values, otherwise the same value will be added in bulk to all accounts when performing an **Update All** operation.

- c. If needed, click **Add Attribute** to add a new attribute to the account. Available attributes will be limited to those on the template being migrated to. Select from the available attributes and click **Add**. If **Update All** is selected, the attribute will be added for all accounts.

- d. Click **Remove** to remove an attribute. That attribute will no longer be tracked in the managed account.

Note: **Remove** does not remove the attribute from the account in the domain.

- e. Click **Next** in the upper right-hand corner.

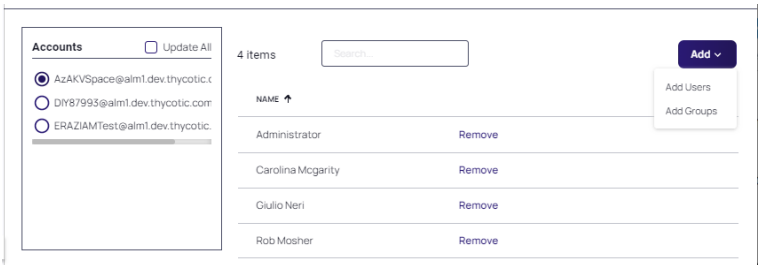
6. **Select Owners.**

1 Select Type & Domain 2 Assign Template 3 Select Accounts 4 Set Attributes 5 Select Owners 6 Finalize

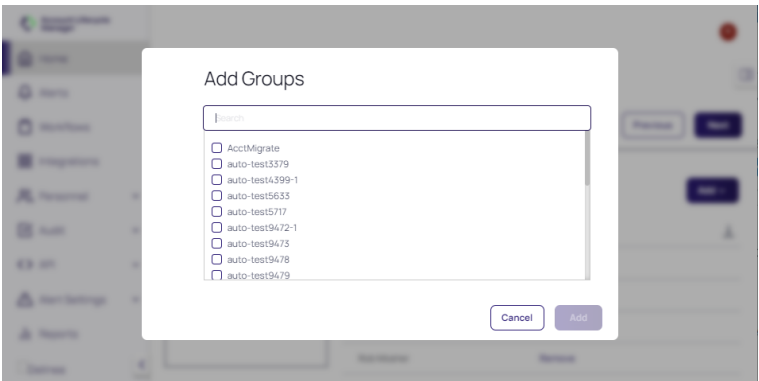
Cancel Previous Next

Accounts Home

- a. Next, assign owners for each account. You can set the owners for each individual account, or assign the same group of owners to all accounts. Click **Remove** next to a user or group in the list to remove the user or group from the account.

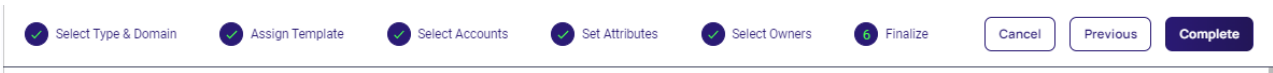


To add a user or group, click **Add** and select either **Add Users** or **Add Groups**. When prompted, select the users or groups to add as owners and click **Add**.



- b. Click **Next** in the upper right-hand corner.

7. Finalize.



- a. Review the domain name, workflow template, review interval, lifecycle end date, accounts, and owners. Change information by clicking on the previous steps. Make sure to click **Next** on any updated fields.
- b. Once you have verified that the information is correct, click **Complete** to finalize the wizard and move the accounts.

Bulk Renew

1. On the Home page, click **Start Bulk Renew** to display only accounts that are in the review period. The total number of accounts is reflected in the count displayed next to the Search field. (To exit from the bulk renew operation, click **End Bulk Renew**.)

Account Lifecycle Manager

Home

Alerts

Workflows

Integrations

Personnel

Audit

API

Alert Settings

Email Templates

Webhook Authorization

Webhooks

Reports

Configuration

Delinea

Home

Managed Requests Approvals

Discover, Migrate and Manage the life cycle of your Service Accounts.

Migrate Accounts Discover Accounts

110 items Search... Filters

End Bulk Renew

ACCOUNT NAME ↑	STATUS	END OF LIFE ACTION	REVIEW DATE
☐ AADRAWS228@alm1.dev.t...	Active	Review	05/03/2022
☐ AADRAWS343@alm1.dev.t...	Active	Review	03/27/2022
☐ almdsvtest2	Active	Review	08/18/2021
☐ almdsvtest4	Active	Review	02/07/2022
☐ almdsvtest4	Active	Review	03/03/2022
☐ almdsvtest5	Active	Review	03/02/2022
☐ almdsvtest5	Active	Review	02/07/2022
☐ almdsvtest6	Active	Review	02/07/2022

2. Enable the associated checkboxes for each account to be renewed. When all accounts for renewal have been selected, click **Renew**.
Depending on your workflow, you may be prompted for a new **Lifecycle End Date** for the lifecycle or you can edit the account **Description**.
3. At the **Renew Accounts?** prompt, click **Renew** again to confirm.

 **Note:** For accounts with the **Delete** or **Expire** end-of-lifecycle actions, a section of the dialog that appears allows the user to submit a note with the renew request. For accounts that allow a custom lifecycle end date, a section in the dialog that appears allows the user to select the end date.

Account Lifecycle Manager

Home

Alerts

Workflows

Integrations

Personnel

Audit

API

Alert Settings

Email Templates

Webhook Authorization

Webhooks

Reports

Configuration

Delinea

Home

ManagedRequestsApprovals

Discover, Migrate and Manage the life cycle of your Service Accounts.

Migrate AccountsDiscover Accounts

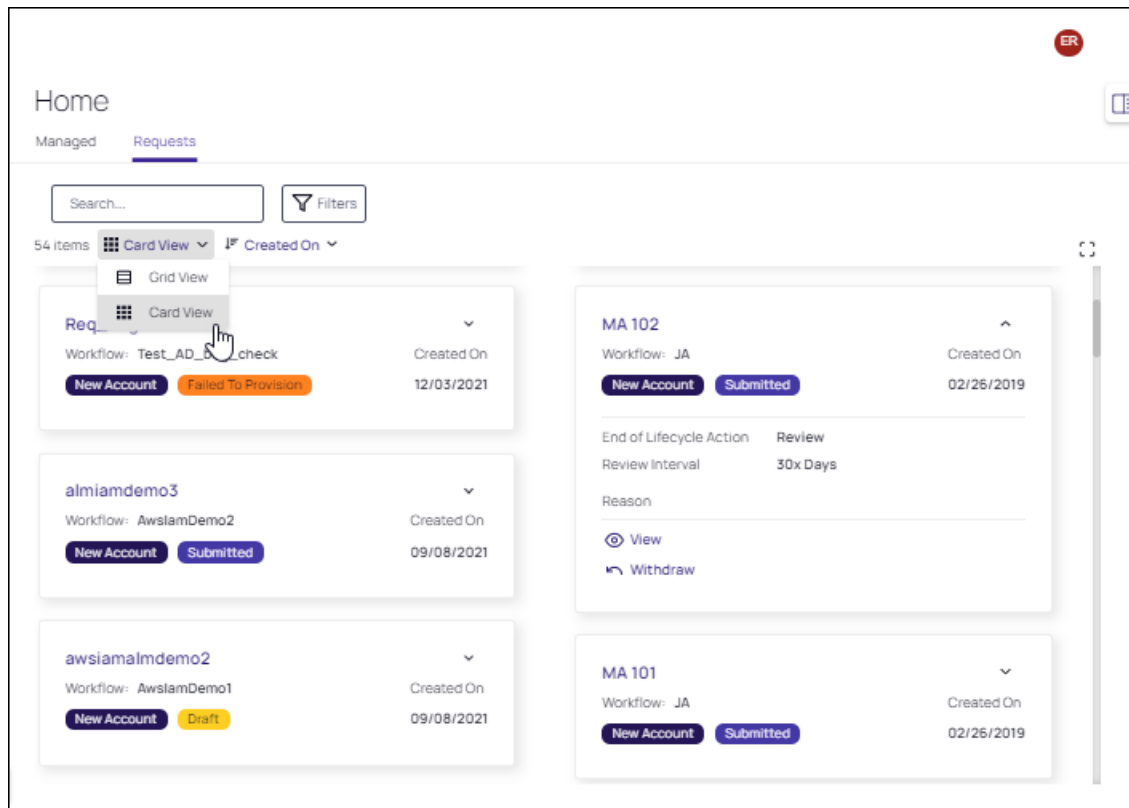
110 itemsSearch...FiltersRenew

ACCOUNT NAME	STATUS	END OF LIFE ACTION	REVIEW DATE
AADRAWS228@alm1.dev.t...	Active	Review	05/03/2022
AADRAWS343@alm1.dev.t...	Active	Review	03/27/2022
almdsvtest2	Active	Review	08/18/2021
almdsvtest4	Active	Review	02/07/2022
almdsvtest4	Active	Review	03/03/2022
almdsvtest5	Active	Review	03/02/2022
almdsvtest5	Active	Review	02/07/2022
almdsvtest6	Active	Review	02/07/2022

Viewing and Creating New Requests

Review New Requests

To address pending requests, select the **Requests** tab on the Home page for accounts. In Card view, click **View** to do to the request details. Click **Withdraw** to remove a submitted request from the workflow. **Edit** is only available if the request is in a draft state.



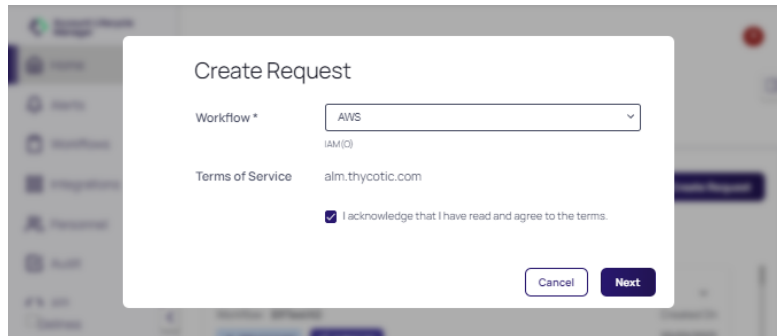
By default, approved and provisioned accounts are excluded in the accounts **Filter**.

- To view a customized subset of requests, click **Filter** and specify parameters that further limit the requests returned for display.
- The Requestor's reason for requesting the account appears in the **Reason** field.

 **Note:** The Request's reason is a required field.

Creating New Requests

1. On the Home page, select the **Requests** tab and click **Create Request** to generate a new request.
2. Select the Workflow Template that will be used to manage the request and acknowledge the request. Click **Next**.



Create Request

Workflow * AWS

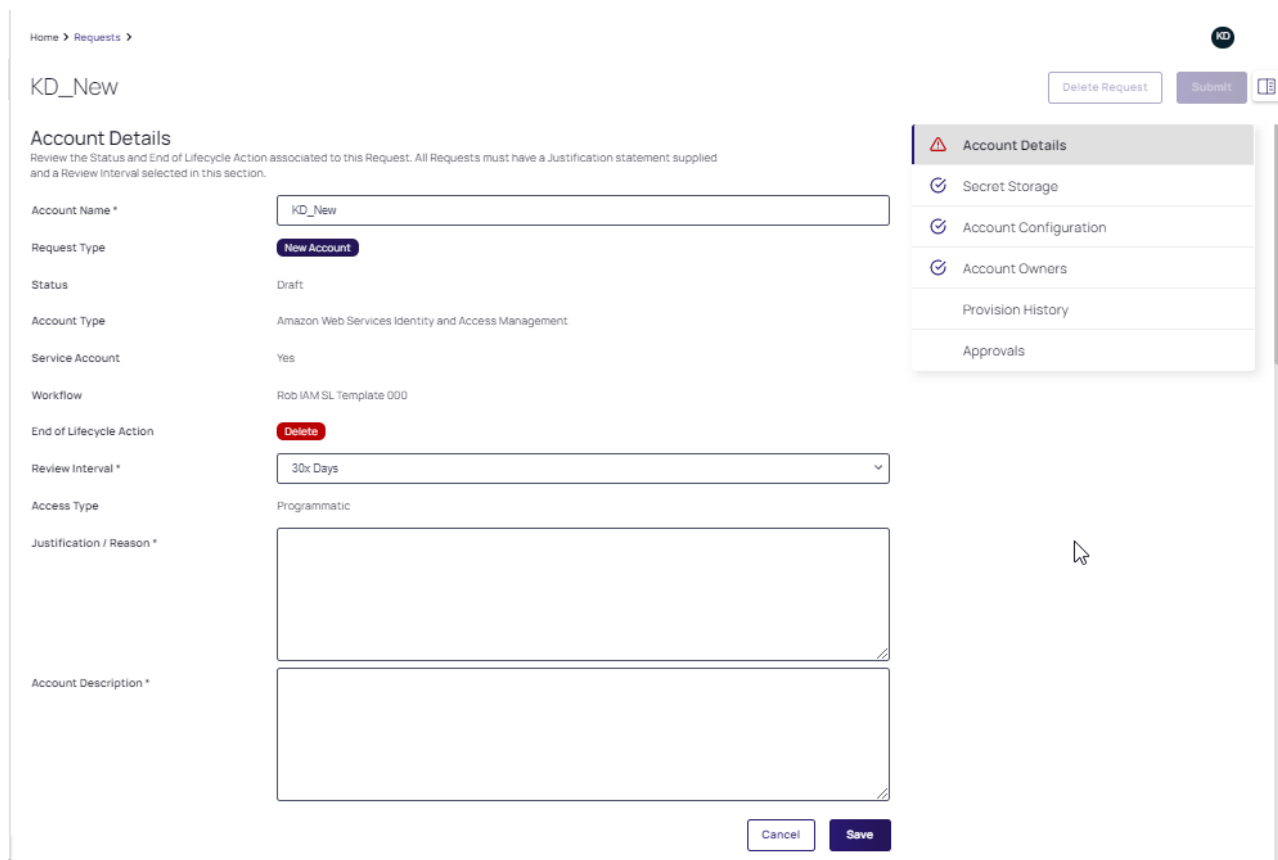
IAM (0)

Terms of Service alm.thycotic.com

☒ I acknowledge that I have read and agree to the terms.

Cancel Next

- Next, supply a name for the request and click **Create Request**.
- The newly created Request page displays. Supply information for the remaining parameters on the **Account Details** section. Required fields are indicated by an asterisk (*).



Home > Requests >

KD_New

Delete Request Submit KD

Account Details

Review the Status and End of Lifecycle Action associated to this Request. All Requests must have a Justification statement supplied and a Review Interval selected in this section.

Account Name * KD_New

Request Type New Account

Status Draft

Account Type Amazon Web Services Identity and Access Management

Service Account Yes

Workflow Rob IAM SL Template 000

End of Lifecycle Action Delete

Review Interval * 30x Days

Access Type Programmatic

Justification / Reason *

Account Description *

Cancel Save

- Account Details
- Secret Storage
- Account Configuration
- Account Owners
- Provision History
- Approvals

Scroll down the page or click a section in the right selection panel to view the current groups of parameters. Click **Save** when complete.

- If needed, click **Edit** to make updates in each group of parameters. At this time, the request is in a draft state and appears on the Requests page with a **Draft** tag.

Accounts Home

KD_New

Workflow: Rob IAM SL Template 000

Created On

New Account

Draft

04/26/2023

6. Click **Submit** when the request is complete. Click **Submit** at the confirmation prompt. The request appears on the Request page with a **Submitted** tag.

KD_New

Workflow: Rob IAM SL Template 000

Created On

New Account

Submitted

04/26/2023

Viewing Request Details

To view request details, click the **Name** of the request in either Card view or Grid view.

The Request Details page displays: **Account Details**, **Secret Storage**, **Account Configuration**, **Account Owners**, **Provision History**, and **Approvals**.

If the request has been submitted, **Withdraw Request** can be used to remove the request from ALM.

Home > Requests >

KD_New

Account Details

Review the Status and End of Lifecycle Action associated to this Request. All Requests must have a Justification statement supplied and a Review Interval selected in this section.

Account Name *

KD_New

Request Type

New Account

Status

Draft

Account Type

Amazon Web Services Identity and Access Management

Service Account

Yes

Workflow

Rob IAM SL Template 000

End of Lifecycle Action

Delete

Review Interval *

30r Days

Access Type

Programmatic

Justification / Reason *

Account Description *

Cancel

Save

Delete Request

Submit

Account Details

Secret Storage

Account Configuration

Account Owners

Provision History

Approvals

Approving Requests

On the Approvals page, the pending requests are listed.

Alerts

Account Lifecycle Manager

Home

Alerts

Workflows

Integrations

Personnel

Audit

API

Alert Settings

Reports

Configuration

Home

Managed Requests Approvals

Approve/Deny pending service account provisioning Requests or view the approval status of previous Requests.

38 items Search by Name, Requester, Type

ShortTest2

Requester: Kyle Bartholomew Create

Type: RenewExpired 04/13/2022

Workflow ShortTime

Account Owner Eric Remington

End of Life Action Expire

Review Interval 2x Days

Reason test

Deny Account

Approve Account

ADDefAttr

Requester: Rob Mosher Create

Type: New 09/29/2021

RobSnTest08

Requester: SNow Admin Create

Type: New 02/09/2021

RobWithdrawal

Requester: Rob Mosher Create

Type: New 09/24/2021

RobSnTest07

Requester: SNow Admin Create

Type: New 02/09/2021

almiamdemo3

Requester: Enza Requestor Create

Type: New 09/08/2021

Rob AD Internal 00

Requester: Rob Mosher Create

Type: New 02/09/2021

To approve or deny a request:

1. Click the down arrow (Card view) and click the **Name** of the request. In list view, clicking the **Name** of the request accesses the Request Details page directly.
2. Select the corresponding control to **Approve** or **Deny** the request.

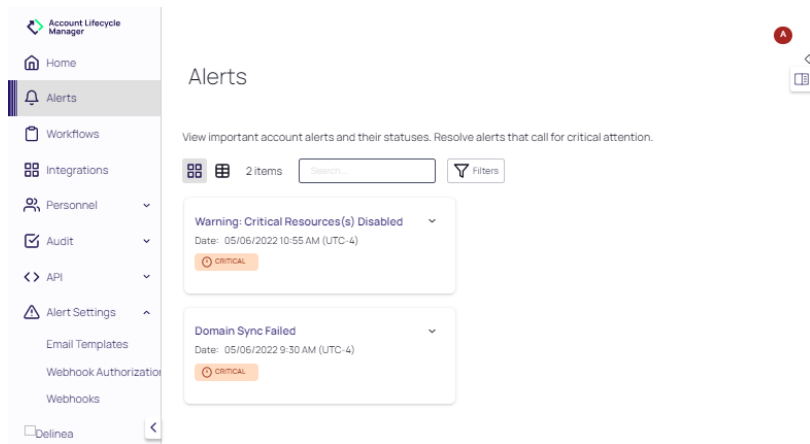
Approving the request will provision the Service Account and notify the Requestor that their account has been approved. Denying the request will notify the Requestor of the denial and the reason.

Alerts

The Alerts page displays important account alerts, the date and time the alert was generated and their statuses so that critical alerts can be addressed.

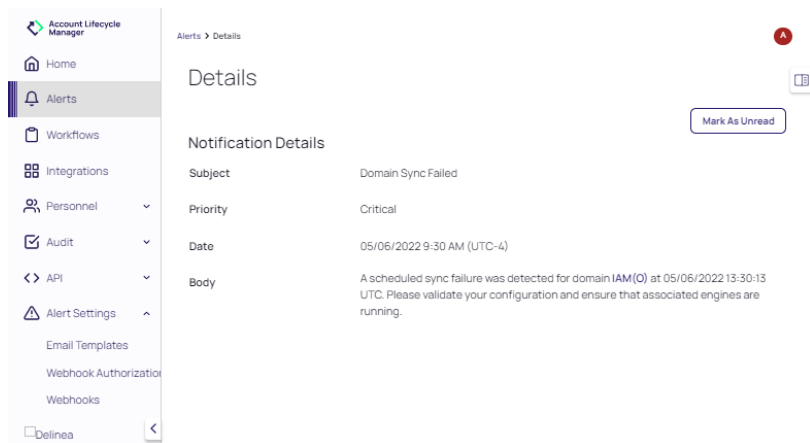
Click **Alerts** in the left navigation panel.

Workflows



Select any alert to view its Details page. After viewing an alert, you can update the disposition of the alert as either read or unread.

Click **Mark as Read** or **Mark as Unread**, as appropriate.



Workflows

Workflows in ALM define the approval processes for Service Accounts. Once a Template is completed and published, Requestors can use ALM to request that a Service Account be created.

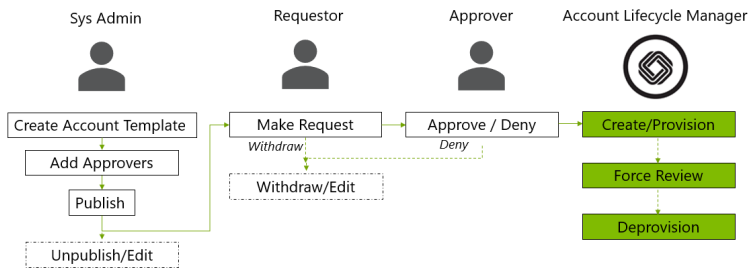
Overview

ALM supplies a straightforward, Roles-driven workflow system to support your oversight of new AD account creation, review, and eventual renewal or retirement.

ALM represents your approval processes as Workflow Templates. Each template defines the approval process for a particular service account kind or category as defined by your organization.

ALM's workflow system follows a simple, linear process from template definition through account Requests and Approvals.

Workflows



Workflow Template Fields

The fields that define a Workflow Template are defined by the [Workflow Template Wizard](#). The wizard is accessed when a Workflow Template is created and edited.

Workflow Template fields include:

- Template Details - basic descriptors that include: name, version, status, and EOL action.
- Secrets Vault - determines how Secrets are stored and managed by the workflow.
- Directory Services - describes the platform that manages and provisions the accounts.
- Ownership - restricts the ownership of the managed accounts.
- Account Lifecycle - determines how ALM actions the End of Lifecycle (EOL).
- Workflow Groups - the groups allowed to request managed accounts using the Workflow Template.
- Approval Flow - the steps that define the approvals required for account provisioning.

Building Workflow Templates

Create and manage Workflows from the Workflows page. Click **Workflow** in the left navigation panel. The Workflow Template is displayed.

The screenshot shows the 'Workflows' page in the Account Lifecycle Manager. The left navigation panel includes links for Home, Alerts, Workflows (selected), Integrations, Personnel, Audit, API, Alert Settings, Reports, Configuration, and Delinea. The main content area displays a table of workflow templates with 365 items. The table has columns for Workflow Template Name, Template Version, Status, Modified On, and Created On. A 'Create Template' button is visible in the top right corner.

Workflow Template ..	Template Version	Status	Modified On	Created On
AADetAWS3232@@	3.0	Published	05/04/2022	05/04/2022
test publish	1.0	Draft	05/04/2022	05/04/2022
n	1.0	Draft	04/20/2022	04/20/2022
mmknn	1.0	Draft	04/18/2022	04/18/2022
Test Create	1.0	Draft	04/07/2022	04/07/2022
AD Attributes Unpubli...	1.0	Draft	04/04/2022	04/04/2022
AADAWSR343%	1.0	Published	03/28/2022	03/28/2022

Create a Workflow

Use this procedure to create the Workflow Templates necessary to support your organization's use cases. You must have the System Administrator Role to perform this procedure, and you must have already connected ALM to your Secrets Vault.

- Click **Create Template** in the upper right hand corner to bring up the **Workflow Template Wizard**

Workflow Templates >

New Template

1 Setup 2 Vault 3 Directory Services 4 Ownership 5 Lifecycle 6 Groups 7 Approval Flow Next

Template Details
This tool will guide you through the process of creating and publishing a Workflow Template to use for creating managed accounts.

Template Name

Account Type

End of Lifecycle Action

Service Account ☒

Terms of Service

Purpose

1. Template Setup

- 1 Template Setup 2 Secrets Vault 3 Active Directory 4 Ownership Configuration 5 Account Lifecycle 6 Approval Flow

- Give the Template a name and select the **Account Type** from the drop-down menu. The Account Type should correspond to the directory service that will be used for this Template.
- Select an **End of Lifecycle Action**. Later in the wizard, you will choose the time interval for these actions to take effect.
 - Review-** a notification will be sent to the User reminding them that the Service Account is active. ALM will not change the Service Account at this point. Users are given the following options
 - **Renew-** extends the account's lifecycle until the next Review date. The renewal period starts at UTC 00:00.
 - **Disable-** deactivates the account in ALM and AD. The User **can** re-enable the account.
 - **Delete Account and Secret-** removes the Service Account.
 - Disable-** the Service Account will be automatically disabled unless it is **Renewed** by the Account Owner. Users are given the following options

- **Renew**- extends the account's lifecycle until the next Review date. The renewal period starts at UTC 00:00.
 - **Disable**- deactivates the account in ALM and AD. The User **can** re-enable the account.
 - **Delete Account and Secret**- removes the Service Account.
- iii. **Expire**- the Service Account will be automatically deactivated, but it can still be reactivated by repeating the Approval process. Users are given the following options
- **Submit for Approval to Renew**- the Account is submitted again to the Approvers. If approved, the account is renewed. If denied, the account will expire.
 - **Disable**- deactivates the account in ALM and AD. The User **can** re-enable the account.
 - **Delete Account and Secret**- removes the Service Account.
- iv. **Delete**- the Service Account is disabled, and **cannot be renewed**. Users are given the following options
- **Disable**- deactivates the account in ALM and AD.
 - **Delete Account and Secret**- removes the Service Account.
 - **Clone as New Request**- generates a new request identical to the provisioned account. The User then completes the new request and submits for approval.
- c. The **Terms of Service** should reflect your organization's guidelines for the use of new Service Accounts. The Requestor of the new account must agree to the terms you set before the account is provisioned.
- d. Enter the **Purpose** for the Workflow. The purpose will be provided to Users when they request a new account, so they know which template to choose for their request.
- e. Click **Save + Next**.

2. Secrets Vault

✓ Template Setup 2 Secrets Vault 3 Active Directory 4 Ownership Configuration 5 Account Lifecycle 6 Approval Flow

- a. For **System**, choose the Secrets Vault to use for Accounts on this Template. The **Type** of Vault should populate automatically based on your selection.
- b. For **Template**, choose the directory type associated with the workflow.
- c. Click **Select Folders** and choose where the secrets for this workflow will be stored. Checking **Allow Folder Override** will let the requestor choose folders within the selected index to store the account's secrets.
- d. Click **Save + Next**.

3. Active Directory

✓ Template Setup ✓ Secrets Vault 3 Active Directory 4 Ownership Configuration 5 Account Lifecycle 6 Approval Flow

- a. Choosing a **Name Prefix** is optional, but it is *highly recommended* that you use a prefix if your organization has a large number of Service Accounts. Using prefixes will make organizing large numbers of accounts easier.
- b. Defining **Name Regex** is also optional. Setting regex will force Requestors to follow specific naming conventions when using this Template. You can input any limiting pattern using *.NET native* regex.
- c. Select the **Active Directory Server** that Service Accounts on the template will use.
- d. For **OU Distinguished Name**, click **select** and choose the Organization Unit(s) that Service Accounts will belong to. Click **add**.
- e. Toggling **Allow Choosing Sub-OUs** to **Yes** will allow the Requester to choose a sub-ou within the folder you have designated. Toggling to **No** will restrict the Requester to only the OU you have designated.
- f. Use the drop-down menu to select the **Attributes** for the Service Accounts. You have the option to **Require** each attribute or mark it as **Read-only**. Click the **plus** to add the attribute. Edit the attribute using the **pencil** icon, or remove it by clicking the red **X**.
- g. Selecting **Groups** will limit access to this template to Users in the selected Group. Use the drop-down menu to find the Group and click the **plus**. You may add multiple Groups.

4. Ownership Configuration

✓ Template Setup ✓ Secrets Vault ✓ Active Directory ④ Ownership Configuration ⑤ Account Lifecycle ⑥ Approval Flow

- a. Toggling **Allow Group Ownership** to **Yes** will allow the newly created account to be shared among multiple owners without restrictions.
- b. Toggling **Allow Group Ownership** to **No** will bring up additional ownership options.
 - Toggling **Requester Only Owner** to **Yes** will restrict ownership of new accounts to only the Requester. Toggling to **No** will allow other users to have ownership of the account.
 - Set the number of **Minimum Owners** and **Maximum Owners** for new accounts using this template.

5. Account Lifecycle

✓ Template Setup ✓ Secrets Vault ✓ Active Directory ✓ Ownership Configuration ⑤ Account Lifecycle ⑥ Approval Flow

- a. The **Review/Expire Period Options** section shows the lifecycle length options that will be available to the Requestor when they request a new account. You can customize the options by editing the **number field** and selecting **Day(s)** or **Year(s)**. Click the **plus** to add the option.
- b. **Enable re-approval before end of lifecycle** will allow the Account Owner to request a renewal of the account before the chosen date of Review/Expiration. Use the arrows to set the re-approval time period.
- c. Check **Send notification when renewal is available** to automatically notify the Account Owner when re-approval is available.

- d. You can have the renewal notification resent at intervals. Check **send reminder to owner** and use the arrows to set the interval that ALM will send notifications.
- e. You can also have more frequent reminders sent. Check **Send urgent notifications** and use the arrows to set an hourly interval to send reminders and the number of days before the end-of-lifecycle to begin sending the hourly reminders.
- f. Check **Include system administrators** to have ALM send the reminder to the Account Owner and the System Admin.
- g. To stop reminders automatically, check **Stop sending notifications** and use the arrows to select the number of days after the start of notifications to stop sending.

6. Approval Flow

✓ Template Setup ✓ Secrets Vault ✓ Active Directory ✓ Ownership Configuration ✓ Account Lifecycle ⑥ Approval Flow

- a. Toggling **Hide Approver Names From Requesters** to **Yes** will restrict users requesting a new account from seeing who in the organization can approve their request.
- b. The Approval Flow will dictate which approvals are required before the account is provisioned.
- c. Click **Add** to add a step to the Approval Flow.
- d. From the **Actions** drop-down list, select a User or Group of Users that can Approve new Accounts using this template.
- e. In the **Require at least** box, use the arrows to change the number of approvers needed from the list of Users/Groups.
- f. You can add another step to change the number of approvals needed from separate Groups or Users by clicking **Add Step** from the Actions drop-down.
- g. Click **Publish** to finish creating the template. **Once a Template is Published, it cannot be edited further without first being unpublished.**

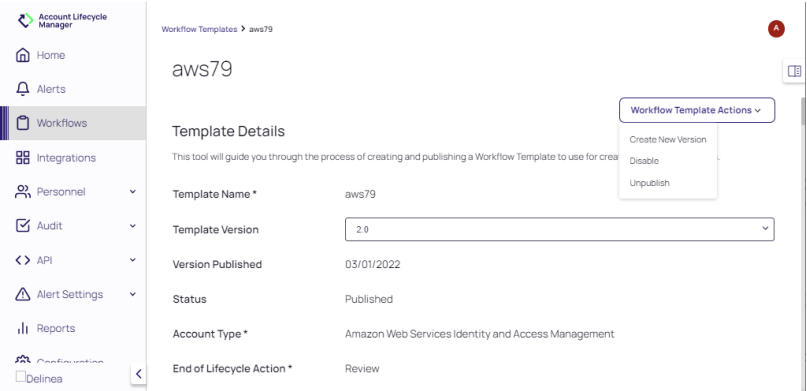
 **Note:** Requiring approval from one, specific individual can create a bottleneck. To avoid creating a bottleneck, Delinea recommends choosing a Group of managers and requiring two approvers.

Managing Workflow Templates

Review and make changes to a Workflow Template by clicking on the Template Name to bring up the Template page.

Select the desired action from the **Workflow Template Actions** pull-down. The actions available depend on the **Status** of the Workflow Template.

Workflows



Action	Template State	Description
Create New Version	Published	Updates the version of the Workflow Template
Disable	Published	Requestors will no longer be able to select this Template when requesting a new Service Account
Unpublish	Published	Returns the Workflow Template to a Draft Status and allows editing
Edit	Draft	Before a Workflow Template is published, you can edit the Template Setup, Secrets Vault, Active Directory, Account Lifecycle, and Approval Flow. Select Edit to access the template wizard. Published Templates must be unpublished before they are edited.
Delete	Draft	Removes the Workflow Template from the application

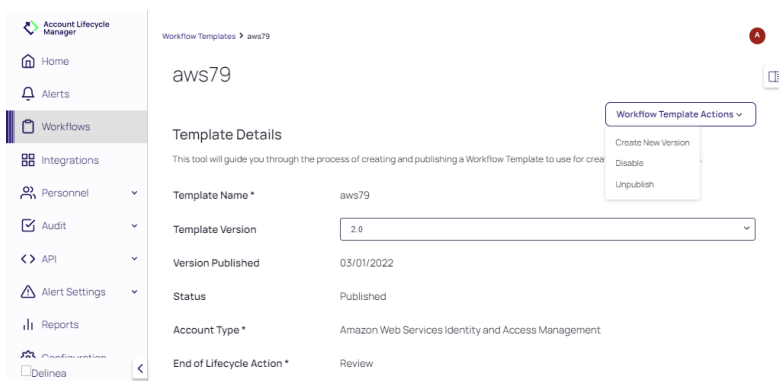
Workflow Template Versioning

Workflow Template versioning allows System Administrators to update a published Workflow without needing to disable or unpublish the Template.

To create a new version of an existing Workflow Template:

Managing Integrations

1. Open the Template and select **Create New Version**.

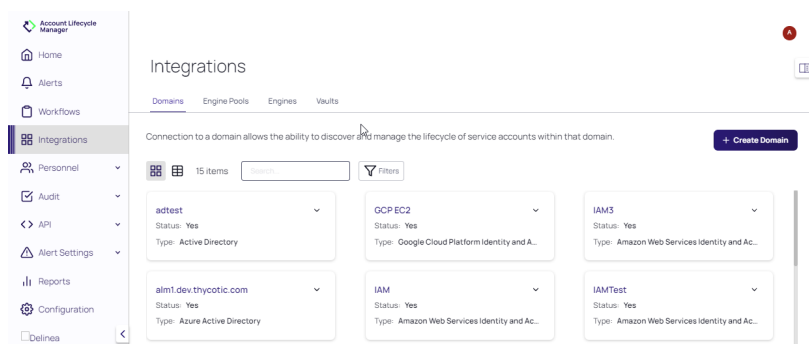


2. ALM will prompt for confirmation that the System Administrator wants to create a new version of the Workflow Template.
3. When a new version of a Workflow Template is published, all new Account Requests will use the newest Template version.
4. All accounts previously provisioned to prior versions will remain associated to the version they were provisioned against.

Users with permissions to access Workflow Templates will be able to view the specification of previous versions for change tracking. The Managed Accounts view will display which version of a Workflow Template the account is provisioned against.

Managing Integrations

Click **Integrations** in the left navigation panel to view the currently configured domains, engine pools, engines, and vaults.



The tabs available on the Integration page allow you to manage these configurations after [Initial ALM Setup](#) with the following features:

- [Managing Domains](#) - viewing, creating, editing and deleting domains.
- [Managing Engine Pools](#) - viewing, creating, and editing engine pools.

Managing Integrations

- [Managing Engines](#) - viewing, downloading, activating, disabling, and reassigning engines.
- [Managing Vaults](#) - viewing, creating, and editing vaults.

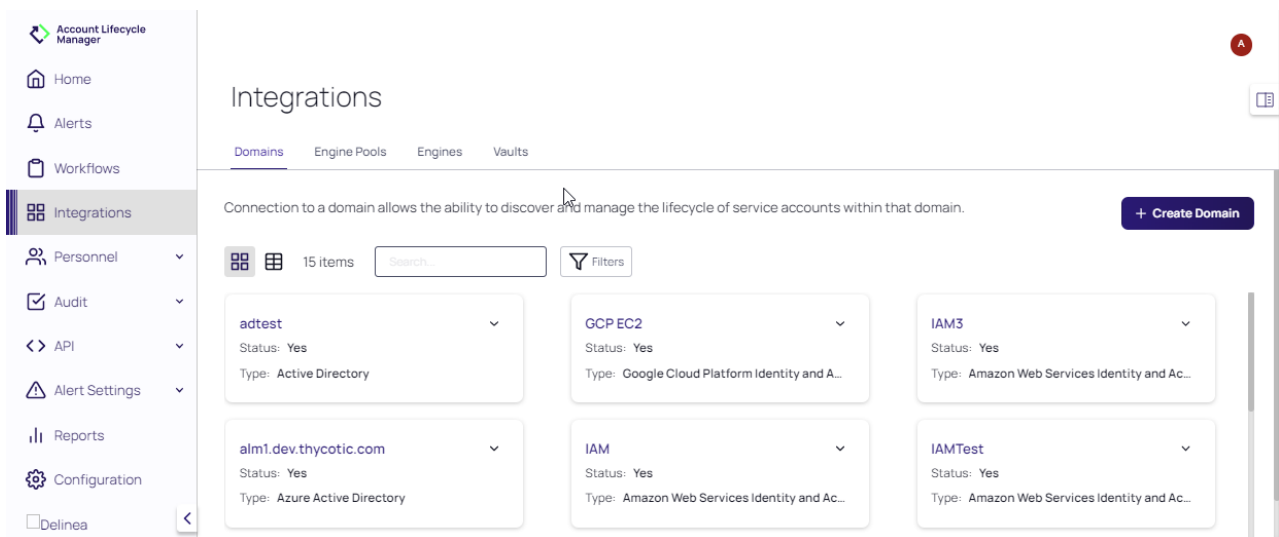
Managing Domains

Domains provide the means to discover and manage the lifecycle of service accounts within that domain.

Viewing Domains

To view the domains currently integrated with ALM:

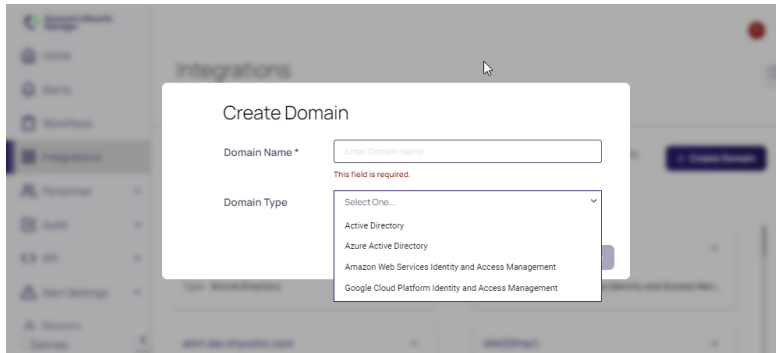
1. Select **Integrations** in the left navigation panel.
2. Select the **Domains** tab. The currently integrated domains are displayed.



Domains can be viewed as cards or viewed as a list, using the Viewing Mode icons. When viewing a card, click the down arrow on a card to expand the card and view its summary fields. When viewing a domain in list mode, column headers represent summary fields.

Creating a Domain

1. On the Integrations page, click **Create Domain**.



2. Specify a **Domain Name** and select the **Domain Type** from the available domains integrated into the application.
3. Click **Create Domain**. The domain appears in the list of domains on the Integration page.

Viewing Domain Details

1. On the Integrations page, click the name of the domain to access the Domain Details page.

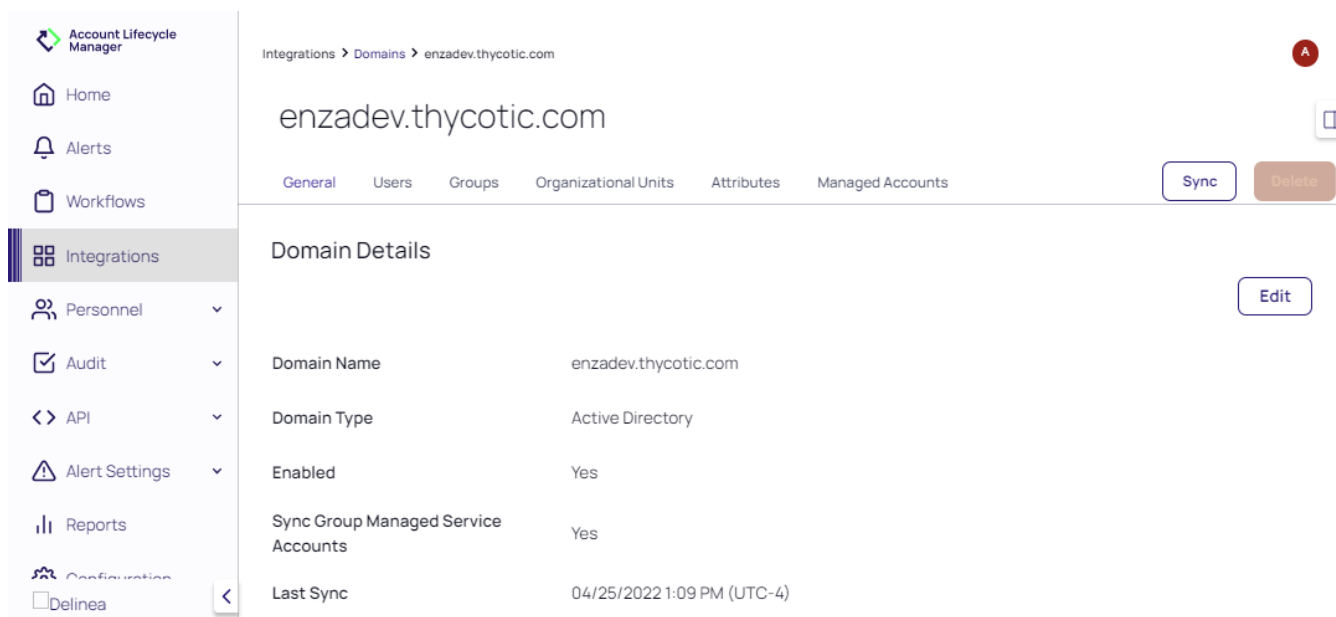
The **General** tab on the Domain Details page identify the name, type, enabled/disabled state, sync status, and sync schedule.

Note: The tabs available on the Domain Details page are dependent on the type of domain selected (for example: existing users, groups, and organization units, resources, attributes, and Managed Accounts).

Editing Domains

1. On the Integrations page, select a domain to access the Domain Details page.

Managing Integrations



1. Select the tab with the parameters to edit.

Note: The parameters available for editing are dependent on the type of domain selected.

The **Users**, **Groups**, and **Organizational Units** tabs provide functionality for adding, syncing and deleting the users, groups, and organizational units.

Likewise, the domain's attributes, resource, and Managed Accounts can be viewed, added, and synced on the **Attributes**, **Resources**, and **Managed Accounts** tabs, respectively.

1. Select **Edit** and replace the desired values.
2. Click **Save**.

Deleting Domains

1. On the Integrations page, select a domain to access the Domain Details page.
2. Click **Delete**.
3. At the **Delete Domain?** confirmation prompt, click **Delete**.

Managing Engines

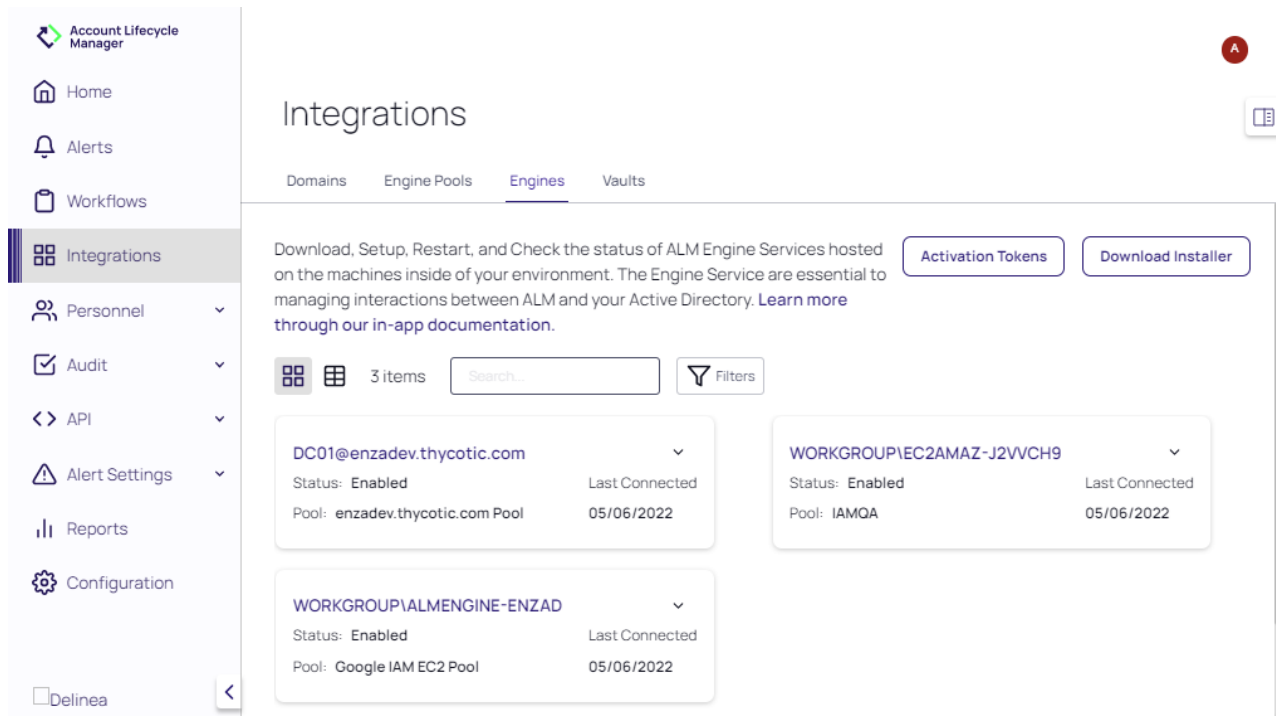
The Engine Service are essential to managing interactions between ALM and your Active Directory.

Viewing Engines

To view the engines currently integrated with ALM:

Managing Integrations

1. Select **Integrations** in the left navigation panel.
2. Select the **Engines** tab. The currently integrated engines are displayed.



Engines can be viewed as cards or viewed as a list, using the Viewing Mode icons. The name, **Status**, associated **Pool**, and **Last Connected** date and time for each engine is provided.

Downloading an Engine

1. On the Integrations page, select the **Engines** tab and click **Download Installer**.

The alm_engine_svc_x86.zip file is copied to the download folder.

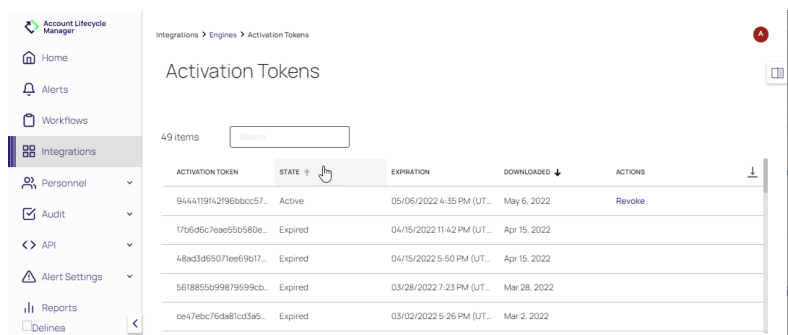
Reviewing Activation Tokens

1. On the Integrations page, select the **Engines** tab and click **Activation Tokens**.

The **ACTIONS** column allows you to revoke any token.

Managing Integrations

2. Locate the desired token and make any necessary changes to **Revoke** the token.



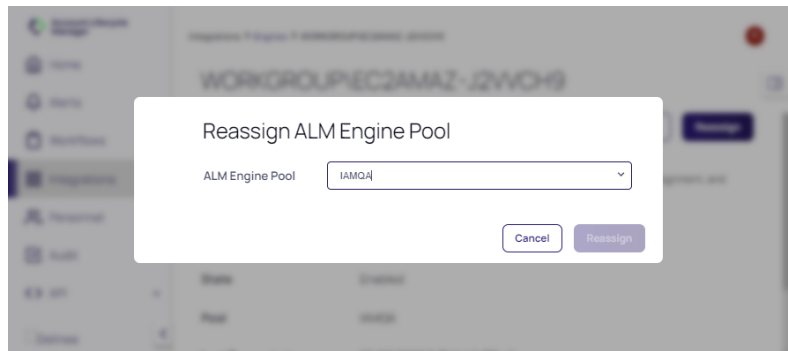
Viewing, Enabling/Disabling and Reassigning Engines

The Engine Details page allows for enabling and disabling of an engine, engine pool assignment, and viewing the time an engine last connected to ALM.

1. On the Integrations page, select the **Engines** tab and click the name of the engine to access the Engine Details page.



2. Depending on the current state of the engine, click **Enable** or **Disable** to update the status of the engine, if needed.
3. If an engine needs to be reassigned to another engine pool, click **Reassign**.
4. At the **Reassign Engine Pool** prompt box, select the new engine pool and click **Reassign**.



Managing Engine Pools

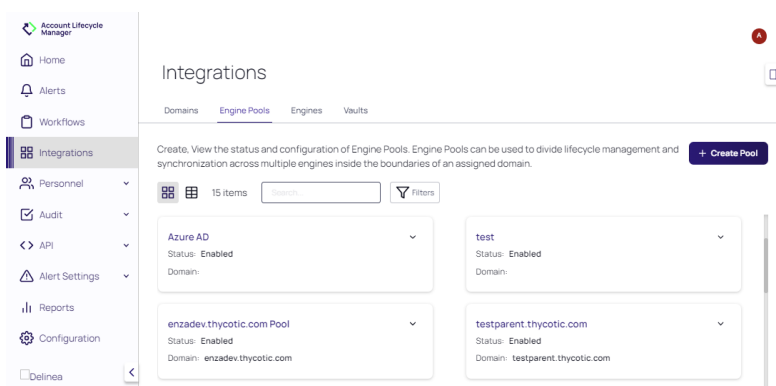
Engine pools can be used to divide lifecycle management and synchronization across multiple engines inside the boundaries of an assigned domain.

Viewing Engine Pools

To view the engine pools currently integrated with ALM:

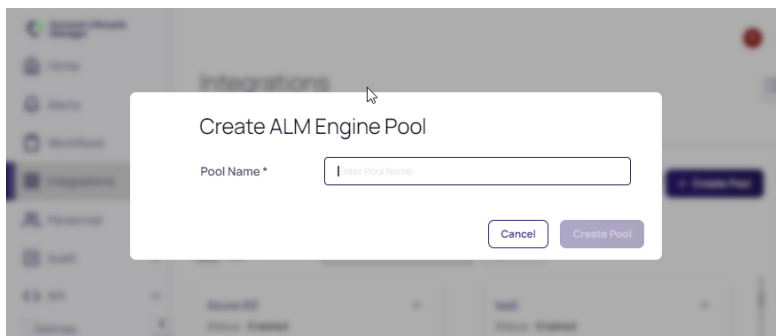
1. Select **Integrations** in the left navigation panel.
2. Select the **Engine Pools** tab. The currently integrated engine pools are displayed.

Engine pools can be viewed as cards or viewed as a list, using the Viewing Mode icons. The name, **Status** and **Domain** for each engine pool is provided.



Creating an Engine Pool

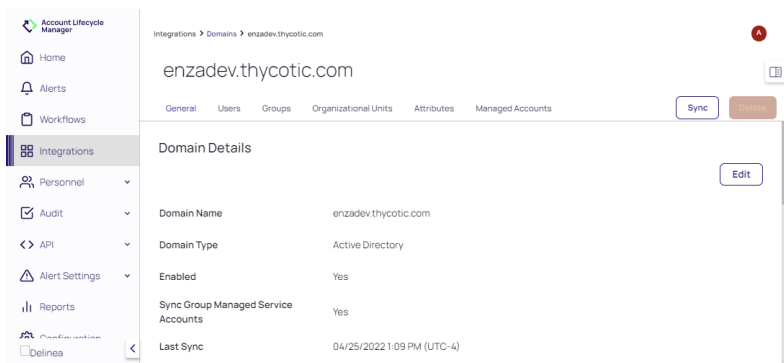
1. On the Integrations page, select the **Engine Pools** tab and click **Create Pool**.



2. Specify a **Pool Name**.
3. Click **Create Pool**. The engine pool appears in the list of engine pools on the Integration page.

Viewing and Editing Engine Pool Details

1. On the Integrations page, select the **Engine Pools** tab and click the name of the engine pool to access the Engine Pool Details page.



2. Select **Edit** and replace the desired values for the **Manage Pool** and **Assigned Engines** parameters.
3. Click **Save**.

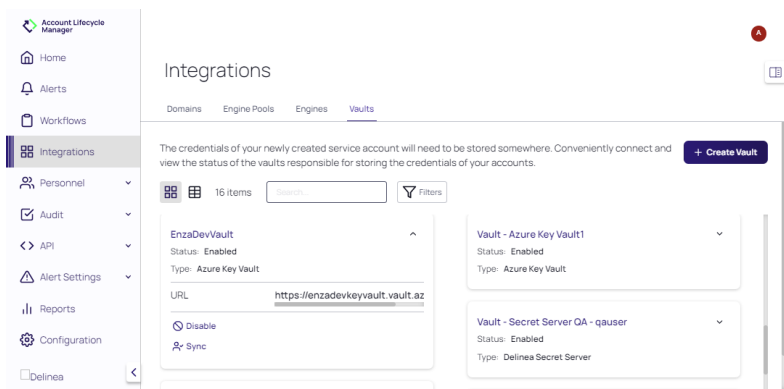
Managing Vaults

Vaults responsible for storing the credentials of your accounts.

Viewing Vaults

To view the vaults currently integrated with ALM:

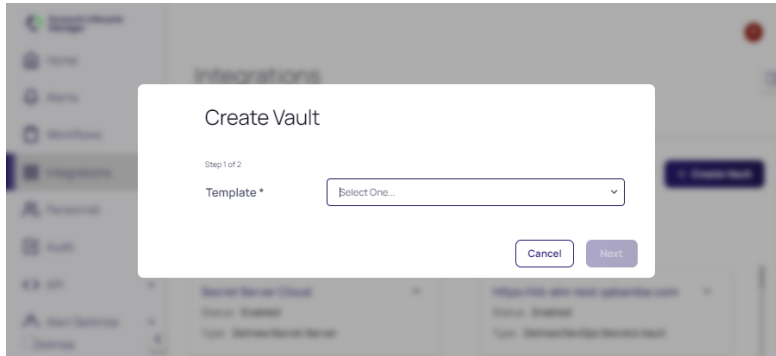
1. Select **Integrations** in the left navigation panel.
2. Select the **Vaults** tab. The currently integrated vaults are displayed.



Vaults can be viewed as cards or viewed as a list, using the Viewing Mode icons. When viewing a card, click the down arrow on a card to expand the card and view its summary fields. When viewing a domain in list mode, column headers represent summary fields.

Creating a Vault

1. On the Integrations page, click **Vaults**, then click **Create Vault** on the Vault Details page.
2. At the **Create Vault** prompt box, select template used to create and manage the vault and click **Next**.



3. Supply the requested parameters according to the template selected for use and click **Create Vault**.

Viewing and Editing Vault Details

1. On the Integrations page, select the **Vaults** tab and click the name of a vault to access the Vault Details page.

The **General** tab on the Vault Details page identifies the **Vault Template**, **Display Name**, **URL**, and where the vault is **Enabled** or **Disabled**.

 **Note:** The tabs available on the Vault Details page are dependent on the type of domain selected (for example: templates, engines, folders).

2. Click **Edit** to update the available values on any tab and click **Save**.
3. Click **Sync** to sync changes.

Working with Personnel

This section covers the following administrative topics.

Users

Thycotic One accounts

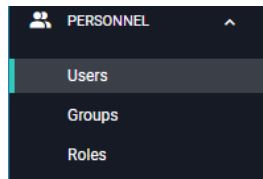
Users log into ALM using their **Thycotic One** account. New Users can create an account at [Thycotic One](#).

Creating ALM Users

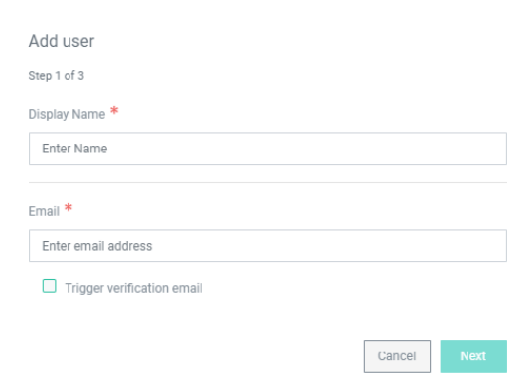
To create a new ALM User

Working with Personnel

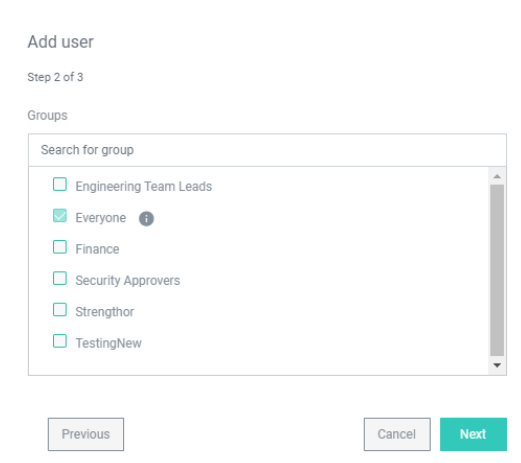
1. On the left-hand navigation menu, open the **PERSONNEL** drop-down and click **Users**.



2. In the upper right-hand corner, click **Create User**. The **Add user** window appears.

A light gray window titled 'Add user' with a subtitle 'Step 1 of 3'. It contains two text input fields: 'Display Name *' with a red asterisk and 'Email *' with a red asterisk. Below the email field is a checkbox labeled 'Trigger verification email'. At the bottom right are 'Cancel' and 'Next' buttons.

3. Enter a **Display Name** and **Email** for the new user. Checking the **Trigger verification email** box will send the new User an email alerting them of the new account and asking them to verify their login before use.
4. Click **next** to continue to the **Groups** window.

A light gray window titled 'Add user' with a subtitle 'Step 2 of 3'. It features a 'Groups' section with a search bar labeled 'Search for group'. Below the search bar is a list of groups with checkboxes: 'Engineering Team Leads', 'Everyone' (checked), 'Finance', 'Security Approvers', 'Strengththor', and 'TestingNew'. At the bottom are 'Previous', 'Cancel', and 'Next' buttons.

5. Check the boxes of the Groups the new User belongs. By default, all Users belong to the *Everyone* group. Click **next** to continue to the **Roles** window.
6. Check the boxes next to the **Roles** to give the new User.

Working with Personnel

Add user

Step 3 of 3

Roles

Search for role

- ☐ TensorGate Operator Class 4
- ☐ new
- ☐ ProvisionApprover
- ☒ ProvisionRequestor ⓘ
- ☐ Custom Role Demo
- ☐ Audit2
- ☐ ProvisionTest

[Previous](#) [Cancel](#) [Save](#) [Save and add another](#)



Tip: Users automatically inherit Roles from the Groups they are assigned.

- Click **Save** to create the User. Click **Save and add another** to create the User and then start the process over to create another new User.

Managing Users

- Clicking on a User's **Display Name** from the User List will bring up the management page. You can edit a User's Roles, Groups, email and display name from the **Manage User** page.

Personnel > Users

Q Search Name, Email

NAME ▾

Test User

Personnel > Users > Approver

[Manage User](#) [Emails](#) [Groups](#) [Roles](#)

Manage User

Users represent each authenticated person using ALM. For managing a User you have the ability to change the name of the User, as well as enabling/disabling the User. Disabling a User will prohibit the user from performing any functions in ALM, including authentication.

ALM Users can be linked to Ldap Active Directory users. Linking a user will enable or disable the ALM in to match changes in Ldap Active Directory.

Display Name

Approver

Enabled No ☒ Yes

Linked AD Account None

Change Display Name

- Click **Edit** to the right of the User's name to change their **Display Name**.
 - Enter the new name in the *Edit Display Name* window. Click **Update** for the change to take effect.

Enable/Disable User

- Use the green toggle switch to **Enable** and **Disable** the User account. Disabling the account will revoke the user's access within ALM. You can return the User's permissions by clicking **Enable**.

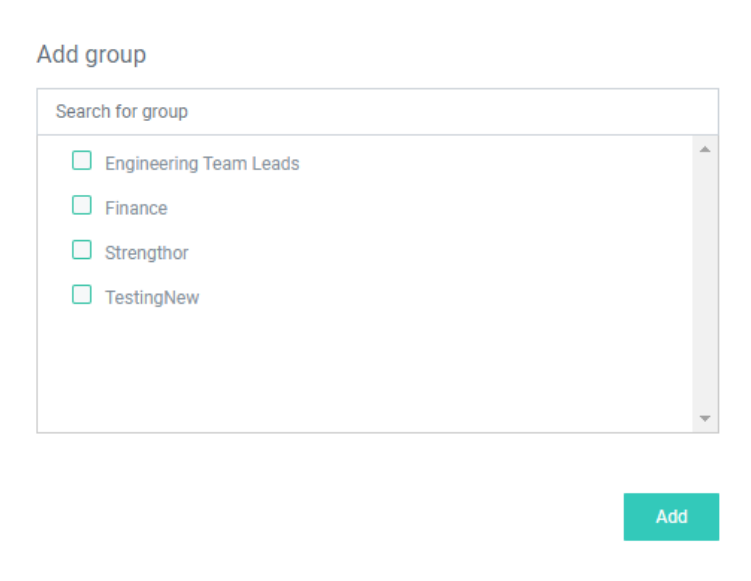
Add User email

- Select the **Emails** tab. Click **Add email** to assign the User an additional address. Notifications for this User will be delivered to all listed addresses.

Add/Remove User Groups

Groups can be added/removed from the **Groups tab** at the top of the screen.

- To add a Group
 - Click **Add group** to bring up a list of available groups.



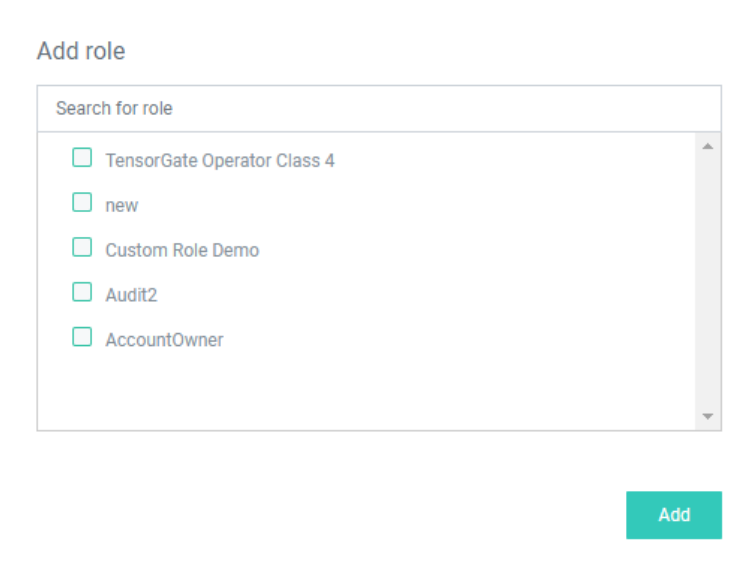
- Check the boxes next to the new Group(s) for the User and click **Add**.
- To remove a User from a Group
 - On the right side of the Group name row, click **Remove**.

Add/Remove User Roles

Roles can be added/removed from the **Roles tab** at the top of the screen. The Roles that the User has are listed in the Role row.

Working with Personnel

- To add a User Role
 - Click **Add role** to bring up a list of available Roles.



Add role

Search for role

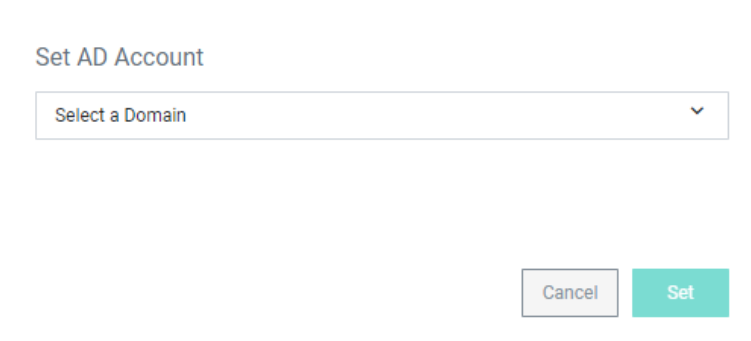
- ☐ TensorGate Operator Class 4
- ☐ new
- ☐ Custom Role Demo
- ☐ Audit2
- ☐ AccountOwner

Add

- Check the boxes next to the new Role(s) for the User and click **Add**.
- To remove a User Role
 - On the right hand side of the Role name row, click **Remove**.

Link an Active Directory Account

- To link the User to an AD Account
 - On the right side of the Linked AD Account row, click **Locate AD Account** to bring up the *Set AD Account* window.



Set AD Account

Select a Domain

Cancel Set

- Select a domain from the drop-down list and click **Set** to link the User's ALM and AD accounts.

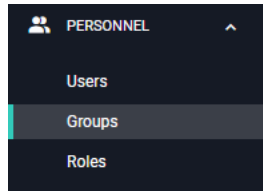
Groups

Groups define privileges for categories of Users. Using Groups, you can assign the same Roles and permissions to multiple Users.

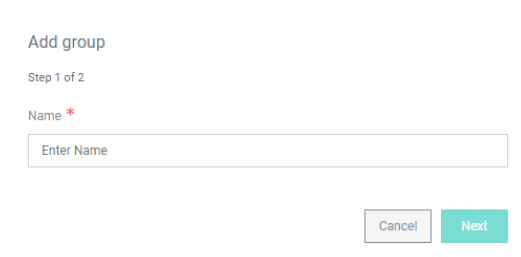
 **Note:** ALM Groups do **not** correspond to Active Directory Groups.

Creating Groups

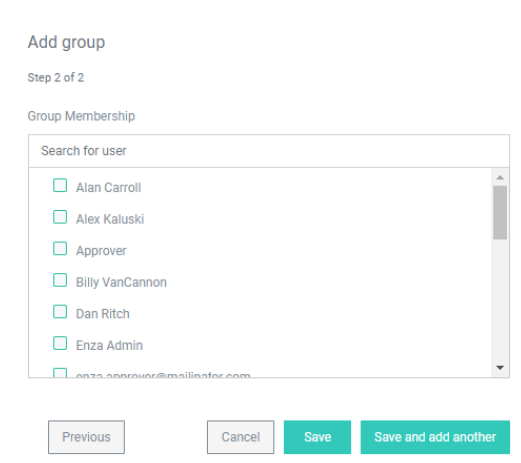
1. Using the left-hand navigation menu, click **PERSONNEL** and then click **Groups** to open the Groups page.



2. In the upper right-hand corner, click **Create Group**. The **Add group** window appears.

A light gray window titled 'Add group' with 'Step 1 of 2' below it. It contains a label 'Name *' and a text input field with the placeholder 'Enter Name'. At the bottom right are two buttons: 'Cancel' and 'Next'.

3. Enter a Name for the new Group and click **Next**.
4. On the **Group Membership** window, choose the Users to add to the group by **checking** the box next to each name.

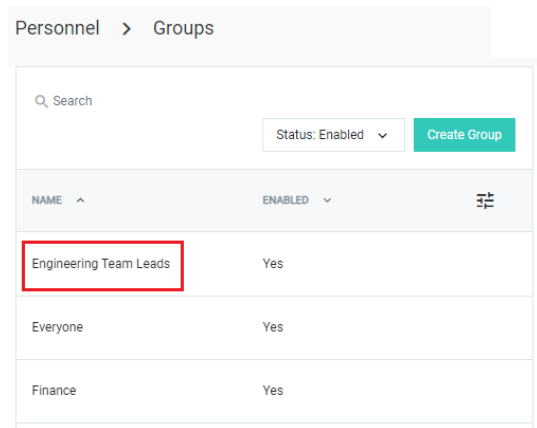
A light gray window titled 'Add group' with 'Step 2 of 2' below it. The section is labeled 'Group Membership'. It features a search bar 'Search for user' and a list of users with checkboxes: Alan Carroll, Alex Kaluski, Approver, Billy VanCannon, Dan Ritch, Enza Admin, and jess.vancannon@mollietec.com. At the bottom are four buttons: 'Previous', 'Cancel', 'Save', and 'Save and add another'.

5. Click **Save** to create the Group. Click **Save and add another** to create the group and restart the process for another new Group.

Managing Groups

To manage a group, click the **Group name** on the Groups page.

Working with Personnel



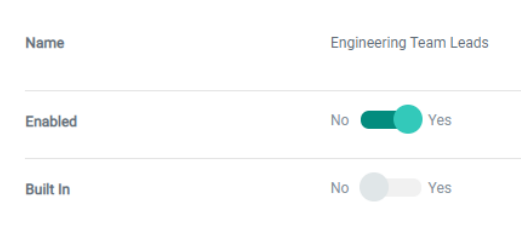
From the Manage Groups page, you can enable/disable the Group, add/remove Users, and add/remove Roles.

Enable/Disable Group

Enabling a group will give the Group's permissions to Users in the Group. Groups are enabled by default.

Disabling a group will remove the permissions Users are given from membership in the Group. Disabling will **not** disable the Users, only their permissions from the Group.

- To **enable** a Group, click the green switch so the dot points to **Yes**.



- To **disable** a group
 - Click the green switch so the dot points to **No**.
 - If the Group is attached to a Workflow Template, you will be given the option to **replace** the Group in the Workflow. Check the box next to the Group that will replace the Group you are disabling.

Working with Personnel

Replace Group

This Group is currently an Approver on the Workflow Templates below

☐	Workflow Template	Approval Step	Minimum Required Approval
☐	Engineering Template (Auto-Expire)	Step 1	1
☐	Engineering Template	Step 1	1

1 - 2 of 2<>

Would you like to replace this Group with another user or group to fulfill the Workflow Template Approval Step Process?

Cancel

Replace

Disable

- Click **disable**.

Add/Remove Users

To manage Users within the Group, click the **Users** tab next to Manage Group.

Manage Group

Users

Roles

Manage Group

For managing a Group you have the ability to change the name of the Group, as well as enabling/disabling the Group. Disabling a Group will not disable the Users within the Group. A Built In Group is one that has come pre-configured in ALM.

Note: ALM Groups do not correspond to Active Directory Groups.



To add Users to the Group

1. Click **Add User** in the top-right corner.
2. On the **Add user** window, check the boxes next to the name(s) of Users to add to the group.

Working with Personnel

Add user

Search for user

☐ Approver
☐ Billy VanCannon
☐ Dan Ritch
☐ Enza Admin
☐ enza.requestor@mailinator.com
☐ Grace Kim
☐ Justin Gordon

Add

3. Click **Add**

To remove Users from the Group

- Click the **X** to the right of the User's name.

5 Users in this Group [Add User](#)

NAME	ACTIONS
enza.approver@mailinator.com	X

Add/Remove Roles

To manage Roles within the Group, click the **Roles** tab next to Manage Group.

[Manage Group](#) [Users](#)

Roles

Manage Group

For managing a Group you have the ability to change the name of the Group, as well as enabling/disabling the Group. Disabling a Group will not disable the Users within the Group. A Built In Group is one that has come pre-configured in ALM.

Note: ALM Groups do not correspond to Active Directory Groups.

To Add Roles to the Group

- Click **Add Role** in the top-right corner.
- On the **Add role** window, check the boxes next to the Role(s) to give to the Users in the Group.

Working with Personnel

Add role

Search for role

☐ ProvisionApprover

☐ Custom Role Demo

☐ Audit2

☐ ProvisionTest

☐ Auditor

☐ AccountOwner

☐ ALMEngine

Add

3. Click **Add**.

To Remove Roles from the Group

- Click the **X** to the right of the Role.

3 Roles in this Group

Add Role

Q Search

NAME	ACTIONS
new	X
TensorGate Operator Class 4	X
ProvisionRequestor	X

Create and Manage Roles

Roles control privileges within ALM. To access the Role page, click **Personnel** in the left-hand menu and then click **Roles**.

Account Lifecycle Manager

Home

Alerts

Workflows

Integrations

Personnel

Users

Groups

Roles

Audit

API

Alert Settings

Delinea

Personnel > Roles

Roles

+ Create Role

31 items

Search...

Filters

NAME ↑	ENABLED	BUILTIN	↓
"EntityType": "User", "EntityId": "1ecef8a1-53c4-4c77-9b98-753b6ab38c37", "Action": "Sign In", "EntityName": "enza.system@mailinator.com", "ContextualData": { "args": { "ProviderName": "AuthenticationTypes.Federation", "ProviderKey": "28dd2109-1445-4f87-9812-4bc7a2edbaab", "Email": "enza.system@mailinator.com", "DisplayName": "enza.system@mailinator.com" } } }			

ALM Engine Logs

1. Select **Audit** in the left navigation panel. Then, select **ALM Engine Logs**.
2. Click any ALM Engine in the table to display its Audit Details page.

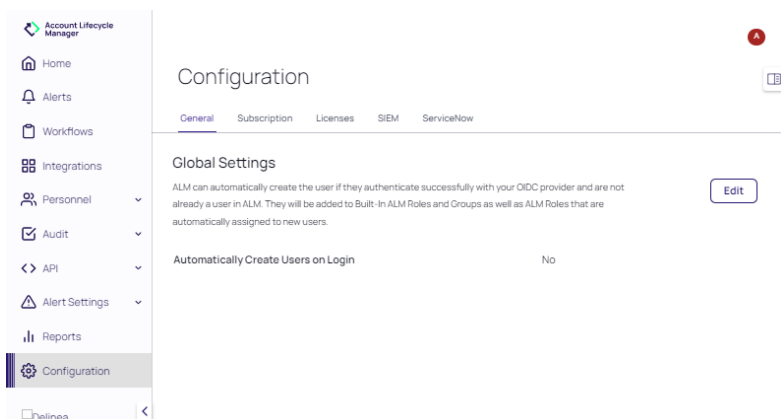
Configuration

Click **Configuraition** in the left navigation panel to access the following settings for ALM:

- **General** - Global settings to automatically create the user if they authenticate successfully with your OIDC provider and are not already a user in ALM
- **Subscription** - Information regarding the type, date, users and engines for the subscription
- **Licenses** - Information regarding any licenses applied
- **SIEM** - Allows management of SIEM integrations in the application

Configuration

- [ServiceNow](#) - Allows ServiceNow Integrations to be enabled or disabled in the application



Integrate with Other Applications

Continue setup by integrating with other services/applications that your organization will use.

ALM Supports Integrations with:

- [ServiceNow](#)
- [SIEM Services](#)

SIEM Integration

ALM supports integration with security information and event management (SIEM) tools. The following is a list of events that can be sent to SIEM:

Event	Description
Account Owner Changed	A managed account has had an owner added or removed.
Account Provisioned	An account was successfully provisioned.
Account Requires Renewal	An account is up for renewal.
Account Secret ID Changed	An account's secret ID was changed.
End of Life Notification	An account's End of Life action will be taken in a number of days.
External Groups Disabled	Some groups in the domain were disabled in ALM during the last domain sync.
New External User	Accounts have been added since the last sync and are not being managed by ALM.
New Synced User	Sent a new user welcome email.

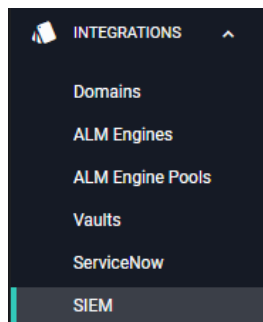
Configuration

Event	Description
Provision Approval Step Changed	A provision step requires approval.
Provision State Changed	A request failed to provision.
Provision Template State Changed	A provision template was updated to a new state.
Remote Worker Integration Access Error	A remote worker cannot access the configured domain.
Request State Changed	The state of a request has changed.
User Disabled by AD User Sync	The last Active Directory Sync disabled a number of users.
Any Audit Record	All audits are sent to SIEM.

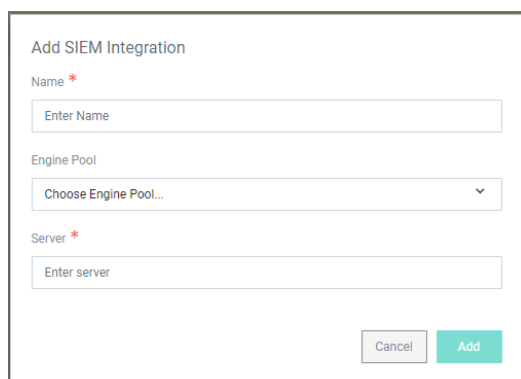
Creating a SIEM Integration

To create a new integration:

1. Click **Integrations** on the left-hand navigation menu and select **SIEM**.



2. Click **Create SIEM Integration** in the top right-hand corner to bring up the **Add SIEM Integration** window.

A screenshot of the 'Add SIEM Integration' dialog box. It has a title bar 'Add SIEM Integration'. Inside, there are three labeled input fields: 'Name *' with a text input containing 'Enter Name', 'Engine Pool' with a dropdown menu showing 'Choose Engine Pool...', and 'Server *' with a text input containing 'Enter server'. At the bottom right, there are two buttons: 'Cancel' and 'Add'.

3. Enter a **Name** for the integration.

Configuration

4. Choose an **Engine Pool** for the integration.
5. Enter the **Server URL** where ALM will send data.
6. Click **Add** to bring up the **Manage SIEM Integration** page.

Name	Test SIEM	Edit
Engine Pool	enzadev	Edit
Server	https://www.example.com:514	Edit
Port	514	Edit
Protocol	UDP	Edit
Output Type	Syslog	Edit
Enabled	Yes	No ☐ Yes ☒

7. On the Manage SIEM Integration page, click **Edit** to change the values for each section.
Note: The **Port** and **Protocol** automatically fill with default values. Make sure to change the values to match your server settings. The **Output Type** defaults to Syslog. It can be changed to JSON or CEF.
8. Set the **Enabled** toggle to **Yes** to activate the SIEM integration.
9. When the integration is configured, click **Test SIEM Integration** in the upper right-hand corner. Clicking will immediately send ALM data to your chosen server.

Deleting a SIEM Integration

Any of the currently configured SEIM integrations, listed on the Integrations > SIEM page, can be deleted. To refine the list of currently configured integrations, use the Search field to locate a specific configuration. Use the **Filters** drop-down to restrict the list to **All**, **Disabled**, or **Enabled** configurations, as well as a specified **Search Term**.

To delete an existing SIEM configuration:

1. Click the SIEM configuration to be deleted.
2. At the **Manage SIEM Integration** page, click **Delete**. A message indicating that the configuration has been

Alert Settings

deleted is displayed.

Integrations > SIEM > SIEMtest2

Test SIEM Integration

Delete

Manage SIEM Integration [Edit](#)

Name *	SIEMtest2
Enabled	Yes
Engine Pool *	test
Server *	10.60.20.19
Port *	530
Protocol	UDP
Output Type	JSON

ServiceNow Integration

ServiceNow delivers popular IT service management solutions. Organizations that employ both Account Lifecycle Manager and ServiceNow IT Service Management can benefit from an integrated workflow.

As much of other IT management operations are handled in ServiceNow by organizations, now too can the ALM Workflow! This includes the ability in ServiceNow to:

- Submit a Request using an ALM Workflow Template
- View Request statuses
- View and Approve/Deny Requests for assigned Approvers

Refer to Integrating ALM with Service Now [here](#).

Once the connection has been set up successfully, ServiceNow will be ready to receive requests from ALM.

Alert Settings

Select Alert Settings in the left navigation panel.

Alert Settings

Account Lifecycle Manager

Alert Settings > Email Templates

Email Templates

26 items

NAME ↑	ENABLED	LAST MODIFIED
Account End of Lifecycle Reminder	No	02/11/2022 4:16 PM (UTC-5)
Account Lifecycle Ended Remind...	Yes	04/25/2019 4:08 PM (UTC-4)
Account Owner Changed	Yes	08/22/2019 4:31 AM (UTC-4)
Account Provisioned	Yes	03/21/2019 10:19 AM (UTC-4)
Account Provisioning Failed	Yes	04/15/2019 1:51 PM (UTC-4)
Account Renewal	Yes	03/12/2019 3:53 PM (UTC-4)
Accounts Added	Yes	10/16/2019 3:33 PM (UTC-4)

Alerts can be configured to be triggered by any of the following:

- [Email Templates](#)
- [Webhooks](#)
- [Webhook Authorization](#)

Alerts for Email Templates

Administrators and Users with **Email Template Permissions** can modify and enable/disable emails that are generated and sent automatically by ALM. To modify an **Email Template**:

1. Navigate to **Alert Settings** and click **Email Templates**. The Templates are named after the event in ALM that will trigger the Email.

Alert Settings

NAME ↑	ENABLED	LAST MODIFIED
Account End of Lifecycle Reminder	No	02/11/2022 4:16 PM (UTC-5)
Account Lifecycle Ended Remind...	Yes	04/25/2019 4:08 PM (UTC-4)
Account Owner Changed	Yes	08/22/2019 4:31 AM (UTC-4)
Account Provisioned	Yes	03/21/2019 10:19 AM (UTC-4)
Account Provisioning Failed	Yes	04/15/2019 1:51 PM (UTC-4)
Account Renewal	Yes	03/12/2019 3:53 PM (UTC-4)
Accounts Added	Yes	10/16/2019 3:33 PM (UTC-4)

- Click the name of the Template to bring up the **Manage Email Template** page. From here you can:
 - Change the **Subject** line of the Email.
 - Change the **Body** of the Email. Use the **Parameters** variables to customize the message. You can add the Parameters by retyping them or clicking **insert**.
- Enable** or **Disable** the Email using the toggle.
- Click **Save** when you are finished.

Alerts for Webhooks

ALM allows Administrators and Users with **Webhook Permissions** to set up custom integrations using webhooks.

Creating a Webhook

To create a webhook:

- Navigate to **Alert Settings** and click **Webhooks**.
- In the upper right-hand corner, click **Create Webhook** to bring up the **Add Webhook** window.

Add Webhook

Description *

Enter Description

Event

Choose an event...

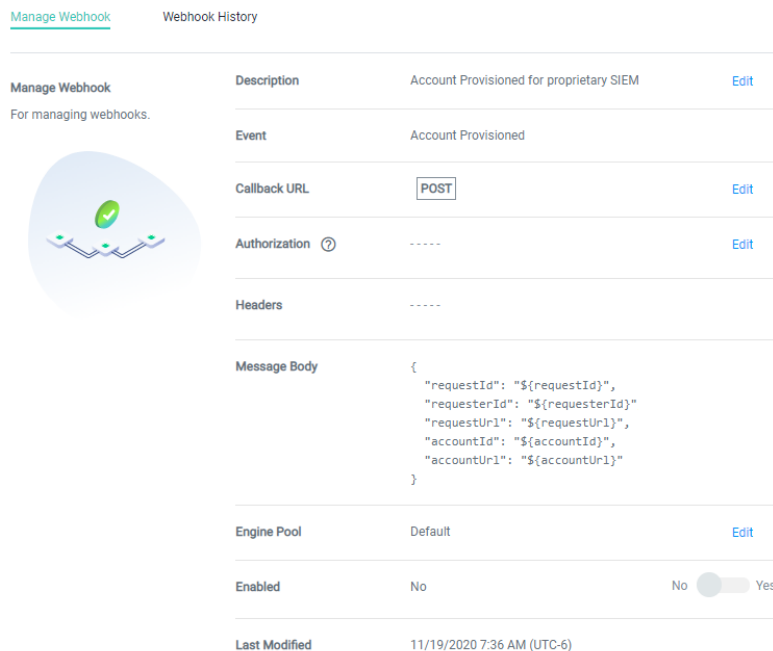
Cancel Save

Alert Settings

3. Enter a description of the webhook.
4. Choose the **Event** within ALM that will trigger the webhook.
5. Click **Save** to bring up the **Manage Webhook** page.
6. On the **Manage Webhook** page, enter the complete **Callback URL**. The **Message Body** shows the data that will be sent to the URL.
7. Set the **Enabled** toggle to **Yes** to activate the webhook. Leave the toggle on **No** to keep the webhook inactive. It can be enabled later from this page.
8. (Optional) Once you have enabled the webhook, the **Test Webhook** button will appear in the upper right-hand corner. Click **Test Webhook** to send a test call to the callback URL.



9. (Optional) Add **Authorization** to the webhook by clicking Edit and selecting the corresponding authorization from the drop-down. You can also adjust the authorization header for the callback url of the webhook. *If you have not previously configured Webhook Authorization, see the section below. If needed, you can save the webhook and return later to add authorization.*

The image is a screenshot of the 'Manage Webhook' form. On the left, there is a sidebar with a 'Manage Webhook' section containing a green checkmark icon and the text 'For managing webhooks.' The main form area contains the following fields:

- Description:** 'Account Provisioned for proprietary SIEM' with an 'Edit' link.
- Event:** 'Account Provisioned'.
- Callback URL:** A text input field containing 'POST' with an 'Edit' link.
- Authorization:** A dropdown menu with a question mark icon and a value of '-----' with an 'Edit' link.
- Headers:** A text input field with a value of '-----'.
- Message Body:** A text area containing a JSON object:

```
{  "requestId": "${requestId}",  "requesterId": "${requesterId}",  "requestUrl": "${requestUrl}",  "accountId": "${accountId}",  "accountUrl": "${accountUrl}"}
```
- Engine Pool:** 'Default' with an 'Edit' link.
- Enabled:** A toggle switch currently set to 'No' (labeled 'No' and 'Yes').
- Last Modified:** '11/19/2020 7:36 AM (UTC-6)'.

10. Click **Save** to create the webhook.
11. Once the webhook is created and enabled, you can view its usage details from the **Webhook History** tab at the top of the page.

Alerts for Webhook Authorization

You can enable Webhook authentication using **Webhook Authorization**. To create a new Webhook Authorization:

- [Importing and migrating Accounts](#)
- [Creating Requests](#)
- [Approving or Denying Requests](#)
- Creating and managing [Workflows](#)
- Calibrating the [ALM engine](#)
- [Service Account Migration Tool](#)
- [Configuring Alert Settings](#) such as Email Templates and Webhooks
- [Managing Personnel](#) (Users, Groups, and Roles)
- [Defining Configuration Settings](#)

Calibrating the ALM Engine

To use the ALM Engine Calibration tool:

1. Go to the **Vaults** page.
2. Select the Vault for which you need an active ALM Engine connection to be established.
3. On the **Vault Details** page, go to the **ALM Engines** tab.
4. Click **Calibration**.

This will queue a **ALM Engine Calibration Job** and prompt a modal dialog stating:

- ALM Engine Calibration started, this may take several minutes to complete.

The ALM Engine Calibration Job connects with the ALM Engines, tasking each one to authenticate with the Secret Server Vault you selected. The Calibration Job keeps track of which ALM Engines successfully authenticate to the Vault, creating a list of ALM Engines known to have access to that Secret Server.

- That list populates a table on the ALM Engines tab of the Vault Details page.
- ALM Engines that did not authenticate will not appear on the list.
- If no ALM Engine authenticated, the Vault Details page will indicate that “No ALM Engines calibrated to integration.”

An ALM Engines Calibration Job runs as part of any Scheduled Sync for a Vault, with the list of successfully authenticating ALM Engines updating on completion of the sync job.

Service Account Discovery Tool

This free tool helps assess the level of risk associated with your inventory of service accounts in AD by connecting to Windows machines across your network and scanning for local and service account usage.

To download the tool visit the [Free IT Tool](#) section of the Delinea website.

Prerequisites

The Service Account Discovery Tool supports Windows 7, 8, 8.1, and 10.

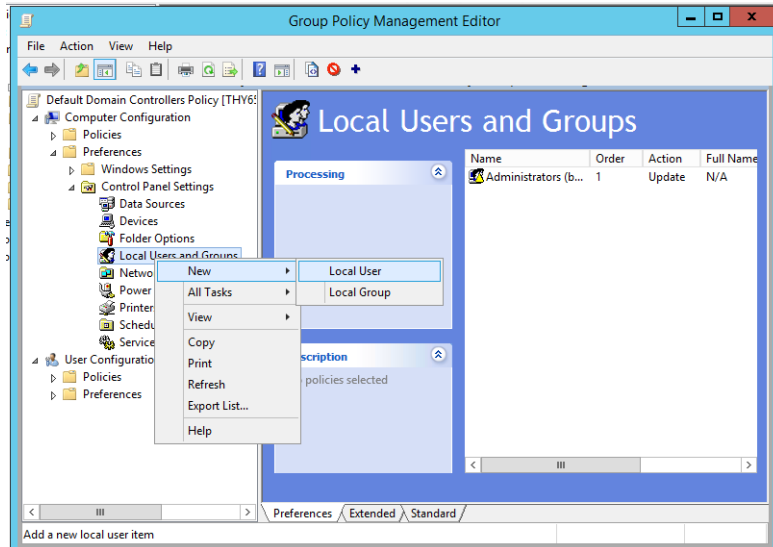
The machine on which it executes must have Microsoft's .NET Framework 4.5.1 or higher.

ALM Administration

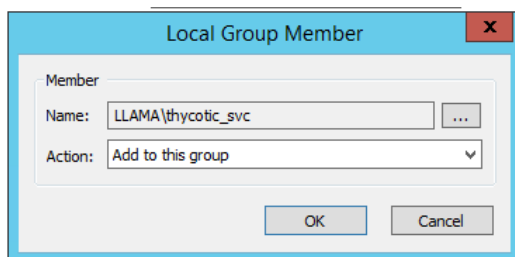
In order to scan for service accounts, the account entered must be a domain account that is in the Administrators Group on the target machines. Using a domain admin account to run the tool will often be sufficient for scanning your network.

These steps will ensure the account has the appropriate privileges to run a successful scan.

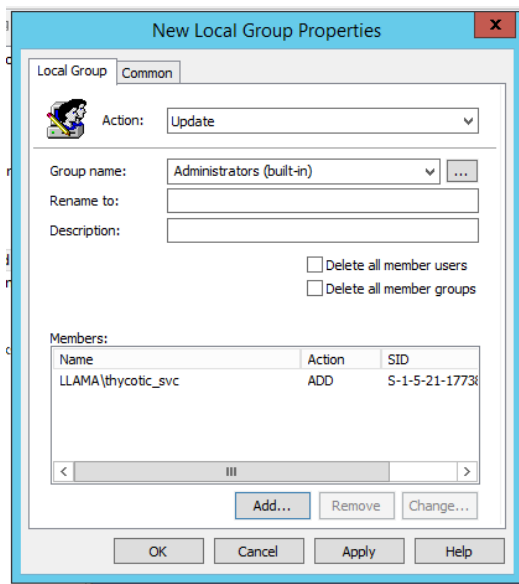
- Open the Group Policy editor for your domain policy.
- Go to **Computer Configuration > Preferences > Control Panel Settings**.
- Right-click **Local Users and Groups** and select **New > Local Group**.



- Leave the **Action** value set as **Update**.
- For **Group name**: use the drop-down menu to select **Administrators (Built-in)**.



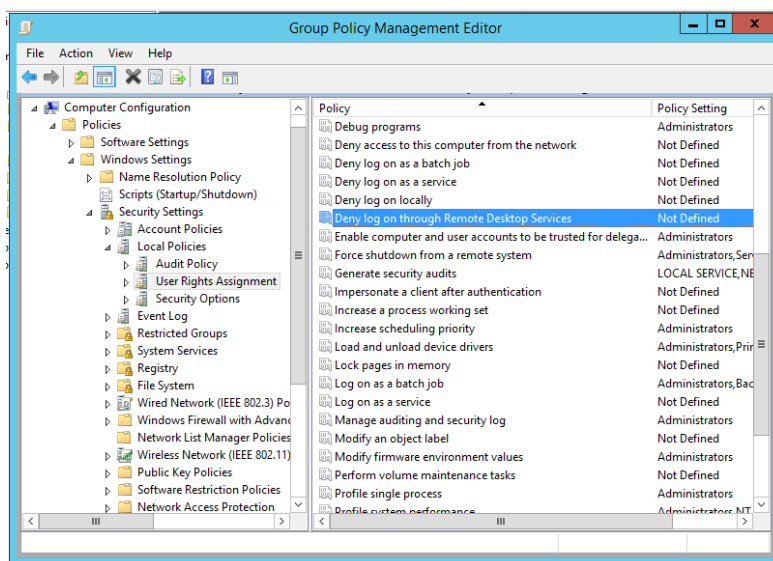
- Click **Add...** and search for the account you will use for Discovery scanning.



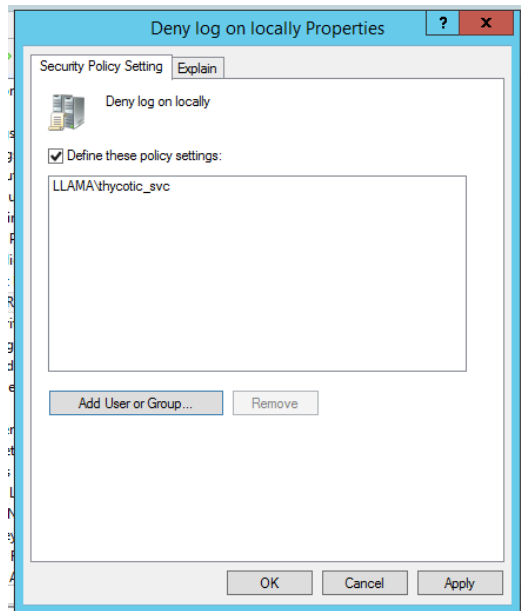
- Click **OK** to save your changes. The next time the Group policy updates across your environment, the Discovery Account will be part of the Local Administrators Group.

For the best security, configure Group Policy to limit the logon privileges of that account:

- In the Group Policy editor for your domain policy, go to **Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > User Rights Assignment**.



- Add your Discovery account to the **Deny log on locally** and **Deny log on through Remote Desktop Services** policies at right.



- Optional: make sure that the account is not part of the Remote Desktop Users Group.

Ports

The Discovery scan makes use of several ports to connect to the target Windows machines to scan them for local and service account usage.

Traffic Type	Ports Used
RPC Dynamic Port Range	1025-5000, 49152-65535
Microsoft DS	445
epmap	135

The RPC Dynamic Port ranges are a range of ports utilized by Microsoft’s Remote Procedure Callback (RPC) functionality. This port range varies by operating system. For Windows Server 2008 or greater, this port range is 49,152 to 65,535. This entire port range must be open for RPC technology to work.

Walkthrough

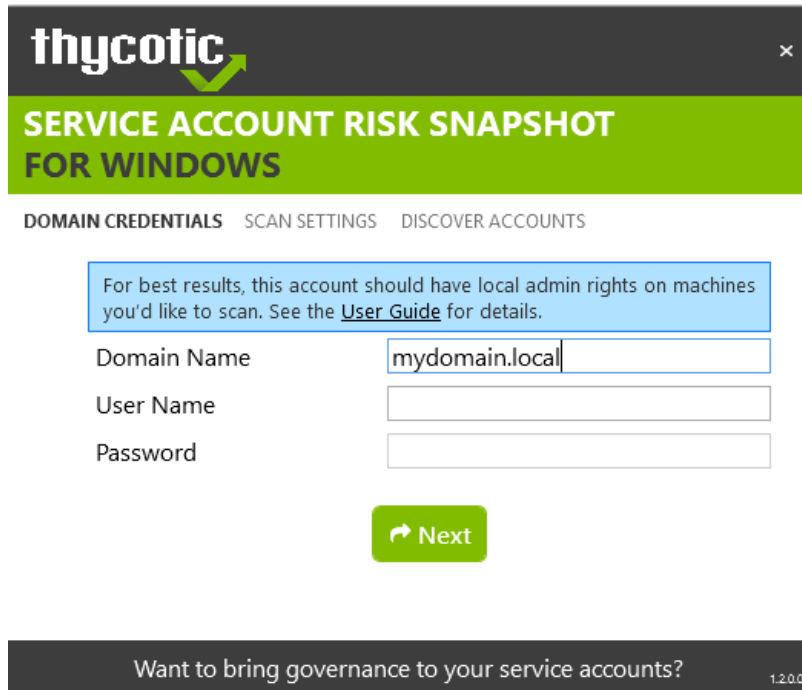
After downloading the Discovery Tool, unzip it and run **ThycoticServiceAccountRiskSnapshotAnalyzer.exe** or, if you prefer, rename the executable file to something easier to type, and then run it.

Domain Credentials

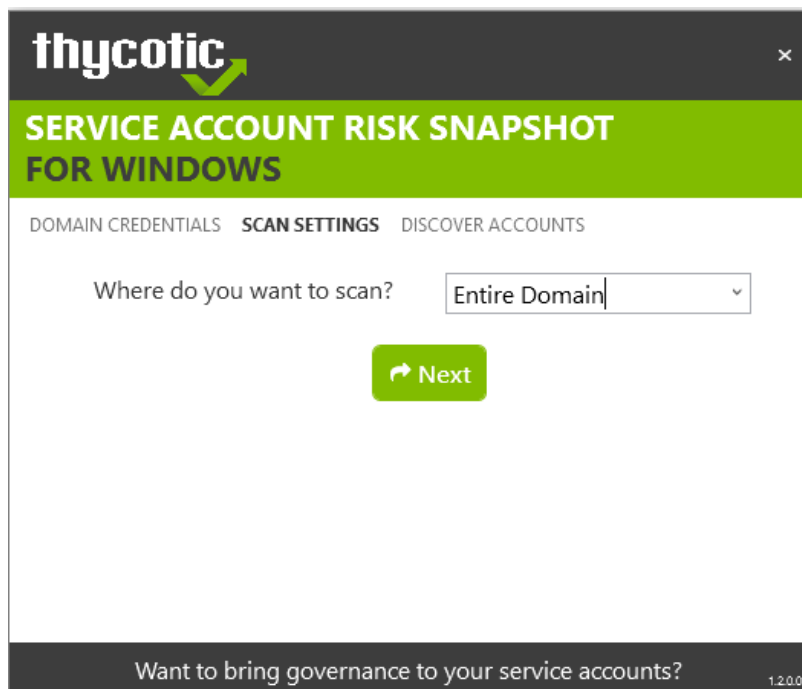
The scanner will first prompt for credentials and the fully-qualified domain name (FQDN) of the domain you would like to scan. Use the credentials you configured earlier.

- These will be used for scanning, but the scanner tool does not save them for subsequent use.
- When you have provided the credentials, use the **Next** control to proceed.

If the scanner cannot reach the domain or the credentials are not valid, it will state that it cannot connect to the domain with supplied credentials.



The screenshot shows the 'thycotic' logo at the top left. Below it is a green banner with the text 'SERVICE ACCOUNT RISK SNAPSHOT FOR WINDOWS'. Underneath the banner are three tabs: 'DOMAIN CREDENTIALS' (selected), 'SCAN SETTINGS', and 'DISCOVER ACCOUNTS'. A blue informational box states: 'For best results, this account should have local admin rights on machines you'd like to scan. See the [User Guide](#) for details.' Below this box are three input fields: 'Domain Name' (containing 'mydomain.local'), 'User Name' (empty), and 'Password' (empty). A green 'Next' button with a right arrow is positioned below the input fields. At the bottom of the window, a dark bar contains the text 'Want to bring governance to your service accounts?' and the version number '1.2.0.0'.



The screenshot shows the 'thycotic' logo at the top left. Below it is a green banner with the text 'SERVICE ACCOUNT RISK SNAPSHOT FOR WINDOWS'. Underneath the banner are three tabs: 'DOMAIN CREDENTIALS', 'SCAN SETTINGS' (selected), and 'DISCOVER ACCOUNTS'. The main content area has the text 'Where do you want to scan?' followed by a dropdown menu showing 'Entire Domain'. A green 'Next' button with a right arrow is positioned below the dropdown. At the bottom of the window, a dark bar contains the text 'Want to bring governance to your service accounts?' and the version number '1.2.0.0'.

In that case, check your credentials or use different credentials.

Scan Settings

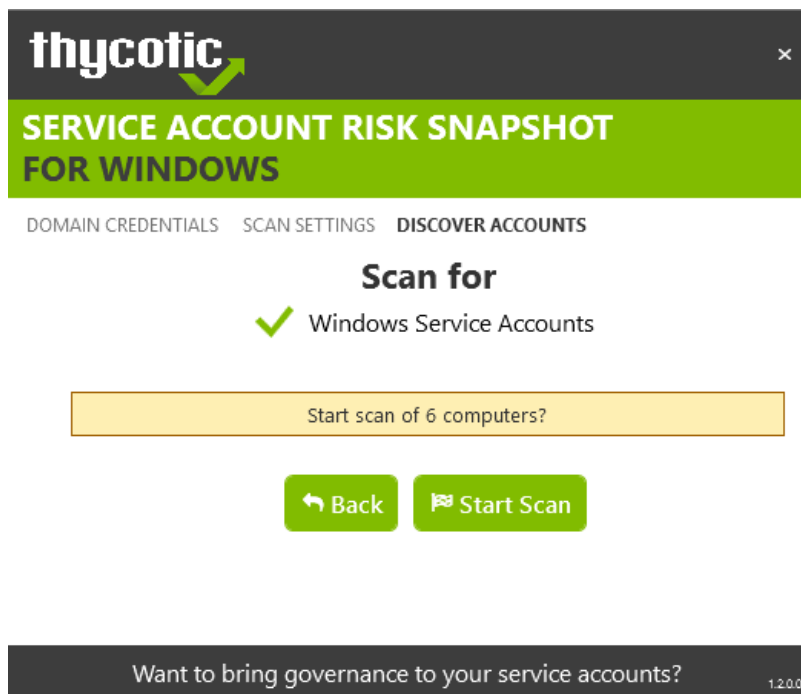
The scanner allows you to choose whether to discover accounts across the entire domain or only accounts in a specific OU. Scanning a specific OU will limit the number of computers the tool investigates.

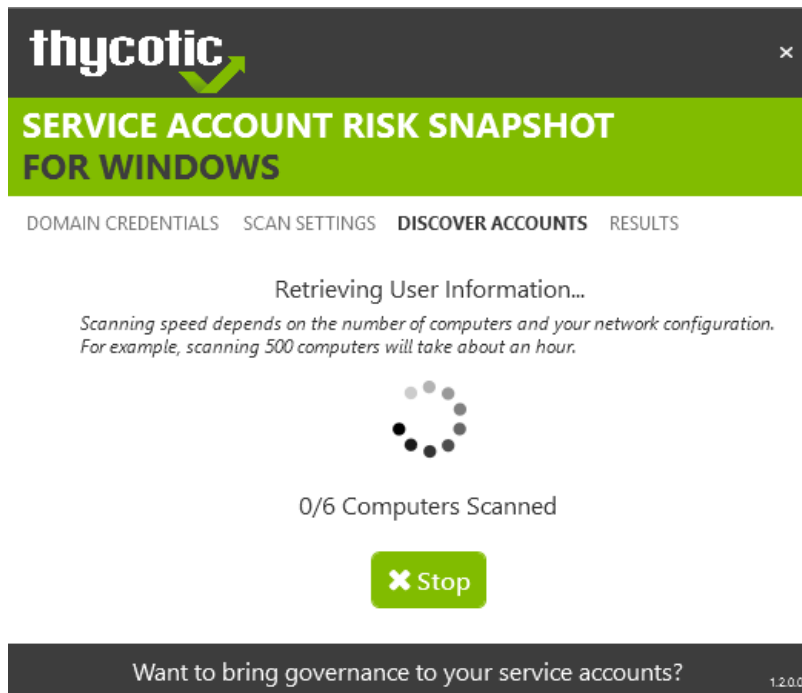
Discovering Accounts

Before you start the scan, review the number of computers the discovery tool retrieved from Active Directory based on what OU or domain you chose to scan. If the numbers seem ballpark, click **Start Scan**. If you think the number of computers to be scanned seems improbably high, consult your IT support staff for guidance.

While the scan runs, you will see the number of computers scanned progress. You can stop the scan at any point and generate the reports based off of the accounts discovered so far.

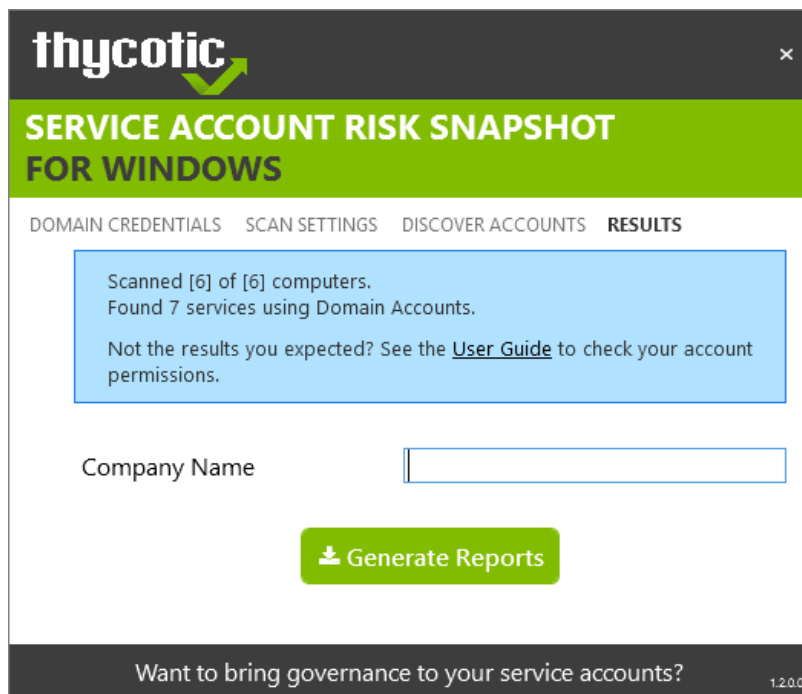
The time to complete the scan will vary based on network latency, the number of machines, and how many machines actually exist. Testing in a large environment resulted in a scan of approximately 1,000 Windows machines in slightly under an hour.





Results

Once the scan completes, you can generate the Executive Summary report and the detailed CSV reports. Just enter a company name and click **Generate Reports**.



The reports will be created in the folder you select. They consist of two files.

Reports

File	Description
ThycoticServiceAccountRiskSnapshot.html	Summary report of findings
ThycoticServiceAccountRiskSnapshot.pdf	Summary report of findings

FAQ

Q: Why doesn't the inventory report show results for all machines in my domain?

A: If there were any issues connecting to a machine, such as network connectivity, insufficient permissions, or closed ports, the machine will not show up in the results. You can investigate the scan log located in the tool folder's **log** subfolder, which will contain errors for machines that couldn't be scanned.

Q: How long will it take to scan my domain?

A: The time to discover accounts will vary depending on network latency and number of machines that respond. A test environment of approximately 1,000 Windows machines took 50 minutes. We recommend testing out your scan first on a smaller OU to get a sense of time and results before scanning a larger OU or your full domain.

Q: The PDF report has inconsistent margins or page breaks.

A: Some display drivers or screen resolutions can cause these PDF defects. Run the scan from a different machine or use the HTML version. The HTML file contains the same information as the PDF.

Q: Where can I download the free tool?

A: The Service Account Discovery Tool, along with other Free IT Tools, can be found on the Delinea website [here](#)

Reports

The ALM application provides a set of predefined reports, each of which runs an associated built-in SQL query to produce easy displayed results.

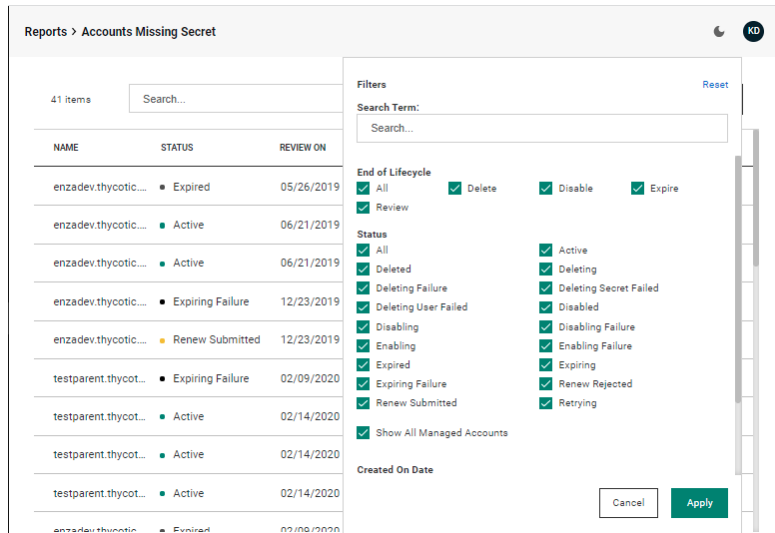
Report	Description
Accounts Created Over Time	This report provides a list of all accounts created in the application.
Accounts Missing Secret	Any managed accounts that are missing secrets (Secret Server, Azure Key Vault or AWS Secrets Manager) are presented.
All Managed Accounts	This report lists accounts specific to a Workflow Template (with a secondary sort applied alphabetically for each template).
Expiring Accounts	Any account that have an Expiration Date will appear in this report.
Orphaned Accounts	Any account that does not have at least one active User or Group assigned as an Account Owner are listed in this report.

Release Notes

1. On the left navigation panel, click **Reports**.

 **Note:** Users must have read rights to view Reports.

2. Click the entry that corresponds to the desired report. The results from the query are displayed on the reports screen. The example below shows an Accounts Missing Secret report.



Reports > Accounts Missing Secret

41 items

Search...

NAME	STATUS	REVIEW ON
enzadev.thycotic...	Expired	05/26/2019
enzadev.thycotic...	Active	06/21/2019
enzadev.thycotic...	Active	06/21/2019
enzadev.thycotic...	Expiring Failure	12/23/2019
enzadev.thycotic...	Renew Submitted	12/23/2019
testparent.thycot...	Expiring Failure	02/09/2020
testparent.thycot...	Active	02/14/2020
testparent.thycot...	Active	02/14/2020
testparent.thycot...	Active	02/14/2020
enzadev.thycotic...	Expired	05/26/2019

Filters

Search Term:

Search...

Reset

End of Lifecycle

☒ All ☒ Review ☒ Delete ☒ Disable ☒ Expire

Status

☒ All ☒ Deleted ☒ Deleting ☒ Deleting Secret Failed ☒ Deleted User Failed ☒ Disabling ☒ Disabling Failure ☒ Enabling ☒ Enabling Failure ☒ Expiring ☒ Expiring Failure ☒ Renew Submitted ☒ Renew Rejected ☒ Retrying

Created On Date

Cancel Apply

3. Use the options available in the **Filters** modal to tailor the display of accounts presented in the report.

Release Notes

As a cloud application updates become available to all Users as they occur—the current version is always the only version available. Delinea periodically updates Account Lifecycle Manager to introduce additional features and provide fixes and improvements.

This article tracks those changes to ALM.

Account Lifecycle Manager: Change Log

Update	Notes
February 2024	improvement: The account Description can now be edited when renewing a Managed Account.
	improvement: Audit records now display the old and new values for fields in the Audit Details page. The Audit list page now shows a searchable Notes column that lists the fields that were modified.
	improvement: Managed Accounts no longer create audit records when checking the Active Directory account status if there are no changes.
	improvement: Upgraded the ALM platform to Angular 17 and .NET 8.0
	fix: Fixed security vulnerabilities in Docker Compose and the Docker image used by SQL Server.
	fix: Deprecated the Engine configuration website.
May 2023	improvement: Submitting a request is more intuitive. Required fields are indicated by an asterisk (*) and draft requests are indicated by "Not started," indicating that approval is not yet pending.
	fix: Resolved an issue where the domain sync fails when the ALM Engine does not have permission to access the distinguishedName property of an Organizational Unit.
	fix: Fixed an issue with bulk renew. The Account Owner role has access to Start Bulk Renew and can bulk renew service accounts ready to be renewed.
	fix: An issue with setting up a Secret Server vault through the ALM engine has been resolved.
September 2022	fix: Resolved an issue that prohibited groups from being added when creating an AWS request with a template.
	fix: Delinea branding is now applied in the New Synced User Welcome email template.
	fix: Resolved an issue where the Everyone group was being removed from built-in roles.
	fix: Resolved an issue that cause a workflow group to be deleted from the previous template when creating a new template.

Update	Notes
August 2022	fix: Resolved an issue that inhibited the display of menu items in the left navigation panel for browser language settings other than English. Menu items now correctly display for any language setting.
	fix: Fixed an issue preventing the ALM self-hosted version from loading the UI.
	fix: Fixed an issue where accounts that have been removed from a LDAP or AzureAD domain were mistakenly included in an email alerting system administrators to accounts created without using ALM after each domain sync.
	 Note: Going forward, domains must be manually synced if they are not regularly scheduled.
May 2022	improvement: The visual appearance and functionality of the UI has been updated to represent our Delinea company brand .
	improvement: For ease of referencing, the user experience for Amazon Web Services (AWS) now combines all AWS resources into a single Resources tab on the Domains page. The new Resources tab includes information for users, groups, and policies.
	improvement: To streamline account management, account migration, renewal, and discovery are accessed from the accounts Home page.
	improvement: Bulk Renew allows multiple accounts to be selected and renewed in one action.
	improvement: Added ability to dynamically add trusted origins for fixing CORS-related issues upon request. Speak with a Delinea support or sales representative and your origin will be added to the list of trusted origins.
	fix: Fixed an issue where accounts were being deleted with an AD domain sync.

Update	Notes
February 2022	improvement: When there are more than 10 external group completion items in a sync, they are now combined into a single auditing entry into the audit database table.
	fix: Resolved the issue with Workflow Template migration not working for discovered ALM accounts.
	fix: Resolved the issue of not being able to set the AD attribute <code>mstSExpireDate</code> .
	fix: Fixed an issue that required a manual (second) sync after adding a new Secret Server Vault.
	fix: Secrets for accounts in an external domain now successfully sync with a ManagedAccountSecret in ALM and create the secrets in the newly managed account.
	fix: Workflow Templates that included more than 15 Secret Server folders will now display all folders on the requests screen.
January 2022	improvement: Overall performance improvements of the application through various backend enhancement and fixes.
	improvement: Usability improvement, providing an increased data range display for managed account history. The data range is configurable to meet individual business needs. Default: 90 days, min/max setting: Today/Show All.
	fix: Corrected an issue where the account URL on an email template incorrectly showed all managed accounts.
December 2021	feature: Added the ability to sort and filter Managed Accounts by Workflow Template. Additionally, a Report displaying all Managed accounts is now added.
	improvement: Updated the User page to allow unlinking an Active Directory or Azure Active Directory domain from an ALM User.
	fix: Validation no longer fails when attributes are defined as read-only on the template.
	fix: An issue is resolved for accounts not renewing when the account name is set incorrectly through the API. This affected accounts with an updated name in the format <code>accountname@domain.com</code> .
	fix: When defining a Workflow Template for SAP, folders now display correctly.
	fix: An issue with the Renew button not being enabled immediately after an end of lifecycle event is addressed.

Update	Notes
November 2021	feature: Google Cloud Platform Service Account Provisioning is now available in ALM. This gives ALM the ability to manage the lifecycle around GCP IAM service accounts, as well as assign roles and permissions.
	improvement: A Delete button is added that allows the user to delete an existing SIEM configuration.
	improvement: The Webhook URL field and Webhook Authorizations URL field no longer require HTTPS validation, however, the URL field cannot be blank.
	fix: A nightly automated task is set to find any account that is stuck in the Retrying status and attempt to place it back into the appropriate actionable state. A bug existed in this logic that was accepting "Retrying" as an actionable state. This is fixed.
	fix: The Accounts Missing Secrets report now only reports Managed accounts missing secrets.
	fix: A bug was introduced that caused the nightly refresh of managed accounts to fail. This refresh updates ALM to match the Enabled/Lockout (where applicable) states, as well as account attributes that are being tracked by ALM to reflect the values present on the domain where the managed account resides. This is resolved with Patch 3.9.1 and the nightly refreshes are now working as expected.
October 2021	improvement: Using the Account Migration Wizard, the ability to update Active directory attributes directly on the accounts in AD is now available. Administrators can also move existing accounts to different workflow templates or between different versions of a template.
	improvement: When accounts are added via Discovery, administrators receive email alerts.
	improvement: When authenticating to AWS Secrets Manager using an EC2 instance, ALM does not need to store the credentials as Authentication is handled directly in AWS.
	improvement: The Description field on Account Requests has been renamed to Account Description and is now required. The Justification/Reason field is no longer displayed for a Managed Account.
	fix: Request rejected for accounts with longer than 20 characters in the name. This issue is resolved.
	fix: Managed accounts now allow editing the secret after account creation.

Update	Notes
September 2021	improvement: AWS IAM Account Provisioning adds the ability to provision and manage AWS Identity and Access Management (IAM) accounts and groups in ALM. Additionally, the ability to sync Users, Groups and Policies is available.
	fix: Users are now able delete a managed account when they have the sys admin role directly or via group membership.
	fix: When working with Managed Accounts, users no longer remain in the Retrying Status.
	fix: The Audits page no longer generates an API error.
August 2021	improvement: Workflow Groups can now be assigned from the Groups page.
	improvement: Added the ability to customize recipients for email templates.
	improvement: Domains can now be permanently deleted.
	fix: When saving a domain/vault sync, the time will now save correctly as UTC.
	fix: A rare bug preventing LDAP synced accounts from being deleted or disabled is resolved.
	fix: RegEx validation now prevents space characters from being added to the end of account names.
July 2021	improvement: Account Request forms now show the email addresses associated with the requester's ALM account.
	improvement: On the Workflow Templates page, deprecated templates are now filtered by default.
	improvement: On the users page, the role tab editing workflow is updated.
	fix: On requests, a default secret folder is no longer selected in the case of folder override or multiple selected folders.
	fix: Approvals now function as intended with ServiceNow authentication.
	fix: A rare bug causing an "Access Denied" pop-up on the Approvals page has been resolved.
June 2021 Release 2	improvement: ALM now supports the latest version of SNOW (Paris).
	fix: Fixed small, non-critical bugs for enhanced performance and user experience.

Update	Notes
June 2021 Release 1	improvement: Updated Account Lifecycle Managers UI framework for an improved look and feel in the application.
	feature: ALM now supports Azure AD role sync .
May 2021	feature: ALM now integrates with HashiCorp Vault.
April 2021	improvement: Minor enhancements and improvements.
March 2021	feature: ALM now integrates with Azure Key Vault and AWS Secrets Manager.
	improvement: UI updates throughout ALM.
February 2021	feature: The Account Migration page allows administrators to change the workflow template, review interval, lifecycle end date, and owners of an existing service account.
	improvement: Workflow templates include the option to hide the names of approvers from requesters.
	improvement: Workflow templates include the option to allow a requester to choose sub-organization units within a designated folder.
	improvement: Webhooks can now be tested from the Webhook Management page.
January 2021	feature: The SIEM integrations page allows administrators to integrate ALM with SIEM applications.
	improvement: Updated UI for webhook authorization, workflow templates, account discovery, and custom HTTP headers.
	improvement: Administrators can specify the maximum number of service account owners when creating a template.

Update	Notes
December 2020	feature: The webhook authorization page allows administrators and users with webhook permissions to add authentication to webhooks.
	improvement: Administrators and users with webhook permissions can add custom HTTP headers to webhooks.
	improvement: When creating or editing an Active Directory template, administrators can restrict users from changing passwords.
	improvement: When creating a workflow template, administrators can define a regex check on Service Account names.
	improvement: When a Secret Server vault sync is run, ALM will search for managed accounts without a SecretID.
November 2020	improvement: Updated UI for managing Roles in ALM.
	improvement: Account rejection explanation appears on the Request details page.
	improvement: Requestors can specify a reason for requesting an account renewal.
	fix: The configuration tab on a Managed Account now updates and reloads automatically after updating a SecretID.
October 2020	First general availability release of ALM Self-Hosted.
September 2020	feature: ServiceNow Requests - ALM's ServiceNow integration will now support submitting ALM Requests via ServiceNow. This update presents the opportunity for users of ALM and ServiceNow to handle both the Requests and Approval process directly within ServiceNow. Requests can be made for Active Directory and AzureAD accounts.  Note: Customers that already have the ALM ServiceNow application installed in ServiceNow must update to latest version.
	feature: AzureAD Group Synchronization - ALM now has the ability select AzureAD Groups from a connected Azure Domain and have them synchronized with ALM. This allows the users to leverage existing AzureAD accounts for establishing the userbase for ALM. Any changes made in AzureAD for Groups enabled in the synchronization will automatically updated in ALM, upon the completion of the determined synchronization schedule.

Update	Notes
August 2020	feature: Inbox - Provides in-app notifications within ALM. Inbox is comprised of three categories of notifications which allows a user to see notifications relevant to their Role and Accounts within ALM.
	feature: ALM Engine Local Account Support - Support for the ALM Engine to allow for a local machine account to run the service.
	feature: Orphaned Accounts - Set of controls to prevent accounts going without at least one active User or Group assigned as Account Owner.
July 2020	feature: Managed Account Dependencies - Ability for ALM to display the dependencies associated with managed accounts. This is pulled from the Secret Server secret into ALM during the Vault sync.
	feature: Vault Sync - : Sync functionality updated to allow ad-hoc sync of the vault, as well as enable dependency synchronization.
	improvement: Tool tips and assisting text added to UI to support aspects of gMSA Workflow Template configuration in ALM.
	improvement: Dashboard page updated to provide more room for widgets.
June 2020	feature: Group Managed Service Accounts (gMSA) Support - A group Managed Service Account (gMSA) provides the same functionality within the domain but also extends that functionality over multiple servers. ALM adds support in the form of the ability to control the lifecycle of gMSA's.
	improvement: Reason Column on Approvals Table - Approvers are provided the account request reason directly in the Approvals table, for easier access and expedited review.
	improvement: Renewal Status in Managed detail screen - To make it easier for Account Owners to view renewal request status, a link is added in the Account Status row for the ability to navigate from the Managed Account detail page to the request for further detail.
May 2020	beta feature: ServiceNow Integration - Ability to reject an ALM Request in ServiceNow. Note: New version of ServiceNow ALM app must be installed.
	improvement: Added the ability to select rows to be displayed in any table in ALM.

Update	Notes
April 2020	beta feature: ServiceNow Integration - Provides a integration to from ALM, to ServiceNow, for reviewing and approving requests made in ALM.
	feature: EOL OU Retirement - For the use case of keeping Organization Units (OUs) organized and manageable, this feature offers the option to select which OU an account is sent to when ALM disables the account at the end of its determined lifecycle.
	improvement: Webhook History - A tab in UI of the Webhooks pages allows Administrators and Users with the necessary permissions to view the activity history of a given webhook.
March 2020	feature: Azure Active Directory Support - ALM extends its directory service support to include Azure AD. This allows ALM to manage accounts located in Azure AD
	feature: Onboarding Assistance - Users that are synced into ALM from Active Directory will receive an automated email to assist with onboarding the user to ALM.
February 2020	improvement: Left navigation menu styling update.
	improvement: Update to the design and layout of the Group detail pages.
	fix: ALM Engine UI configurator tool now launches after the ALM Engine installer finishes.
January 2020	feature: ALM Engine Configuration launches a local webpage upon completion of the ALM Engine installer. The tool assists with testing the setup.
	improvement: General application performance enhancements. Enhancements to the Audit log load time.
	improvement: Update to the Managed Account feature which allows a permission set to allow Users with an assigned Custom Role to see all Managed Accounts in ALM.

Update	Notes
December 2019	improvement: increased Secret Server support with DSV is now a vault option for managed accounts
	improvement: syncing features improved via consolidation of formerly separate syncs to run as a single operation
	improvement: new tool allows selection of a specific AD Group for its AD Accounts to be imported and then synced on a schedule
	improvement: new built-in ALM Group “Everyone” includes all ALM Users; applies new built-in Role of “Account Owner” that lets users see their assigned accounts
	improvement: the Remote Worker renamed ALM Engine for clarity; beta features previewed in November continue to be available in December as they mature
	improvement: new UI detailing on Left Panel Wizards and certain detail pages creates more context and helps customers navigate
November 2019	improvement: the Active Directory Account Discovery tool now supports New Account Notification to help ensure all AD accounts benefit from ALM governance tools
	improvement: new ALM Engine Calibration feature automates the determination of what ALM Engines have access to what Vaults and AD farms
	improvement: tabbed interface for Vault Details page brings improved usability
	a beta tool: a new tool for ALM Engine Configuration, intended to streamline the processes related to setting up ALM Engines, is accessible in this update

References

Update	Notes
October 2019	improvement: new Active Directory Account Discovery tool supports bringing any or all service accounts under the management of ALM
	improvement: System Administrators can select the frequency at which domains automatically sync with ALM, plus commit on-demand sync
	improvement: Workflow Templates let System Administrators define account name prefixes to conform accounts provisioned by ALM to naming conventions
	improvement: better audit logging performance helps organizations with high audit log volumes
	improvement: enhanced external AD sync performance benefits organizations with larger AD installations
	improvement: improved table designs: new row hover highlighting, more obvious labeling when column sorting is available, and stationary header row during scrolling
	improvement: the design of ALM modules appears more uniform across the application
	improvement: icons used within ALM feature more effective designs
	improvement: the Workflow Template Wizard has an improved visual design
August 2019	first General Availability release

References

- [API documentation portal](#)
- [GDPR](#)
- [SLAs](#)
- [SOC2](#)

SLAs and Related Operational Considerations

Account Lifecycle Manager offers a 99.9% Uptime SLA based on the Azure uptime SLAs of its component products and services.

Business Continuity

Every 5 to 10 minutes, ALM backs up transaction logs to local storage. This supports a Recovery Point Objective (RPO) of ten minutes.

Every hour, ALM backs up transaction logs to a geographically redundant location, supporting an RPO of 1 hour.

References

ALM also creates differential backups approximately every 12 hours, and full database backups approximately every 24 hours.

Disaster Recovery

The failure of an entire Azure Region would cause complete loss of access to Delinea's cloud entities located in the failed region for an indefinite, ongoing time.

To recover from such, Delinea would rebuild an ALM instance in another Azure region. The target for rebuilding and connecting to the geographically redundant database is 12 hours, although Delinea cannot guarantee that target.

Confidentiality

Data-at-rest

ALM encrypts some critical data, including requests, audits, Secret Server connection information, and any other stored credentials such as API Tokens.

Encryption transparently applies to all data stored in the Azure SQL Server databases. This includes application audit logging. ALM does not encrypt the ALM Engine logs.

Data-in-Transit

ALM establishes HTTPS connections in conformance with TLS 1.2 protocols. This includes API and ALM Engine connections.

Client Authentication

Authentication proceeds using OIDC to Thycotic One.

Integrity: Code Signing

Code signing applies to the ALM Engine software, which is downloaded to the customer's premises to coordinate interactions among ALM and the customer's Active Directory and Secret Server resources.

General Data Protection Rule (GDPR)

ALM requires certain Personally Identifiable Information (PII) to identify each User's account. This includes the User's name, email address, and password, these being the minimum necessary for authentication.

ALM tracks IP addresses to support access auditing.

Only select, trusted employees of Delinea can access customer data and decrypt it, and only by a controlled process that generates an audit trail inaccessible to those employees. This serves the interests of Users without compromising their privacy and control.

In GDPR terms, Delinea customers are the data controllers, and Delinea is the data processor.

Each ALM customer entirely controls their Users, their User Roles, and the access to data by their Users, according to the policies of the customer organization. ALM logs activity so the customer can monitor access and changes to the Secrets, Users, and Roles, all according to the customer's policies.

References

Delinea conducts a Privacy Impact Assessment (PIA) annually to verify continued conformance to GDPR principles.

SOC II

Delinea offers its customers a SOC II Type II Annual Report documenting two rounds of checks. A third party creates the report as an independent assessment of Delinea's control environment.

The SOC II report, issued annually in accordance with the AICPA's AT Section 101 (Attest Engagements) and based on the AICPA's Trust Services Criteria, addresses the Security, Availability, and Confidentiality criteria.

New This Month: November

Use this file only for months with extensive changes.

November saw Account Lifecycle Manager add New Account Notifications (an Account Discovery feature), ALM Engine Calibration (a Vault tool), and more usable Vault Detail pages, which now sport a tabbed interface. You can also opt to try out the beta release of a tool that will streamline the processes for setting up ALM Engines.

New Account Notifications

October saw the addition of the Active Directory Account Discovery Tool, which provided bulk discovery and import of extant AD accounts when introducing ALM to the enterprise or extending its reach. With this November's update, you can catch new accounts as they appear—when ALM discovers new accounts in AD that have been created with no corresponding managed account record in ALM, it sends an email naming the AD accounts to the System Administrator.

ALM includes a Webhook for this event notification, allowing you to set up additional events to occur automatically when ALM finds unmanaged accounts in AD.

ALM Engine Calibration

ALM can automatically assess which ALM Engines can connect to what Secrets vaults and directory services. MSPs may particularly embrace this tool, as they often must deal with multiple Secrets vaults and AD environments.

Tabbed Interface for Vault Detail Pages

The tabbed interface now applied to Vault Detail pages increases the volume of information available for ready perusal, while making the User interface less cluttered.

Beta Feature Release: ALM Engine Configuration Website Tool

On successful installation of an ALM Engine on a machine, a website hosted locally on that machine will be set to automatically load to provide an interface and toolset for configuring the Secret Server vault, setting up the External Domain (Active Directory), and creating ALM Engine Pools. This should streamline the overall setup process for ALM Engines.

In this November beta release of the feature it has been set not to autoloading. To learn how you can try out this beta feature, see [Setup the ALM Engine Service](#).