



Cyturus On-Boarding

On-Boarding 101

Version: 1.1

December 2024

Contents

New Client Setup	4
Step 1 – Client Configuration	5
Step 2 – Client Contract	6
Step 3 – Enabling Framework Access	9
Finalizing Adding a New Client	9
Starting a New Engagement	10
Step 1 – Establishing an Engagement	10
Step 2 – Creating a New Engagement	11
Step 3 – Adding Engagement User Access	12
Step 4 – Adding Authorizations	14
Step 5 – Adding Access to Client	15
Step 6 – Selecting the Engagement	15
Step 7 – Adding Entitlements	16
Repository Setup and Configuration	17
Step 1 – Accessing Storage Repository Configuration	17
Step 2 – Configuring a Repository	18

On-Boarding 101

Welcome to the Cyturus CRT, the SaaS-based Compliance and Maturity Control Center designed to simplify your compliance journey, mitigate risks, and empower your organization to achieve continuous operational excellence. This onboarding document is your starting point, providing a step-by-step guide to help you maximize the value of our platform from day one.

At Cyturus, we understand that navigating rigorous compliance requirements and managing risks can be complex. Our intuitive platform, real-time insights, and automated workflows are tailored to help you streamline these processes, ensuring your organization remains compliant, efficient, and audit-ready. This document will walk you through the key features, initial setup, and best practices for seamlessly integrating the CRT into your operations.

Our goal is to set you up for success. Whether you're attesting to controls, assessing risks, or tracking progress against compliance standards, this guide is here to ensure a smooth onboarding experience. Should you have any questions or require support, our dedicated compliance management and platform support teams are always available to assist you.

Thank you for choosing Cyturus. We are excited to be part of your compliance and risk management journey.

New Client Setup¹

Please note that all tasks in this document are from an administrative entitlement perspective. If you do not have an administrative role and associated entitlements assigned to your user account within the CRT, these configuration settings will not be available to you.

We need to gather some basic information before configuring a new client within the CRT. The following form highlights the *required* data fields when initially setting up a Client.

¹ For more detailed instructions, please refer to the Cyturus Support CRT Training site:
<https://support.cyturus.com/kb/crt-training>

Step 1 – Client Configuration

Client Details

Organization

Please Select ▼

Account Number

Parent Client

Please Select ▼

Name

* Required

Short Name

* Required

Vertical

Please Select ▼

* Required

Industry

Please Select ▼

* Required

Source

Please Select ▼

Client Type

Please Select ▼

* Required

TimeZone

Please Select ▼

* Required

Corporate Website Address

POA&M Identification Number

Portal Type

Please Select ▼

* Required

Client Logo

Browse...

No file selected.

Status

Please Selc ▼

* Required

Below, we will define the required fields and provide an [EXAMPLE] of the data requested.

- Name – Full Client Name [ACME Tool and Machine]
- Short Name – Initials or common name [ACME]
- Industry – used for data analysis across industries [Defense]
- Vertical – used for data analysis across verticals [Manufacturing]
- Client Type – Establishes the type of client for specific options [Direct]
- TimeZone – provides a variable on which to calculate local time vs UTC [EST – UTC – 5.00]
- Portal Type – defines the Client Portal access Self-Guided or Full CRT [CRT]²
- Status – Activate or Deactivate a client [Active]

Step 2 – Client Contract

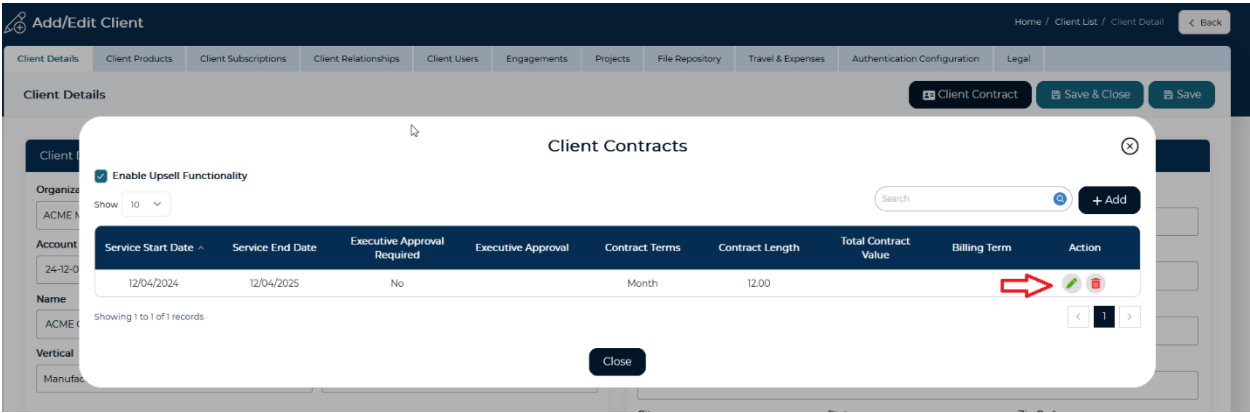
Once the basic information has been entered and initially saved, the CRT requires a Client Contract to be generated with the modules to which the Client will have access.

Click on the Client Contract Button from the header.

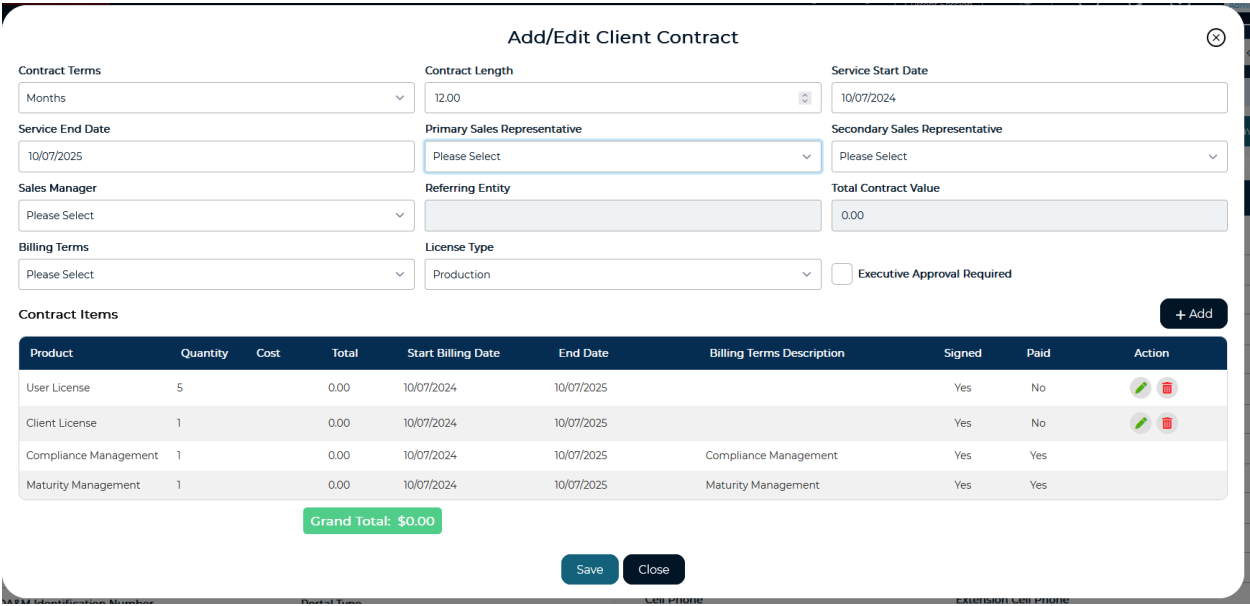
The screenshot displays the 'Add/Edit Client' interface. At the top, a navigation bar includes tabs for 'Client Details', 'Client Products', 'Client Subscriptions', 'Client Relationships', 'Client Users', 'Engagements', 'Projects', 'File Repository', 'Travel & Expenses', 'Authentication Configuration', and 'Legal'. Below this, a sub-header 'Client Details' is visible. A red arrow points to a button labeled 'Client Contract' in the top right corner of the form area. To the right of this button are 'Save & Close' and 'Save' buttons. The main form is divided into two sections: 'Client Details' on the left and 'Client Contact Details' on the right. The 'Client Details' section contains fields for Organization (ACME Manufacturing Association), Account Number (24-12-00072), Parent Client (Please Select), Name (ACME Global), Short Name (AG), Vertical (Manufacturing), Industry (Defense), Source (Referral), Client Type (Direct), TimeZone (UTC-05:00 Eastern Time (US & Canada)), and Corporate Website Address. The 'Client Contact Details' section contains fields for Contact Person, Contact Email, Job Title, Address 1, Address 2, City, State, Zip Code, Office Phone (with a flag icon and number 201 555-0123), and Extension Office Phone.

² A client can only be one Portal Type at a time. Only choose SGA if the client is going to utilize the Self-Guided Assessment portal. For more guidance, please contact Cyturus.

Select the Edit icon to edit the Client Contract:



You can now add the applicable modules that are available to the new client. Remember, Cyturus will bill based on the licenses and access generated during this step.



Once each module and option has been added, save the contract. Then, select the Client Products from the available tabs in the header.

The screenshot shows the 'Client Details' form in a software application. The top navigation bar includes tabs for 'Client Details', 'Client Products', 'Client Subscriptions', 'Client Relationships', 'Client Users', 'Engagements', 'Projects', 'File Repository', 'Travel & Expenses', 'Authentication Configuration', and 'Legal'. The 'Client Details' tab is active, and a red arrow points to it. The form is divided into two main sections: 'Client Details' and 'Client Contact Details'. The 'Client Details' section contains fields for Organization (ACME Manufacturing Association), Account Number (24-12-00072), Name (ACME Global), Vertical (Manufacturing), Source (Referral), Parent Client (Please Select), Short Name (AG), Industry (Defense), and Client Type (Direct). The 'Client Contact Details' section contains fields for Contact Person, Contact Email, Job Title, Address 1, Address 2, City, State, and Zip Code. At the top right of the form, there are buttons for 'Client Contract', 'Save & Close', and 'Save'.

Licenses have been generated and activated for the various modules, as indicated in the example below.

The screenshot shows the 'Client Products' form in a software application. The top navigation bar is the same as in the previous screenshot. The 'Client Products' tab is active. The form is divided into two main sections: 'Compliance Management' and 'Maturity Management'. The 'Compliance Management' section contains fields for Monthly Charge (\$ 500), Compliance Management Start Date (10/07/2024), Compliance Management End Date (10/07/2025), Renewal Date, Assessment Types Available (CMMC v2), and License Key (6332d9d7-e98f-47f3-bee3-abfde4775d04). A red arrow points to the 'License Key' field, which is highlighted with a red box. At the top right of the form, there are buttons for 'Save & Close' and 'Save'.

Step 3 – Enabling Framework Access

The next crucial step in setting up a client is selecting which Assessment Frameworks this client can access. This multi-select field enables you to limit the visible frameworks available to this client from a single framework like CMMC to the example below, which has many global frameworks available to this example client.

The screenshot displays the 'Client Products' configuration interface. The 'Compliance Management' section is active, showing a 'Monthly Charge' of 500, a 'Compliance Management Start Date' of 04/21/2024, and a 'Compliance Management End Date' of 04/21/2025. A red box highlights the 'Assessment Types Available' multi-select field, which contains a list of frameworks including C2MA, C2MA Lite, GDPR, CCPA, HHS SRA - HIPAA, CMMC v1, Incident Response, IR - HIPAA, HITrust, Vendor Risk - Medium, TISAX, FedRAMP Rev4, S/G - Lite, SCSSA, CIS v8, CSF, ISO 27001, TPISR, CMMC v2, SOC 2, 800-53 R5, FedRAMP Rev5, and 800-53 R4. A red arrow points to this field.

Finalizing Adding a New Client

Once you have saved the data into the CRT, you have completed adding a new client. Start a new client engagement based on the frameworks you have enabled for this client.

Starting a New Engagement

Within the Cyturus CRT, a separate engagement is required for each different regulatory framework, and each client has the potential for unlimited engagements. This architectural design enables the separation of regulatory compliance by a user. A client might have SOC2, PCI, and CMMC as required regulatory frameworks, but the users requiring access to CMMC might be different resources than those working on PCI. This enables the Cyturus CRT to support the requirements of least privilege access and zero trust methodologies.

There are multiple paths to establish a new engagement within the CRT. Still, since having an Engagement is a prerequisite to assigning users and the associated user entitlements, we will continue by creating a new Client from where we left off.

Step 1 – Establishing an Engagement

Once the applicable assessment types have been assigned, select the Engagements tab from the Header.

The screenshot shows the 'Client Products' page in the Cyturus CRT. The 'Engagements' tab is selected in the header. A red arrow points to the 'Engagements' tab. The 'Compliance Management' section is active, showing fields for Monthly Charge, Start Date, End Date, Renewal Date, Assessment Types Available (C2MA, TISAX, CMMC v2, CSF 2.0, CSF+), and License Key.

You will notice there are no Engagements for the newly created Client. Click the Create New Engagement button to create a new Engagement for this Client.

The screenshot shows the 'Engagements' page in the Cyturus CRT. The 'Engagements' tab is selected in the header. A red arrow points to the '+ Create New Engagement' button. The page shows two sections: 'Open Engagement List' and 'Closed Engagement List', both displaying 'No data available in table'.

Step 2 – Creating a New Engagement

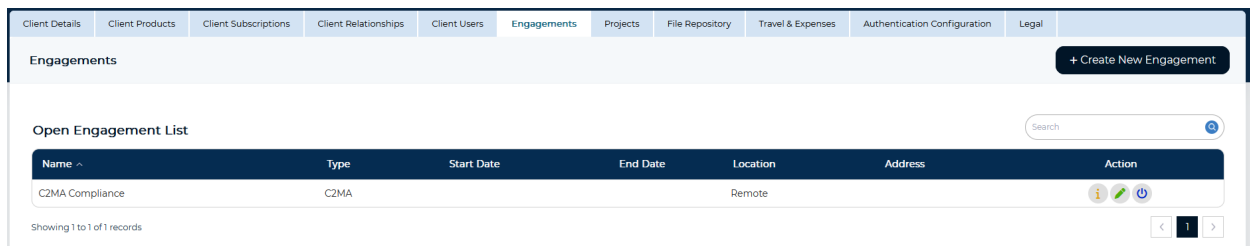
The Create New Engagement form is now ready to create the Engagement.

The screenshot shows the 'Engagement Management' form. At the top, there's a 'Client' field with 'ACME Global' and an 'Engagement Name' field. Below these are 'Location Address' and 'Share Point URL' fields. A section titled 'Assessment Detail' is expanded, showing 'Available For SGA Portal' with 'Yes' and 'No' radio buttons. Below this are fields for 'Assessment Type', 'Partner', 'Start Date', 'End Date', 'Assessment Hours', 'Actual Hours', 'Send Notification Start Days', 'No Of Times Notification Send', 'Cost', 'Installments', 'Estimated Travel Cost', and 'Actual Travel Cost'. All these fields are currently empty or set to default values like '0' or '\$ 0.00'. A 'Save' button is at the bottom right.

Enter an Engagement Name and Select the Compliance Framework for this Engagement.

This screenshot shows the same form as before, but with the 'Engagement Name' field and the 'Assessment Type' dropdown menu highlighted with a red box. The 'Engagement Name' field now contains 'CZMA Compliance'. The 'Assessment Type' dropdown is open, showing options: 'Please Select', 'CSF+', 'CZMA', 'CMMC v2', 'TISAX', and 'CSF 2.0'. A red arrow points to the 'CZMA' option, which is currently selected. The 'Save' button remains at the bottom right.

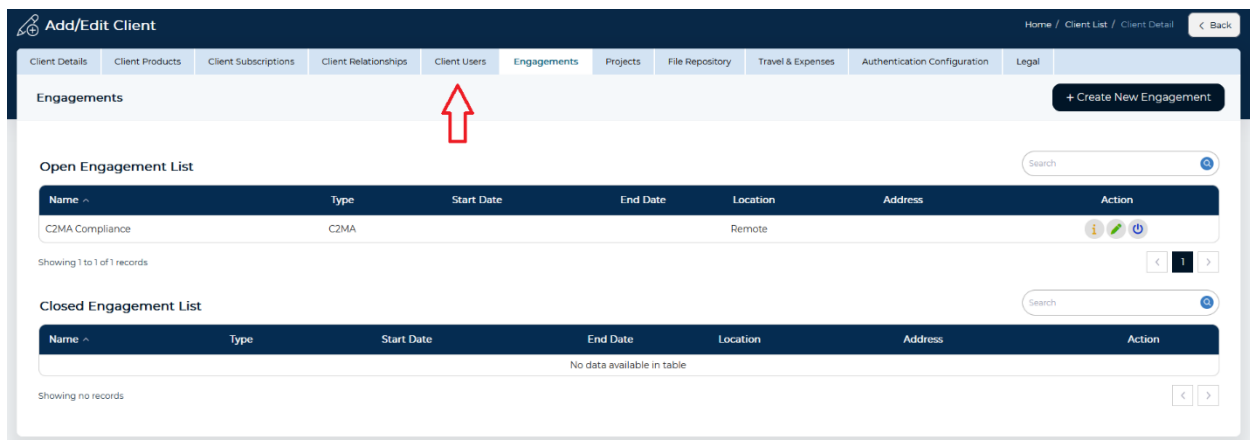
The Engagement location, dates, and other details are optional and not required. Click Save to finalize the creation of this new Client's first engagement.



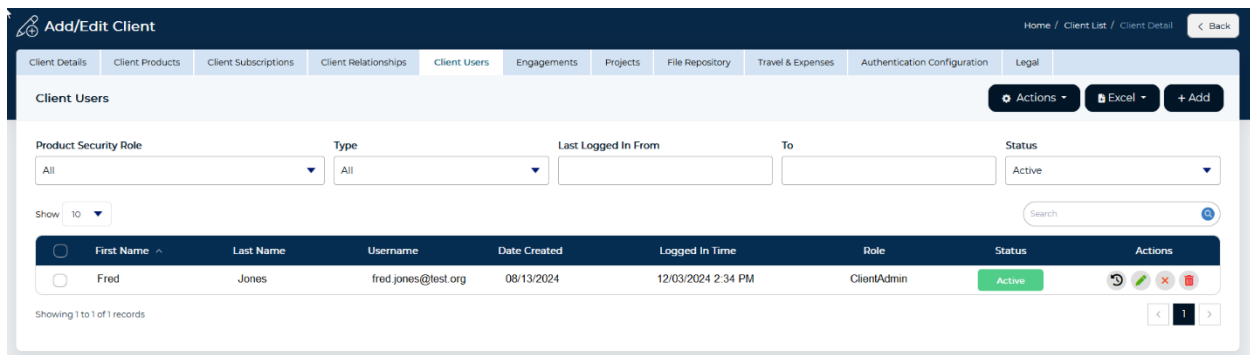
Now that an Engagement has been created adding some Users and providing access through the Cyturus CRT 3D RBAC is time.

Step 3 – Adding Engagement User Access

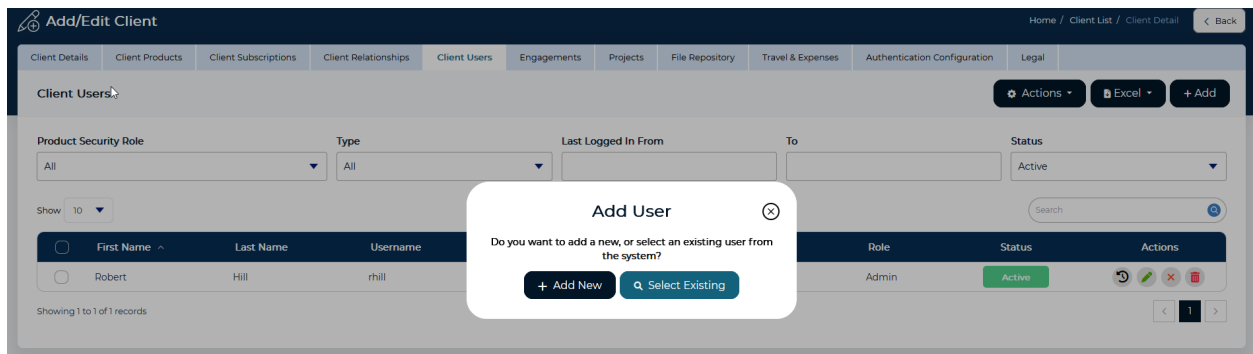
Please select the Client Users tab from the Header to access the Users.



Upon opening the Client Users tab, you will notice that the user creating the Client has already been added as a user.



Adding new Users is as simple as selecting the **+Add** button from the Header. You can now select to add a New User or select from an existing CRT User to provide access to this new Client.



We will select Add New.

A User Details form will open, enabling the addition of new user details. The required fields can be highlighted by pressing the Save button.

The screenshot shows the 'User Add/Edit' application interface. At the top, there's a navigation bar with 'User Add/Edit' and a breadcrumb trail 'Home / Client List / Client Detail / User Details'. Below this is a tabbed interface with 'User Details' selected. The form is divided into two sections: 'User Details' and 'User Account Details'. The 'User Details' section includes fields for First Name, Last Name, Cell Phone Number, Office Phone Number, Portal Type, Type, and Timezone. The 'User Account Details' section includes fields for Username, Default Homepage, Status, Disable Date, No Login Start Time, and No Login End Time. Red boxes highlight the required fields: First Name, Last Name, Username, and Email.

Step 4 – Adding Authorizations

Once you have entered the required details for the new user account, click on the Authorizations tab from the Header.

The screenshot shows the 'User Details' form in a web application. The form is divided into two main sections: 'User Details' and 'User Account Details'. The 'User Details' section includes fields for First Name (Jimmy), Last Name (Johnson), Cell Phone Number, Office Phone Number, Portal Type (CRTUser), Type (Client Resource), and TimeZone (UTC-05:00 Eastern Time (US & Canada)). The 'User Account Details' section includes fields for Username (jimmyjohnson@test.org), Default Homepage (General Dashboard), Status (Active), Disable Date, No Login Start Time, and No Login End Time. The form has a 'Save & Close' button and a 'Cancel' button.

First, one must select a Product Security Role. In this example, we will select the User as the PSR.

The screenshot shows the 'Authorizations' form in a web application. The form is divided into two main sections: 'Product Security Role' and 'Permissions Granted'. The 'Product Security Role' section includes a dropdown menu for 'Product Security Role' (User) and a 'Create Resource' toggle. The 'Permissions Granted' section includes a dropdown menu for 'Engagement' and a 'Compliance Management' section with checkboxes for various roles: Project Manager, Compliance Manager, Evidence Manager, Compliance Contributor, Evidence Contributor, Compliance Viewer, Evidence Viewer, Compliance Owner, Auditor, Evidence Auditor, and SSP Manager. The form has a 'Save & Close' button, a 'Save' button, a 'Set Initial Password' button, a 'Change Password' button, and a 'Cancel' button.

Step 5 – Adding Access to Client

Next, we must select the Client to whom we are providing access,

The screenshot shows the 'User Add/Edit' interface with the 'Authorizations' tab selected. The 'Product Security Role' is set to 'User'. The 'Client' dropdown is open, showing 'ACME Global' selected. A red arrow points from the 'ACME Global' option in the 'Client' dropdown to the 'Permissions Granted' section, which lists 'ACME Global'. The 'Engagement' dropdown is set to 'Please Select'. The 'Compliance Management' section has several checkboxes, all of which are unchecked.

The Client is now listed in the Permissions Granted. One or more Clients may be selected to which this new User is being provided access.

Step 6 – Selecting the Engagement

Select the Engagement we previously created.

The screenshot shows the 'User Add/Edit' interface with the 'Authorizations' tab selected. The 'Product Security Role' is set to 'User'. The 'Client' dropdown is set to 'ACME Global'. The 'Engagement' dropdown is open, showing 'Please Select' and 'C2MA Compliance' as options. A red arrow points to the 'C2MA Compliance' option. The 'Compliance Management' section has several checkboxes, all of which are unchecked.

Step 7 – Adding Entitlements

As you select the appropriate level of access to the various Modules for this Client, specific to this new User, the authorizations will populate in the right-hand pane.

The screenshot displays the 'Authorizations' configuration page. At the top, there are tabs for 'User Details', 'Authorizations', 'MFA', 'Subscriptions', and 'Authentication'. Below the tabs, a 'Product Security Role' dropdown is set to 'User'. The 'Product Entitlements' section includes a 'Client' dropdown set to 'ACME Global' and a 'Create Resource' toggle. Under the 'Engagement' section, 'C2MA Compliance' is selected. In the 'Compliance Management' section, the 'Compliance Manager' checkbox is checked, and a red arrow points from it to the 'Permissions Granted' pane on the right. This pane shows a hierarchical tree of permissions, including 'ACME Global', 'C2MA Compliance', 'Dashboards', 'Home', 'Client (General Dashboard)', 'Compliance Management', 'Client', 'Modules', 'Engagements', and 'Engagement List'. The 'Engagement List' section shows 'Create New Engagement' and 'Edit Engagement' permissions.

You have successfully on-boarded a new Client, created their first Engagement, and added user access.

Repository Setup and Configuration

In an effort to protect confidential client details, the Cyturus CRT only stores operational data and requires a client-hosted repository to be configured per client for the storage of attestation and evidentiary data. This repository can be configured to access most of the popular data repositories, including SharePoint Commercial and GCC-High.

Step 1 – Accessing Storage Repository Configuration

From the Client Details form, select the File Repository tab from the Header.

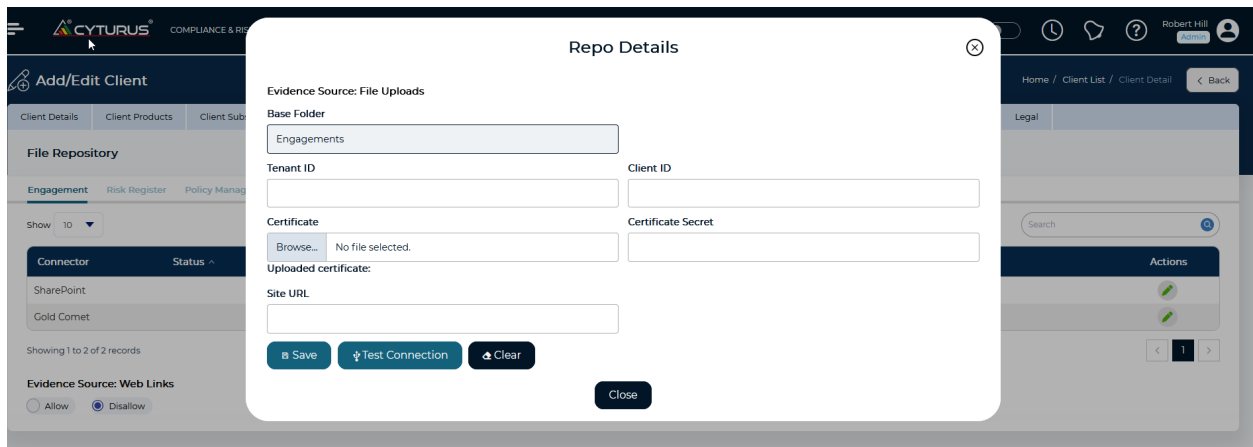
The screenshot shows the 'Add/Edit Client' interface. The top navigation bar includes tabs for Client Details, Client Products, Client Subscriptions, Client Relationships, Client Users, Engagements, Projects, File Repository, Travel & Expenses, Authentication Configuration, and Legal. The 'Client Details' tab is active. Below the navigation bar, there are buttons for 'Client Contract', 'Save & Close', and 'Save'. The main form is divided into two sections: 'Client Details' and 'Client Contact Details'. The 'Client Details' section includes fields for Organization (ACME Manufacturing Association), Account Number (24-12-00072), Parent Client (Please Select), Name (ACME Global), Short Name (AG), Vertical (Manufacturing), Industry (Defense), Source (Referral), Client Type (Direct), TimeZone (UTC-05:00 Eastern Time (US & Canada)), and Corporate Website Address. The 'Client Contact Details' section includes fields for Contact Person, Contact Email, Job Title, Address 1, Address 2, City, State, Zip Code, Office Phone, and Extension Office Phone.

We can now review the available repository options for this client. These can be configured at the instance level, so if you do not see the repository you are expecting, please contact Cyturus to activate additional repo types for the Client.

The screenshot shows the 'File Repository' configuration page. The top navigation bar includes tabs for Client Details, Client Products, Client Subscriptions, Client Relationships, Client Users, Engagements, Projects, File Repository, Travel & Expenses, Authentication Configuration, and Legal. The 'File Repository' tab is active. Below the navigation bar, there are buttons for 'Engagement', 'Risk Register', 'Policy Manager', 'TPRM', 'Reporting', 'DCMS', and 'Incident Commander'. The 'Engagement' button is active. The main section displays a table of connected engagements. The table has columns for Connector, Status, Connected Engagements, and Actions. The table shows two records: 'SharePoint' and 'Gold Comet'. Below the table, there is a search bar and a 'Showing 1 to 2 of 2 records' indicator. At the bottom, there is a section for 'Evidence Source: Web Links' with radio buttons for 'Allow' and 'Disallow'.

Step 2 – Configuring a Repository

Clicking on the green pencil to edit the Repository Configuration, a Repo Details form will appear.



The screenshot shows the 'Repo Details' form in the foreground, which is a modal window. The background shows the 'Add/Edit Client' page with the 'File Repository' section active. The 'Repo Details' form has the following fields and controls:

- Evidence Source:** File Uploads
- Base Folder:** Engagements
- Tenant ID:** [Text input field]
- Client ID:** [Text input field]
- Certificate:** [Browse... button] No file selected.
- Certificate Secret:** [Text input field]
- Uploaded certificate:** [Text input field]
- Site URL:** [Text input field]
- Buttons:** Save, Test Connection, Clear, Close

The background page shows the 'Add/Edit Client' form with the 'File Repository' section active. It includes a 'Connector' dropdown menu with 'SharePoint' and 'Gold Comet' options. The 'Evidence Source: Web Links' section has 'Allow' and 'Disallow' radio buttons. The 'Status' dropdown is set to 'Active'.

Cyturus does not perform this configuration, so the connection details are never provided to Cyturus resources. This must be configured before evidence can be attached as attestation.

The following [link](#) provides a detailed walk-through for configuring a SharePoint repository.

<https://support.cyturus.com/kb/use-azure-ad-application-permissions-authentication-with-sharepoint-online>

Glossary

- **3D RBAC (Three-Dimensional Role-Based Access Control):** Cyturus's approach to assigning user security role and entitlements based on product, engagement, and client level.
- **Active vs. Inactive Status:** The operational state of a client account, determining whether users can access their CRT instance.
- **Approach Progression:** The Domain-specific objectives and practices describe the progression of the approach to cybersecurity for each Domain in the model. Approach refers to the completeness, thoroughness, or level of development of an activity in a Domain. As an organization progresses from one MIL to the next, it will have more complete or more advanced implementations of the core activities in the Domain. At MIL1, while only the initial set of practices for a Domain is expected, an organization is not precluded from performing additional practices at higher MILs.
- **Assets:** Entities of value to an organization. Assets can be physical, logical, or include software.
- **Assessment Framework:** A regulatory or compliance standard an organization is either required to or has chosen to adhere to.
- **Assessment Type:** A CRT designation for a specific set of Controls or Practices that can be aligned with either internal or external frameworks.
- **Attestation Data:** Definitive information or evidence used to prove compliance with regulatory requirements.
- **Azure AD Authentication:** A method of connecting to a system or repository using Microsoft Azure's identity management system for authentication.
- **Client Configuration:** The process of setting up basic client information.
- **Client Contract:** The agreement outlining the modules and frameworks a client has licensed and can access within the CRT.
- **Client Type:** A classification that determines the services or modules available to a client.
- **CMI® (Cyber Maturity Index):** A quantifiable scoring methodology providing a measurable index that is organizational size, vertical, and industry agnostic.
- **Compliance Framework:** A structured set of requirements and controls necessary to meet to obtain regulatory compliance.
- **CRT (Compliance and Risk Tracker):** Cyturus's SaaS platform for managing compliance and maturity processes.
- **Domain:** Contains a structured set of cybersecurity practices. Each set of practices represents the activities an organization can perform to establish and mature capability within the Domain.
- **Document:** To support and record in writing information that has been previously identified and defined.
- **Engagement:** A project or compliance effort within an active client account tied to a specific compliance framework, known within the CRT as an Assessment Type.
- **Engagement Location:** An optional detail in engagement setup specifying the physical or virtual location tied to the engagement.

- Entitlements: Permissions granted to a user for accessing specific modules, functionality within those modules, or even client access.
- Evaluate: The act of assessing or appraising information or activities for effectiveness or quality.
- Evidentiary Data: Documentation or artifacts submitted to support compliance audits.
- Examine: To inspect in detail to determine nature, condition, or proficiency.
- Framework Enablement: The process of assigning specific compliance standards (e.g., SOC2, CMMC) to a specific client.
- Green Pencil Icon: The visual cue for editing within the CRT.
- Group: Each of the tactical Practices within the C2MA model belongs to a specified Group. These Groups contain relevant Practices from all Domains, enabling cross-Domain views and focus on remediation activities.
- Header Tabs: Menu options at the top of the CRT interface used for data organization or access.
- Identify: To establish or indicate who or what someone or something is. Does not require written form, unlike documentation.
- Instance Level Configuration: Configuration settings applied at the system level rather than Organization, Client, or user-specific configuration options.
- Least Privilege Access: A principle of granting users the minimum level of access required to perform their job. The CRT is designed with implicit deny-all and explicit access-required methodology within our deployment of 3D RBAC.
- Maturity Model: A set of characteristics, attributes, indicators, or patterns representing capability and progression in a discipline. Typically includes best practices and may incorporate standards or other codes of practice.
- MIL (Maturity Indicator Levels): The C2MA defines three Maturity Indicator Levels—MIL1 through MIL3—applying independently to each Domain.
 - MIL1: Beginning/foundational—identified and thought about.
 - MIL2: Intermediate/performed—written and performed.
 - MIL3: Advanced/managed—matured.
- Multi-Select Field: A dropdown or input field that allows users to select multiple options simultaneously.
- Objective: Practices within each Domain are organized into Objectives, which support maturity progression and logical groupings. They represent the business goals for requirements.
- Organizationally-defined frequency: The timeframe decided by the organization after considering risk tolerance. Frequencies longer than 12 months should be documented as a risk.
- Parameters: Parts of each Practice that, when all are completed and evidence is available, allow the Practice to be fully implemented.
- Permissions Granted: The list of access privileges assigned to a user for specific clients, engagements, or modules.
- Portal Type:
 - Self-Guided: Sharing of a self-guided assessment with the client.

- Full CRT: Collaborative working environment with the client within the CRT.
- Practices: Actions performed with the intent to improve organizational resilience. Includes Controls, Processes, Procedures, Policies, Guidelines, Standards, or other maturity-building activities.
- Product Security Role (PSR): A role grouping that defines a user's potential access within the CRT. Defines maximum entitlements available for a user.
- Repository Configuration: The setup of a client-hosted secure data storage location, such as SharePoint, for evidentiary and reporting data.
- Save Button Behavior: Clarifies that pressing "Save" also highlights required fields as an indication of missing data.
- SharePoint GCC-High: A specific version of SharePoint approved for handling sensitive US Government managed data.
- Storage Repository: A secure location for storing client attestation and evidence data (e.g., SharePoint, Box, Dropbox).
- Strategy: A comprehensive plan of action to accomplish specific goals.
- Time Zone Configuration: This setting enables local time calculations for reports and notifications.
- Zero Trust: A security model requiring strict identity verification for every user or device attempting to access resources.