



Cloud Compliance User Guide



Table of Contents

Overview.....	2
1 Cloud Compliance.....	3

Product Version	Document Revision	Date
SecurEnds GRC Cloud Compliance User Guide 1.0	1.0	April 17, 2022

Overview

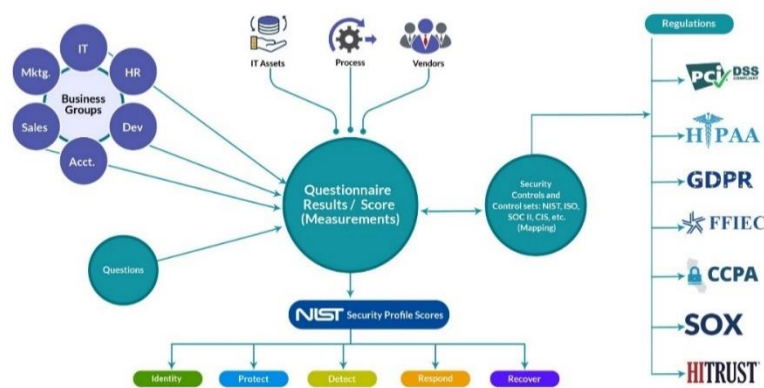
This Administration User Guide outlines the steps to conduct a campaign and produce reports. The steps go through the process of creating an asset within the business hierarchy and associating questions to conduct a campaign which results in an assessment report. The experience of completing the steps in this User Guide will enable the administrator to tailor complex campaigns for each organization.

What we do!

SecurEnds GRC is an accessible SaaS solution that helps achieve a reliable enterprise security score through a simple interface. It can be managed quarterly or annually, even by those who lack experience with managing security or compliance controls. The SecurEnds GRC method of completing risk assessments includes flexible scoring and configuration of the questions, answers, and measurements with a choice of templates for quick implementation.

Assessments are applied to operational activities and security control requirements. Each assessment adds to the enterprise posture score for security and privacy. The current profile is automatically updated and compared with the master target profile to show maturity progress. Participants interact with

the questionnaire for measure responses or utilize the capability to reassign when delegation or additional expertise is required. The participant(s) can add evidence and comments for review before it is presented to audit.



Why SecurEnds GRC?

Achieve a reliable Enterprise Security Posture that is resilient in a dynamic infrastructure and regulated environment

The SecurEnds GRC application develops an overall enterprise score which is comprised of a questionnaire based on risk management, remediation of compliance and audit requirements. The questionnaires are associated with assets, control sets and business units, supplying a multi-view measurement perspective. Encompassing all areas of an organization, external vendors, or external assessments; the aggregation leads to an enterprise security posture score that goes beyond a two-dimensional spreadsheet.

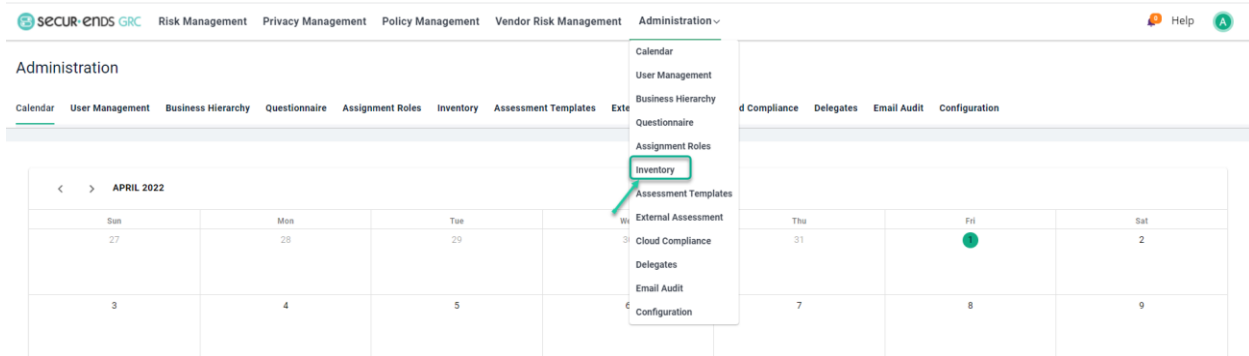
1 Cloud Compliance



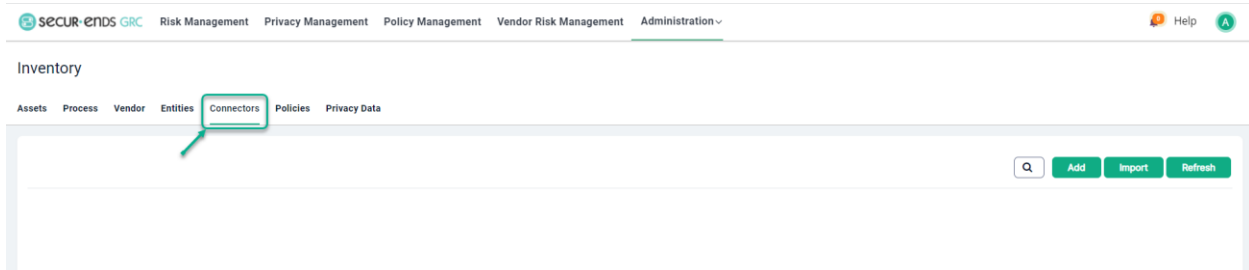
Integrated modules bring the cloud journey across various compliance frameworks into partnership with the full compliance platform that is SecurEnds GRC.

Step 1: Create Inventory for Connectors

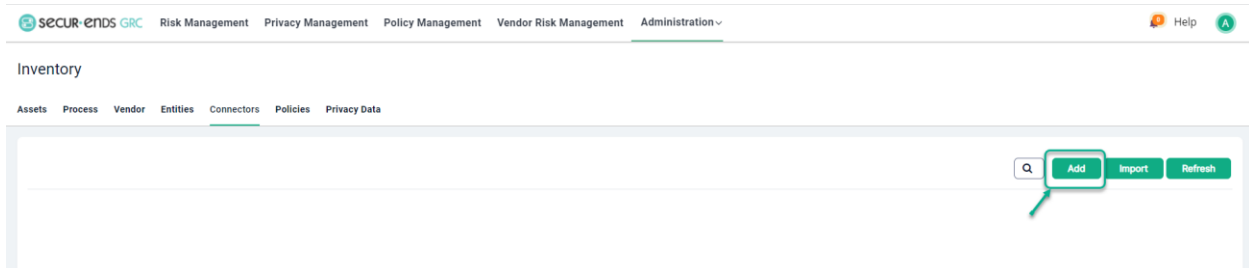
Click the **Administration** tab on the main menu and select **Inventory** from the drop-down list



Click the **Connectors** tab.



Click the **Add** button.



Enter Name and Connector Owner.

SECUR-ENDS GRC Risk Management Privacy Management Policy Management Vendor Risk Management Administration

Add Connector Back

Setup Connector

Name*

Connector Owner* Add

Assign Business Unit/Department/Division No Yes

Questionnaire Source Connector

Select the Connector radio button on Questionnaire Source.

SECUR-ENDS GRC Risk Management Privacy Management Policy Management Vendor Risk Management Administration

Add Connector Back

Setup Connector

Name*

Connector Owner* Add

Assign Business Unit/Department/Division No Yes

Questionnaire Source Connector

Search...

To activate additional connectors contact sales@broadgrc.com

ADP ADP Active Directory Active Directory Office 365 Office 365 SharePoint SharePoint Salesforce Salesforce

See all

Click the See all option to select the required Connector from the list.

SECUR-ENDS GRC Risk Management Privacy Management Policy Management Vendor Risk Management Administration

Add Connector Back

Setup Connector

Name*

Connector Owner* Add

Assign Business Unit/Department/Division No Yes

Questionnaire Source Connector

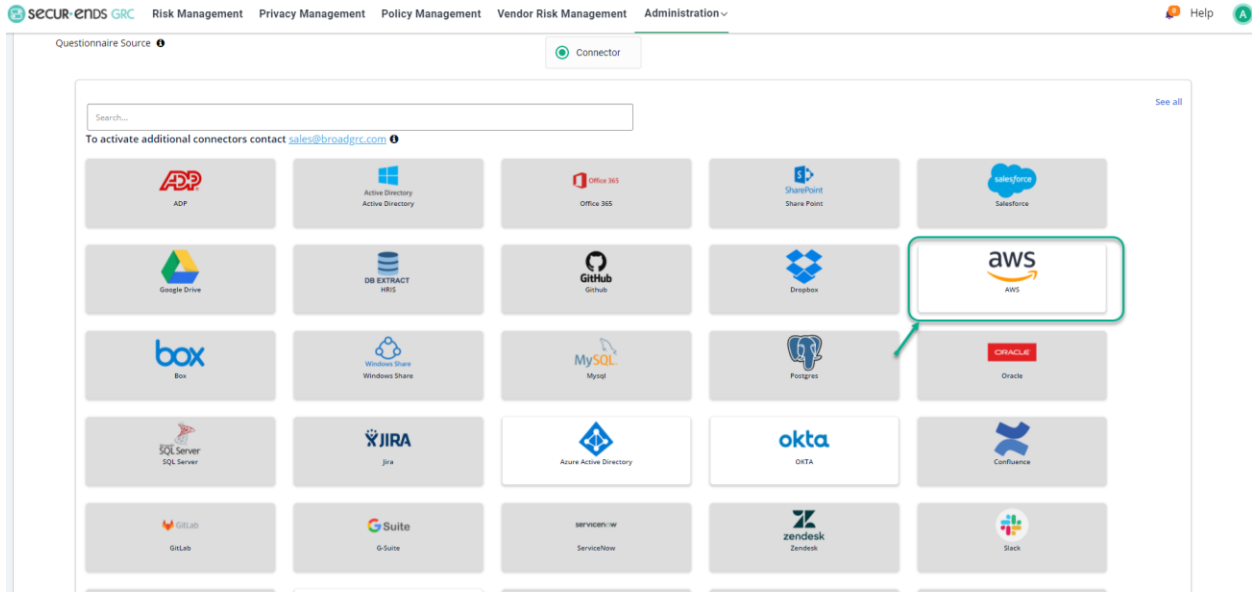
Search...

To activate additional connectors contact sales@broadgrc.com

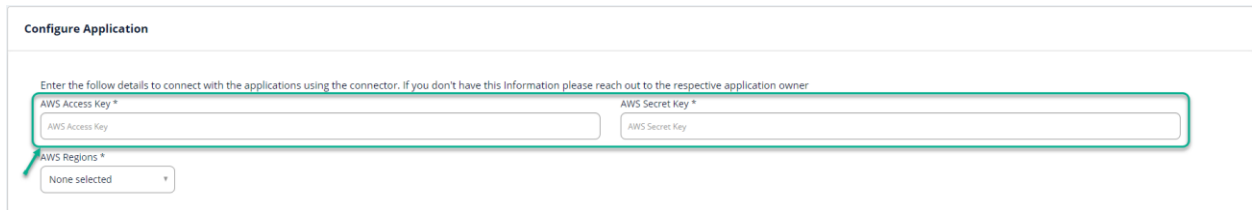
ADP ADP Active Directory Active Directory Office 365 Office 365 SharePoint SharePoint Salesforce Salesforce

See all

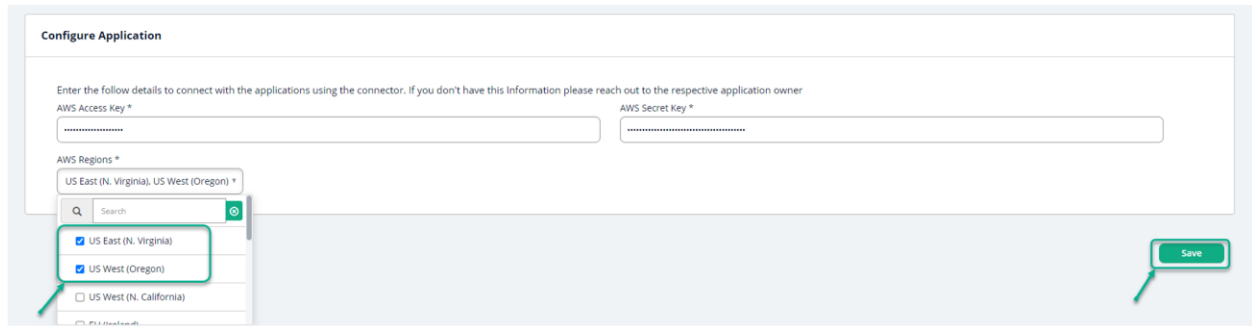
Select the Connector from the list



Enter the Connectors Access Key and Secret Key on Configure Application.

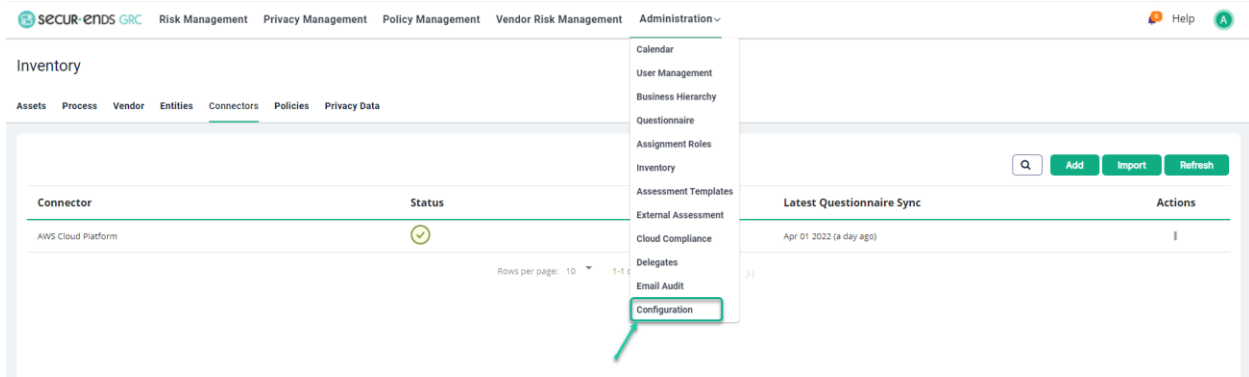


Select first two in AWS Regions and click the Save button.

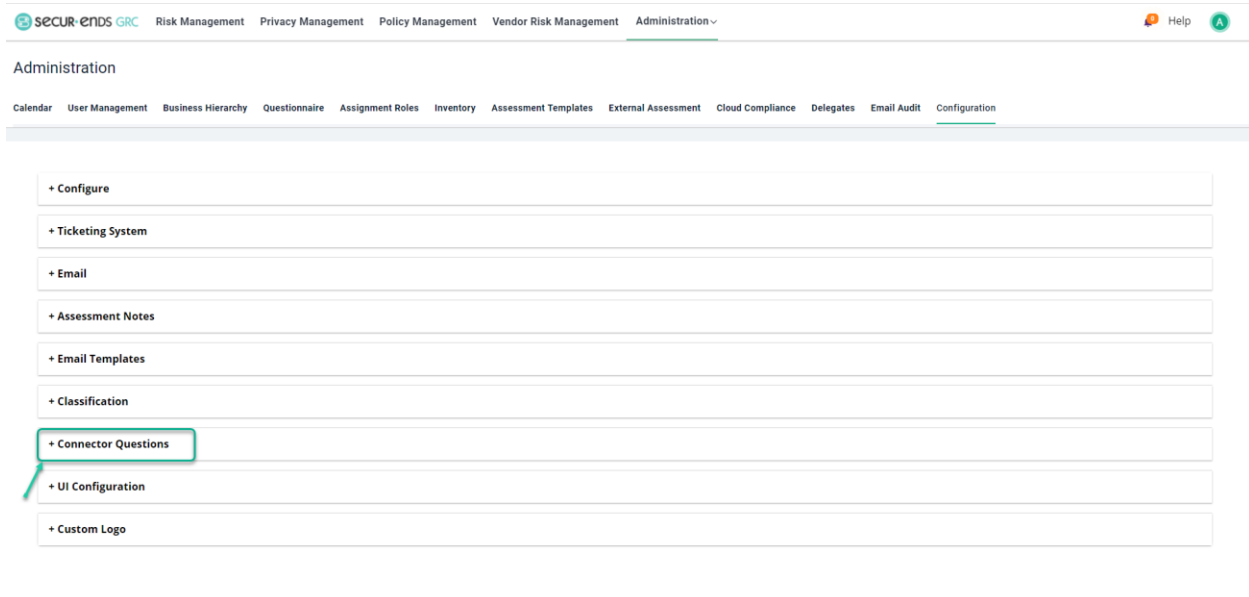


Step 2: Mapping Questions with Metadata

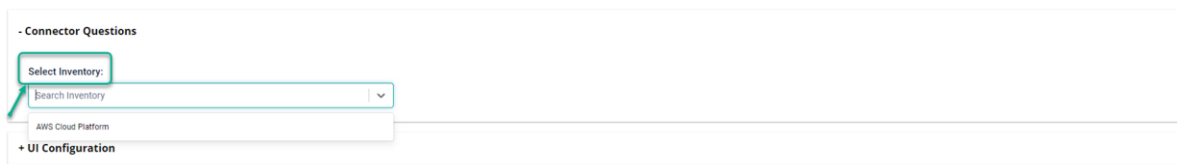
Click the **Administration** tab on the main menu and select **Configuration** from the drop-down list.



Select Connector Questions.



Select Inventory from the drop-down list.



Map the Question with the Metadata and click on **Save** button.

Note: For mapping Question with Metadata, Search the Question from the column that is same as Metadata and select Question from the drop-down list.

The screenshot shows the 'Connector Questions' configuration interface. At the top, there are navigation tabs: 'SECUR-ENDS GRC', 'Risk Management', 'Privacy Management', 'Policy Management', 'Vendor Risk Management', and 'Administration'. A search bar and a 'Help' icon are also present. Below the navigation, there are two dropdown menus: 'Select Inventory:' (set to 'AWS Cloud Platform') and 'Select Control:' (set to 'CIS'). A search icon is on the right. The main area is a table with three columns: 'Metadata', 'Value', and 'Question'. The table contains ten rows of data, each representing a security check and its corresponding question. A 'Save' button is highlighted in the bottom right corner of the table area.

Metadata	Value	Question
IsIAMAccessAnalyzerEnabledForAllRegions	false	Is the IAM Access analyzer enabled for all regions?
DoAnySecurityGroupsAllowIngressRemoteServerAdministrationPorts	false	Do any security groups allow ingress from 0.0.0.0/0 to remote server administration...
IsObjectLevelLoggingForReadEventsEnabledForS3Bucket	false	Is Object-level logging for read events enabled for S3 bucket?
DoesLogMetricFilterAndAlarmExistForDisablingOrScheduledDeletionOfCustomerCreatedCM...	false	Does log metric filter and alarm exist for disabling or scheduled deletion of customer...
AreNetworkACLsRestrictingIngressAccessFromRemoteServerAdministrationPorts	false	Are Network ACLs restricting ingress access from 0.0.0.0/0 to remote server admini...
IsS3BucketPolicySetToDenyHTTPRequests	false	Is S3 Bucket Policy set to deny HTTP requests?
DoesLogMetricFilterAndAlarmExistForChangesNetworkAccessControlLists	false	Does log metric filter and alarm exist for changes to Network Access Control Lists (...)
DoesLogMetricFilterAndAlarmExistForAWSManagementConsoleAuthenticationFailures	false	Does log metric filter and alarm exist for AWS Management Console authentication f...
DoesLogMetricFilterAndAlarmExistForIAMPolicyChanges	false	Does log metric filter and alarm exist for IAM policy changes?
IsMFADeleteEnabledOnS3Buckets	false	Is MFA Delete enabled on S3 buckets?

Step 3: In Inventory click Connector's tab and click the **Actions** column for the connector and select **Sync Questionnaire**.

The screenshot shows the 'Inventory' page. At the top, there are navigation tabs: 'SECUR-ENDS GRC', 'Risk Management', 'Privacy Management', 'Policy Management', 'Vendor Risk Management', and 'Administration'. A search bar and a 'Help' icon are also present. Below the navigation, there are tabs: 'Assets', 'Process', 'Vendor', 'Entities', 'Connectors', 'Policies', and 'Privacy Data'. The 'Connectors' tab is selected. The main area is a table with four columns: 'Connector', 'Status', 'Latest Questionnaire Sync', and 'Actions'. The table contains one row of data for 'AWS Cloud Platform'. The 'Status' column shows a green checkmark, and the 'Latest Questionnaire Sync' column shows 'Feb 21, 2022 (an hour ago)'. The 'Actions' column has a dropdown menu open, showing options: 'Sync Questionnaire', 'Update', 'Clone', 'Delete', 'Assessments Questionnaire', and 'Disable'. The 'Sync Questionnaire' option is highlighted.

Connector	Status	Latest Questionnaire Sync	Actions
AWS Cloud Platform	✓	Feb 21, 2022 (an hour ago)	<ul style="list-style-type: none">Sync QuestionnaireUpdateCloneDeleteAssessments QuestionnaireDisable

Click on **Refresh** button.

The screenshot shows the 'Inventory' page in the SecurEnds GRC application. The navigation bar includes 'Risk Management', 'Privacy Management', 'Policy Management', 'Vendor Risk Management', and 'Administration'. The 'Connectors' sub-menu is active. A table lists connectors, with 'AWS Cloud Platform' shown. The 'Actions' column for this connector has a dropdown menu open, with the 'Refresh' button highlighted by a red box and an arrow.

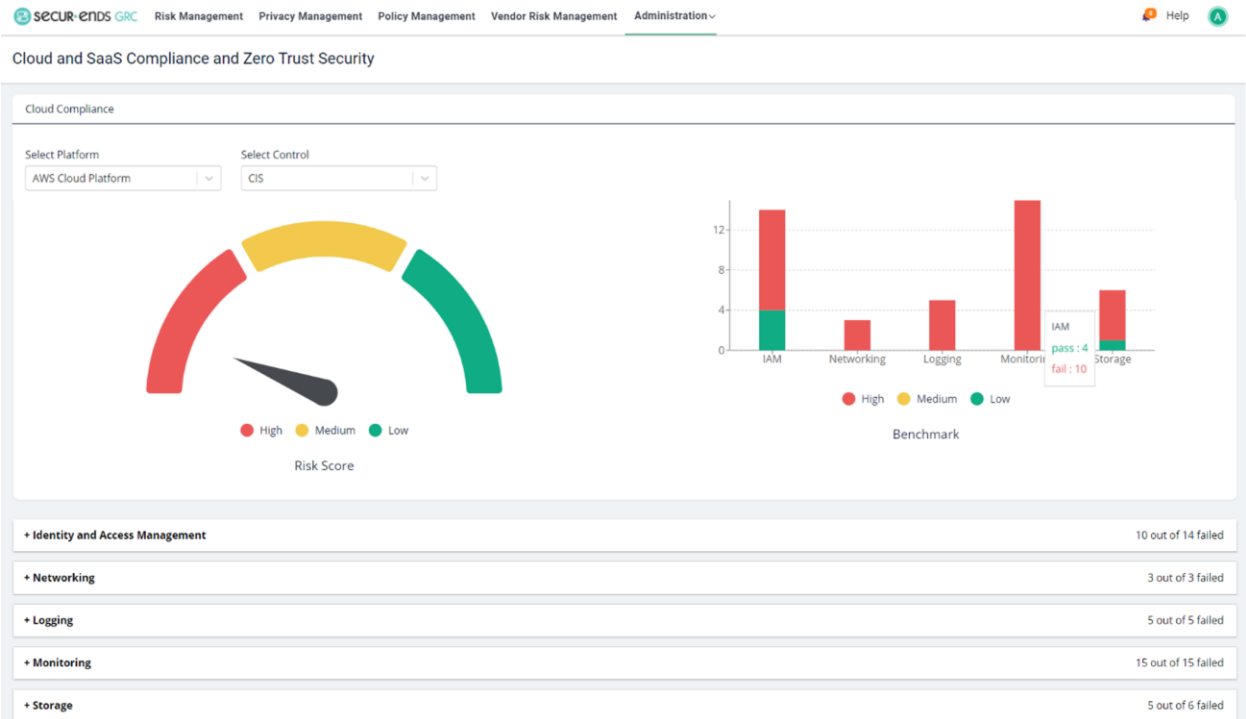
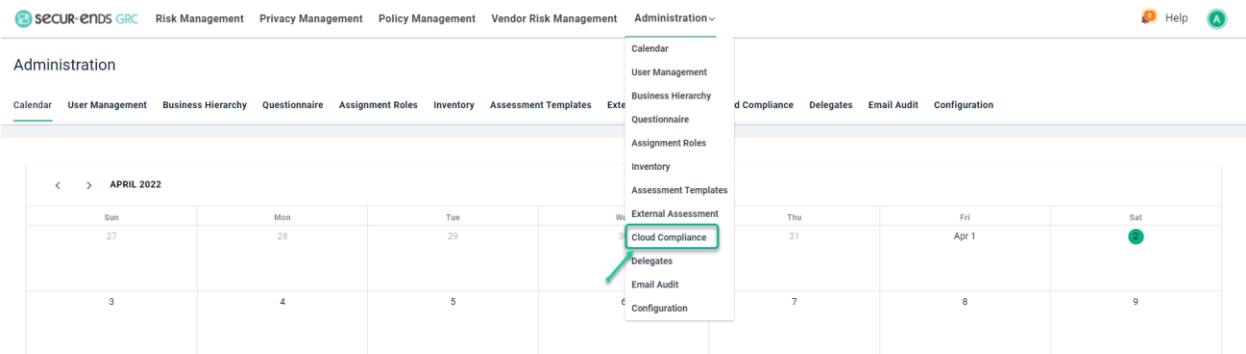
Select the **Assessment Questionnaire** option on the **Actions** menu.

This screenshot is similar to the previous one, but the 'Refresh' button is no longer highlighted. Instead, the 'Assessments Questionnaire' option in the 'Actions' dropdown menu is highlighted with a red box and an arrow. The status of the 'AWS Cloud Platform' connector is now shown as a green checkmark.

The screenshot shows the 'Assessment Questionnaire' page. It features a 'Back' button in the top right corner. The main content is a table with two columns: 'Category' and 'Assessment Questionnaire'. The table lists ten assessment questions related to Identity Management and Access Control, such as 'Are current contact details maintained?' and 'Is MFA enabled for the root user account?'. A search bar is located in the top right of the table area.

Step 4:

Select **Cloud Compliance** tab on the **Administration** tab and select **Connector** from the drop-down list



[End of Cloud Compliance User Guide]