Qualys CloudView v1.x

Version 1.7
January 7, 2019

Here's what's new in Qualys CloudView 1.7!

Support for Microsoft Azure CIS Benchmark

We have now added a new policy titled CIS Microsoft Azure Foundations Benchmark that supports 33 new controls for Azure CIS v1.0.0.

Go to Policies tab and click the policy title, the Controls pane then lists the controls. The details of the same are listed below.

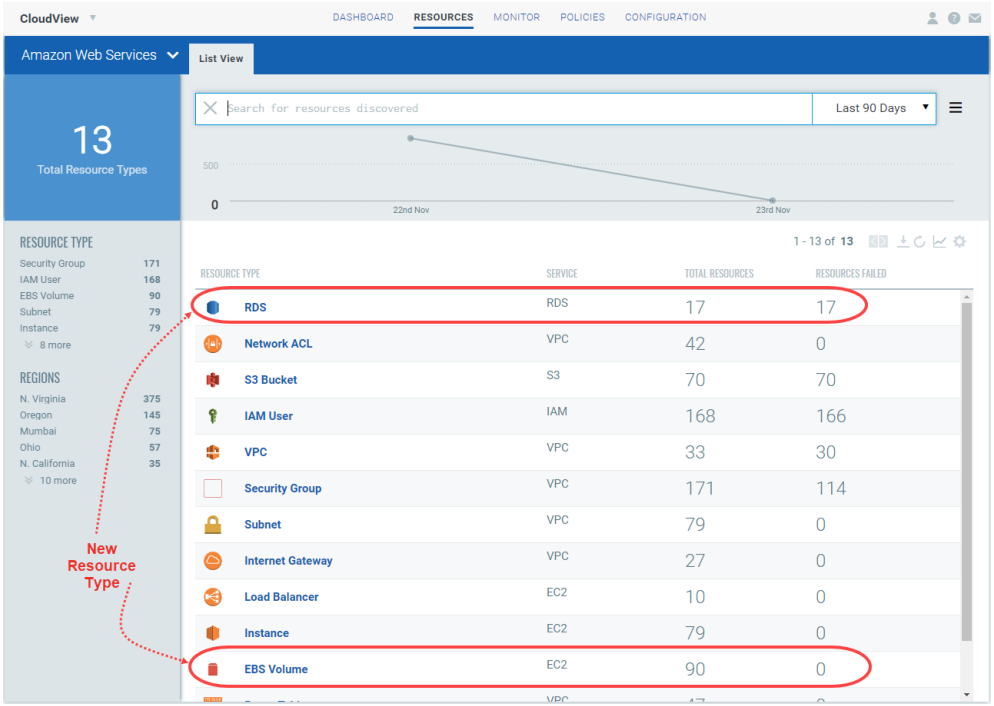
Section #	CID	CIS v1.0.0	Title
2	**Security Center**		
	50015	2.1	Ensure that standard pricing tier is selected
	50004	2.2	Ensure that 'Automatic provisioning of monitoring agent' is set to 'On'
	50005	2.3	Ensure ASC Default policy setting Monitor System Updates is not Disabled
	50006	2.4	Ensure ASC Default policy setting Monitor OS Vulnerabilities is not Disabled
	50007	2.5	Ensure ASC Default policy setting Monitor Endpoint Protection is not Disabled
	50008	2.6	Ensure ASC Default policy setting Monitor Disk Encryption is not Disabled
	50009	2.7	Ensure ASC Default policy setting Monitor Network Security Groups is not Disabled
	50010	2.8	Ensure ASC Default policy setting Monitor Web Application Firewall is not Disabled
	50016	2.9	Ensure ASC Default policy setting Enable Next Generation Firewall(NGFW) Monitoring is not Disabled
	50017	2.10	Ensure ASC Default policy setting Monitor Vulnerability Assessment is not Disabled
	50018	2.11	Ensure ASC Default policy setting Monitor Storage Blob Encryption is not Disabled
	50019	2.12	Ensure ASC Default policy setting Monitor JIT Network Access is not Disabled
	50003	2.13	Ensure ASC Default policy setting Monitor Application Whitelisting is not Disabled
	50014	2.14	Ensure ASC Default policy setting Monitor SQL Auditing is not Disabled
	50025	2.15	Ensure ASC Default policy setting Monitor SQL Encryption is not Disabled
	50020	2.16	Ensure that 'Security contact emails' is set
	50021	2.17	Ensure that security contact 'Phone number' is set
	50022	2.18	Ensure that 'Send me emails about alerts' is set to 'On'
	50023	2.19	Ensure that 'Send email also to subscription owners' is set to 'On'
3	**Storage Accounts**		
	50011	3.1	Ensure that Secure transfer required for a Storage Account is set to Enabled
	50012	3.7	Ensure that 'Public access level' is set to Private for blob containers

4	**SQL Services**		
4.1	**SQL Servers**		
	50013	4.1.1	Ensure that 'Auditing' is set to 'On'
	50013		Ensure that 'AuditActionGroups' in 'auditing' policy for a SQL server is set properly (This will be part of next release of CIS benchmark)
	50028	4.1.2	Ensure that 'Threat Detection' is set to 'On'
	50028	4.1.3	Ensure that 'Threat Detection types' is set to 'All'
	50028	4.1.4	Ensure that 'Send alerts to' is set
	50028	4.1.5	Ensure that 'Email service and co-administrators' is 'Enabled'
	50013	4.1.6	Ensure that 'Auditing' Retention is 'greater than 90 days'
	50028	4.1.7	Ensure that 'Threat Detection' Retention is 'greater than 90 days'
	50035	4.1.8	Ensure that Azure Active Directory Admin is configured for a SQL Server
	50027		Ensure SQL server's TDE protector is encrypted with BYOK (Use your own key) (This will be part of next release of CIS benchmark)
4.2	**SQL Databases**		
	50013	4.2.1	Ensure that 'Auditing' is set to 'On'
	50028	4.2.2	Ensure that 'Threat Detection' is set to 'On'
	50028	4.2.3	Ensure that 'Threat Detection types' is set to 'All'
	50028	4.2.4	Ensure that 'Send alerts to' is set
	50028	4.2.5	Ensure that 'Email service and co-administrators' is 'Enabled'
	50001	4.2.6	Ensure that Data encryption is set to ON for a SQL database
	50013	4.2.7	Ensure that 'Auditing' Retention is 'greater than 90 days'
	50028	4.2.8	Ensure that 'Threat' Retention is 'greater than 90 days'
5	**Logging and Monitoring**		
5	50024	5.1	Ensure that a Log Profile exists
	50024	5.2	Ensure that Activity Log Retention is set 365 days or greater
	50024		Ensure Audit Profile Captures all the activities (This will be part of next release of CIS benchmark)
6	**Networking**		
	50029	6.1	Disable RDP access on Network Security Groups from Internet (ANY IP)
	50031	6.2	Disable SSH access on Network Security Groups from Internet (ANY IP)
	50002	6.3	Ensure that SQL server access is restricted from the internet
7	**Virtual Machines**		
	50032	7.2 & 7.3	Ensure that all the vm disks are encrypted
8	**Other Security Considerations**		

	50030	8.2	Ensure that the expiry date is set on all Secrets
	50026		Ensure keyvault is recoverable (This will be part of next release of CIS benchmark)

AWS: Support for RDS and EBS Resources Added

CloudView now supports two more AWS resources: RDS and EBS Volume. Similar to other resources, the AWS connector will fetch details associated with these newly added resources. You can filter further using the tokens and view the resource information.



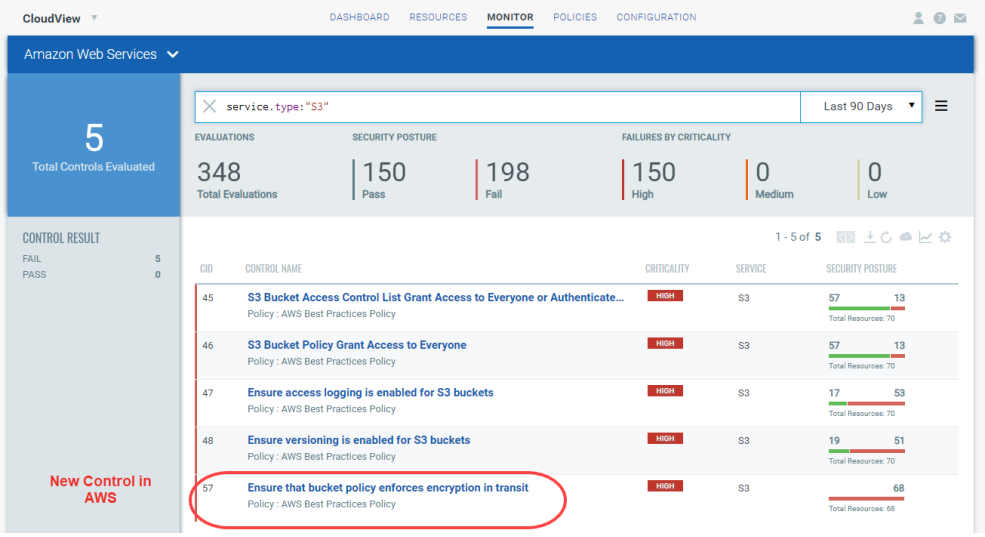
Go to Resources tab and you can view the newly supported resources in the List View.

We have also introduced 6 new controls for RDS in AWS Best Practices Policy. You can view control evaluation in Monitor tab and control details in Policies tab.

Control Number	Control Name
CID-51	Ensure that Public Accessibility is set to No for Database Instances
CID-52	Ensure DB snapshot is not publicly visible
CID-53	Ensure Encryption is enabled for the database Instance
CID-54	Ensure database Instance snapshot is encrypted
CID-55	Ensure auto minor version upgrade is enabled for a Database Instance
CID-56	Ensure database Instance is not listening on to a standard/default port

AWS: New Control for Bucket Policy Enforcing Encryption

We have now introduced a new control to AWS Best Practices Policy that ensures that the S3 bucket policy enforcing SecureTransport exists for all the objects inside of a bucket.



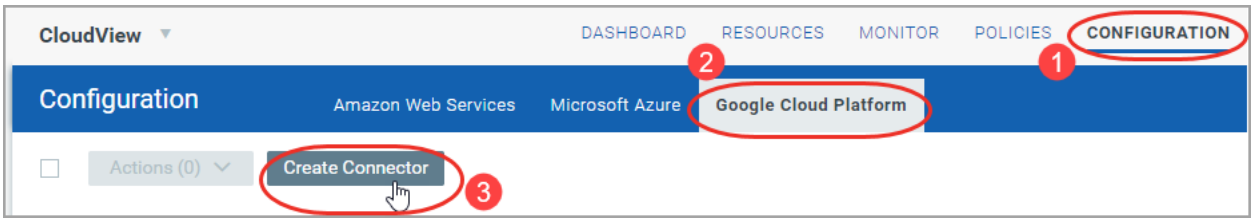
Go to Monitor > Amazon Web Services and search for service.type:S3 and you will notice the new control (CID 57) and its evaluation results

Google Cloud Platform Inventory Support

We now introduced inventory support for Google Cloud Platform (GCP). You can now configure Google Cloud Platform (GCP) connector for gathering resource information from your Google Cloud Platform project. It just takes a couple of minutes.

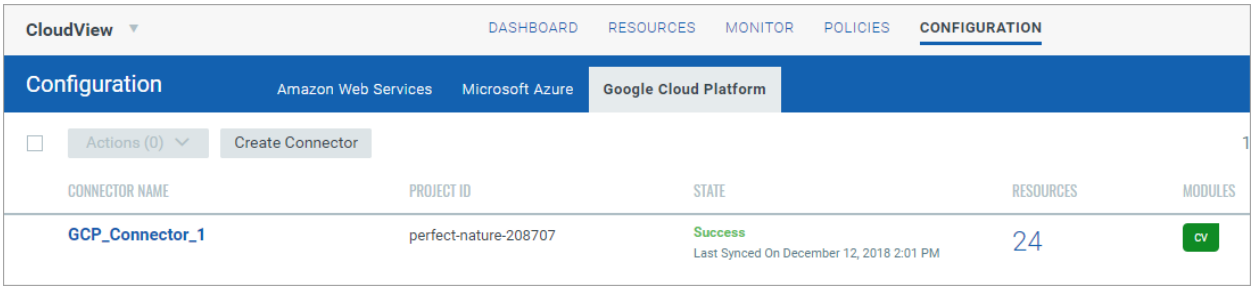
Add GCP Connector

Go to the Configuration > Google Cloud Platform and then click Create Connector. Provide a few connector details.



(1) Enter a name and description (optional) for your connector.
(2) Download the service account key (JSON) file from the GCP console and then upload it to Qualys Cloud Platform to complete GCP connector creation.
(3) Click Create Connector.

That's it! The connector will establish a connection with GCP to start discovering resources from each region.



CloudView will discover and fetch following resources and their corresponding attributes:

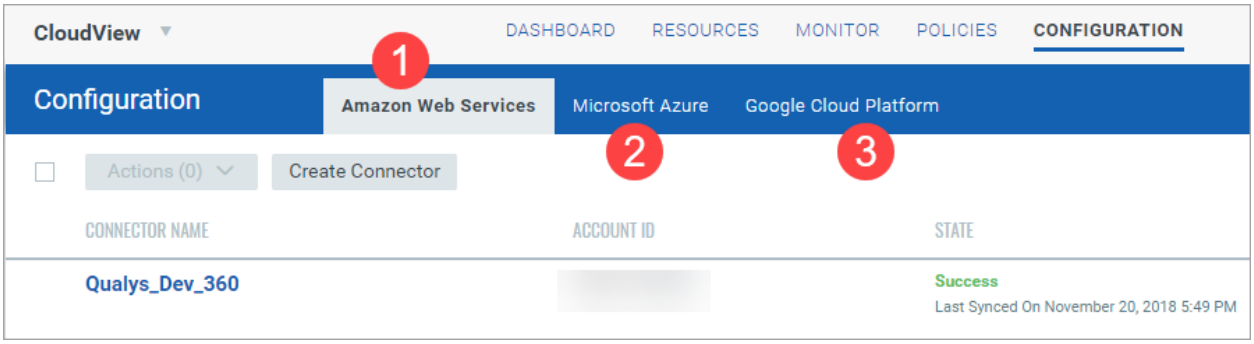
- VM Instances
- Networks
- Firewall Rules
- Subnetworks

Separate Panels for Each Connector Type

We have now added new panels for each connector type making it easier for you to manage each connector type. With each connector type in separate panel, adding new connectors, deleting connectors or editing connectors is now easier.

Go to Configuration tab. The Configuration tab now displays three new panels with one panel for each connector type.

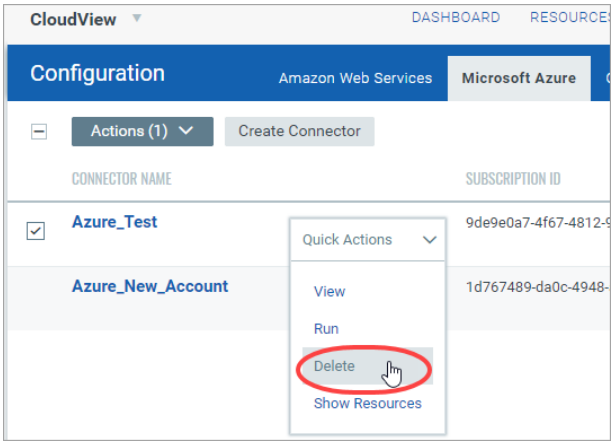
1) Amazon Web Services
2) Microsoft Azure
3) Google Cloud Platform (GCP).



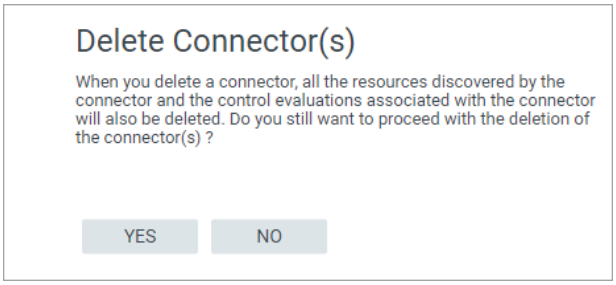
Support for Microsoft Azure Connector Deletion

You can now delete Microsoft Azure connector that you have added in CloudView.

If you want remove an existing Azure connector, simply go to Configuration > Microsoft Azure and select the Azure connector you would want to delete and then simply click Delete from the quick action menu.



Once you click Delete, a confirmation prompt is displayed asking you to confirm the deletion of connector as it also erases all the data associated with the Azure connector.

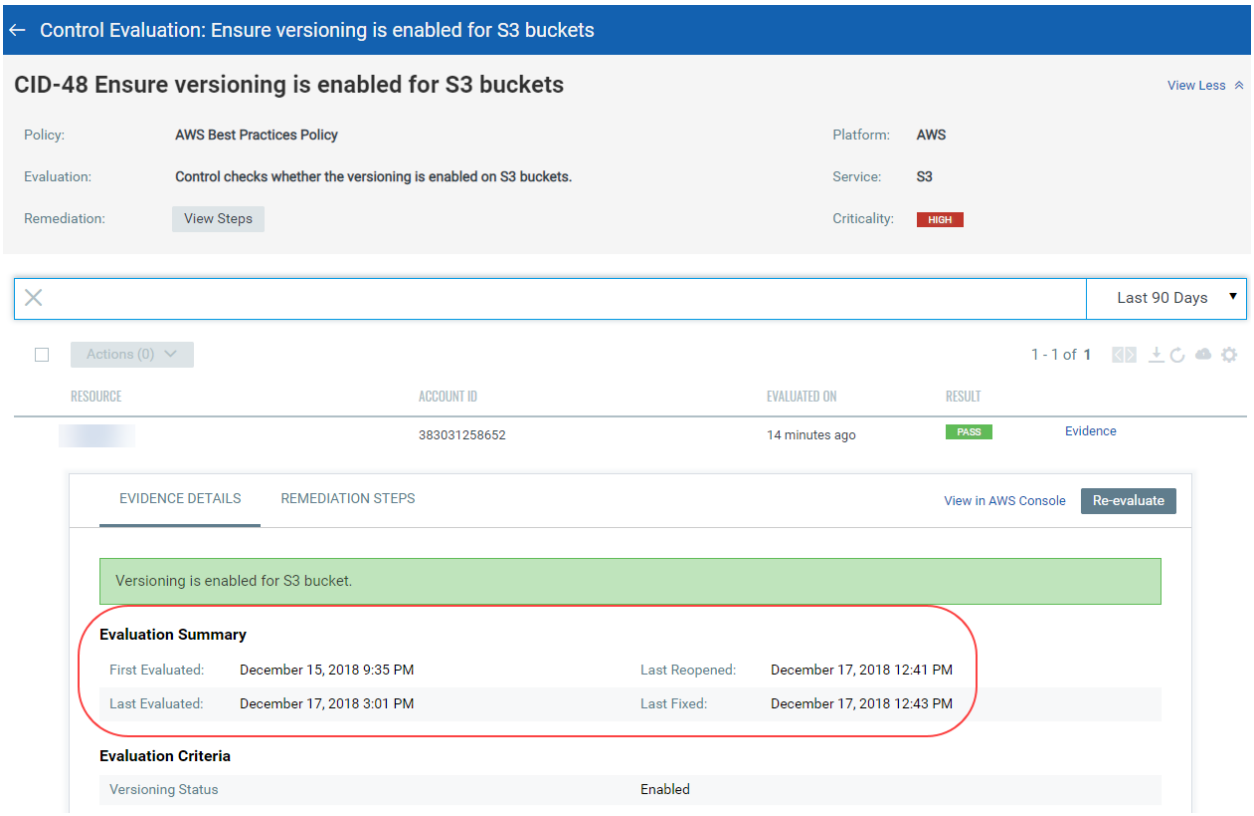


To delete multiple Azure connectors, select the connectors and then select Delete from the Actions menu.

Evaluation Summary Enhanced for Controls

We have now provide you more information regarding the control and its evaluation details.

Go to Monitor tab and select the provider (AWS or Azure). Click the control and then Evidence for the resource on which the control was evaluated.



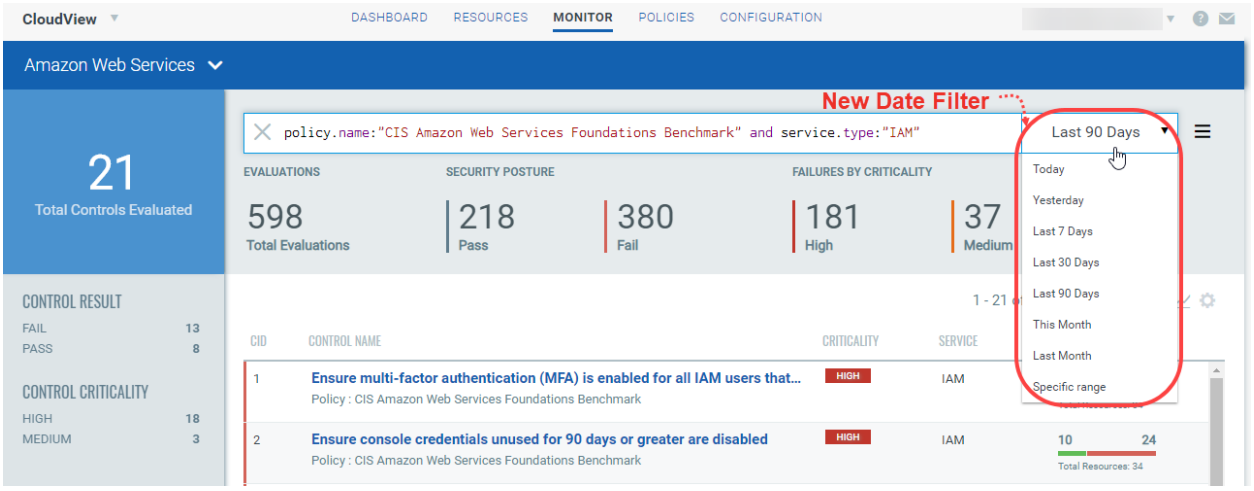
The Evaluation Summary now tells you the following facts:

-First Evaluated: The date when the control was evaluated for the first time.
-Last Evaluated: The latest date when the control was evaluated.
-Last Reopened: The latest date when the control evaluation result is changed from pass to fail.
-Last Fixed: The latest date when the control evaluation control result is changed from fail to pass.

Date range now enabled for Control Evaluations

In Monitor tab, narrow down your search results for controls using our new date filter. The new date filter provides 8 options: Today, Yesterday, Last 7 days, Last 30 days, Last 90 days, This Month, Last Month, and Specific range. Depending on the date option you choose, the search results displays controls that are evaluated within the chosen date range.

Go to Monitor tab, choose the Cloud Service Provider (AWS or Azure), type your search query in the search pane and then choose the date filter to further filter your search results.



New Permissions to Manage Access to CloudView

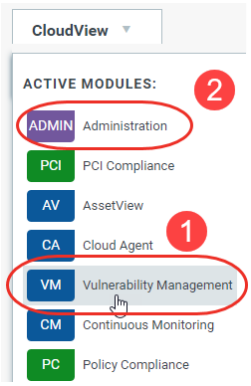
We have now introduced new module level UI-related permissions for CloudView. With the new permissions introduced, you can restrict or provide module-level UI access for a user. Prior to this release, every user had full access to CloudView module. Now onwards, only user with configured permissions will be able to access CloudView module.

You can:
-Block or provide UI access to CloudView module
-Provide UI access to CloudView module with restricted permissions (read-only user)
-Provide full UI access to CloudView module with all permissions

Permissions: Only users with access to Administration module can create sub-users with reader role.

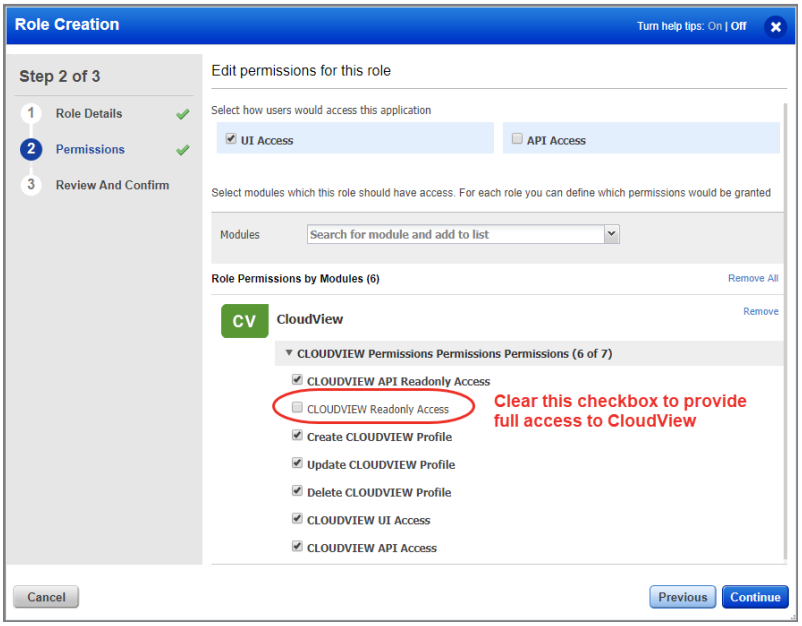
Quick Steps

1) Create a User in Vulnerability Management (Navigate to Vulnerability Management module from module picker and then go to Users tab to create a new user).
2) Create a role in Administration utility (Navigate to Administration utility from module picker and then go to Role Management tab).

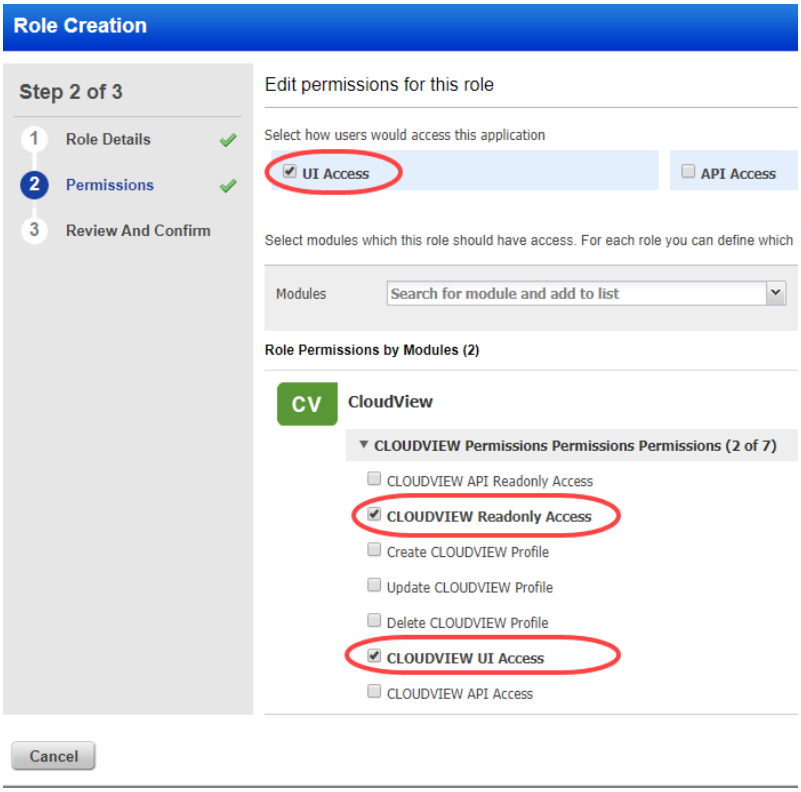


Let us consider scenarios to configure different level of access for users. You could create different roles or modify permissions for an existing role.

Scenario 1: Provide full UI access to CloudView module with all permissions



Scenario 2:Provide UI access to CloudView module with restricted permissions (read-only user)



Ensure that the role has UI access permission and CLOUDVIEW Readonly Access, CLOUDVIEW UI Access enabled

Once you configure the permissions for a role, assign the role to the required users, and the users will gain access as per the configured permissions.